

تحلیل مفهومی مدعیان مالکیت بر داده؛ با تمرکز بر مقررات اتحادیه اروپا و نگرشی بر حقوق ایران

شیما عطار

دانش آموخته دکترای حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبائی، تهران، ایران.

shimaattar@gmail.com

## قابل انتشار در دوره ۲۶ شماره ۷۰ (تابستان ۱۴۰۶) نشریه پژوهش‌های حقوقی

### چکیده

با گسترش ابزارهای دیجیتال و شکل‌گیری اقتصاد داده‌محور، «مالکیت داده» به یکی از چالش‌های جدی در حقوق فناوری تبدیل شده است. حضور گسترده پلتفرم‌ها، شرکت‌های فناورانه و مدل‌های نوین کسب‌وکار، پرسش‌هایی اساسی درباره امکان، حدود و مشروعیت تملک داده‌ها پدید آورده است. در این میان، ظهور فناوری‌های پیشرفته مانند هوش مصنوعی، جایگاه داده را به‌عنوان منبع حیاتی اقتصاد دیجیتال بیش از پیش برجسته کرده و مباحث تازه‌ای را درباره مدعیان مالکیت بر داده مطرح ساخته است.

مقاله حاضر با تمرکز بر تفکیک میان داده‌های شخصی و غیرشخصی، در پی ارائه چارچوبی تحلیلی برای شناسایی «مالک داده» است. بر اساس شدت ارتباط داده با شخص موضوع داده، سه سطح از مالکیت بر داده‌ها تبیین می‌شود: داده‌های با ارتباط قوی، متوسط و ضعیف. این دسته‌بندی، امکان تحلیل دقیق‌تری از مدعیان مالکیت بر داده را فراهم می‌سازد.

هدف مقاله آن است که با بهره‌گیری از دیدگاه‌های حقوقی و اقتصادی و با اتکا به تجربه اتحادیه اروپا، و همچنین با بررسی وضعیت مالک داده در حقوق ایران، تصویری روشن‌تر از جایگاه مالک داده ارائه دهد؛ تصویری که می‌تواند مبنای مناسبی برای سیاست‌گذاری و قانون‌گذاری در این زمینه باشد. در فقدان قانون جامع در حوزه حقوق داده‌ها در ایران، این مطالعه می‌تواند افقی اولیه برای تحلیل مفهوم مالک داده در نظم حقوقی داخلی فراهم آورد و زمینه‌ساز مطالعات کاربردی در سطح ملی گردد.

### کلیدواژه‌ها

مالکیت داده، مالک داده، داده‌های شخصی و غیرشخصی، شخص موضوع داده، کنترل‌گر داده، اقتصاد دیجیتال، هوش مصنوعی.

## مقدمه

در جهان امروز، داده‌ها به یکی از مهم‌ترین دارایی‌های ناملموس تبدیل شده‌اند. اگرچه در ظاهر تکه‌هایی از اطلاعات گذرا به نظر می‌رسند، در واقع نقش حیاتی در تصمیم‌گیری‌های تجاری، مالی و شخصی ایفا می‌کنند و به سوخت محرک بسیاری از فعالیت‌های اقتصادی و فناوریانه تبدیل شده‌اند. به همین دلیل، موضوع مالکیت داده از منظر حقوقی، اقتصادی و سیاست‌گذاری عمومی به یکی از مباحث کلیدی عصر دیجیتال تبدیل شده است.

در اتحادیه اروپا، «قانون داده»<sup>۱</sup> و «قانون هوش مصنوعی»<sup>۲</sup> هر دو مصوب ۲۰۲۴، بدون تعریف صریح از مالکیت، بیشتر به تنظیم روابط میان دارندگان و کاربران داده و مسئولیت‌های استفاده‌کنندگان می‌پردازند. این قوانین نشان می‌دهند که پرسش از «مالک داده» همچنان محل اختلاف و تفسیر است.<sup>۳</sup>

در این سطح، رویکردها متفاوت است: گاه شخص موضوع داده<sup>۴</sup> به‌عنوان ذی‌حق اصلی شناخته می‌شود و گاه کنترل‌گران داده<sup>۵</sup> و بعضاً تولیدکنندگان داده<sup>۶</sup> مدعی حق تصرف و بهره‌برداری‌اند. این تفاوت، به‌ویژه در تمایز میان داده‌های شخصی و غیرشخصی آشکار می‌شود. داده‌های شخصی با هویت انسانی مرتبط هستند و تحت حمایت قواعد حریم خصوصی قرار دارند؛ در حالی که داده‌های غیرشخصی-مانند داده‌های تولیدشده توسط ماشین‌ها یا فرایندهای صنعتی-بیشتر به‌مثابه منابع اقتصادی دیده می‌شوند. در این میان، شرکت‌های بزرگ فناوری خود را «مالک دوفکتو»<sup>۷</sup> داده‌ها معرفی می‌کنند.<sup>۸</sup>

مفهوم مالکیت<sup>۹</sup> نیز برخلاف تصور عمومی از امری مطلق و شخصی، سازه‌ای حقوقی است که توسط دولت‌ها تعریف و اعمال می‌شود.<sup>۱۰</sup> با افزایش حجم داده‌های مصرف‌کننده و وابستگی شرکت‌ها به منابع واسطه‌مانند کارگزاران داده، اکوسیستم مالکیت داده پیچیده‌تر شده است. شرکت‌ها اغلب بدون رضایت کاربران، داده‌ها را جمع‌آوری و تحلیل می‌کنند؛<sup>۱۱</sup> بدون اینکه مالک رسمی داده باشند، آن‌ها را ذخیره و تجاری‌سازی می‌کنند؛ در مقابل، کاربران نیز اغلب فاقد ابزارهای مؤثر برای اعمال کنترل هستند. این وضعیت به ایجاد «مالکیت دوفکتویی» توسط شرکت‌ها منجر شده است. این شکاف، به‌ویژه در زمینه‌هایی مانند آموزش مدل‌های هوش

<sup>1</sup> Data Act (Regulation (EU) 2023/2854)

<sup>2</sup> Artificial Intelligence Act (EU AI Act), Regulation (EU) 2024/1684

<sup>3</sup> در سطح جهانی، گزارش سال ۲۰۲۵ دفتر کمی‌رایت ایالات متحده تأکید دارد که سیاست‌گذاری درباره مالکیت داده‌های ورودی، به‌ویژه در بستر هوش مصنوعی، یکی از چالش‌های آینده خواهد بود.

– Claudio Novelli, Federico Casolari, Philipp Hacker, Giorgio Spedicato, Luciano Floridi, “Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity”, *Computer Law & Security Review*, Volume 55, (November 2024) 6.

<sup>4</sup> Data subject

<sup>5</sup> Data controller

<sup>6</sup> Data producer

<sup>7</sup> De Facto Owner

– واژه حقوقی دوفکتو به معنی درواقع (in fact) یا در واقعیت (in reality) است؛ مالک دوفکتو شخصی است که در عمل مالک است اما مالکیت آن به صورت قانونی نیست.

<sup>8</sup> Malgieri, Gianclaudio, “Ownership of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution”, *Journal of Internet Law*, Vol. 20, n.5. (2016) 7.

<sup>9</sup> برای مطالعه بیشتر در خصوص «مفهوم مالکیت داده‌ها» ن. ک: عطار، شیما، «بالاتکلیفی در مفهوم مالکیت داده»، مجله پژوهش‌های حقوقی، انتشار آنلاین از تاریخ ۱۳ بهمن ۱۴۰۳. قابل انتشار در دوره ۲۵، شماره ۶۷، (پاییز ۱۴۰۵)

<sup>10</sup> Stephen T. Black, “who owns your data?”, *Indiana Law Review*, Volume 54, Number 2, (2021) 316.

<sup>11</sup> Renana Peres, David A. Schweidel, “Putting Consumers in Control of Their Data: Revisiting Data Ownership”, *Emory University’s Goizueta Business School*, (2024) 1.

مصنوعی، نوعی کنترل انحصاری ایجاد می‌کند که عملاً قدرت اقتصادی شرکت‌ها را افزایش داده و ضرورت قانون‌گذاری برای بازگرداندن تعادل را آشکار می‌سازد.<sup>۱۲</sup>

از همین رو، تمایز میان «مالکیت» و «حق کنترل» اهمیت روزافزونی یافته است. مالکیت به تخصیص حقوق سنتی دلالت دارد، حال آن‌که «کنترل» بیشتر به جنبه‌های اجرایی، نظارتی و تصمیم‌گیری در استفاده از داده مربوط می‌شود. تمرکز بر کنترل می‌تواند بازتاب دقیق‌تری از ساختار واقعی قدرت در اکوسیستم داده ارائه دهد. در این مقاله تلاش شده است این تمایز نیز در تحلیل‌های ارائه‌شده انعکاس یابد.

با پذیرش این پیچیدگی‌ها، مقاله حاضر در پی ارائه چارچوبی تحلیلی برای شناسایی مالک داده است؛ چارچوبی که بر اساس شدت ارتباط داده با شخص موضوع آن، داده‌ها را در سه سطح «ارتباط قوی»، «ارتباط متوسط» و «ارتباط ضعیف» طبقه‌بندی می‌کند. در خصوص داده‌های شخصی، پیشنهاد می‌شود مالکیت پیش‌فرض به شخص موضوع داده واگذار شود، هرچند در عمل کنترل‌گران داده همچنان نقش مسلط دارند. در حوزه داده‌های غیرشخصی نیز تولیدکنندگان خواستار شناسایی مالکیت‌اند که این امر می‌تواند به انحصار و مزیت رقابتی منجر شود. در کنار این دیدگاه‌ها، نظریه «مالکیت مشترک»<sup>۱۳</sup> نیز مطرح است که به تقسیم مسئولیت میان ذی‌نفعان مختلف اشاره دارد.

در نهایت، با توجه به اینکه نظام حقوقی ایران هنوز رویکرد مشخصی در قبال حقوق داده ارائه نکرده و مفهوم «مالک داده» به صورت نظام‌مند بررسی نشده است، مقاله حاضر علاوه بر تحلیل تجربه اتحادیه اروپا، وضعیت مالک داده در حقوق ایران را نیز بررسی می‌کند. طرح این موضوع می‌تواند زمینه‌ساز گفتگویی نو برای مواجهه با تحولات دیجیتال در بستر داخلی باشد.

## ۱- مالک داده‌های شخصی

برای شناسایی مالک داده‌های شخصی باید نخست این داده‌ها را تعریف کرد، سپس مدعیان اصلی مالکیت بر این داده‌ها را معرفی و دلایل شناسایی آن‌ها را به عنوان مالک داده‌های شخصی تحلیل نمود.

### ۱-۱- تعریف داده شخصی

داده شخصی هر قطعه واحدی از اطلاعات است که می‌تواند برای شناسایی فرد به کار رود، همچون نام و نام خانوادگی، آدرس الکترونیکی، داده‌های مکانی، آدرس محل سکونت و آدرس پروتکل اینترنتی. هر یک از این اطلاعات ممکن است به تنهایی موجب

<sup>12</sup>Mindy Nuñez Duffourc, Sara Gerke & Konrad Kollnig "Privacy of Personal Data in the Generative AI Data Lifecycle", *NYU Journal of Intellectual Property & Entertainment Law*, Vol. 13:2, (2024) 244.

<sup>13</sup> این مفهوم را می‌توان با روابط والدین و فرزندان مقایسه کرد: فرزند تحت تملک والدین نیست اما والدین در تصمیمات مهم او سهیم‌اند. در مورد داده‌ها نیز می‌توان چنین چارچوب مشترکی برای مدیریت و دسترسی تعریف نمود. با توصیفات گفته شده، چه بسا «مالکیت عمومی» (commons) مفهومی مناسب‌تر باشد. گوااین که وصف عمومی عبارت است از اصل حکمرانی و مدیریت منبع که امکان استفاده پایدار مشترک از برخی منابع خاص را برای افراد و جامعه فراهم می‌آورد. (hess, c. ) (And e. Ostrom (eds.) (2007), *understanding knowledge as a common: from theory to practice*, mit press, cambridge, mass. باز هم با «مالکیت مشترک» تفاوت‌هایی دارد. به‌موجب «مالکیت مشترک»، تولیدکنندگان و جمع‌آوری‌کنندگان داده نسبت به یکدیگر حقوق و مسئولیت‌هایی دارند؛ آن‌ها به‌طور جمعی، مشترک و شفاف در مورد استفاده از داده تصمیم‌گیری می‌کنند. اما، به‌موجب مالکیت «عمومی»، داده‌ها به‌صورت آزادانه، ناشناس، تجمیع‌شده و رقابت‌ناپذیرانه وجود دارند و تمامی حقوق لغو می‌شود. همان‌طور که سازمان توسعه و همکاری اقتصادی بیان کرده، وصف عمومی دلالت بر محیطی دارد که داده‌ها پس از تجمیع و شناسایی کافی، به‌طور عمومی منتشر می‌شوند OECD, "Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use", Summary of The Discussions, 15-16 May 2018, Directorate for Science, Technology and Innovation Committee on Digital Economy Policy, Working Party on Security and Privacy in The Digital Economy, (2018) 28.

شناسایی فرد نشود؛ برای مثال، هزاران نفر با نام مشابه وجود دارند و صرف نام موجبات شناسایی فرد را فراهم نمی‌آورد. اما ترکیب نام با آدرس الکترونیکی یا محل سکونت می‌تواند فرد را به‌طور مشخص قابل شناسایی سازد.

«مقررات عمومی حمایت از داده‌های اتحادیه اروپا»<sup>۱۴</sup> در بند ۱ ماده ۴، داده‌های شخصی را این‌گونه تعریف کرده است: «هرگونه داده مربوط به شخص شناسایی‌شده یا قابل شناسایی؛ شخص قابل شناسایی شخصی است که می‌تواند به‌طور مستقیم یا غیرمستقیم یعنی از طریق ارجاع به شماره شناسایی (مانند شماره امنیت اجتماعی) یا یک یا چند عامل خاص نظیر هویت فیزیکی، فیزیولوژیکی، روحی، اقتصادی، فرهنگی یا اجتماعی (مانند نام و نام خانوادگی، تاریخ تولد، داده‌های بیومتریک، اثر انگشت و ...) شناسایی شود.»<sup>۱۵</sup> بنابراین، داده شخصی به هر نوع داده‌ای اطلاق می‌شود که بتواند یک فرد را به‌طور مستقیم یا غیرمستقیم شناسایی کند.<sup>۱۶</sup>

## ۱-۲- شخص موضوع داده و کنترلگر داده: دو مدعی مالکیت بر داده‌های شخصی

در یک تعریف کلی، «شخص موضوع داده» به فردی اطلاق می‌شود که داده‌های جمع‌آوری‌شده به او مرتبط است. مقررات عمومی حمایت از داده‌های اتحادیه اروپا تعریف مستقلی از این اصطلاح ارائه نکرده، اما در بند (۱) ماده ۴، در چارچوب تعریف «داده شخصی» به آن اشاره کرده است. بر اساس این ماده، داده شخصی اطلاعاتی است که به فردی «شناسایی‌شده یا قابل شناسایی» تعلق دارد. بدین ترتیب، حتی افرادی که هویتشان هنگام جمع‌آوری داده مشخص نیست، اما امکان شناسایی آن‌ها در آینده وجود دارد نیز مشمول تعریف خواهند بود.

طبق بند ۷ ماده ۴، «کنترلگر داده» شخص حقیقی یا حقوقی، نهاد یا مرجعی است که به‌تنهایی یا مشترکاً اهداف و شیوه‌های پردازش داده‌های شخصی را تعیین می‌کند. حتی بدون دسترسی مستقیم به داده‌ها، صرف تعیین هدف و ابزار پردازش برای شناسایی نهاد به‌عنوان کنترلگر کافی است. کنترلگر نقشی اساسی در تصمیم‌گیری دارد: چه داده‌هایی، با چه هدفی و چگونه پردازش شوند.

به‌طور کلی، قوانین حمایت از داده‌های شخصی، پردازش داده‌ها را تنظیم و نوعی «کنترل انحصاری»<sup>۱۷</sup> به «شخص موضوع داده» اعطاء می‌کنند.<sup>۱۸</sup> برای مثال، «یادآور ۶۸ مقررات عمومی حمایت از داده اتحادیه اروپا»<sup>۱۹</sup> صراحتاً می‌خواهد کنترل شخص حقیقی را نسبت به داده شخصی تقویت کند، گواهی که یک گام فراتر رفته و پیش‌فرض مالکیت را برای «اشخاص موضوع داده» متصور شده است. چه بسا این مفهوم می‌تواند برای توصیف حقوق کنترلی<sup>۲۰</sup> به‌کار رود و معادل «حق قابلیت انتقال داده»<sup>۲۱</sup> که به افراد نوعی حس «مالکیت» بر داده‌های شخصی القاء می‌کند، فرض شود.<sup>۲۲</sup>

<sup>14</sup> General Data Protection Regulation (GDPR), Regulation (EU) 2016/679

<sup>15</sup> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

<sup>16</sup> "What is personal data?", European commission, accessed March 2023, [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en).

<sup>17</sup> Monopolistic Control

<sup>18</sup> Malgieri, Gianclaudio, *Op. cit.*, 1.

<sup>19</sup> (Recital 68 GDPR)

<sup>20</sup> Control Rights

<sup>21</sup> Data Portability

<sup>22</sup> چنان‌که، این باور وجود دارد که اگر نتوانید آن را حرکت دهید، مالک آن نیستید. (If you can't move it, you don't own it)

برای مطالعه بیشتر ن. ک:

- OECD, "Digital Economy Outlook 2020", OECD Publishing, Paris. (2020) 44.

شناسایی شخص موضوع داده به عنوان مالک داده شخصی، فهم نظام پیچیده مالکیت داده را تسهیل کرده و همسو با احترام به «حق تعیین سرنوشت اطلاعاتی» است. حتی اگر مالکیت مطلق بر داده شخصی قابل تصور نباشد، حقوق پیش‌بینی‌شده در مقررات حمایت از داده - مانند حق انتقال - گسترده‌ترین سطح مالکیت ممکن را، هرچند محدود، برای اشخاص موضوع داده فراهم می‌کند. از آنجا که حمایت از داده به‌عنوان یک حق بشری و بنیادی شناخته شده است، محدودیت‌هایی همچون محدودیت در انتقال داده به این معناست که فرد نمی‌تواند از تضمین‌های حقوق بشری خود صرف‌نظر کند. در این چارچوب، حقوق محدودتر فرد بر داده شخصی را می‌توان با نهاد «اجاره» در مالکیت زمین مقایسه کرد؛ حقی که بسته به مدت و هدف، محدود اما معتبر باقی می‌ماند.<sup>۲۳</sup>

از منظر اقتصادی نیز اعطای مالکیت به شخص موضوع داده می‌تواند انگیزه بیشتری برای بهره‌برداری کارآمد و حداکثرسازی منافع ایجاد کند. شخص موضوع داده سعی می‌کند سود خود را به حداکثر برساند و نتیجتاً برای رفاه اجتماعی نیز مناسب‌تر خواهد بود. با این حال، بنظر نمی‌رسد که اهداف اقتصادی بتواند مبنای کافی برای اعطای مالکیت داده شخصی به شخص موضوع داده باشد. این واقعیت که یک شخص حقیقی، منبع داده خاصی است و منبع آن خواهد ماند، به معنای حمایت از تخصیص مالکیت داده به شخص موضوع داده و اعطای حقیقی اقتصادی برای بهره‌وری تجاری از داده نخواهد بود؛ چراکه اگر قانون حق مالکیت را مشخص نکرده و یا حتی رد کرده باشد، این «کنترلگر» است که مالک «حقوق باقی‌مانده»<sup>۲۴</sup> در داده‌های شخصی محسوب می‌شود. در خوانش اقتصادی از حقوق مالکیت، حقوق باقی‌مانده به حقوقی اطلاق می‌شود که پس از اختصاص حقوق خاص به سایر طرف‌ها، همچنان نامشخص باقی مانده است. این حقوق باقی‌مانده، حقوق مالکیت تلقی می‌شود. اختصاص دادن حقوق باقی‌مانده به یکی از طرفین تحت عنوان «مالک» راهی برای کاهش هزینه‌های قراردادی است؛ چراکه ذات قراردادهای و حتی در مواردی قوانین، ناقص و تکمیل آن بسیار هزینه‌بر است. بنابراین، در این مفهوم می‌توان گفت که مقررات اتحادیه عملاً و نه به طور رسمی حقوق مالکیت داده‌های شخصی را به کنترلگر داده اعطاء کرده است، هرچند محدودیت‌هایی بر آن وارد می‌شود. در واقع، افراد با دریافت خدمات آنلاین رایگان، به جمع‌آوری کنندگان داده اجازه بهره‌برداری می‌دهند و حقوق خود را در چارچوب مقررات حفظ می‌کنند، در حالی که کنترلگر به حقوق باقی‌مانده دست می‌یابد.<sup>۲۵</sup>

نکته‌ای که باید مورد توجه قرار بگیرد این است که تناقضی میان حمایت از داده‌های شخصی و شناسایی مالکیت برای کنترلگر وجود ندارد. حمایت قانونی از داده‌های اشخاص حقیقی باید تضمین شود، اما این امر مانع از آن نیست که کنترلگر یا شرکت جمع‌آوری‌کننده داده، به‌عنوان دارنده حقوق مالکیت محدود، شناخته شود. در چنین حالتی، قواعد حمایتی صرفاً مانع تجاری‌سازی مستقیم داده‌های شخصی می‌شوند، بی‌آنکه استفاده از داده‌های تجمیع‌شده یا بی‌نام‌شده را برای کسب‌وکارها غیرممکن کنند.<sup>۲۶</sup>

## ۲- مالک داده‌های غیرشخصی

مدعی اصلی مالکیت داده‌های غیرشخصی، تولیدکنندگان این داده‌ها هستند. لذا، در ادامه نخست داده غیرشخصی تعریف می‌شود، سپس تولیدکننده به عنوان مدعی اصلی مالکیت بر این نوع داده‌ها معرفی می‌گردد.

## ۲-۱- تعریف داده غیرشخصی

<sup>23</sup> Purtova, Nadezhda, "Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency", *Journal of Law and Economic Regulation, Tilburg Law School Legal Studies Research Paper Series*. (2017) 8.

<sup>24</sup> Residual Rights

<sup>25</sup> Duch-Brown, Nestor, Martens, & Mueller-Langer, Frank. "The Economics of Ownership, Access and Trade in Digital Data", *JRC Digital Economy Working Paper*, (2017), 17

<sup>26</sup> Drexler, Josef, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access", *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8, (2017) 266.

داده‌های شخصی تنها بخش کوچکی از حجم وسیع داده‌ها هستند که هر لحظه پردازش و ذخیره می‌شوند. سایر داده‌هایی که مشمول تعریف داده شخصی نباشند، در دسته داده‌های غیرشخصی قرار می‌گیرند. «مقررات چارچوب جریان آزاد داده‌های غیرشخصی در اتحادیه اروپا»<sup>۲۷</sup> در بند ۱ ماده ۳ داده غیرشخصی را چنین تعریف کرده است: «هر داده‌ای غیر از داده شخصی تعریف شده در بند ۱ ماده ۴ مقررات عمومی حمایت از داده‌های اتحادیه اروپا»<sup>۲۸</sup>.

داده‌های غیر شخصی را می‌توان بر اساس مبدأ یا منشأ دسته‌بندی کرد: داده‌هایی که در اصل مرتبط با شخص حقیقی شناسایی شده یا قابل شناسایی نباشند، مانند داده‌های مربوط به شرایط آب و هوایی که توسط حسگرهای نصب شده در توربین‌های بادی تولید می‌شوند، یا داده‌های مربوط به نیازهای نگهداری برای ماشین‌های صنعتی؛ یا داده‌هایی که در ابتدا شخصی بوده‌اند، اما پس از فرآیند بی‌نام‌سازی<sup>۲۹</sup> به داده‌های غیرشخصی تبدیل شده‌اند.<sup>۳۰</sup>

از این رو، داده‌های شخصی از طریق بی‌نام‌سازی می‌توانند به داده غیرشخصی تبدیل شوند. با این حال، تمایز میان داده شخصی و غیرشخصی در عمل دشوار است؛ «پرونده بریر»<sup>۳۱</sup> نمونه شاخص این چالش است. در این پرونده، دیوان دادگستری اتحادیه اروپا در تفسیر «دستورالعمل حمایت از داده ۱۹۹۵ اتحادیه اروپا»<sup>۳۲</sup> اعلام کرد که داده می‌تواند حتی زمانی که شناسایی فرد تنها با اطلاعات اضافی اشخاص ثالث ممکن است، همچنان داده شخصی محسوب شود.

علاوه بر این، پیشرفت فناوری و توانایی ترکیب مجموعه‌های داده می‌تواند از داده‌های بی‌نام نیز داده‌های شخصی استخراج کند. به همین جهت است که نظام‌های حقوقی برای داده‌های شخصی و غیرشخصی، چارچوب‌های مقرراتی متمایز با اهداف متفاوت در نظر گرفته‌اند.

## ۲-۲- تولیدکننده: مدعی اصلی مالکیت بر داده‌های غیرشخصی

یکی از نخستین پرونده‌هایی که به موضوع مالکیت داده پرداخته و تولیدکننده را مالک شناخته، پرونده‌ای در دادگاه‌های آلمان است. در سال ۲۰۱۳ «دادگاه تجدیدنظر نورنبرگ»<sup>۳۳</sup> راجع به پرونده‌ای تصمیم‌گیری کرد که به‌طور مستقیم با الگوی جدید مالکیت داده ارتباط داشت. در این پرونده، شرکت مدعی شده بود که کارمندان آن با حذف داده‌های ذخیره شده مربوط به تماس‌های تجاری و مشتریان احتمالی از رایانه‌های متعلق به شرکت، مرتکب «سرقت داده‌ها» شده‌اند و باید مشمول محکومیت مندرج در قانون کیفری آلمان شوند. مطابق قانون، حذف، اخلال یا تغییر غیرقانونی داده‌های رایانه‌ای با ضمانت اجرای حبس تا دو سال یا جزای نقدی همراه است. دادگاه ضمن تأکید بر خلأ قانون در خصوص مالکیت داده، اعلام کرد که «تولیدکننده داده» نسبت به آن حق دارد. بر این اساس، داده‌های تولیدشده توسط کارمند متعلق به اوست، حتی اگر بعداً برای مقاصد تجاری کارفرما مورد استفاده قرار گیرند؛ گرچه کارمند می‌تواند به دلیل این اقدام تحت مقررات کار اخراج شود. دادگاه همچنین مقرر داشت که اگر داده‌ها پیش‌تر در اختیار کارمند قرار گرفته بود،

<sup>27</sup> Free Flow of Non-Personal Data Regulation (FFNPD), Regulation (EU) 2018/1807

<sup>28</sup> Data other than personal data as referred to in Article 4(1) of Regulation (EU) 2016/679.

<sup>29</sup> Anonymization

<sup>30</sup> European Commission, "Commission guidance on free flow of non-personal data – Questions and Answers", accessed July 2022, [https://ec.europa.eu/commission/presscorner/detail/en/MEMO\\_۱۹\\_۲۷۰۰](https://ec.europa.eu/commission/presscorner/detail/en/MEMO_۱۹_۲۷۰۰).

<sup>31</sup> C-582/14, "Patrick Breyer v Bundesrepublik Deutschland." (2016), 779, paragraph 49.

<sup>32</sup> Data Protection Directive (Directive 95/46/EC)

<sup>33</sup> Court of Appeal of Nuremberg

آنگاه کارفرما مالک محسوب می‌شود. اما از آنجاکه در این پرونده داده‌ها توسط کارمند ایجاد شده بودند، حق متعلق به او دانسته شد. بدین ترتیب، دادگاه گرایش آشکاری به شناسایی نوعی حق مالکیت برای «تولیدکننده داده» نشان داد.<sup>۳۴</sup>

از آنجاکه پرونده ارتباطی نزدیک و قوی با حقوق کیفری داشته، پرسش اینجاست که آیا این حکم قابل اعمال در حقوق مدنی نیز هست یا نه؟ در حقوق مدنی که رویکردی منعطف‌تر دارد، اصل مالکیت تولیدکننده می‌تواند به واسطه نهادهایی چون استخدام، نمایندگی یا وکالت تغییر یابد. به بیان دیگر، اگر فردی در قالب رابطه استخدامی برای تولید داده به کار گرفته شده باشد، مالکیت داده به کارفرما تعلق دارد. همین منطق در پرونده دیگری در سال ۲۰۰۷ در «دادگاه تجدیدنظر ساکسونی»<sup>۳۵</sup> آلمان نیز تأیید شد؛ جایی که کارمندی پس از بیماری طولانی مدت، رایانه شرکت را با پاک کردن برنامه‌ها و ایمیل‌ها تحویل داد. دادگاه، مالکیت کارفرما بر نرم‌افزارها و داده‌ها را شناسایی کرد و اقدام کارمند را موجب نقض حق کارفرما و در نتیجه توجیه‌گر اخراج وی دانست.

بنابراین، در هر دو پرونده، اگرچه یکی در حوزه حقوق کیفری و دیگری در حوزه حقوق کار مطرح شد، اصل شناسایی حق مالکیت برای تولیدکننده<sup>۳۶</sup>، ایجادکننده<sup>۳۷</sup> یا تهیه‌کننده<sup>۳۸</sup> داده‌ها تثبیت گردید؛ با این تفاوت که در روابط استخدامی، داده متعلق به کارفرما دانسته شد و در مواردی که داده صرفاً توسط کارمند ایجاد شود، حق به او اعطا گردید.<sup>۳۹</sup>

سال‌ها بعد، کمیسیون اروپا با هدف ارتقاء قابلیت تجاری‌سازی و داد و ستد داده‌های غیرشخصی یا داده‌های تولید شده توسط ماشین‌ها به عنوان یک کالای اقتصادی، بحث مالکیت داده را مطرح کرد. نخستین بار در «بیانیه اقتصاد داده اتحادیه اروپا»<sup>۴۰</sup> در سال ۲۰۱۷ ایده شناسایی «تولیدکننده داده» به عنوان مالک داده‌های غیرشخصی مطرح شد. کمیسیون در این چارچوب پنج هدف اصلی را دنبال می‌کرد: بهبود دسترسی به داده‌های بی‌نام تولید شده توسط ماشین، تسهیل و تشویق به اشتراک‌گذاری این داده‌ها، حمایت از سرمایه‌گذاری در داده‌ها، جلوگیری از افشای داده‌های محرمانه و به حداقل رساندن اثرات lock-in. یکی از گزینه‌های پیشنهادی، شناسایی حق تولیدکننده بر داده‌های غیرشخصی یا بی‌نام بود.<sup>۴۱</sup>

با این حال، کمیسیون به خوبی از تضاد احتمالی میان حقوق تولیدکننده و قواعد حمایت از داده‌های شخصی آگاه بود؛ به همین دلیل این حق را صرفاً به داده‌های غیرشخصی محدود کرد. اما در عمل، تمایز میان داده‌های شخصی و غیرشخصی چندان روشن نیست، زیرا مجموعه‌های داده اغلب ترکیبی از هر دو را در برمی‌گیرند. تنها راه حل پیشنهادی کمیسیون، بی‌نام‌سازی داده‌های شخصی برای ورود به حوزه حق تولیدکننده بود. هرچند اگر شخص موضوع داده به موجب «حق فراموش شدن» خواستار حذف داده‌های خود شود، حق تولیدکننده نیز زائل خواهد شد. این تعارض شبیه وضعیتی است که در حقوق مالکیت فکری وجود دارد؛ جایی که دارنده حق فکری می‌تواند تقاضای نابودی کالای غیرقانونی متعلق به دیگری را مطرح کند.<sup>۴۲</sup>

<sup>34</sup> Hoeren, Thomas., "Big Data and the Ownership in Data: Recent Developments in Europe", European Intellectual Property Review, Issue 12, (2014) 753.

<sup>35</sup> Labor Court of Appeal of Saxony

<sup>36</sup> Originator

<sup>37</sup> Creator

<sup>38</sup> Producer

<sup>39</sup> *Ibid*, pp.753- 754.

<sup>40</sup> Communication on Building a European Data Economy (COM (2017) 9 final)

<sup>41</sup> Drexl, Josef, "Data Access and Control in the Era of Connected Devices, Study on Behalf of the European Consumer Organization", BEUC, Brussels, (2018) 30.

<sup>42</sup> *Ibid*, p. 47.

در نهایت، کمیسیون تصریح کرد که هرگونه مقررگذاری در این زمینه باید دو واقعیت را توأمان در نظر داشته باشد: نخست آنکه مجموعه‌های داده به‌طور ناگزیر داده‌های شخصی را نیز شامل می‌شوند و بنابراین مقررات نباید صرفاً به داده‌های غیرشخصی محدود گردد؛ دوم آنکه، گریزی از رعایت مقررات حمایت از داده‌های شخصی نیست و این مقررات بر حقوق اقتصادی تولیدکننده تقدم دارد.

### ۳- مالک داده‌ها حسب میزان ارتباط با شخص موضوع داده

مالکیت داده اغلب با حقوق، مسئولیت‌ها و فرصت‌هایی درهم‌آمیخته است که با یکدیگر همپوشانی دارند. علاوه بر شخص موضوع داده، بسیاری از ذی‌نفعان دیگر در فرایند مشارکت، جمع‌آوری و کنترل داده‌های شخصی دخیل شده‌اند. بنابراین می‌توان برای داده، «مالکین» متعددی متصور شد و حتی ممکن است «مالکیت مشترک» به رسمیت شناخته شود تا حق انحصاری تنها برای شخص موضوع داده یا کنترلگر ایجاد نشود. در برخی موارد نیز ممکن است داده فاقد مالک شناسایی شود.<sup>۴۳</sup>

با ارائه یک طبقه‌بندی جدید از داده‌های شخصی، می‌توان این فروض را تحقق بخشید و همچنین اسباب رفع تعارض و برقراری تعادل در شناسایی شخص موضوع داده یا کنترلگر به‌عنوان مالک داده شخصی را فراهم آورد.

### ۳-۱- طبقه‌بندی جدیدی از داده‌های شخصی

در عصر اطلاعاتی، داده‌های شخصی صرفاً بیان شخصیت فرد نیستند، بلکه یک عنصر اقتصادی قوی در رابطه میان کسب‌وکارها و کاربران به‌شمار می‌روند. مقررات عمومی حمایت از داده اتحادیه اروپا نیز همسو با این هدف، سطوح متفاوتی از حقوق کنترلی را در تطابق با رویکرد مختص به داده‌های شخصی به رسمیت شناخته است.

برای درک این که چگونه می‌توان حقوق شخصیتی شخص موضوع داده و حقوق مالکیت فکری کنترلگر را با یکدیگر آشتی داد یا هماهنگ ساخت، می‌توان پیشنهاد نمود که داده‌ها نه برپایه «موضوع اصلی» آن‌ها بلکه بر مبنای «میزان مالکیت» آن‌ها دسته‌بندی شوند. گویان که طبقه‌بندی کنونی داده‌ها مبتنی بر «رویکرد موضوع محور»<sup>۴۴</sup> بی‌مورد و بیهوده است؛ چراکه در جهان هوش مصنوعی، صنعت اطلاعات به هرگونه داده مرتبط به کاربر علاقه دارد؛ نه تنها ترجیحات و عادات تجاری؛ بلکه شرایط سلامتی، خانوادگی، مالی و ارتباطات دوستانه کاربران مورد توجه و اهمیت است؛ از این‌رو، داده‌های شخصی را می‌توان با توجه به درجه «مالکیت» طبقه‌بندی نمود.

تعریف مناسب از داده‌های شخصی، «هرگونه اطلاعات «مربوط»<sup>۴۵</sup> به شخص حقیقی شناسایی شده یا قابل شناسایی (شخص موضوع داده) است». تنها عنصر متغیر این تعریف «رابطه»<sup>۴۶</sup> (و در نتیجه میزان «مالکیت») میان اطلاعات و شخص موضوع داده است؛ در نتیجه درک ارزش این «ارتباط»<sup>۴۷</sup> اهمیت می‌یابد. به بیان دیگر، با توجه به این که این تعریف حوزه گسترده‌ای دارد، باید پیوند «ارتباطی»<sup>۴۸</sup> میان اشخاص و داده‌های شخصی درک شود. داده‌ها در صورتی که به هویت، ویژگی‌ها یا رفتار یک فرد ارتباط داشته باشد یا اگر این اطلاعات برای تعیین یا تأثیر در نحوه برخورد یا ارزیابی فرد به کار رود، به فرد ارتباط پیدا می‌کند. در نتیجه، می‌توان میان سه نوع داده قائل به تفاوت شد: داده دارای ارتباط «قوی»، «متوسط» و «ضعیف» با شخص موضوع داده.<sup>۴۹</sup>

<sup>43</sup> OECD, "Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use", *Summary of The Discussions*, (2018) 28.

<sup>44</sup> Subject Matter Approach

<sup>45</sup> Relating To

<sup>46</sup> Relationship

<sup>47</sup> Relation

<sup>48</sup> Relational

<sup>49</sup> Maligni, Gianclaudio, "Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data", *Privacy in Germany - PinG*, n. 4. (2016) 5.

### ۳-۱-۱- داده‌های دارای ارتباط قوی با موضوع داده

زمانی که داده‌های شخصی به طور مستقیم به وسیله شخص موضوع داده به کنترلگر ارائه شود، برای مثال، زمان تکمیل فرم یا زمانی که شخص موضوع داده داده‌های شخصی خود را به صورت مستقل در پروفایل‌های شبکه اجتماعی قرار می‌دهد.

### ۳-۱-۲- داده‌های دارای ارتباط متوسط با موضوع داده

زمانی که داده‌های شخصی به طور غیرمستقیم از طریق شخص موضوع داده ارائه می‌شود و مستقیماً از واقعیت گرفته می‌شود یا به طور غیر مستقیم نتیجه واقعیت است. برای مثال، هنگامی که مکان فرد به وسیله سامانه موقعیت‌یابی جهانی<sup>۵۰</sup> مشخص می‌شود، هنگامی که فعالیت بدنی او به وسیله یک برنامه تلفن همراه کنترل می‌شود یا جستجوهای مکرر وجسته گریخته او، ترجیحات او را نشان می‌دهد، یک رابطه متوسط وجود دارد. چنین داده‌هایی (شرایط سلامتی، مشارکت در یک رویداد، فعالیت‌های بدنی، علائق، سرگرمی-ها، ترجیحات سیاسی، دوستان احتمالی، روابط و موقعیت خانوادگی) در حال حاضر صحیح (یا بسیار محتمل)، به راحتی قابل تأیید و به واسطه تجمیع ساده داده‌های خام قابل دریافت هستند.<sup>۵۱</sup>

### ۳-۱-۳- داده‌های دارای ارتباط ضعیف با موضوع داده

زمانی که داده‌های شخصی به طور غیرمستقیم از واقعیت موجود<sup>۵۲</sup> ناشی شده و به واسطه اثر فکری کسب‌وکارها برای چشم انداز آینده «خلق یا ایجاد» شده است. برای مثال، داده‌های پیش‌بینی شده<sup>۵۳</sup> مرتبط با مطالعات پیچیده رفتاری، پیش‌بینی‌های دراز مدت و پیش‌فرض‌های احتمالی اعمال شده در موارد ویژه، پروفایل روانشناختی و غیره، و همچنین مدل‌های کسب و کار شخصی‌سازی شده. تمامی این داده‌ها (امید به زندگی قابلیت اطمینان، پیش‌بینی‌های رفتاری، شرایط سلامتی و غیره) بالقوه بوده و به سمت آینده است.<sup>۵۴</sup> هرکدام از این دسته‌ها منعکس کننده حقوق نظارتی هستند که به شناسایی مالک داده‌ها کمک می‌کند.

### ۳-۲- مالک داده‌ها بر اساس طبقه‌بندی جدید داده‌های شخصی

حسب میزان ارتباط داده‌ها با شخص موضوع داده، می‌توان مالک داده را خود شخص موضوع داده دانست، یا مالکیت مشترک میان شخص موضوع داده و کنترلگر را متصور شد و حتی در برخی موارد، داده را فاقد مالک تصور کرد. در ادامه وضعیت این سه گروه تشریح می‌گردد:

### ۳-۲-۱- شخص موضوع داده به عنوان مالک در موارد ارتباط «قوی» شخص با داده‌های شخصی

گروه اول از این طبقه‌بندی رابطه، آن دسته از اطلاعات شخصی است که به طور مستقیم به وسیله شخص موضوع داده به کنترلگر داده ارائه می‌شود. این داده‌ها ممکن است «آگاهانه» به کنترلگر ارائه شده باشد؛ برای مثال، زمانی که شخص موضوع داده در یک تارنمای اینترنتی ثبت نام می‌کند، یک حساب کاربری می‌سازد، یک فرم را پر می‌کند، ممکن است با آگاهی کمتری اقدام کرده باشد، چنین داده‌هایی نه تنها به شخص موضوع داده مربوط هستند یا به اصطلاح، در ارتباط با او قرار دارند، بلکه به طور مستقیم به وسیله او ایجاد شده‌اند. در این موارد، ارتباط میان شخص موضوع داده و داده به قدری محکم و قوی است که ممکن است شخص موضوع

<sup>50</sup> Gps

<sup>51</sup> *Ibid.*

<sup>52</sup> Actual Reality

<sup>53</sup> Predictive Data

<sup>54</sup> *Ibid.*, 6.

داده، خود به عنوان «کنترلگر داده» یا «کنترلگر مشترک»<sup>۵۵</sup> موضوع بند ۷ ماده ۴ مقررات اتحادیه اروپا در مورد داده‌های شخصی تعریف شود. از آنجا که شخص موضوع داده آزادانه در مورد به اشتراک گذاری محتوای شخصی تصمیم می‌گیرد، می‌توان اثبات کرد یا این گونه برداشت نمود که او «اهداف و شیوه‌های پردازش داده‌های شخصی را مشخص می‌کند. در واقع همان تعریفی که از کنترلگر داده وجود دارد»<sup>۵۶</sup>.

ساختار حمایت از داده اتحادیه اروپا آشکارا به این گروه از داده‌ها پرداخته است. دستورالعمل ۱۹۹۵ ترتیب خاصی برای چنین داده‌هایی ارائه نکرده بود. تنها در «یادآور ۳۸»<sup>۵۷</sup> اشاره شده بود که «زمانی که اطلاعات از شخص موضوع داده جمع‌آوری می‌شود، باید در نظر گرفتن شرایط جمع‌آوری، اطلاعات صحیح و کامل به او ارائه شود». مقررات عمومی حمایت از داده اتحادیه اروپا در این زمینه بسیار گویاتر است و ماده ۱۳ به تمامی اطلاعاتی که باید در مواردی که داده‌ها از شخص موضوع داده جمع‌آوری شده است، ارائه شود، اشاره کرده است.<sup>۵۸</sup>

ماده ۲۰ مقررات اتحادیه حقوق خاصی را برای این گروه از داده‌ها در نظر گرفته است. این ماده مقرر می‌دارد که «حق انتقال داده» تنها به مواردی اختصاص دارد که شخص موضوع داده، داده‌ها را در دسترس یا اختیار کنترلگر قرار داده باشد، و زمانی که پردازش به صورت خودکار، بر مبنای رضایت، و یا قرارداد صورت گرفته باشد. با توجه به این ماده، کنترل کامل شخص موضوع داده بر این گروه از «داده‌های قویاً مرتبط» وجود دارد. حتی شخص موضوع داده می‌تواند از حق دریافت این اطلاعات «در قالبی ساختارمند، متداول و قابل خواندن توسط ماشین» و «انتقال آن داده‌ها به کنترلگر دیگر» استفاده نماید. در کنار سایر حقوق اشخاص موضوع داده (حق دسترسی، حق فراموش شدن، حق اصلاح، و غیره)، این گروه از داده‌ها تنها موردی است که واجد حق قابلیت انتقال داده گشته است.<sup>۵۹</sup>

نتیجه این که، با این توصیفات، شخص موضوع داده بر «داده‌های قویاً مرتبط» یک شکل انحصاری از مالکیت شبه مالکانه اسرار تجاری برخوردار است، به‌ویژه با در نظر گرفتن حق قابلیت انتقال داده‌ها، به‌عنوان یکی از بزرگترین نمادهای مالکیت و خصوصی‌سازی داده‌ها.<sup>۶۰</sup>

### ۳-۲-۲- مالکیت مشترک در موارد ارتباط «متوسط» شخص با داده‌های شخصی

مالکیت مشترک، مفهومی است بیانگر سطوحی از مالکیت که متقابلاً با یکدیگر همپوشانی دارند و برای انواع گوناگون داده‌های تولید شده در هوش مصنوعی و روش‌های گوناگون ذخیره و آنالیز داده به رسمیت شناخته می‌شود. اهمیت این مفهوم به علت مدیریت مشترکی است که اعمال می‌کند. از یکسو، فرد «مالک» داده‌های شخصی خود است؛ از سوی دیگر، کسب و کار «مالک» داده است، آن‌که داده‌ها را جمع‌آوری و تجمیع می‌کند. برای مثال، داده‌های شخصی توسط کسب‌وکارها ذخیره، تجمیع و آنالیز می‌شود. به همین ترتیب، افراد زمانی که از تلفن هوشمند خود استفاده می‌کنند، زمانی که رانندگی می‌کنند و زمانی که در شبکه‌های اجتماعی فعالیت

<sup>55</sup> Joint Controller

<sup>56</sup> Kuner, Christopher; Bygrave, Lee A.; Docksey, Christopher., *The Eu General Data Protection Regulation (GDPR)- A Commentary*, Oxford University Press. United Kingdom, (2020) 146.

<sup>57</sup> (Recital 38 Directive 1995)

<sup>58</sup> article 13, GDPR

<sup>59</sup> برای مطالعه بیشتر در خصوص «حقوق اشخاص موضوع داده» ن. ک: باقر انصاری و شیما عطار، حقوق کاربران فضای مجازی، تهران: شرکت سهامی انتشار،

۱۴۰۲، ۱۹۸-۱۰۱.

<sup>60</sup> Purtova, Nadezhda, "The Illusion of Personal Data as No One's Property, Law, Innovation, and Technology", Volume 7, Issue 1, Tilburg University - Tilburg Institute for Law, Technology, and Society (TILT) (2013)98.

می‌کنند، داده تولید می‌کنند. واضح است که این اطلاعات در یک مفهوم متعلق به افرادی است که آن را تولید می‌کنند؛ اما به اشخاصی که خدمات تلفن همراه را فراهم آورده‌اند، خودرو را تولید کرده‌اند یا شبکه‌های اجتماعی را مدیریت کرده‌اند، نیز قابل تعلق است. نکته مهم این است که بسیاری از اطلاعات در جهان هوش مصنوعی و اقتصاد دیجیتال، وجه مالکانه پیدا کرده و تجاری شده‌اند.<sup>۶۱</sup>

گروه «رابطه متوسط»، به‌طور بالقوه همه اطلاعات مربوط به زندگی شخص موضوع داده (گذشته یا حال) را در برمی‌گیرد، ولی چنین اطلاعاتی به‌وسیله شخص موضوع داده به‌طور مستقل فراهم نمی‌شود. این گروه، گسترده‌ترین دسته داده‌ها و همین‌طور مسأله-سازترین گروه‌هاست که شامل پروفایل توصیفی<sup>۶۲</sup> (به استثنای داده‌های قابل پیش‌بینی)<sup>۶۳</sup>، به خصوص تمام داده‌های نمایه‌سازی<sup>۶۴</sup> می‌شود که «در حال حاضر» «صحیح»، یا در حد خطای جزئی بسیار محتمل هستند. در این موارد، «رابطه» میان داده‌ها و اشخاص موضوع داده به اندازه داده‌هایی که به‌طور مستقیم ایجاد و تولید می‌شود، قوی نیست اما کماکان به دو علت رابطه‌ای مرتبط و وابسته تلقی می‌شود؛ نخست، از ترکیب ساده داده‌های خام ناشی می‌شود (برای مثال، محلی‌سازی جغرافیایی ترکیب‌شده با عکس‌های فراهم‌آمده به‌وسیله کاربر؛ کوکی‌ها که جستجوگر و یا تارنماهای بازدید شده و غیره را ترکیب می‌کند). دوم، چنین داده‌هایی در حال حاضر صحیح هستند (با حاشیه بسیار کمی از خطا) و جهت پیش‌بینی برای آینده به‌کار نمی‌روند.<sup>۶۵</sup>

این داده‌ها «حقایق» را نشان می‌دهند، حتی حقایق ذاتی یا روانشناختی. چنین اطلاعاتی، هویت شخصی کاربر را نمایان می‌سازد و پردازش آن مخل حق تعیین سرنوشت اطلاعاتی است. بنابراین این داده‌ها به‌طور پیش‌فرض متعلق به «شخص موضوع داده» هستند.<sup>۶۶</sup>

اثر فکری کسب‌وکارها یا فعالیت کنترلگر در مورد چنین داده‌هایی زمانی به چشم می‌آید که کسب‌وکار یا کنترلگر از ترکیبات پیچیده داده‌های خام با بررسی‌های دقیق علمی، جامعه‌شناختی و روانشناختی، برای ایجاد یا خلق داده‌های جدید استفاده کند. این داده‌های جدید ایجاد شده به‌وسیله کنترلگر در حال حاضر «واقعی»<sup>۶۷</sup> نیستند، اما این امکان را فراهم می‌آورند که کنترلگر، رفتار، حوادث یا خطرات آینده را پیش‌بینی کند. به این ترتیب، این داده‌ها می‌توانند به مبنای مدل‌های کسب‌وکاری شخصی‌سازی‌شده تبدیل شوند. این داده‌ها می‌توانند «اسرار تجاری»- در مفهوم کاملاً سنتی آن- را تشکیل دهند. با این حال، زمانی که ترکیبات ساده داده‌های خام برای درک موقعیت‌ها، شرایط مالی یا ترجیحات واقعی به‌کار می‌رود، می‌توان آن را «واقعی» به‌شمار آورد، بنابراین، این اطلاعات نیز متعلق به شخص موضوع داده است. دوگانگی علمی میان «داده‌کاوی توصیفی»<sup>۶۸</sup> و «داده‌کاوی قابل پیش‌بینی»<sup>۶۹</sup> به خوبی تفاوت میان این دو گروه را مشخص می‌کند. در واقع، داده‌کاوی یا استخراج داده، متداول‌ترین عملیات پردازش داده در اقتصاد داده‌محور و مبتنی بر هوش مصنوعی است و می‌تواند هم برای تعیین داده‌های شخصی مربوط به زمان حال و هم برای پیش‌بینی داده‌های آینده مربوط به کاربران مورد استفاده قرار گیرد.<sup>۷۰</sup>

61 Hofheinz, Paul, Osimo, David, "Making Europe a Data Economy: A New Framework for Free Movement of Data in the Digital Age", Lisbon Council Policy Brief, Vol. 11, No. 1, (2017) 16-17.

62 Descriptive Profiling

63 Predictive Data

64 Profiling Data

65 Malgieri, Gianclaudio, *Op. cit.*, p. 7.

66 Purtova, Nadezhda, *Op. cit.*

67 Real

68 Descriptive Data Mining

69 Predictive Data Mining

70 Malgieri, Gianclaudio, *Op. cit.*, p. 8.

این طبقه‌بندی را می‌توان هم از دستورالعمل ۱۹۹۵ و هم از مقررات عمومی حمایت از داده‌ها استنباط کرد. «یادآور ۳۹ دستورالعمل حمایت از داده»<sup>۷۱</sup> اظهار می‌دارد: «زمانی که کنترلگر، داده‌ها را به‌طور مستقیم از شخص موضوع داده جمع‌آوری نکرده باشد، شخص موضوع داده به هنگام ثبت داده و یا حداقل به هنگام افشای آن برای نخستین بار به شخص ثالث، باید از این موضوع مطلع شود». مشخص است که در مورد چنین داده‌هایی کنترل کامل وجود دارد، که در بردارنده کنترل بر استفاده شخص ثالث از داده نیز می‌شود.<sup>۷۲</sup> توصیف دیگر، از «یادآور ۴۱ دستورالعمل ۱۹۹۵»<sup>۷۳</sup> قابل استنباط است که در «یادآور ۶۳ مقررات عمومی حمایت از داده‌های شخصی»<sup>۷۴</sup> نیز مجدداً انعکاس یافته است: «حق دسترسی نباید به‌طور معکوس حق مالکیت فکری یا اسرار تجاری را تحت تأثیر قرار دهد». نتیجه این که، برخی اطلاعات (به‌غیر از داده‌هایی که به‌طور مستقیم توسط شخص موضوع داده فراهم شده) باید همواره به هنگام اعمال حق دسترسی افشاء شود.

در مورد رابطه متوسط میان داده و شخص موضوع داده، نمی‌توان منکر حق دسترسی شد؛ چراکه هیچ تلاش فکری ارزشمندی از سوی کسب‌وکار یا کنترلگر برای جمع‌آوری این داده‌ها وجود ندارد. بنابراین، افشای چنین داده‌هایی به شخص موضوع داده، تأثیر منفی یا معکوس برای کنترلگر به همراه ندارد. علاوه بر این، «حق فراموش شدن» مندرج در ماده ۱۷ نه تنها در مواردی که شخص موضوع داده به‌طور مستقیم داده‌ها را فراهم آورده، بلکه برای هر داده شخصی مرتبط با او، زمانی که از رضایت خود انصراف داده، به پردازش داده‌ها اعتراض کرده و یا پردازش در تطابق با مقررات نبوده، قابل اجراء است. البته در این موارد معمولاً حداقل تلاشی از سوی کنترلگر برای کسب این داده‌ها وجود دارد. این تلاش فکری اندک کنترلگر - به‌ویژه در داده‌های روانشناختی و رفتاری - بسیار پیچیده‌تر از زمانی است که شخص موضوع داده به‌طور مستقیم داده‌ها را فراهم می‌کند یا ارائه می‌دهد. در نتیجه، حقوق مالکانه شخص موضوع داده کامل نیست اما تا حد متوسطی وجود دارد. در واقع، شخص موضوع داده نمی‌تواند در چنین داده‌هایی حق قابلیت انتقال داده را اعمال نماید.<sup>۷۵</sup>

چنین داده‌هایی می‌توانند اسرار تجاری کسب‌وکار یا کنترلگر محسوب شوند، اما در این موارد منافع شخص موضوع داده باید مقدم بر منفعت تجاری کسب‌وکار باشد. به عبارت دیگر، کسب‌وکارها می‌توانند با رعایت شرایط، از این داده‌ها تحت عنوان سر تجاری حفاظت کنند، اما نمی‌توانند چنین حقی را علیه حقوق مالکانه شخص موضوع داده که اولی است، اعمال نمایند. مشخص است که افشای چنین داده‌هایی برای شخص موضوع داده ممکن است سبب تضعیف حمایت سر تجاری شود.

### ۳-۲-۳- نبود مالک در موارد ارتباط «ضعیف» شخص با داده‌های شخصی

آخرین گروه «طبقه‌بندی ارتباطی» داده‌های شخصی مربوط به آن دسته از اطلاعات شخصی است که تنها به‌طور غیرمستقیم از واقعیت حقیقی<sup>۷۶</sup> ناشی می‌شوند، به عبارت دیگر، داده‌های پیش‌بینی شده «تولید شده» به‌واسطه اثر فکری کسب‌وکار یا کنترلگر. مثال این مورد در «یادآور ۷۵ مقررات حمایت از داده‌های شخصی»<sup>۷۷</sup> بیان شده است: «پیش‌بینی جنبه‌های مربوط به انجام کار، موقعیت اقتصادی، بهداشت، ترجیحات شخصی یا علایق، قابلیت اعتماد یا رفتار، مکان یا حرکات».

<sup>71</sup> (Recital 39 Directive 1995)

<sup>72</sup> Purtova, Nadezhda. *Op. cit.*, p. 105.

<sup>73</sup> (Recital 41 Directive 1995)

<sup>74</sup> (Recital 63 GDPR)

<sup>75</sup> Malgieri, Gianclaudio, (2016a), *Op. cit.*, pp. 8-9.

<sup>76</sup> Actual Reality

<sup>77</sup> (Recital 75 GDPR)

تمام فعالیت‌های نمایه‌سازی یا پروفایلینگ در این گروه «رابطه ضعیف» قرار نمی‌گیرند. تنها زمانی که «تولید فکری»<sup>۷۸</sup> کنترلگر با استفاده از مطالعات علمی، جامعه‌شناختی و روانشناختی در جمع‌پیچیده داده‌های خام جمع‌آوری شده به روش‌های مختلف، ایجاد شده باشد، می‌توان حقی برای شخص موضوع داده در نظر گرفت. داده‌های جدید ایجاد شده توسط کنترلگر در حال حاضر واقعی نیستند، اما پیش‌بینی رفتارها، اتفاقات یا خطرات آتی را در برمی‌گیرند. توسعه چنین داده‌هایی تنها توسعه اطلاعات نیست، بلکه توسعه «دانش»<sup>۷۹</sup> است؛ چراکه می‌تواند به عنوان مبنای مدل کسب‌وکار شخصی‌سازی شده در نظر گرفته شود. برای مثال، زمانی که شرکت‌های بیمه امید به زندگی مشتریان یا شرایط بالقوه سلامت آن‌ها را برای ۲۰ سال آینده محاسبه می‌کنند؛ زمانی که بانک‌ها اعتبار شخصی یک نفر را پیش‌بینی می‌کنند؛ زمانی که شرکت‌های فروش اجناس پیش‌بینی می‌کنند که کاربر احتمالاً توانایی خرید کالای جدید را دارد. این داده‌ها را نمی‌توان به عنوان «صحیح» یا «اشتباه» تعریف کرد؛ چراکه ذاتاً نامعلوم و «غیرقطعی» هستند و اثبات تحقق آن ممکن نیست، برای مثال، نمی‌توان پیش‌بینی کرد که آیا فرد در طی سی سال از دنیا می‌رود، دچار حمله قلبی می‌شود، جرمی مرتکب می‌شود، پرداخت وام را کامل می‌کند و غیره.

از آنجاکه این داده‌ها «جدید» هستند؛ زیرا به واسطه اثر فکری کسب‌وکار یا کنترلگر ایجاد شده‌اند و به صورت غیر مستقیم با «واقعیت» روزانه شخص موضوع داده ارتباط دارند، نمی‌توانند در زمره حقوق مالکانه کاربر قرار گیرند. در عوض، این داده‌ها اسرار تجاری کنترلگر محسوب می‌شوند.<sup>۸۰</sup>

#### ۴- مالک داده در حقوق ایران

در نظام حقوقی ایران، تاکنون مقرره‌ای جامع و الزام‌آور که به‌طور مستقیم و نظام‌مند به حقوق داده و مالکیت داده‌ها بپردازد، تصویب نشده است. با این حال، برخی قوانین و اسناد قابل بررسی‌اند که ظرفیت تحلیل وضعیت مالک داده را فراهم می‌کنند، از جمله این اسناد می‌توان به «قانون تجارت الکترونیکی» و اسناد اخیر تنظیم‌گری حوزه داده و فضای مجازی اشاره کرد.

در این راستا، «پیش‌نویس طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی» در سال ۱۳۹۹ توسط کمیسیون فرهنگی مجلس ارائه شد، اما به تصویب نهایی نرسید و در مراحل کارشناسی باقی ماند. همچنین، «طرح نظام تنظیم مقررات خدمات فضای مجازی» (معروف به طرح صیانت) در سال ۱۴۰۰ با هدف ایجاد نهاد تنظیم‌گر واحد و گسترش چارچوب مقرراتی فضای مجازی ارائه شد، اما فرایند تصویب آن متوقف گردید. به موازات این اسناد، «پیش‌نویس لایحه حمایت از داده و حریم خصوصی در فضای مجازی» و «طرح حمایت و حفاظت از داده و اطلاعات شخصی» (که با الهام از مقررات عمومی حمایت از داده در اتحادیه اروپا تدوین شده‌اند) منتشر شد که هنوز در مسیر تصویب رسمی قرار نگرفته‌اند. سرانجام، «قانون مدیریت داده‌ها و اطلاعات ملی» در سال ۱۴۰۱ به تصویب مجلس رسید، اما این قانون نیز به‌طور مستقیم مالکیت داده‌ها را تعریف نکرده و بیشتر به مدیریت داده‌ها و چارچوب‌های نظارتی پرداخته است.

<sup>78</sup> Intellectual Output

<sup>79</sup> Knowledge

<sup>80</sup> Malgieri, Gianclaudio, *Op. cit.*, p. 11.

## ۴-۱- مالک داده از منظر قوانین مرتبط

### ۴-۱-۱- قانون مدیریت داده‌ها و اطلاعات ملی

بر اساس مفاد این قانون، مالکیت خصوصی بر داده‌ها به رسمیت شناخته نشده است و دولت اختیار حاکمیتی بر «داده‌ها و اطلاعات ملی» دارد. در چارچوب مقاله حاضر، چنین رویکردی در عمل مالکیت را از حوزه خصوصی خارج کرده و به سطحی می‌برد که هیچ یک از ذی‌نفعان خصوصی، حتی شخص موضوع داده، مالک شناخته نمی‌شوند؛ بنابراین، این وضعیت خارج از سه سطح ارتباط قوی، متوسط یا ضعیف قرار می‌گیرد و صرفاً مدل مالکیت حاکمیتی را بازتاب می‌دهد. تحلیل حقوقی این امر را می‌توان در چند محور اصلی تبیین نمود:

نخست، مطابق بند «ت» ماده ۱، «داده‌ها و اطلاعات ملی» نه تنها شامل داده‌های تولیدشده توسط دستگاه‌ها و نهادهای مشمول، بلکه دربرگیرنده هر نوع داده و اطلاعاتی است که به موجب قوانین و مقررات در اختیار این دستگاه‌ها قرار می‌گیرد. این تعریف موسع، قلمرو داده‌های ملی را به گونه‌ای ترسیم می‌کند که بخش قابل توجهی از داده‌های موجود، از جمله داده‌های حاصل از فعالیت بخش خصوصی یا حتی اشخاص حقیقی می‌تواند در شمول آن قرار گیرد.

دوم، بر اساس ماده ۴، داده‌ها و اطلاعات ملی «در اختیار دولت جمهوری اسلامی ایران» قرار دارند. این گزاره، که فاقد هرگونه تصریح به حقوق اشخاص بر داده‌هاست، بیانگر پذیرش یک مدل مالکیت و کنترل حاکمیتی است که در آن دولت به‌عنوان متولی و ذی‌حق اصلی نسبت به داده‌های ملی شناخته می‌شود. در این ساختار، داده‌ها نه به‌عنوان «مال» یا «دارایی» خصوصی، بلکه به‌مثابه «سرمایه ملی» و ابزار حکمرانی تعریف می‌شوند؛ چنان‌که ماده ۲، هدف نظام داده کشور را «افزایش قدرت حکمرانی» اعلام کرده است.

سوم، هرچند در مواد ۴ و ۶ به «محرمانگی اطلاعات اشخاص» و «صیانت از داده‌های شخصی» اشاره شده است، این ملاحظات جنبه حمایتی و حفاظتی دارند و متضمن هیچ حق مالکانه یا حق تصرف اقتصادی برای اشخاص حقیقی نیستند. به عبارت دیگر، حمایت پیش‌بینی شده در قانون، از سنخ حقوق شخصیتی و حریم خصوصی است و نه حق مالکیت بر داده.

چهارم، تمامی تصمیمات راهبردی و اجرایی مرتبط با تولید، نگهداری، پردازش، یکپارچه‌سازی، تبادل و تعیین سطح دسترسی به داده‌ها و اطلاعات ملی، ذیل نهادهای حاکمیتی از جمله «شورای عالی فضای مجازی» و «کارگروه تعامل‌پذیری دولت الکترونیکی» سامان می‌یابد (مواد ۲ و ۳). این تمرکز تصمیم‌گیری در سطوح عالی حاکمیت، به همراه الزامات اجرایی مقرر در مواد ۵ و ۸، عملاً امکان اعمال هرگونه اختیار مستقل توسط اشخاص غیردولتی را در بهره‌برداری از داده‌های ملی محدود می‌سازد.

پنجم، الزامی بودن مجوزهای دولت برای تبادل داده‌ها و اطلاعات بین دستگاه‌های اجرایی و کسب‌وکارها (ماده ۷) و نیز پیش‌بینی ضمانت‌اجراه‌های کیفری برای متخلفان (ماده ۹)، نشان‌دهنده رویکرد سخت‌گیرانه قانون نسبت به کنترل جریان داده‌ها در کشور است.

در نهایت، این قانون را می‌توان نمونه‌ای از مدل حکمرانی داده<sup>۸۱</sup> دانست که در آن دولت به‌عنوان صاحب اختیار اصلی، سیاست‌گذار و ناظر بر چرخه حیات داده‌های ملی ایفای نقش می‌کند و جایگاه اشخاص خصوصی در بهترین حالت، به‌عنوان ذی‌نفعان فرعی در حوزه حمایت از داده‌های شخصی محدود می‌شود. چنین رویکردی، هیچ بنیانی برای شناسایی یا حمایت از مالکیت اشخاص بر داده‌ها

<sup>81</sup> Data Sovereignty

در بر ندارد و در تفاوت با نظام اتحادیه اروپاست که مفهوم «داده ملی» با تعریف امنیتی وجود ندارد و داده‌های مربوط به بخش عمومی تحت چارچوب قوانین داده باز<sup>۸۲</sup> مدیریت می‌شوند، که بیشتر بر شفافیت، دسترسی عمومی و قابلیت استفاده مجدد از داده‌ها تأکید دارد. به این ترتیب، حاکمیت داده در اروپا مبتنی بر توازن میان دسترسی آزاد به داده‌های بخش عمومی و حمایت قانونی از داده‌های شخصی است، بدون تخصیص مالکیت صریح «داده ملی» به دولت.

#### ۴-۱-۲- قانون تجارت الکترونیکی

ماده ۵۸ این قانون، پردازش داده شخصی بدون رضایت فرد را ممنوع کرده است، که نشانه‌ای از ارتباط قوی میان داده و شخص موضوع داده است و حکایت از وجود حق کنترل و تصمیم‌گیری اولیه فرد بر داده‌های خود دارد. اگرچه هدف اصلی قانون، حمایت از حریم خصوصی است و لزوماً مالکیت کامل را به فرد اعطاء نمی‌کند، اما می‌توان از منظر حقوق داده، شخص موضوع داده را به‌عنوان مالک داده در نظر گرفت.

مطابق ماده ۵۹، پردازش داده‌ها با رضایت فرد و رعایت شرایط مشخص (اهداف مشخص، صحیح و به‌روز بودن، امکان دسترسی، اصلاح یا حذف داده‌های نادرست) مجاز است. درواقع، این ماده با پیش‌بینی امکان اصلاح یا حذف داده‌ها، در کنار حق کنترل برای پردازش، حالتی نزدیک به ارتباط متوسط ایجاد می‌کند که در آن کنترلگر و شخص موضوع داده هر دو در بهره‌برداری نقش دارند و به نوعی مالکیت مشترک میان فرد و کنترلگر داده ایجاد شده است. حق حذف داده در هر زمان، که ماده ۵۹ پیش‌بینی کرده، نشان‌دهنده کنترل قابل توجه شخص موضوع داده است، اما از آنجا که کنترل کامل در دست فرد نیست، این وضعیت در چارچوب پیشنهادی مقاله حاضر در دسته ارتباط متوسط قرار می‌گیرد.

#### ۴-۲- مالک داده از منظر اسناد تنظیم‌گر حوزه داده

##### ۴-۲-۱- طرح نظام تنظیم مقررات خدمات فضای مجازی

این طرح از دو جهت قابل بررسی است: از یکسو، مالکیت داده به‌طور مستقیم تعریف نشده، اما از دل تعاریف و ساختار تنظیم‌گری فضای مجازی برداشت می‌شود که مالکیت داده تابع حاکمیت ملی است و داده‌ها به‌عنوان بخشی از خدمات فضای مجازی، تحت نظارت و تنظیم‌گری نهادهای حاکمیتی مانند شورای عالی فضای مجازی و کمیسیون عالی قرار دارند. این نهادها وظیفه تعریف و تصویب ضوابط حکمرانی داده‌ها، به‌ویژه داده‌های حساس و حیاتی کاربران ایرانی را بر عهده دارند و کنترل، مجوزدهی و حمایت از داده‌ها را در راستای منافع ملی و امنیت فضای مجازی دنبال می‌کنند. بنابراین، مالکیت داده در این چارچوب نه صرفاً به‌عنوان حقوق فردی یا خصوصی، بلکه به عنوان موضوعی ترکیبی از حقوق مالکانه، حاکمیتی و تنظیم‌گری دیده می‌شود که با هدف تأمین امنیت، حریم خصوصی و حمایت از اقتصاد دیجیتال کشور ساماندهی می‌گردد.

از سوی دیگر، در بند «ج» ماده ۱۵ همین قانون با تصریح بر «عدم حذف حساب کاربران و محتوای مجاز مگر به درخواست مالک آنها»، به‌طور ضمنی شخص صاحب حساب کاربری یا تولیدکننده محتوا به‌عنوان مالک داده شناسایی شده است. این رویکرد، مفروض می‌گیرد که شخص موضوع داده از حق مالکیت کامل نسبت به داده‌های خود برخوردار است. چنین تلقی‌ای از مالکیت، دامنه اختیار شخص موضوع داده را به سطح تصمیم‌گیری مطلق درباره داده گسترش می‌دهد و در مدل مقاله حاضر، این حالت به‌عنوان ارتباط قوی طبقه‌بندی می‌شود؛ امری که می‌تواند پیامدهای مهمی در نحوه اعمال حقوق مالکانه در محیط دیجیتال داشته باشد.

<sup>82</sup> Open Data

#### ۴-۲-۲- پیش نویس طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی

تبصره (۲) ماده ۲۵ این پیش نویس با تصریح بر این که «خدمات پایه کاربردی، مالک داده‌های کاربران ایرانی نیستند»، مالکیت داده را از ارائه‌دهندگان خدمات سلب می‌کند، اما در عین حال، مالکیت را به‌طور صریح به کاربر نیز منتسب نمی‌سازد.

بررسی تبصره (۲) ماده ۲۵ پیش‌نویس طرح حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی و بند «ج» ماده ۱۵ طرح نظام تنظیم مقررات خدمات فضای مجازی - که نسخه متأخر و اصلاحی آن محسوب می‌شود - حاکی از تغییر معنادار رویکرد قانون‌گذار در خصوص مالکیت داده است. در متن نخست، صرفاً مالکیت داده‌های کاربران از خدمات پایه کاربردی سلب شده بود، بدون تصریح بر مالکیت کاربر - که حالت ارتباط متوسط را تداعی می‌کند؛ اما در متن دوم، قانون‌گذار صریحاً کاربر را مالک داده معرفی کرده و آن را به سطح ارتباط قوی ارتقاء داده است. این تحول را می‌توان هم نشانه‌ای از تلاش برای شفاف‌سازی جایگاه حقوقی شخص موضوع داده و تقویت اختیارات وی دانست، و هم بازتابی از نبود انسجام نظری و تغییرات ناگهانی در سیاست‌گذاری، که نشان می‌دهد قانون‌گذار هنوز به نگرش پایدار و سنجیده‌ای در حوزه حقوق داده نرسیده است.

#### ۴-۲-۳- طرح حمایت و حفاظت از داده و اطلاعات شخصی

ماده ۱۱ طرح حمایت و حفاظت از داده و اطلاعات شخصی با مشروط کردن بهره‌برداری مالکانه از داده‌های شخصی به رضایت «شخص موضوع داده»، عملاً وی را در جایگاه مالک داده مفروض می‌گیرد و به سمت ارتباط قوی گرایش دارد. البته، چون اصطلاح «مالک» به‌طور صریح به کار نرفته است، می‌توان بحث کرد که قانون‌گذار صرفاً «حق کنترل» برای فرد قائل شده و نه مالکیت. با این حال، قرینه لفظی «بهره‌برداری مالکانه» و وابستگی آن به رضایت فرد، به شدت به سمت مالکیت گرایش دارد و در کنار اسنادی مانند طرح نظام تنظیم مقررات خدمات فضای مجازی که مالکیت کاربر را صراحتاً تأیید می‌کند، نشان می‌دهد قانون‌گذار در مسیر قانون‌گذاری به سمت پذیرش شخص موضوع داده به عنوان مالک داده حرکت کرده است.

#### ۴-۲-۴- پیش‌نویس لایحه حمایت از داده و حریم خصوصی در فضای مجازی

تحلیل پیش‌نویس لایحه حمایت از داده و حریم خصوصی در فضای مجازی نشان می‌دهد که قانون‌گذار به‌طور ضمنی، شخص موضوع داده را به‌عنوان مالک داده‌های شخصی خود در نظر گرفته است. ماده ۲ با قائل شدن حق دسترسی و نظارت برای فرد، امکان کنترل و پیگیری نحوه پردازش داده‌ها را فراهم می‌آورد و ماده ۳ با الزام به رضایت صریح یا ضمنی پیش از هرگونه پردازش، عملاً بهره‌برداری بدون اجازه شخص موضوع داده را محدود می‌سازد. علاوه بر این، ماده ۶ با تصریح به اینکه حق مالکیت فکری بر داده‌ها نافی حقوق افراد نیست و در صورت تزامم، حق شخص موضوع داده اولویت دارد، نگاه قانون‌گذار را به سمت تأیید مالکیت یا حق تصرف فرد بر داده‌های خود تقویت می‌کند. بدین ترتیب، اگرچه اصطلاح «مالک» به‌صورت صریح در متن لایحه به کار نرفته، مجموعه حقوق دسترسی، کنترل، رضایت برای پردازش و اولویت حقوق افراد، چارچوبی نزدیک به ارتباط قوی ترسیم می‌کند که نگرش قانون‌گذار را نزدیک به تلقی مالکانه نسبت به داده‌های شخصی فرد نشان می‌دهد.

#### نتیجه

در شرایطی که نظم حقوقی کلاسیک، توانایی برخورد مؤثر با چالش‌های حقوقی ناشی از مالکیت داده را ندارد، ارائه رویکردهای تحلیلی نوین برای تبیین روابط حقوقی مرتبط با داده ضرورت می‌یابد. چارچوب پیشنهادی مقاله حاضر، با طبقه‌بندی داده‌ها بر مبنای شدت ارتباط آن‌ها با شخص موضوع داده در سه سطح «ارتباط قوی»، «ارتباط متوسط» و «ارتباط ضعیف»، تلاش کرده است مدلی برای

ادعاهای مالکیت بر داده ارائه دهد. مطابق این مدل، در داده‌های دارای ارتباط قوی، شخص موضوع داده به‌عنوان مالک اصلی شناخته شده و از حقوق کامل مالکانه از جمله حق کنترل، انتقال و حذف داده برخوردار است؛ در داده‌های با ارتباط متوسط، رابطه‌ای مشترک میان شخص موضوع داده و کنترلگر داده مفروض است که حقوق نظارتی فرد را در حدی متعادل تضمین می‌کند؛ در داده‌های با ارتباط ضعیف، ادعای مالکیت فردی موجه نیست، اما حقوقی چون اطلاع‌رسانی و تضمین امنیت پردازش به‌عنوان ابزارهای جبرانی پیش‌بینی می‌گردد.

تحولات نوظهور در حوزه هوش مصنوعی، حتی در قوانین و مقررات متمرکز اتحادیه اروپا، از مقررات عمومی حمایت از داده‌های شخصی گرفته تا قانون هوش مصنوعی، حوزه مالکیت داده را با چالش‌های جدیدی مواجه می‌سازد. پرسش‌هایی پیرامون مالکیت داده‌های آموزشی، حقوق کاربران نسبت به داده‌های تولیدشده توسط مدل‌ها، و مسئولیت ناشی از محتوای ماشینی، ضرورت بازنگری در مفاهیم سنتی مالکیت را تشدید می‌کند. در این زمینه، تمرکز از تملک صرف داده‌ها به‌سوی مفاهیمی نظیر «حق کنترل» و «حکمرانی داده» سوق پیدا کرده است؛ مفاهیمی که در آن‌ها، شفافیت، پاسخ‌گویی و قابلیت نظارت بر استفاده از داده‌ها، بیش از تصاحب حقوقی مطلق، اهمیت می‌یابد؛ برخلاف اسناد اخیر منتشرشده در ایران که تمایل به شناسایی صریح یا ضمنی مالکیت فرد بر داده‌های شخصی در آن مشاهده می‌شود. هرچند این رویکرد هنوز تثبیت نشده و گاه با مدل مالکیت حاکمیتی تداخل پیدا می‌کند. درحالی‌که در حقوق ایران تاکنون قانون جامع و مشخصی در زمینه حقوق داده‌ها به تصویب نرسیده است و نظم حقوقی همچنان با خلأ تقنینی و پراکندگی مقررات در این حوزه روبروست.

مطالعه تجربه اتحادیه اروپا نشان می‌دهد که به‌جای اتکا بر مفهوم سنتی مالکیت، می‌توان با تعریف مجموعه‌ای از حقوق کنترلی، ساختاری منظم برای تنظیم‌گری داده‌ها طراحی کرد. این رویکرد می‌تواند الگویی راهگشا برای ایران باشد و ضمن سازگاری با مفاهیم فقهی و اصول حقوق مدنی، امکان شناسایی حقوق اشخاص ذی‌نفع در چرخه حیات داده را بدون ورود به تعارض‌های مفهومی مالکیت فراهم سازد.

سخن آخر آن‌که، با توجه به جایگاه داده به‌عنوان منبع قدرت، نوآوری و تصمیم‌سازی در عصر دیجیتال، بازاندیشی در ساختارهای مالکیت داده ضرورتی انکارناپذیر است. به‌ویژه در عصری که فناوری‌هایی نظیر هوش مصنوعی به‌شدت متکی بر داده‌های کلان و متنوع‌اند، نیاز به بازنگری در مفاهیم سنتی بیش از پیش احساس می‌شود. چراکه سازوکارهای حقوقی حاضر پاسخ‌گوی پیچیدگی‌های موجود نیستند و لازم است با تکیه بر مفاهیم جدید، بستری برای تنظیم‌گری مؤثر و عادلانه فراهم گردد. این مقاله در پی ارائه پاسخ نهایی نبوده، بلکه کوشیده است گامی نظری برای روشن‌سازی ابعاد مسأله و تحقیقات آتی به‌ویژه در حقوق ایران فراهم آورد. شایسته است که پیوند این چارچوب با موضوعاتی نظیر حریم خصوصی و حکمرانی داده مورد توجه جدی قرار گیرد؛ تا بتوان نظام حقوقی را برای مواجهه با واقعیت‌های پیچیده اقتصاد داده و فناوری‌های نوین آماده ساخت.

## منابع

## فارسی

## کتاب

انصاری، باقر، شیما عطار، حقوق کاربران فضای مجازی، تهران: شرکت سهامی انتشار، ۱۴۰۲.

## مقاله

عطار، شیما، «بالاتکلیفی در مفهوم مالکیت داده»، مجله پژوهش‌های حقوقی، انتشار آنلاین از تاریخ ۱۳ بهمن ۱۴۰۳. قابل انتشار در دوره ۲۵، شماره ۶۷، (پاییز ۱۴۰۵)

## اسناد قانونی

- پیش‌نویس طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی، ۱۴۰۰
- <https://shenasname.ir/laws/8780-%D8%B7%D8%B1%D8%AD-%D8%AD%D9%85%D8%A7%DB%8C%D8%AA-%D8%A7%D8%B2-%D8%AD%D9%82%D9%88%D9%82-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86>
- طرح حمایت و حفاظت از داده و اطلاعات شخصی، ۱۳۹۹
- [https://rc.majlis.ir/fa/legal\\_draft/show/1675111](https://rc.majlis.ir/fa/legal_draft/show/1675111)
- طرح نظام تنظیم مقررات خدمات فضای مجازی، ۱۴۰۰
- <https://www.ekhtebare.ir/%D9%85%D8%AA%D9%86-%DA%A9%D8%A7%D9%85%D9%84-%D8%A2%D8%AE%D8%B1%DB%8C%D9%86-%D9%86%D8%B3%D8%AE%D9%87-%D8%B7%D8%B1%D8%AD-%D8%B5%DB%8C%D8%A7%D9%86%D8%AA-%D9%88%DB%8C%D8%B1%D8%A7%DB%8C%D8%B4-%D8%A8%D9%87/>
- قانون تجارت الکترونیکی مصوب ۱۳۸۲
- قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱
- پیش‌نویس لایحه حمایت از داده و حریم خصوصی در فضای مجازی
- <https://discuss.tp4.ir/uploads/default/original/1X/15e1b1943b9ad74cd414c2ac3266f24ecb8f1a6e.pdf>

## لاتین

### Books

- Bergel, Jean-Louis ; Cimamonti, Sylvie ; Roux, Jean-Marc ; Tranchant, Laetitia, *Traité de droit civil, Les biens*, LGDJ, 2ème édition, 2010
- Kuner, Christopher; Bygrave, Lee A.; Docksey, Christopher., *The Eu General Data Protection Regulation (GDPR)- A Commentary*, Oxford University Press. United Kingdom, 2020

### Articles

- Claudio Novelli, Federico Casolari, Philipp Hacker, Giorgio Spedicato, Luciano Floridi, “Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity”, *Computer Law & Security Review*, Volume 55, (2024)
- Demsetz, Harold, “Towards a Theory of Property Rights”, *The American Economic Review*, 57 (2), (1967)
- Drexel, Josef, “Designing Competitive Markets for Industrial Data – Between Propertisation and Access”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8, (2017)
- Hess, charlotte, Ostrom, Elinor (eds.) “Understanding Knowledge as A Commons: From Theory to Practice”, *MIT press*, Cambridge, Massachusetts London, England. (2007)
- Hoeren, Thomas., “Big Data and the Ownership in Data: Recent Developments in Europe”, *European Intellectual Property Review*, Issue 12, (2014)
- Hofheinz, Paul, Osimo, David, “Making Europe a Data Economy: A New Framework for Free Movement of Data in the Digital Age”, *Lisbon Council Policy Brief*, Vol. 11, No. 1, (2017)

- Malgieri, Gianclaudio, “Ownership of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution”, *Journal of Internet Law*, Vol. 20, n.5. (2016)
- Malgieri, Gianclaudio, “Property and (Intellectual) Ownership of Consumers’ Information: A New Taxonomy for Personal Data”, *Privacy in Germany - PinG*, n. 4. (2016)
- Mindy Nuñez Duffourc, Sara Gerke & Konrad Kollnig “Privacy of Personal Data in the Generative AI Data Lifecycle”, *NYU Journal of Intellectual Property & Entertainment Law*, Vol. 13:2, (2024)
- Purtova, Nadezhda, “Do Property Rights in Personal Data Make Sense after the Big Data Turn? Individual Control and Transparency”, *Journal of Law and Economic Regulation, Tilburg Law School Legal Studies Research Paper Series*. (2017)
- Purtova, Nadezhda, “The Illusion of Personal Data as No One’s Property, Law, Innovation, and Technology”, Volume 7, Issue 1, *Tilburg University - Tilburg Institute for Law, Technology, and Society (TILT)* (2013)
- Renana Peres, David A. Schweidel, “Putting Consumers in Control of Their Data: Revisiting Data Ownership”, *Emory University’s Goizueta Business School*, (2024)
- Stephen T. Black, “who owns your data?”, *Indiana Law Review*, Volume 54, Number 2, (2021)

### Legal documents

- 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, OJ L 281, 23.11.1995
- Recital 38 Directive 1995
- Recital 39 Directive 1995
- Recital 41 Directive 1995
- Recital 63 GDPR
- Recital 68 GDPR
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union
- regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act)
- regulation (EU) 2024/1684 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828

### Reports and Studies

- Drexl, Josef, “Data Access and Control in the Era of Connected Devices, Study on Behalf of the European Consumer Organisation”, *BEUC*, Brussels, (2018)
- Duch-Brown, Nestor, Martens, & Mueller-Langer, Frank. “The Economics of Ownership, Access and Trade in Digital Data”, *JRC Digital Economy Working Paper*, (2017),
- European Commission, “Communication: Building a European Data Economy”, COM (2017)
- OECD, “Digital Economy Outlook 2020”, OECD Publishing, Paris. (2020)
- OECD, “Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use”, Summary of The Discussions, 15-16 May 2018, Directorate for Science, Technology and Innovation Committee on Digital Economy Policy, Working Party on Security and Privacy in The Digital Economy, (2018)
- OECD, “Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use”, *Summary of The Discussions*, (2018)

### Websites

- European commission, "What is personal data?", accessed March 2023, [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en).
- European Commission, “Commission guidance on free flow of non-personal data – Questions and Answers”, accessed July 2022, [https://ec.europa.eu/commission/presscorner/detail/en/MEMO\\_19\\_2750](https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_2750)

### Judgment

- C-582/14, “Patrick Breyer v Bundesrepublik Deutschland.” (2016), 779, paragraph 49.

