



بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی اتحادیه اروپا و ایران

بهناز احمدوند^{۱*}، آرتین جهانشاهی^۲

۱. استادیار، حقوق عمومی، گروه مطالعات نظری، علم، فناوری و نوآوری، مرکز تحقیقات سیاست علمی کشور، تهران، ایران
۲. دانشجوی کارشناسی ارشد، حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه شیراز، شیراز، ایران

تاریخ ارسال: ۱۴۰۱/۱۰/۱۲ تاریخ پذیرش: ۱۴۰۲/۰۳/۰۶

چکیده

داده شخصی به عنوان یکی از مفاهیم کلیدی در حوزه قانون‌گذاری حفاظت از داده‌های شخصی، در مقررات عمومی حفاظت از داده اتحادیه اروپا به معنی هرگونه اطلاعات مربوط به یک شخص با هویت مشخص (شناخته شده) یا قابل شناسایی تعریف شده است. ارتباط داده، با شخص حقیقی و امکان شناسایی فرد از طریق آن، ممکن است از طریق محتوای داده یا هدف از پردازش داده‌ها و یا اثرگذاری پردازش داده بر فرد باشد. در حقوق اتحادیه اروپا برای تشخیص این‌که شخص حقیقی از طریق پردازش داده‌ها قابل شناسایی است یا خیر، باید تمام ابزارهایی که به‌طور منطقی و معقول احتمال استفاده از آن توسط کنترل‌گر یا پردازش‌گر وجود دارد در نظر گرفته شود. برای اطمینان از این‌که آیا احتمال معقولی برای شناسایی شخص حقیقی وجود دارد یا خیر، باید تمام عوامل عینی، مانند هزینه و مدت زمان مورد نیاز برای شناسایی و فناوری موجود در زمان پردازش در نظر گرفته شوند. بر اساس معیار قابلیت شناسایی، داده‌هایی نیز که به‌طور بالقوه ممکن است در آینده منجر به شناسایی فرد شود تحت پوشش قانون است؛ چنین معیاری می‌تواند پویایی لازم در قوانین ایجاد کند. قانون‌گذار ایران در حمایت از داده‌های خصوصی و غیرخصوصی قائل به تفکیک شده و رعایت قواعد پردازش را محدود به دسته اول کرده است؛ اما رویکرد پیش‌نویس لایحه حمایت از داده مشابهت‌هایی با حقوق اتحادیه اروپا دارد و حمایت گسترده‌تری ارائه کرده است با این حال نیازمند اصلاح از جمله افزودن معیار قابلیت شناسایی به تعریف قانونی و همچنین حفاظت از داده‌های درگذشتگان است.

کلیدواژگان: داده شخصی، شناسایی شخص حقیقی، معقول بودن شناسایی، مقررات عمومی حفاظت از داده، قانون تجارت الکترونیکی، لایحه حمایت از داده و حریم خصوصی در فضای مجازی.





۱. مقدمه

جهان به سرعت در حال تغییر است؛ در آینده ای نزدیک، زیستگاه اصلی انسان ها در پلتفرم ها و سامانه های مجازی هوشمند خواهد بود. توسعه ی فناوری های نوین، از جمله اشیای هوشمند متصل به اینترنت از طریق فناوری اینترنت اشیا^۱، افزایش قابلیت تولید، جمع آوری و پردازش داده های محیط اطراف در مقیاس گسترده و نیز برپاسازی پایگاه های داده برای تصمیم گیری بر اساس هوش مصنوعی، زندگی انسان ها و کسب و کارها را به طور قابل توجهی تغییر می دهد (لطیف زاده و همکاران، ۱۴۰۰: ۴۴۰). گسترش علم داده در مواردی همچون یادگیری عمیق و نیز روش های تحلیل داده و استفاده از داده های افراد برای اهداف متعددی همچون ارائه خدمات یا بازاریابی تجاری، به کلید اقتصاد مدرن مبتنی بر داده تبدیل شده است (OECD, 2010). با توجه به اینکه تجارت الکترونیکی برخلاف تجارت سنتی، عمدتاً مبتنی بر بازاریابی است؛ از این رو اطلاعات افراد، هرچند کم اهمیت مانند آدرس ایمیل یا سلیقه خرید، از جمله مواردی هستند که شرکت های تجاری حاضرند برای دسترسی به آن ها هزینه های گزافی پرداخت کنند (حیدری و جعفری، ۱۳۹۸: ۵۲). ارتباط داده های شخصی^۲ با حریم خصوصی افراد به عنوان جنبه ای از آن، و اهمیت حفاظت از داده ها به دلیل انتظار عمومی شهروندان، قانون گذاران قواعد و ضوابطی پیرامون شرایط پردازش داده های شخصی مقرر کرده اند. رویکرد اتحادیه اروپا به عنوان یکی از بازیگران اصلی و پیشرو در زمینه حفاظت از داده (Schwartz, 2019: 773)، در رابطه با ارائه چهارچوب قانونی جامع و مؤثر برای حفاظت از داده های افراد به علت جامعیت (قناد و علیقلی، ۱۳۹۹، ص. ۳۰۵) و انعطاف پذیری آن در برابر شتاب فناوری (Misek, 2018: 333) و همچنین اهمیت تجارت داده میان کشورها با دولت های عضو اتحادیه اروپایی، در کانون توجه قرار گرفته است.

داده هایی که باعث شناسایی هویت فرد صاحب آن اطلاعات می شوند، موضوع اصلی قانون گذاری های مربوط به حفاظت از داده هستند (Wong, 2018: 1). نوع حمایت ارائه شده در رویکرد اروپایی، به ویژه در مقررات عمومی حفاظت از داده، بر این واقعیت مبتنی است که چون فناوری اطلاعات و ارتباطات روز به روز در حال گسترش و دگرگونی است و اطلاعات افراد موضوع داده^۳ در قالب های مختلف جمع آوری و برای اهداف متعدد مورد استفاده می گیرد،

^۱ Internet of Things

^۲ Personal Data

^۳ Data subject



لازم است داده‌های تحت حمایت قانون، ماهیتی خنثی^۱ نسبت به فناوری داشته و به اندازه‌ای موسع باشد که بتوان هر اطلاعاتی که ممکن است حتی به‌طور بالقوه باعث شناسایی فرد بشود را تحت شمول قانون قرار داد. برای تعمیم این نگاه در قانون، معیار قابلیت شناسایی در تعریف داده شخصی گنجانده شده است. در حقوق ایران قانون تجارت الکترونیکی و لایحه حمایت از داده قواعد تفکیک‌شده‌ای برای حفاظت از داده‌های شخصی مقرر شده است و هر یک تعریفی از داده شخصی مطرح کرده‌اند که مشابهت‌هایی با مقررات عمومی حفاظت از داده دارد.

در ادبیات پژوهشی داخلی اگرچه اهمیت حفاظت از داده‌های شخصی در عصر فناوری اطلاعات و ارتباطات به‌عنوان امری مسلم پذیرفته شده است، و مقررات عمومی حفاظت از داده^۲ نیز به‌عنوان الگو برای اصلاح نظام حقوقی داخلی پیشنهاد شده است (قناد و علیقلی، ۱۳۹۹: ۳۰۵) و اصول پردازش و حقوق افراد موضوع داده و مقایسه آن مقررات با ق.ت.ا شرح داده شده است (قناد و شریف، ۱۴۰۰: ۸)، با این حال درباره اینکه داده‌های شخصی از چه مواردی تشکیل می‌شوند و اینکه چه زمانی مربوط به شخص حقیقی هستند، تنها به سطوری چند اکتفا شده است (لطیف‌زاده و همکاران، ۱۴۰۰: ۴۴۶). با توجه به اینکه موارد اشاره شده، از جمله اصول حاکم بر پردازش داده‌ها و حقوق و تکالیف بازیگران این حوزه‌اند به تفصیل مورد بررسی قرار گرفته است (لطیف‌زاده، ۱۳۹۸ و انصاری، ۱۳۸۶ و انصاری، ۱۴۰۱). در این پژوهش تنها به تحلیل تعاریف قانونی داده شخصی پرداخته خواهد شد و برای اشاره به نکات ضروری به توضیحات مختصر بسنده خواهیم کرد و خوانندگان را به منابع مرتبط ارجاع خواهیم داد. هدف پژوهش حاضر بررسی تطبیقی مفهوم داده شخصی در دو نظام حقوقی و یافتن مشابهت‌ها و تفاوت‌های میان آن دو برای اصلاح احتمالی نظام حقوقی داخلی است. سازمان‌دهی پژوهش به ترتیب زیر است: در گفتار اول نظام حقوقی اتحادیه اروپا و داده‌های تحت حمایت بررسی خواهد شد؛ در گفتار دوم داده‌های تحت حمایت در قوانین موضوعه ایران و مشابهت‌ها و تفاوت‌های آن با نظام حقوقی اتحادیه بررسی خواهد شد؛ در گفتار سوم مؤلفه‌های تشکیل‌دهنده داده شخصی به‌طور تطبیقی بررسی خواهد شد.

۲. حقوق حفاظت از داده شخصی اتحادیه اروپا

پارلمان و شورای اتحادیه اروپا به منظور ارائه چارچوب واحد و یکسان‌سازی قواعد حاکم بر پردازش داده‌های شخصی در سال ۱۹۹۵ دستورالعمل ۹۵/۴۶ را با ترکیب رهنمودهای

^۱ General Data Protection Regulation, Recital 15.

^۲ از این پس م.ع.ج.د



سازمان همکاری و توسعه اقتصادی و همچنین پیش‌بینی قواعد جدید به تصویب رساند. با توجه به اهمیت موضوع، متعاقب این دستورالعمل، اتحادیه اروپا در سال ۲۰۰۰ منشور حقوق و آزادی‌های اساسی را به تصویب رساند و در ماده ۸ حقی تحت عنوان حق حفاظت از اطلاعات شناسایی کرد. در سال ۲۰۱۰ اتحادیه اروپا سند «رویکرد جامع در مورد محافظت از داده‌ها در اتحادیه اروپا» را به منظور تقویت حقوق اشخاص و گسترش ابعاد بازار داخلی و پوشش بُعد جهانی حفاظت از داده با رویکرد غیرکیفری تصویب کرد.^۱ به دنبال تصویب این سند، کمیسیون اتحادیه اروپایی بسته پیشنهادی اصلاحات در چارچوب حقوق اتحادیه را در ژانویه سال ۲۰۱۲ مطرح نمود. این بسته اصلاحات پس از سال‌ها مباحث سیاسی در نهایت منجر به تصویب «مقررات اتحادیه اروپا به شماره ۲۰۱۶/۶۷۹ مصوب پارلمان و شورای اروپا در تاریخ ۲۷ آوریل ۲۰۱۶ در مورد حمایت از اشخاص حقیقی در برابر پردازش داده‌های شخصی و جریان آزاد این داده‌ها و لغو دستورالعمل شورای اتحادیه اروپایی در مورد محافظت از افراد در برابر پردازش داده‌های شخصی و جریان آزاد این داده‌ها (م.ع.ح.د) شد. به‌عنوان سند موضوع بحث حاضر به تصریح ماده ۹۹ م.ع.ح.د. بیست روز پس از انتشار آن در روزنامه رسمی اتحادیه اروپایی از تاریخ ۲۵ مه سال ۲۰۱۸ لازم‌الاجرا شده است.

مخاطبان م.ع.ح.د کنترل‌کننده‌ها، پردازنده‌ها^۲ و افراد موضوع داده^۴ فارغ از ملیت و محل اقامتشان است. از نظر قلمروی اجرایی نیز ماده ۳ مقرر داشته است این مقررات بر هر کنترل‌کننده و پردازندگانی که محل استقرارشان اتحادیه اروپاست صرف‌نظر از اینکه پردازش در داخل مرزهای اتحادیه انجام می‌شود یا خیر اعمال می‌شود. همچنین دامنه اجرایی این مقررات هر کنترل‌کننده و پردازنده‌ای که داده‌های افراد موضوع داده اروپایی را پردازش می‌کنند را نیز دربر می‌گیرد.

منظور از کنترل‌کننده هر شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که به تنهایی یا به‌طور مشترک با دیگران، اهداف و ابزار پردازش داده‌های شخصی را تعیین می‌کند. به‌عبارت دیگر هرگاه هر مرجع و شخصی اعم از اینکه حقیقی باشد یا حقوقی تصمیم به پردازش داده بگیرد و چگونگی و دلیل این پردازش را تعیین کند کنترل‌گر محسوب خواهد

¹ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: 'A comprehensive approach on personal data protection in the European Union', COM (2010) 609 final.

² Controller

³ Processor

⁴ Data subject



شد. کنترل‌گر معمولاً خود داده‌ها را پردازش نمی‌کند و برای انجام این کار به دیگری نیابت می‌دهد، فردی که به او نیابت داده شده تا عملیات پردازش را انجام دهد پردازنده است که ممکن است اعم از شخص حقیقی یا حقوقی باشد (ماده ۴ م.ع.ح.د).

۲-۱. مقررات عمومی حفاظت از داده

م.ع.ح.د در بند ۱ ماده ۴ در تعریفی مشابه آنچه در دستورالعمل حفاظت از داده مصوب ۱۹۹۵ آمده، با تغییراتی^۲ داده شخصی را چنین تعریف کرده است: «منظور از داده شخصی هرگونه اطلاعات مربوط به شخص حقیقی شناخته شده یا قابل شناسایی است؛ شخص حقیقی قابل شناسایی فردی است که به طور مستقیم یا غیرمستقیم، به ویژه با ارجاع به یک شناسه از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه آنلاین یا ارجاع به یک یا چند ویژگی خاص مانند هویت فیزیکی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی شناسایی شود». این تعریف در کنوانسیون مدرن برای حفاظت از اشخاص در رابطه با پردازش داده‌های شخصی مصوب شورای اروپا^۳ با اصلاحات سال ۲۰۱۸ نیز منعکس شده است؛ با توجه به اینکه کمیسیون اروپا به دولت‌های عضو خود اجازه الحاق به این کنوانسیون را صادر کرده است که خود نشان از عدم تعارض مفاد آن با م.ع.ح.د می‌باشد می‌توان از آن برای بررسی مفهوم داده شخصی استفاده کرد.

پردازش دسته‌ای از داده‌های شخصی علاوه بر اینکه هویت فرد را برای پردازنده داده برملا می‌کنند رابطه مستقیمی با ابعاد محرمانه و خصوصی زندگی انسان‌ها دارند، به گونه‌ای که افراد تمایلی به استفاده یا افشای این دست اطلاعات توسط دیگران ندارند و در صورت افشا ممکن است خساراتی اعم از مادی یا معنوی به بار آورند. با توجه به حساسیت و اهمیت موضوع که

Directive 95/46/EC^۱ این دستورالعمل با هدف یکسان‌سازی قواعد اعضای اتحادیه درباره پردازش داده‌های شخصی در سال ۱۹۹۵ به تصویب پارلمان و شورای اتحادیه اروپا رسید. به علت ماهیت غیرالزام‌آور دستورالعمل و تشتت آراء در اعمال قواعد از حیث حدود و ثغور قواعد توسط دولت‌های عضو و نیز به علت پیشرفت‌های حاصل در فناوری اطلاعات و ارتباطات در سال ۲۰۱۶ جای خود را به م.ع.ح.د داد. مقررات مذکور بدون نیاز به تصویب قوانین داخلی به عنوان قانون در کشورهای عضو لازم‌الاجرا می‌باشد. با توجه به عدم تفاوت و تعارض مقررات دستورالعمل با م.ع.ح.د در خصوص داده‌های شخصی می‌توان از آن برای مقایسه استفاده کرد.

^۲ تنها تفاوت میان دستورالعمل و م.ع.ح.د اضافه شدن شناسه آنلاین، اطلاعات مکانی و ژنتیکی است.

^۳ The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981 and 2018 amendment.



ارتباط نزدیکی با حریم خصوصی و خانوادگی افراد به عنوان یکی از حقوق به رسمیت شناخته شده دارد (ماده ۷ منشور حقوق و آزادی های اساسی اتحادیه اروپا) و همچنین با توجه به اینکه یکی از اهداف قواعد حفاظت از داده شخصی احترام به حقوق و آزادی های اساسی به ویژه بر زندگی خصوصی است (مشروح شماره ۲) م.ع.ح.د و ق.ت.ا قواعد خاصی برای پردازش داده های شخصی «حساس»^۱ یا «خاص»^۲ مقرر کرده اند. در م.ع.ح.د اصطلاح داده های حساس به طور صریح استفاده نشده و در ماده ۹ از این داده ها تحت عنوان داده های خاص یاد شده است. داده های شخصی حساس داده هایی هستند که ماهیتاً ارتباط مستقیمی با حقوق و آزادی های اساسی شناسایی شده^۳ در منشور حقوق بنیادین و آزادی های اساسی دارند و پردازش آنها ممکن است موجب نقض این آزادی ها^۴ یا منجر به تبعیض رفتاری بین افراد گردد (Georgieva & Kuner, 2020: 369).

چنان که اشاره شد در قوانین مرقوم تعریفی از داده های شخصی حساس ارائه نشده است و تنها به برخی از مصادیق آن اشاره شده است؛ در این باره ماده ۹ م.ع.ح.د پردازش داده های شخصی مربوط به افشای مبدأ نژادی و قومی، عقاید مذهبی و فلسفی، و پردازش داده ژنتیکی، داده بیومتریک با هدف شناسایی منحصر به فرد افراد، داده مربوط به سلامتی یا گرایش جنسی اشخاص جز در موارد مصرح در قانون ممنوع اعلام شده است. با توجه به حساسیت پردازش این گونه داده ها، تکالیف ویژه ای برای کنترل گران و پردازش گران مقرر شده است. به موجب ماده ۲۵ م.ع.ح.د، با توجه به ماهیت، قلمرو، موضوع و اهداف پردازش و همچنین خطرات متنوع از نظر احتمال و شدت برای حقوق و آزادی های فردی، کنترل گر باید معیارهای فنی و سازمانی مناسبی را برای تضمین و اثبات تطابق پردازش با این قوانین را پیاده سازی کند و هر زمان که لازم باشد، این معیارها باید بازبینی و به روزرسانی شوند. با توجه به این مقرر به خوبی برداشت می شود که سطح معیارهای فنی و سازمانی برای حفاظت از داده های شخصی حساس باید با توجه به ماهیت آنها صورت بگیرد که در جای خود ممکن است بیشتر از داده های شخصی عادی باشد. همچنین به موجب ماده ۳۵ م.ع.ح.د، زمانی که نوعی از پردازش با استفاده از فناوری های جدید، با در نظر گرفتن ماهیت، قلمرو، موضوع و اهداف پردازش، منجر به خطر بالا برای حقوق و آزادی های اشخاص حقیقی شود، کنترل گر باید پیش از انجام پردازش، اثرات

¹ Sensitive Data

² Special Data

³ Recital 51

⁴ European Court of Human Rights, Case Drelon v France 2022.



عملیات پردازش را ارزیابی^۱ کند. علاوه بر موارد اشاره شده، هنگامی که فعالیت‌های محوری کنترل‌گر یا پردازش‌گر شامل پردازش مقیاس بزرگی از داده‌های حساس باشد، باید فردی تحت عنوان «مأمور حفاظت از داده»^۲ منصوب کند؛ هدف از این انتصاب نظارت بر عملکرد کنترل‌گر و پردازش‌گر و حصول اطمینان از سازوکارهای حفاظتی اتخاذشده توسط اشخاص مذکور است.

۳. حفاظت از داده شخصی در نظام حقوقی ایران

نقطه عطف نظام موضوعه حقوق ایران در مواجهه با فناوری‌های نوین و لزوم توجه به فراهم‌سازی بسترهای قانونی برای آن، تصویب قانون تجارت الکترونیکی در سال ۱۳۸۲/۱۰/۱۷ بود؛ در این قانون برای اولین بار اصطلاحاتی جدیدی از جمله «داده‌پیام» و «داده‌پیام‌های شخصی» و نظیر آن وارد بدنه نظام حقوقی شد. در این قانون، برخی از اطلاعات تحت حمایت قانون‌گذار قرار گرفته است و نقض آن با قید مجازات کیفری ممنوع شده است. هدف از وضع ق.ت.ا به تصریح ماده ۱، مبادله آسان و ایمن اطلاعات در واسط‌های الکترونیکی و با استفاده از سیستم‌های ارتباطاتی جدید است. با تحول اذهان عمومی درباره اطلاعات و اهمیت آن، قانون انتشار و دسترسی آزاد به اطلاعات در ۱۳۸۷/۱۱/۰۶ تصویب شد؛ متعاقب قانون اخیرالذکر، در ۱۳۸۸/۰۳/۰۵ قانون جرائم رایانه‌های تصویب شد و برخی اعمال غیرمجاز در پردازش داده‌ها، از جمله دسترسی غیر و تغییر غیرمجاز داده‌های افراد و نقض حریم خصوصی از طریق داده‌ها را جرم‌انگاری کرد. با تصویب قانون اخیرالذکر و در کنار آن، ق.ت.ا، رویکرد حمایتی قانون‌گذار نسبت به داده‌های شخصی به حمایت کیفری تبدیل شد؛ در این قوانین با یک رویکرد کیفری برای ناقضان محرمانگی، امنیت و تمامیت داده‌ها مجازات حبس و جزای نقدی و جبران خسارت مدنی پیش‌بینی شده است. به دنبال شتاب روزافزون در حوزه فناوری اطلاعات و ارتباطات و فراهم شدن بستر تجارت از طریق داده‌های افراد، نیاز به قوانین عام و تخصصی و متناسب با اقتضائات این حوزه و نیز رویکرد غیرکیفری در کشور احساس شد؛ در سال ۱۳۹۶ سازمان فناوری اطلاعات با همکاری پژوهشگاه قوه قضاییه و دانشگاه علم و فرهنگ پیش‌نویسی تحت عنوان «لایحه حمایت از داده و حریم خصوصی در فضای مجازی» منتشر کرد. در سال ۱۳۹۷ نیز پیش‌نویس دیگری در سازمان فناوری اطلاعات تحت عنوان «لایحه صیانت از داده‌های شخصی» تدوین شد و پس از بررسی، به کمیسیون دولت الکترونیک

^۱ Data protection impact assessment

^۲ Data protection officer



جهت تصویب هیأت وزیران ارسال شد؛ در این اثنا طرحی تحت عنوان «طرح حمایت و حفاظت از داده و اطلاعات شخصی» به مجلس ارسال شد که تاکنون تحت بررسی می باشد. در این لایحه اصطلاحاتی به کار برده شده که مشابه م.ع.د می باشد؛ طبق بند ۴ ماده ۱ کنترل گر، شخص حقوقی یا حقیقی است که اهداف و سازوکار پردازش داده های شخصی را تعیین می کند و پردازشگر شخص حقوقی یا حقیقی است که به درخواست کنترل گر، داده های شخصی را پردازش می کند. (بند ۵ ماده ۱). قلمرو لایحه مرقوم در مقایسه با قوانین موجود بسیار گسترده است و اشخاص خارج از قلمرو کشور را نیز در برمی گیرد. طبق ماده ۲ لایحه پردازش داده های شخصی در صورتی مشمول این قانون است که توسط مؤسسات خصوصی صورت گیرد و یکی از شرایط زیر وجود داشته باشد: ۱. کنترل گری یا پردازشگری در ایران و در مورد داده های شخصی افراد واقع در قلمرو صلاحیت جمهوری اسلامی ایران یا ایرانیان خارج از کشور صورت گیرد، ۲. کنترل گر یا پردازشگر در خارج از ایران باشد اما داده های شخصی افراد واقع در قلمرو صلاحیت جمهوری اسلامی ایران را پردازش کند و در ایران شعبه یا نمایندگی داشته باشد.

۱-۳. قانون تجارت الکترونیکی ایران

ق.ت.ا ایران در تعریف داده پیام مقرر داشته است «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می شود». قانون مدیریت داده ها و اطلاعات ملی نیز در تعریفی مشابه داده را این گونه تعریف کرده است: «داده، مجموعه ای از اعداد و حروف و علائم و نشانه هایی هستند که به صورت قراردادی در ابزارهای الکترونیکی یا رقومی یا توسط هر نوع فناوری جدید ارتباطاتی و اطلاعاتی تولید می شوند». طبق تعریف ق.ت.ا، داده پیام شخصی هرگونه نماد، علامت، اطلاعات یا مفهوم است که صرف نظر از ماهیت و قالبی که دارد مربوط به یک شخصی حقیقی مشخص و معین است.^۱ قانون انتشار و دسترسی آزاد به اطلاعات نیز بی آنکه ضابطه ای برای تشخیص اطلاعات شخصی و عمومی ارائه دهد، اطلاعات فردی نظیر نام و نام خانوادگی، نشانی های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادات های فردی، ناراحتی های جسمی، شماره حساب بانکی و رمز عبور را به عنوان اطلاعات شخصی معرفی کرده است. شیوه نامه تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از

^۱ بند ۲ ماده ۲ قانون تجارت الکترونیکی



اطلاعات عمومی^۱ ضمن تفکیک بین اطلاعات مربوط به حریم خصوصی (ماده ۱) و اطلاعات (داده‌های) شخصی (ماده ۴)، با تفصیل بیشتری داده‌های اخیر را به مواردی همچون داده‌های هویتی، مکانی، اقتصادی، سلامت، ارتباطاتی و... تقسیم کرده و برای هر یک مواردی را به‌عنوان مثال مطرح کرده است. در شیوه‌نامه نیز تعریفی از داده‌های شخصی نشده است؛ اما بررسی مصادیق مندرج در آن نشان می‌دهد داده‌های شخصی اطلاعاتی هستند که موجب شناسایی فرد موضوع آن به شکل متمایز از دیگران می‌شود. این ملاک برای تعریف داده‌های شخصی در ق.ت.ا (داده‌های مربوط به فرد مشخص و معین) به خوبی برداشت می‌شود.

فصل سوم ق.ت.ا تحت عنوان «حمایت از داده‌پیام‌های شخصی» برای برخی از داده‌پیام‌های شخصی مقررات ویژه‌ای مقرر کرده است. به موجب ماده ۵۸ ذخیره، پردازش و توزیع داده‌پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده‌پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است؛ مگر آنکه فرد موضوع داده به آن رضایت دهد، مشروط بر اینکه محتوای داده‌پیام‌ها مطابق قوانین مصوب باشند (ماده ۵۹ ق.ت.ا). به نظر می‌رسد هدف قانون‌گذار از وضع ماده ۵۸ حفاظت از اطلاعات حساس و مربوط به حریم خصوصی و آزادی‌های مشروع افراد بوده است حال آنکه تنها به ذکر مصادیقی از آن بدون قید تمثیل اکتفا کرده است. با توجه به حساسیت این گونه از داده‌ها، قانون‌گذار برای پردازش آن‌ها اصولی را مقرر کرده است: 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 تعیین‌شده مورد استفاده قرار گیرد؛ ج) داده‌پیام باید صحیح و روزآمد باشد؛ د) شخص موضوع داده‌پیام باید به پرونده‌های رایانه‌های حاوی داده‌پیام‌های شخصی مربوط به خود دسترسی داشته و بتواند داده‌پیام‌های ناقص و یا نادرست را محو یا اصلاح کند؛ ه) شخص موضوع داده‌پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه‌های داده‌پیام‌های شخصی مربوط به خود را بنماید. ضمانت اجرای تخلف از هر یک از موارد اشاره شده به تصریح ماده ۷۱، یک تا سه سال حبس در پی دارد. پیش‌بینی مجازات کیفری سنگین، آن هم از نوع حبس، می‌تواند از مانع بروز و ظهور و ادامه فعالیت‌های اقتصادی مبتنی بر فناوری‌های نوین، به‌ویژه از طریق پردازش داده‌های شخصی شود؛ به همین دلیل است که

^۱ مصوبه کمیسیون انتشار و دسترسی آزاد به اطلاعات ۹۸/۰۹/۱۰



ضمانت اجرای پذیرفته شده در نظام حقوقی اتحادیه اروپا، غیرکیفری و مبتنی بر جزای نقدی بازدارنده^۱ است. در لایحه حمایت از داده و حریم خصوصی در فضای مجازی چنین تدبیری اندیشیده شده است. در لایحه حمایت از داده و حریم خصوصی برای نقض قواعد، ضمانت اجرایی همچون تعلیق دائم یا موقت و پرداخت جریمه در مواردی که منجر به منفعت مالی متخلف شده، معادل ۲ تا ۴ برابر منفعت مالی ناشی از نقض و در سایر موارد پرداخت جریمه نقدی معادل ۱۰۰ میلیون تا ۲ میلیارد ریال پیش بینی شده است که به نظر می رسد بازدارندگی کافی داشته باشد.

مقایسه قواعد حاکم بر حفاظت از داده شخصی در اتحادیه اروپا و ایران نشان می دهد قانونگذار ایران برخلاف قانونگذار اتحادیه اروپا، رعایت الزامات حاکم بر پردازش داده و همچنین حقوق فرد موضوع داده پیام که در ماده ۵۹ مقرر شده است را تنها محدود به داده پیام های شخصی مبین ریشه های قومی یا نژادی، دیدگاه های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام های راجع به وضعیت جسمانی، روانی و یا جنسی کرده است؛ این درحالی است که در م.ع.د اتحادیه اروپا، اصول و الزامات حاکم بر پردازش داده نسبت به تمامی داده های شخصی که مربوط به شخص حقیقی شناخته شده یا قابل شناسایی است قابلیت اعمال دارد و علاوه بر آن، برای حفاظت از داده های شخصی حساس قواعد مضاعفی همچون انجام ارزیابی حفاظت از داده و انتخاب مأمور حفاظت از داده مقرر کرده است. با توجه به این موارد می توان گفت در ق.ت.ا ایران، داده پیام های شخصی غیرحساس خارج از شمول ماده ۵۸ و ۵۹ و ضمانت اجرای ماده ۷۱ است (حیدری و جعفری، ۱۳۹۹: ۵۹)؛ این درحالی است که با گسترش فناوری های جدید و همچنین روش های تحلیل داده می توان از طریق ترکیب برخی از داده پیام های شخصی غیرحساس به داده پیام های حساس افراد دسترسی پیدا کرد.

لایحه حمایت از داده و حریم خصوصی در فضای مجازی، «داده های حساس» را معرفی کرده است و برای حفاظت از آن تعهدات پویایی برای کنترل گر مقرر نموده. طبق بند ۲ ماده ۱ لایحه، منظور از داده های شخصی حساس داده های آشکارکننده دیدگاه های سیاسی یا فلسفی، عقاید مذهبی، عادت های رفتاری، داده های ژنتیک، زیست سنجی، وضعیت سلامت شخص موضوع داده و داده های مربوط به رسیدگی های کیفری است». طبق ماده ۱۸ هر کنترل گر و

^۱ طبق ماده ۸۳ م.ع.د، نقض تعهدات و تکالیف قانونی مربوط به پردازش داده ها جریمه نقدی تا سقف ۱۰ میلیون یورو یا تا ۲٪ کل تراکنش سالیانه آخرین سال مالی به دنبال دارد.



پردازش‌گری اعم از آنکه به صورت انفرادی فعالیت کند یا در قالب مشارکت و همکاری با دیگر کنترل‌گر و پردازش‌گرها، موظف است با توجه به اهداف، زمینه‌ها، هزینه‌ها و خطرات احتمالی پردازش داده‌های شخصی، اقدامات امنیتی لازم را برای حفاظت از داده‌های شخصی با توجه به میزان حساسیت داده‌های مورد پردازش انجام دهد.

۴. تحلیل تعریف داده شخصی

چنان‌که در ابتدا اشاره شد م.ع.ح.د، داده شخصی را این‌گونه تعریف کرده است: «منظور از داده شخصی هرگونه اطلاعات مربوط به شخص حقیقی شناخته شده یا قابل شناسایی است؛ شخص حقیقی قابل شناسایی فردی است که به طور مستقیم یا غیرمستقیم، به ویژه با ارجاع به یک شناسه از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه آنلاین یا ارجاع به یک یا چند ویژگی خاص مانند هویت فیزیکی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی شناسایی شود». در ق.ت.ا ایران و لایحه حمایت از داده و حریم خصوصی در فضای مجازی به ترتیب داده شخصی این‌گونه تعریف شده است: «داده‌پیام‌های شخصی یعنی داده‌پیام‌های مربوط به یک شخص حقیقی مشخص و معین»؛ «هر نمادی از واقعه، اطلاعات یا مفهوم که به تنهایی یا در ترکیب با داده‌های دیگر می‌تواند به شناسایی یک شخص حقیقی زنده منجر شود». با توجه به تعاریف فوق، می‌توان تعریف داده شخصی را به چهار مؤلفه تقسیم کرد. در تحلیل بخش‌های مربوط به حقوق اتحادیه اروپا به نظریات مشورتی کارگروه ماده ۲۹^۱ و نیز مشروحات م.ع.ح.د استناد خواهد شد.

۴-۱. هرگونه اطلاعات

پیش از بررسی اولین مؤلفه در تعریف داده‌های شخصی لازم است اشاره‌ای به تفاوت بین

^۱ کارگروه ماده ۲۹، با نام رسمی کارگروه حفاظت از افراد در برابر پردازش داده‌های شخصی، به موجب ماده ۲۹ دستورالعمل حفاظت از داده مصوب ۱۹۹۵ به عنوان یک نهاد مشورتی مستقل تشکیل شد و پس از تصویب م.ع.ح.د، هیئت حفاظت از داده اتحادیه اروپا (European Data Protection Board) جایگزین آن شد. با وجود جایگزینی کارگروه ماده ۲۹ نظریات مشورتی آن کماکان به عنوان مبنایی برای تحلیل مواد مرتبط در محدوده م.ع.ح.د مورد استفاده قرار می‌گیرد (Finck & Pallas, 2020: 11).



داده^۱ و اطلاعات^۲ شود. گرچه در اغلب موارد این دو عبارت به طور مترادف استعمال می‌شوند؛ با این حال از نظر مفهومی بین این دو تفاوت‌هایی وجود دارد. در علم اطلاعات منظور از داده، اعداد و کاراکترها، علائم زبانی، ریاضی و دیگر علائم مورد توافق همچون صدا و تصویر و غیره هستند که برای نمایاندن وقایع، اشیا، رخدادها و مفاهیم، به کار می‌روند (زینس و دیانی، ۱۳۹۰: ۵)؛ داده‌ها به خودی خود واجد ارزش و معنا نیستند مگر زمانی که به گونه‌ای نظام‌مند طبقه‌بندی و محاسبه و پردازش شوند. بنابراین می‌توان گفت اطلاعات، داده‌های پردازش شده‌ای است که می‌توان از آن معنایی استخراج کرد. به همین جهت است که م.ع.ج.د، داده‌های شخصی را به معنی هرگونه اطلاعات مربوط به یک شخص حقیقی تعریف می‌کند؛ به عبارتی دیگر داده‌های شخصی اطلاعات معناداری هستند که مربوط به فرد موضوع داده می‌باشد (Finck & Pallas, 2020: 13). در ق.ت.ا ایران داده‌پیام را هر نمادی از واقعه، اطلاعات یا مفهوم که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود تعریف کرده است. از این حیث قانون مرقوم با م.ع.ج.د هم‌پوشانی دارد چراکه هر اطلاعاتی را صرف‌نظر از قالب آن به عنوان داده در نظر گرفته است.

استفاده از عبارت کلی در اشاره به اطلاعات در تعریف داده شخصی نشان‌دهنده رویکرد موسع قانون‌گذار اروپایی و ایران است که هدف آن پوشش تمامی انواع اطلاعات است. اطلاعات را می‌توان از منظر ماهیت، محتوا و قالب تحلیل کرد.^۳ از نظر ماهیت، اطلاعات ممکن است عینی^۴ باشد یا ذهنی.^۵ اطلاعات عینی، اطلاعات فیزیکی و مشهود مربوط به یک فرد است همچون نام، نشانی محل سکونت، نشانی پروتکل اینترنت، ویژگی‌های زیستی و مواردی از این قبیل. درمقابل اطلاعات ذهنی مواردی همچون نظرات و عقاید فلسفی، سیاسی و مذهبی و علایق فرد موضوع داده یا ارزیابی‌های مربوط به او است. با توجه به اطلاق عبارت هرگونه اطلاعات می‌توان گفت برای اینکه اطلاعاتی جزء داده‌های شخصی محسوب شوند؛ لازم نیست محتوای آن اطلاعات صحیح، واقعی یا اثبات‌شده باشند؛ پیش‌بینی حقی تحت عنوان حق اصلاح داده‌های شخصی در ماده ۱۶ م.ع.ج.د و بند د ماده ۵۹ ق.ت.ا که مقرر داشته فرد موضوع داده باید به پرونده‌های رایانه‌های حاوی داده پیام‌های شخصی مربوط به خود دسترسی داشته و بتواند داده پیام‌های

¹ Data

² Information

³ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 2007.

⁴ Objective information

⁵ Subjective information



ناقص و یا نادرست را محو یا اصلاح کند این برداشت را تأیید می‌کند.

در خصوص محتوای داده‌ها، دیوان دادگستری اتحادیه اروپا در حکم پیتر نواک در برابر کمیسر حفاظت از داده‌ها^۱ اعلام داشته «استفاده از عبارت هرگونه اطلاعات منعکس‌کننده هدف قانون‌گذار اتحادیه اروپا برای اختصاص دامنه وسیعی به این مفهوم است که محدود به اطلاعات حساس یا خصوصی نیست، بلکه به‌طور بالقوه شامل همه انواع اطلاعات، نه تنها عینی بلکه ذهنی، در قالب نظرات و ارزیابی‌ها می‌باشد مشروط بر اینکه مربوط به فرد موضوع داده باشد». از حیث قالب نیز برای اینکه اطلاعاتی داده شخصی محسوب شود لازم نیست در شکل و قالب خاصی باشد؛ بنابراین ممکن است در شکل الفبایی، عددی، گرافیکی، صوتی و تصویری باشد.

۴-۲. مربوط به شخصی حقیقی زنده

ارتباط اطلاعات با فرد موضوع داده جزء مؤلفه‌های اصلی و اساسی تعریف داده‌های شخصی می‌باشد. کارگروه ماده ۲۹ در تفسیر این عنصر اعلام داشته است اطلاعات زمانی مربوط به یک شخص حقیقی می‌باشد که درباره او باشد (Article 29 Data Protection Working Party, 2007: 9). در برخی از موارد ارتباط بین اطلاعات و فرد مستقیم است، برای مثال نشانی پروتکل اینترنت فرد موضوع داده که به‌طور مستقیم مربوط به یک شخص می‌باشد یا اطلاعات مربوط به اشتغال یا سلامتی افراد در پایگاه‌های اطلاعاتی. گاهی ارتباط بین اطلاعات و فرد موضوع داده محرز و آشکار نیست بلکه این ارتباط به‌طور غیرمستقیم بین فرد و اطلاعات قابل برداشت است. برخلاف مؤلفه قابلیت شناسایی فرد موضوع داده که به‌تصریح مشروح شماره ۲۶ م.ع.ح.د باید هنگام تصمیم‌گیری، تمام وسایل معقول و منطقی قابل استفاده برای شناسایی فرد مورد توجه قرار گیرد، چنین قیدی در مورد ارتباط اطلاعات به فرد وجود ندارد و بنابراین برای احراز ارتباط غیرمستقیم کافی است تا بگوییم اطلاعات مربوط به فرد می‌باشد. بر اساس نظریه کارگروه اطلاعات ممکن است از حیث محتوا، هدف یا اثرگذاری مربوط به یک شخص حقیقی باشد (Article 29 Data Protection Working Party, 2007:10). ارتباط اطلاعات از حیث محتوا زمانی است که آن اطلاعات مربوط به فرد باشد-در معنای محدود آن- برای مثال داده‌هایی که در خانه‌های هوشمند از طریق فناوری‌های قابل استفاده در اینترنت اشیا همچون سامانه بازشناسی امواج رادیویی^۲ تولید و جمع‌آوری و پردازش می‌شوند

^۱ Court of Justice of the European Union Case C-434/16 Peter Nowak [2017].

^۲ Radio Frequency Identification



از حیث محتوا مربوط به کاربر آن می باشد. در مورد کوکی ها که امروزه استفاده آن توسط صاحبان سایت ها و شرکت ها تبلیغاتی افزایش یافته است مثال بارز داده هایی است که نه تنها باعث شناسایی هویت از طریق دسترسی به آدرس پروتکل اینترنت کاربر می شود بلکه با جمع آوری اطلاعات جستجوی فرد در سایت و مواردی که از آن ها بازدید کرده است و در اختیار قراردادن آن برای اهداف بازاریابی و تبلیغات اطلاعات شخصی افراد را در اختیار اشخاص دیگر قرار می دهند. شناسه های تبلیغاتی نیز که در گوشی های هوشمند جهت ثبت پیشینه فعالیت های کاربر به صورت ناشناس اختصاص داده می شود از جمله چالش های حریم خصوصی مربوط به داده های شخصی می باشد که با بررسی آن توسط شرکت های تبلیغاتی می توانند به الگوهای رفتاری کاربر آن پی ببرند. با توجه به اینکه سابقه فعالیت افراد در این موارد ذخیره می شود و با پردازش آن می توان فرد را شناسایی کرد؛ از این رو این داده های جمع آوری شده نیز مشمول تعریف داده شخصی قرار می گیرند.

با وجود این ممکن است اطلاعات از نظر محتوا مربوط به شخص نباشد اما هنگامی که از داده ها با هدف ارزیابی رفتار یا تأثیرگذاری بر وضعیت یا رفتار فرد استفاده شود؛ مانند تحلیل اطلاعات مربوط به خریدهای روزانه یک فرد و استفاده از آن با هدف ترغیب مصرف کننده به خرید یک کالای ویژه یا احتمال استفاده آن برود آن داده ها مربوط به شخص تلقی می شوند. با توسعه اینترنت اشیا و تولید داده ها با حجم و سرعت بالا و استفاده از کلان داده های جمع آوری شده (قطبی راوندی و ابراهیمی و بنی اسدی، ۱۳۹۹: ۱) توسط نهادهای مختلف و به ویژه کسب و کارها از طریق داده کاوی و استفاده از نتایج آن برای اهداف بازاریابی و تجاری می توان گفت در عصر حاضر هر داده ای که از افراد جمع آوری و استفاده می شود قابلیت این را دارد که برای اهداف متعددی تحت پردازش قرار بگیرد از این رو بنابر تفسیر کارگروه ماده ۲۹ می تواند داده شخصی تلقی شود.

گذشته از این موضوع، طبق تفسیر کارگروه ماده ۲۹ که برای مؤلفه ارتباط داده با شخص سه معیار برای تشخیص ارائه داده است؛ کافی است یکی از معیارهای محتوا، هدف و تأثیر در پردازش داده ها وجود داشته باشد تا بتوان گفت پردازش داده مربوط به یک شخص حقیقی است. بر این اساس ممکن است اطلاعات از حیث محتوا و هدف مربوط به یک شخص نباشد اما اگر استفاده از داده های شخص بر حقوق و منافع او تأثیرگذار –هرچند نسبی و یا به طور احتمالی– باشد یا احتمال آن برود می توان گفت داده های استفاده شده یا قابل استفاده مربوط به

¹ Cookie



شخص حقیقی می‌باشد.

با توجه به تصریح بند ۱ ماده ۴ م.ع.ح.د و بند ۲ ماده ۱ ق.ت.ا ایران در تعریف داده‌های شخصی، قواعد این مقررات تنها داده‌های شخصی اشخاص حقیقی را تحت پوشش خود قرار می‌دهند. بر این اساس داده‌های اشخاصی که فوت شده‌اند^۱ با توجه به اینکه پس از مرگ شخصیت حقوقی خود را از دست می‌دهند، داده‌های آنان نیز به تبع فوت از شمول مقررات حاکم خارج می‌شوند. همچنین به تصریح مشروح شماره ۱۴ م.ع.ح.د، داده‌های مربوط به اشخاص حقوقی تحت پوشش مقررات حفاظت از داده قرار نمی‌گیرند. دلیل عدم شمول م.ع.ح.د برای داده‌های اشخاص حقوقی را می‌توان در دغدغه قانون‌گذار اروپایی در حمایت و حفاظت از کرامت، خودمختاری و حقوق و آزادی‌های اساسی و منافع شخصی اشخاص حقیقی دانست و همچنین با توجه به اینکه در عمل آنچه که برای بازاریابی و تجارت مورد استفاده قرار می‌گیرد داده‌های اشخاص حقیقی است از این رو تأکید قانون‌گذار بیشتر حفاظت از اینگونه داده‌ها است (van der Sloot, 2015: 27). با توجه به فقدان ممنوعیتی مبنی بر حفاظت از داده‌های اشخاص حقوقی، دولت‌های عضو اتحادیه اروپا می‌توانند قوانینی برای پردازش اطلاعات این اشخاص مقرر کنند.^۲ در رویه قضایی دیوان دادگستری اتحادیه اروپا پس از تصویب م.ع.ح.د در رأی پرونده C-398/16 مورخ ۹ مارس ۲۰۱۷ می‌توان مشاهده نمود که به تفکیک مقررات مربوط به حفاظت از داده اشخاص حقیقی از حقوقی تأکید شده است.

در ق.ت.ا ایران فرد موضوع داده داده‌پیام‌های شخصی یک شخص حقیقی اعلام شده که ظهور در زنده بودن فرد موضوع داده دارد از این رو داده‌پیام‌های شخصی افراد متوفی را دربر نمی‌گیرد. عدم حمایت م.ع.ح.د از داده‌های مربوط به افراد فوت شده و اشخاص حقوقی مانع از ارائه حمایت‌های قانونی توسط دولت‌های عضو اتحادیه اروپا در قالب قانون‌گذاری داخلی نیست (Hamulak, Kocharyan & Kerikmäe, 2021: 3 & Bygrave & Tosoni, 2020: 114). همچنین اگرچه اشخاص مذکور از شمول مقررات خروج موضوعی دارند اما با توجه به تفسیر موسع از معیارهای موجود در تعریف داده‌های شخصی ممکن است تحت شرایطی، داده‌های مربوط به اشخاص متوفی و اشخاص حقوقی حمایت حقوقی غیرمستقیمی، هرچند جزئی دریافت کنند؛ برای مثال می‌توان گفت داده‌های ژنتیکی مربوط به افراد متوفی، همراه با برخی از داده‌های بهداشتی این افراد در صورتی که نشان‌دهنده وضعیت ژنتیکی یا

^۱ General Data Protection Regulation, Recital 27.

^۲ General Data Protection Regulation, Recital 27.



سلامتی خویشاوندان بیولوژیکی زنده آن فرد باشند و باعث شناسایی یا احتمال شناسایی آنان شوند داده شخصی محسوب می شوند. در تأیید لزوم حفاظت از داده های افراد متوفی باید گفت اگرچه شخصیت حقوقی شخص حقیقی پس از موت به پایان می رسد با وجود این تمام منافع فرد با مرگ به پایان نمی رسد (Sperling, 2008:304) به ویژه اینکه امروزه داده های شخصی دیگر صرفاً جنبه ای از شخصیت انسان نیست، بلکه به یک عنصر اقتصادی قوی در روابط بین شرکت ها و مصرف کنندگان تبدیل شده است (Malgieri, 2016:133) از این رو ارائه حمایت قانونی هرچند نه به اندازه داده های شخصی افراد زنده برای داده های افراد فوت شده لازم است.

۳-۴. شناخته شده یا قابل شناسایی

به تصریح م.ع.ح.د، فرد حقیقی قابل شناسایی شخصی است که به طور مستقیم یا غیرمستقیم، به ویژه با ارجاع به یک شناسه از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه آنلاین یا ارجاع به یک یا چند ویژگی خاص مانند هویت فیزیکی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی شناسایی شود. به طور کلی، زمانی می توان یک شخص حقیقی را «شناخته شده» در نظر گرفت که در درون گروهی از افراد، از سایر اعضای گروه «متمايز» باشد (Bygrave & Tosonoi, 2020: 110). همچنین شخص حقیقی زمانی «قابل شناسایی» است که اگرچه هنوز شناسایی نشده است، اما امکان شناسایی آن وجود داشته باشد. چنان که از تعریف داده شخصی در نظام حقوق اتحادیه اروپایی برمی آید، آنچه ملاک تعیین شخصی بودن داده است قابلیت انتساب داده به فرد و امکان شناسایی او از طریق داده ها می باشد. در ق.ت.ا معیار معین و مشخص بودن فرد موضوع داده، مورد پذیرش قانون گذار قرار گرفته است، اگرچه همانند م.ع.ح.د به امکان شناسایی فرد اشاره نشده است اما معین و مشخص بودن شخص ظهور در آن دارد که داده پیام شخصی داده ای است که می توان آن فرد را از دیگران متمایز کرد و به هویت او پی برد. معیار معین و مشخص بودن شخص در بند ر ماده ۲ ق.ت.ا که داده پیام های شخصی را مربوط به شخص حقیقی مشخص و معین می داند ظهور بیشتری دارد.

شناسایی معمولاً از طریق اطلاعات خاصی به دست می آید که در تعریف م.ع.ح.د از آن ها تحت عنوان شناسه یاد می شود و منظور اطلاعات یا مجموعه ای از اطلاعات است که به تنهایی یا با ترکیب دیگر اطلاعات موجبات شناخت یا قابلیت شناسایی فرد را فراهم می کند. شناسایی فرد به طور مستقیم معمولاً از طریق یک شناسه صورت می گیرد مثل نام و نام خانوادگی یا



سایر اطلاعات منحصر به فرد از جمله شماره شناسایی ملی، حساب بانکی و حتی داده‌های بیومتریک مربوط به شخص. شناسایی فرد به طور غیرمستقیم زمانی است که شناسه‌های موجود برای شناسایی فرد کافی نباشند اما قابلیت آن را داشته باشند در ترکیب با سایر اطلاعات موجب شناسایی فرد شوند مانند یک یا چند ویژگی خاص مانند هویت فیزیکی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و اجتماعی.

عنصر قابلیت شناسایی شخص از طریق اطلاعات، نقش پویایی در تعریف داده‌های شخصی دارد و باعث می‌شود حسب مورد اطلاعاتی که در ابتدا و ظاهر امر باعث شناسایی فرد نمی‌شوند نیز ذیل تعریف داده‌های شخصی و احکام و الزامات قواعد حفاظت از داده قرار گیرند؛ بنابراین داده‌هایی نیز که مستعار شده‌اند اما امکان و احتمال شناسایی فرد در آن می‌رود نیز جزء داده‌های شخصی می‌باشند. بند ۵ ماده ۴ م.ع.ج.د دربارهٔ مستعارسازی داده اعلام داشته منظور از پردازش داده به گونه‌ای است که نتوان بدون ترکیب با سایر اطلاعات موجود و در دسترس و بدون توسل به عملیات فنی یا سازمانی به شخصی ارتباط داد. به طور کلی مستعارسازی یکی از روش‌های حفاظت از داده‌های اشخاص در برابر خطرات احتمالی می‌باشد که در آن شناسه‌های کلیدی از داده‌های اشخاص جداسازی شده و به طور جداگانه نگه‌داری می‌شوند.

با وجود اینکه م.ع.ج.د، از برخی داده‌ها حتی زمانی که به طور بالفعل موجب شناسایی فرد نمی‌شوند اما ممکن است در آینده این امکان فراهم شود حمایت می‌کند و کنترل‌گر را موظف به رعایت قواعد مربوط به پردازش می‌کند، در نظام حقوقی ایران با توجه به بند ۲ ماده ۲۱ ق.ت.ا و بند ۱ ماده ۱ لایحه حمایت از داده و حریم خصوصی در فضای مجازی، تنها داده‌هایی که به طور بالفعل موجب شناسایی فرد می‌شوند در تعریف داده شخصی قرار می‌گیرند. این استدلال را می‌توان از ملاک مشخص و معین بودن فرد موضوع داده به خوبی برداشت کرد. با این تفسیر، می‌توان گفت حجم گسترده‌ای از داده‌ها از شمول قوانین خارج هستند؛ چنان که شرح آن گذشت، بسیاری از داده‌ها وجود دارند که پردازش آن‌ها به تنهایی منجر به شناسایی فرد نمی‌شود اما با توجه به روش‌های نوین تحلیل داده می‌توان آن‌ها را با ترکیب با سایر داده‌ها -حتی داده‌های ناشناس- به اطلاعات حساسی از فرد دست یافت. بنابراین تفاوت اصلی نظام حقوقی ایران با نظام حقوقی اتحادیه اروپا در این است که دادهٔ شخصی در نظام اخیر حالتی پویا دارد و داده‌های بالقوه را نیز دادهٔ شخصی تلقی کرده و حمایت گسترده‌تری ارائه

¹ General Data Protection Regulation, Recital 28.



می‌دهد، اما در حقوق ایران تنها داده‌هایی که به‌طور بالفعل، فرد را شناسایی می‌کنند حمایت می‌شود. با توجه به موارد گفته‌شده می‌توان در قانون‌گذاری‌های آتی برای حمایت مؤثر و آینده‌نگر، این معیار را به تعریف قانونی داده شخصی افزود.

۱-۳-۴. ملاک تعیین قابلیت شناسایی فرد موضوع داده

از مشروح شماره ۲۶ م.ع.ج.د به خوبی برداشت می‌شود که تشخیص اینکه آیا یک شخص حقیقی قابل‌شناسایی است یا خیر بر عهده کنترل‌گر داده یا سایر اشخاصی است که به نحوی پردازش اطلاعات را بر عهده دارند. بر اساس مشروح اشاره شده برای تشخیص اینکه آیا شخص حقیقی به‌طور مستقیم یا غیرمستقیم قابل‌شناسایی است باید تمام ابزارهایی که به‌طور منطقی و معقول احتمال استفاده از آن توسط کنترل‌گر یا شخص دیگری وجود دارد در نظر گرفته شود و برای اطمینان از اینکه آیا احتمال معقولی برای شناسایی شخص حقیقی وجود دارد یا خیر، باید تمام عوامل عینی، مانند هزینه‌ها و مدت زمان مورد نیاز برای شناسایی، با در نظر گرفتن فناوری موجود در زمان پردازش در نظر گرفته شوند. بنابراین اگرچه قابلیت شناسایی فرد یک معیار پویا و موسع است؛ با وجود این توسط ملاک معقول بودن ابزارهای قابل استفاده برای پردازش و زمان و هزینه لازم برای شناسایی با در نظر گرفتن پیشرفت‌های موجود در فناوری محدود شده است. بر این اساس می‌توان گفت صرف اینکه احتمال آن برود شخص حقیقی قابل‌شناسایی است برای داده شخصی تلقی کردن آن کافی نیست بلکه باید در پرتو سایر عوامل مؤثر بررسی شود (Purtova, 2018: 46). با توجه به موارد اشاره‌شده، می‌توان گفت در نظام حقوقی اتحادیه اروپا ضابطه تشخیص ماهیت داده‌های مورد پردازش از حیث شخصی یا غیرشخصی بودن، معقول بودن امکان شناسایی است. بنابراین کنترل‌گر باید پیش از اقدام به پردازش داده‌های افراد، با توجه به ابزارها و فناوری‌هایی که در دست دارد و همچنین با در نظر گرفتن مدت زمان و هزینه لازم برای شناسایی تصمیم بگیرد که آیا عملیات پردازش شامل داده شخصی است یا خیر. گزارش تفسیری کنوانسیون حفاظت از اشخاص در رابطه با پردازش داده‌های شخصی مصوب شورای اروپا نیز معیار معقول و منطقی بودن ابزارهای قابل استفاده را به‌عنوان ملاک تشخیص قابلیت شناسایی شخص حقیقی پذیرفته و اعلام داشته اگر شناسایی فردی به زمان، تلاش یا منابع غیرمنطقی نیاز داشته باشد شخص «قابل‌شناسایی» تلقی نمی‌شود.

۴-۳-۱. انتقادات وارد بر معیار قابلیت شناسایی



در باره معیار قابلیت شناسایی شخص حقیقی گفته شده است دسترسی به فناوری‌های لازم ممکن است از کنترل‌گری به کنترل‌گر دیگر متغیر باشد. همین امر باعث می‌شود دامنه اجرایی مقررات حفاظت از داده با نوعی ابهام مواجه شود. این استدلال به‌ویژه در مورد کسب‌وکارهای کوچک به دلیل محدود بودن امکانات مالی و امکان دسترسی به فناوری‌های مطابق روز صادق است (Poritskiy, et.al., 2019: 519) که ممکن است به دلیل عدم توانایی مطابقت با م.ع.ح.د با جریمه‌های سنگین مواجه شوند و از عرصه رقابت خارج شوند. از سوی دیگر اگرچه ممکن است کنترل‌گر یا سایر اشخاص ثالث با هدف عدم اطلاق عنوان داده شخصی بر داده‌های مورد پردازش، این قبیل داده‌ها را به صورت ناشناس پردازش کنند یا از روش‌های فنی ناشناس‌سازی داده برای جلوگیری از شناسایی افراد موضوع داده استفاده کنند، با این وجود، تجربه نشان داده است این روش‌ها به‌طور کامل مؤثر و غیرقابل بازگشت نمی‌باشند (Mehmood, et.al, 2016: 1821) و علاوه بر این توسعه برخی الگوریتم‌ها این امکان را فراهم می‌سازند تا داده‌های ناشناس پس از مدتی تبدیل به داده‌هایی شوند که قابلیت شناسایی فرد را در معنایی که گفته شد فراهم کنند. گذشته از این، با توجه افزایش حجم اطلاعات جمع‌آوری و ذخیره‌شده در پایگاه‌های داده و امکان در اختیار قرار دادن آن در دست دیگران برای اهداف متعدد، می‌توان گفت این امکان معقول و منطقی وجود دارد تا هر داده‌ای را قابل شناسایی تلقی کنیم. بر این اساس برخی پا را فراتر گذاشته و معتقدند تفکیک بین داده‌های قابل شناسایی و غیرقابل شناسایی امری زاید است و باید از تعریف داده شخصی کنار گذاشته شود (Tene & Polonetsky, 2013: 258).

نتیجه انتقادات وارده در مجموع به این نکته اشاره دارد که رویکرد موسع و توسعه‌گرای اتحادیه اروپا با وجود مطلوب بودن آن در حفاظت از داده‌های شخصی به عنوان یک حق اساسی و بنیادین، در آینده به قدری توسعه خواهد یافت که تمامی داده‌ها را بتوان داده شخصی تلقی کرد؛ نتیجه این گستردگی زاید ممکن است باعث تورم در نظام حقوقی شود و به عنوان مانعی بر سر راه کاربردهای سودمند استفاده از داده‌ها گردد. اگرچه در حال حاضر نمی‌توان گفت فناوری‌های موجود و حجم داده‌های موجود در پایگاه‌های داده به نقطه اوج خود که بتوان گفت در آن تمام داده‌ها شخصی محسوب می‌شوند رسیده است؛ با این حال این واقعیت صرفاً یک فرضیه احتمالی نمی‌باشد و از این رو باید میان حفظ منافع حقوق افراد موضوع داده و کاربردهای گوناگون داده‌ها و عدم تحمیل الزامات گسترده برای حفاظت از داده‌ها توسط کنترل‌گر یا سایر اشخاص، تعادلی ایجاد شود.



یک راه احتمالی می‌تواند حذف معیار قابلیت شناسایی از تعریف داده‌های شخصی باشد و از این‌رو تنها از داده‌هایی حفاظت شود که به‌طور مستقیم باعث شناخته شدن هویت فرد موضوع داده می‌شوند. با این حال این راهکار نیز خالی از ایراد نیست، چراکه باید حداقل نسبت به داده‌هایی که امکان اثرگذاری بر حقوق و منافع افراد را دارند حمایتی قانونی هرچند نه به وسعت داده‌های شخصی شناسایی شده ارائه شود. راهکار دیگری که می‌تواند بدون کنار گذاشتن معیار قابلیت شناسایی کارساز باشد، تفکیک ضمانت اجرا نسبت به پردازش داده‌های شخصی مربوط به فرد شناخته شده و داده‌های شخصی با احتمال شناسایی است؛ با این توضیح که برای دسته دوم ضمانت اجرای سبک‌تری پیش‌بینی گردد. راهکار دیگری که توسط برخی از نظریه‌پردازان (Schwartz, Solove, 2011) مطرح شده تفکیک بین داده‌های شخصی مربوط به فرد شناخته شده و داده‌های شخصی با قابلیت شناسایی است با این توضیح که برای دسته اول تمامی اصول پردازش داده اعمال گردد و فرد موضوع داده بتواند از تمامی حقوقی که در م.ع.ج.د پیش‌بینی شده برای کنترل جریان پردازش داده‌های خود استفاده کند؛ و برای پردازش داده‌های دسته دوم، تنها برخی از اصول و حقوق همچون پردازش منصفانه، شفاف و قانونی، اصول مربوط به کیفیت داده و امنیت داده قابلیت اجرا داشته باشد آن هم در صورت وجود خطری مبنی بر امکان شناسایی، در نظر گرفته می‌شود. برای نظام‌های حقوقی نوپا که به تازگی وارد عرصه فناوری‌های نوین شده‌اند، به نظر می‌رسد پیش‌بینی معیار قابلیت شناسایی در حفاظت مؤثر از اطلاعات افراد می‌تواند نقش اساسی ایفا کند و هم انتظار عمومی شهروندان در حفاظت از اطلاعات شخصی را فراهم کند. برای جلوگیری از تورم تکالیف و تعهدات بازیگران این حوزه، می‌توان از راهکارهای ارائه شده برای اصلاح م.ع.ج.د استفاده کرد؛ از جمله تفکیک بین داده‌هایی که بالفعل فرد را شناسایی می‌کنند و داده‌هایی که با توجه به معیارهای فنی موجود، امکان شناسایی هویت فرد را در آینده ممکن می‌سازد. برای دسته اول می‌توان تمام اصول پذیرفته شده در پردازش داده را اعمال کرد و برای دسته دوم تنها اصولی برای تأمین امنیت آن‌ها در نظر گرفت.

۵. نتیجه‌گیری

نظام حقوقی اتحادیه اروپا با تصویب قانون جامع مقررات عمومی حفاظت از داده، قواعد مفصلی در رابطه با پردازش داده‌های شخصی و تعهدات کنترل‌گران و پردازش‌گران پیش‌بینی کرده است. در این نظام حقوقی منظور از داده شخصی هرگونه اطلاعات مربوط به شخص حقیقی شناخته شده یا قابل شناسایی است. تشخیص اینکه آیا شخص حقیقی به‌طور مستقیم یا



غیرمستقیم قابل‌شناسایی است باید تمام ابزارهایی که به‌طور منطقی و معقول احتمال استفاده از آن توسط کنترل‌گر یا شخص دیگری وجود دارد در نظر گرفته شود و برای اطمینان از اینکه آیا احتمال معقولی برای شناسایی شخص حقیقی وجود دارد یا خیر، باید تمام عوامل عینی، مانند هزینه‌ها و مدت زمان مورد نیاز برای شناسایی، با در نظر گرفتن فناوری موجود در زمان پردازش در نظر گرفته شوند. پیش‌بینی معیار قابلیت شناسایی در تعریف داده‌های شخصی موجب می‌شود حمایت قانونی ارائه‌شده توسط قانون‌گذار ماهیتی پویا داشته و در پرتوی توسعه‌های فناوری حرکت کند؛ از این منظر در نظام حقوقی اتحادیه اروپا داده‌هایی که به‌طور بالفعل منجر به شناسایی شخص نمی‌شوند اما در آینده ممکن است با دسترسی به پایگاه‌های داده و روش‌های تحلیل داده توسط کنترل‌گر شناسایی شوند نیز تحت حمایت قانون قرار دارند. در نظام حقوقی ایران داده شخصی داده‌ی مربوط به شخص حقیقی مشخص و معین است؛ از ظاهر این تعریف برداشت می‌شود که قانون‌گذار تنها از داده‌های شخصی بالفعل حمایت به عمل آورده و داده‌های بالفعل خارج از شمول حمایت قانونی هستند. باتوجه به سرعت پیشرفت فناوری‌ها در این مقاله پیشنهاد شده است تعریف قانونی داده شخصی اصلاح گردد تا دامنه شمول حمایت‌های قانونی همچون مقررات عمومی گسترش یابد.

با توجه به اهمیت اطلاعات حساس و خصوصی افراد، همچون اطلاعات مربوط به زندگی فردی، جنسی، سلامت و عقاید سیاسی یا فلسفی، مقررات عمومی حفاظت از داده قواعد ویژه‌ای برای حفاظت از این‌گونه داده‌ها مقرر کرده است، از جمله انجام ارزیابی خطرات احتمالی توسط کنترل‌گر و انتصاب مأمور حفاظت از داده. وجود تفکیک داده‌های شخصی و داده‌های شخصی حساس نشان می‌دهد در این نظام حقوقی هم داده‌های شخصی غیرخصوصی و هم داده‌های شخصی خصوصی تحت حمایت قانون‌گذار قرار گرفته و برای دسته دوم مقررات ویژه‌ای پیش‌بینی شده است. در نظام حقوقی ایران طبق ماده ۵۸ ق.ت.ا تنها داده‌پیام‌های شخصی خصوصی (حساس) تحت حمایت قانون‌گذار قرار گرفته است و قواعد و الزامات مربوط به پردازش داده که باید توسط کنترل‌گر رعایت گردد صرفاً محدود به داده‌های اخیر است. این درحالی است که باید از داده‌های شخصی غیرخصوصی نیز حمایت به‌عمل آورد؛ زیرا در بسیاری از موارد داده‌های اخیرالذکر ممکن است اطلاعات خصوصی افراد را برملا کند. برای رفع خلاء در این خصوص لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی تفکیکی همانند قانون اتحادیه اروپا قائل شده است و حمایت‌های قانونی را نسبت به تمامی داده‌هایی که منجر به شناسایی فرد می‌شوند تسری داده است.



هدف از وضع مقررات در مورد داده‌های شخصی، حمایت و حفاظت از داده‌های مربوط به افراد و نیز استفاده قانونی و قاعده‌مند از آن‌ها در کسب و کارهای مبتنی بر داده است؛ با توجه به این واقعیت در نظام حقوقی اتحادیه اروپا قواعد مفصلی برای کنترل‌گران و پردازش‌گران مقرر شده است که از آن‌ها تحت عنوان اصول و الزامات حاکم بر پردازش داده‌های شخصی یاد می‌شود. برای عدم ایجاد مانع در مسیر کسب‌وکارها و رشد فناوری، مقررات عمومی حفاظت از داده ضمانت اجرای غیرکیفری از جمله جزای نقدی بازدارنده و تعلیق فعالیت و غیره پیش‌بینی کرده است تا بازیگران این حوزه بدون داشتن واژه‌ای از تحمل مجازات کیفری همچون حبس در صورت نقض عمدی یا غیرعمدی قواعد، به فعالیت بپردازند. در نظام حقوقی ایران جز در لایحه پیش‌نویس حمایت از داده و حریم خصوصی در فضای مجازی و سایر پیش‌نویس‌های مربوط مقررات تفصیلی در مورد تعهدات و وظایف کنترل‌گر و پردازش‌گر وجود ندارد و ضمانت اجرای نقض قواعد از نوع کیفری است که برای رشد فناوری‌ها و کسب‌وکارها نوعی مانع به حساب می‌آید. برای رفع این نواقض، ضمانت اجرای غیرکیفری از نوع جزیمه نقدی به میزان بازدارنده پیشنهاد داده شده است.

طبق تعریف مندرج در مقررات عمومی حفاظت از داده و قوانین ایران، تنها پردازش داده‌های شخصی اشخاص حقیقی زنده تحت شمول قواعد پردازش قرار می‌گیرند؛ از این‌رو پردازش داده‌های اشخاص حقوقی و اشخاص متوفی از قوانین موجود خروج موضوعی دارند. در این‌باره اتحادیه اروپا به دولت‌های عضو این اجازه را داده است که در قوانین داخلی خود حمایت‌هایی برای پردازش داده‌های شخصی اشخاص متوفی مقرر کنند. با توجه به اینکه قانون تجارت الکترونیکی و پیش‌نویس لایحه حمایت از داده در این‌باره ساکت است پیشنهاد می‌شود این نکته مورد توجه واقع شود



۶. منابع

۶-۱ منابع فارسی

الف) کتب

۱. انصاری، باقر (۱۳۸۶). حقوق حریم خصوصی، تهران، سمت.
۲. انصاری، باقر (۱۴۰۰). حقوق داده‌ها و هوش مصنوعی، تهران، سمت.
۳. انصاری، باقر (۱۴۰۱). مطالعه تطبیقی حمایت از داده‌های شخصی در اروپا، آمریکا، چین و ایران، تهران، شرکت سهامی انتشار.
۴. ب) مقالات
۵. حیدری، علی مراد و علی جعفری (۱۳۹۹). «جرایم علیه داده‌پیام‌های شخصی در تجارت الکترونیکی»، پژوهشنامه حقوق کیفری، ۱۱(۱)، صص ۷۴-۵۱.
۶. زینس، پیام و محمدحسین (۱۳۹۰). «معنای سه مفهوم پرکاربرد داده، اطلاع و دانش»، کتابداری و اطلاع‌رسانی، ۱۴(۲)، صص ۵-۹.
۷. قطبی راوندی، مریم، معصومه السادات ابراهیمی و مریم بنی اسدی (۱۳۹۹). «تحلیل اینترنت اشیاء و کلان داده‌ها»، همین کنگره سراسری فناوری‌های نوین در حوزه توسعه پایدار، تهران.
۸. قناد، فاطمه و الهام شریف (۱۴۰۰). «مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا»، حقوق فناوری‌های نوین، صص ۱-۲۲.
۹. قناد، فاطمه و امیره علیقلی (۱۳۹۹). «مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی»، حقوق فناوری‌های نوین، ۲۹۷-۳۲۲.
۱۰. لطیف زاده، مهدیه، سید محمد مهدی قبولی درافشان، سعید محسنی و محمد عابدی (۱۴۰۱). «شناسایی ماهیت داده شخصی و جستجوی بستر



حقوقی مناسب جهت حمایت از آن در نظام حقوقی ایران»، فصلنامه مطالعات فقه و حقوق اسلامی، صص ۳۶۱-۳۹۴.

۱۱. ۹ لطیف زاده، مهدیه، سید محمدمهدی قبولی درافشان، سعید محسنی و محمد (۱۴۰۰). «تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا»، پژوهشنامه پردازش و مدیریت اطلاعات، صص ۴۳۹-۴۷۲.

۱۲. ج) پایان نامه و رساله

۱۳. لطیف زاده، مهدیه (۱۳۹۸). حمایت از داده های شخصی و محدودیت های آن در حقوق ایران و اتحادیه اروپا، پایان نامه برای اخذ مدرک دکترا، دانشکده حقوق و علوم سیاسی دانشگاه فردوسی مشهد.

۱۴. ۲-۳ منابع انگلیسی

A) Books

15. Bygrave, Lee (2014). *Data Privacy Law—An International Perspective*, Oxford, University Press.
16. European Union Agency for Fundamental Rights and Council of Europe (2018). *Handbook on European data protection law*, Luxembourg, Publications Office of the European Union
17. Kubben, Pieter & Dumontier, Michel & Dekker, Andre (2019). *Fundamentals of Clinical Data Science*, Springer Nature.
18. 14. Misek, Jakub (2018). "Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing)", in: Svantesson, Dan Jerker & Kloza, Dariusz. (Eds.), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Cambridge University Press.
19. Sperling, Daniel (2010). *Posthumous interests: legal and ethical perspectives*, Cambridge University Press.

20. B) Articles

21. 15. Bygrave, Lee & Luca, Tosoni (2020). "Article 4(1). Personal data", in: C. Kuner & L. Bygrave, C. Docksey & L. Drechsler (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press. pp.103-115.
22. 16. Finck, Michele & Pallas, Frank (2020). "They who must not



- be identified—distinguishing personal from non-personal data under the GDPR”, *Max Planck Institute for Innovation and Competition Research Paper Series*, 19-14, pp. 1-47.
23. 17. Georgieva, Ludmila & Kuner, Christopher (2020). “Processing of special categories of personal data”, in: C. Kuner & L. Bygrave, C. Docksey & L. Drechsler (eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford University Press, pp. 365- 385.
 24. 18. Hamulak, O., & Kocharyan, H., & Kerikmäe, T (2021). “The Contemporary Issues Of Post-Mortem Personal Data Protection In The EU after GDPR Entering into Force”, *EU Digital Sovereignty Hub*, pp. 225-238.
 25. 19. Malgieri, Gianclaudio (2016). “Property and (Intellectual) Ownership of Consumers’ Information: A New Taxonomy for Personal Data”, *Privacy in Germany*, 2016(4), pp. 133-150.
 26. 20. Mehmood, Abid, Natgunanathan, Iynkaran, Xiang, Yong, Hua, Guang & Guo, Song (2016). “Protection of Big Data Privacy”, *IEEE Access*, 4, pp. 1821–1834.
 27. 21. Poritskiy, Nazar, Oliveira, Flávio & Almeida, Fernando (2019). “The benefits and challenges of general data protection regulation for the information technology sector”, *Digital Policy, Regulation and Governance*, 21(5), pp. 510–524.
 28. 22. Purtova, Nadezhda (2018). “The law of everything. Broad concept of personal data and future of EU data protection law”, *Law, Innovation and Technology*, 10(1), pp. 40–81.
 29. 23. Schwartz, Paul & Solove, Daniel (2011). “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, *New York University Law Review*, Vol. 86, pp. 1814-1894.
 30. 24. Schwartz, Paul (2019). “Global Data Privacy: The EU Way”, *New York University Law Review*, 94(4), pp. 772-818.
 31. 25. Tene, Omer, & Polonetsky, Jules (2013). “Big Data for All: Privacy and User Control in the Age of Analytics”, *Northwestern Journal of Technology and Intellectual Property*, 11(5), pp. 239-273.



32. 26. van der Sloot, Bart (2015). "Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system", *Computer Law & Security Review*, 31(1), 26–45.
33. 27. Wong, Benjamin (2019). "Delimiting the concept of personal data after the GDPR", *Legal Studies*, 39(3), pp. 517–532.
- 34. D) Reports & Opinions**
35. 29. International Association of Privacy Professionals, Global Comprehensive Privacy Law Mapping Chart, 2022.
36. 30. OECD. 2010. The economics of personal data and privacy: 30 years after the OECD guidelines.
At: http://www.oecd.org/internet/ieconomy/theeconomicsofpersonaldataandprivacy30yearsaftertheoecd_privacyguidelines.htm.
37. 31. Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 2007.
38. 32. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981 and 2018 amendment.Explanatory report.
- 39. E) Cases**
40. 33. AMANN v. SWITZERLAND [2000]
41. 34. ECJ Case C-434/16 Peter Nowak [2017]
42. 35. European Court of Human Rights, Case Drelon v France [2022].
- 43. F) Legislation & Regulations**
44. 36. 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
45. 37. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
46. 38. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981 and 2018 amendment.
47. 39. Charter of Fundamental Rights of the European Union Article (2000).



Comparative Studying the Personal Data in the European Union and Iranian Legal System

Behnaz Ahmadvand^{1*} & Artin Jahanshahi²

1. Assistant Professor, Public Law, Department of Theory-Oriented STI Studies, National Research Institute for Science Policy, Tehran, Iran
2. MA. Student, Private Law, Faculty of Law & Political Sciences, University of Shiraz, Shiraz, Iran

Receive: 2023/01/02 Accept: 2023/05/27

Abstract

Personal data, as one of the key concepts in the field of personal data protection legislation, is defined in the General Data Protection Regulation as any information relating to an identified or identifiable natural person. Identifying a person directly or indirectly may be through data content or the purpose of data processing or the effect of data processing on the person. In EU law, to determine whether a natural person can be identified through data processing, all means that are reasonably likely to be used by the controller or processor must be taken into account, and to ensure whether there is a reasonable possibility to determine whether a natural person is present or not, all objective factors must be considered, such as the cost and time required for identification and the technology available at the time of processing. Based on the criterion of identifiability, data that may potentially lead to the identification of a person in the future is also covered by the law; such a standard can create the necessary dynamics in the laws. Iran's legislator has differentiated in the protection of private and non-private data and has limited compliance with processing rules to the first category, but the approach of the draft data protection bill has similarities with European Union and has provided broader protection, however, it needs to be amended by adding the criterion of identification to the legal definition, as well as the protection of the data of the deceased.

Keywords: Personal Data, Identification of a Natural Person, Reasonableness of Identification, General Data Protection Regulation, E-Commerce Law, Data Protection Bill, Privacy in Cyberspace

*Corresponding Author: behnazahmadvand@gmail.com

بهناز احمدوند و همکار _____ بررسی تطبیقی مفهوم داده های شخصی.....

