



Legal Basis of Personal Data Exchange

(Comparative Study of EU General Data Protection Regulations and Iranian Law)

Mohsen Esmaeili

Associate Professor, Faculty of Law and Political Science, University of Tehran, Tehran, Iran.

esmaeili1344@ut.ac.ir

mahdi narimanpour (Corresponding Author)

Student of Shahid Motahari University

Ph.D. Student in Jurisprudence and Private Law, Shahid Motahari University, Tehran, Iran.

narimanpourm99@gmail.com

Use your device to scan
and read the article online



Citation Mohsen Esmaeili, mahdi narimanpour. [Legal Basis of Personal Data Exchange (Comparative Study of EU General Data Protection Regulations and Iranian Law) (Persian)]. *Islamic Law (A Quarterly Journal of Law)*. 2024; 21 (82): 131-176

doi [10.22034/ilaw.2023.708599](https://doi.org/10.22034/ilaw.2023.708599)

Received: 26 April 2023 , Accepted: 26 August 2023

Abstract

Today, on the one hand, personal data is considered wealth in the world of digital economy, and on the other hand, there are serious concerns about violating the privacy of real persons. This duality in the way of using personal data has led to the emergence of many legal issues; Legitimacy or illegitimacy of personal data exchange is one of these legal issues. In this research, we aim to examine and investigate the legal possibility of exchanging and trading personal data with a comparative study between European and Iranian laws and citing library sources. This research shows that the existence of market-based approaches, including the property-based approach, facilitates the possibility of legal exchange and, consequently, the possibility of concluding a contract around personal data, on the other hand, human rights approaches limit the possibility of such exchange. In the General Data Protection Regulations of the European Union, there are many strictures regarding the legal possibility of exchange; Nevertheless, the commentators of these regulations have introduced consent as one of the legal bases of data exchange; On the other hand, these strictures are not observed in Iranian law.

Keywords

personal data, exchange, privacy-oriented characteristics, human rights, consent



Copyright © 2024 The Author(s);

This is an open access article distributed under the terms of the Creative Commons Attribution License (CC-BY-NC: <https://creativecommons.org/licenses/by-nc/4.0/legalcode.en>),

which permits use, distribution, and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

Extended Abstract

1. Introduction

Personal data in the digital economy presents a fundamental duality: it is recognized as a valuable economic asset yet simultaneously raises significant concerns about privacy infringement. This inherent tension fuels extensive legal debates regarding the legitimacy of personal data exchange and transactions. The indispensable role of personal data in economic stability and development is widely acknowledged. There is a growing tendency to view data, such as IP addresses, locations, and email profiles, as a form of payment for digital services, leading some to label it "the new currency". However, the collection and sale of such data also carry substantial risks, including data breaches and privacy violations. In response, many jurisdictions have enacted "personal data protection regulations," which often prioritize privacy protection over economic interests, thereby distancing data exchange from conventional contract law. This research comparatively examines the legal permissibility of personal data exchange under European Union (EU) law, specifically the General Data Protection Regulation (GDPR) of 2016, and Iranian law, addressing core questions about its alignment with human rights and general contract principles.

2. Research Methodology

This study employs a comparative legal methodology, primarily drawing upon library resources to analyze the diverse legal frameworks governing personal data exchange in the EU and Iran. The research systematically investigates various conceptual approaches to the legal status of personal data, which critically influence the scope of permissible data exchange. It then delves into the specific stance of the EU GDPR of 2016 concerning the legality of data exchange, followed by an examination of the legal possibilities for personal data exchange within the Iranian legal system. The study highlights a notable gap in Persian-language research specifically on the legitimacy of personal data exchange, although significant English-language scholarship exists, particularly in Europe and America.

3. Research Findings

The research identifies two predominant conceptual approaches to personal data:

- The Ownership-Based Approach, originating primarily in the United States, considers personal data as the property of individuals. Proponents argue it facilitates market exchange, reduces transaction costs, and encourages companies to internalize data collection costs, leading to more informed decisions. It also offers flexibility, allowing individuals to sell data based on personal privacy valuation. However, this approach faces criticism due to "privacy market failure" (binary choices for individuals), potential conflict with "Free Aliena-

bility" when data use is restricted, users' unawareness of data value, information asymmetry, and the risk of privacy becoming a luxury.

- The Human Rights Approach, prevalent in Europe, posits that personal data protection is a fundamental right. Endorsed by the EU Charter of Fundamental Rights (Art. 8) and GDPR, it emphasizes principles like individual autonomy, consent, human dignity, transparency, and non-discrimination. Critics argue that commercializing personal data threatens civil liberties and democracy. However, questions arise whether all types of personal data inherently possess fundamental right characteristics, and data protection regulations serve a dual purpose (balancing individual and controller interests), unlike the singular focus of human rights.

The study acknowledges a dual functionality of personal data: sensitive data generally aligns with the human rights approach, while less critical data (e.g., photos, social media profiles) possesses both economic and non-economic functions. Many human rights-oriented laws implicitly or explicitly allow for limited data exchange.

In the EU's GDPR, direct explicit permission for data exchange is absent; however, its legality is commonly derived from the grounds for processing, especially "consent". For consent to be valid, it must be "freely given" (Art. 4(11), 7(4)), implying genuine choice and control, without coercion or negative consequences. Article 7(4) GDPR and Recital 43 specifically address "bundling," stating that consent is not freely given if conditional on processing non-essential data for contract performance. While a unified view is lacking, the prevailing sentiment leans towards a restrictive interpretation, though not an absolute ban.

In Iran's legal system, the absence of a dedicated personal data law necessitates reliance on general contract principles. The research addresses several challenges:

- "Malit" (Economic Value): Personal data possesses economic value and satisfies needs, and some jurists argue "malit" isn't an absolute prerequisite for contract validity.

- Non-transferability: Iranian law leans towards a human rights approach, but the study argues for a dual nature where the economic value of data can be exchanged, particularly as individuals can consent to exposing their privacy.

- Conflict with Contractual Bindingness ("Luzum"): The "right to withdraw consent" (recognized in GDPR Art. 7(3), Iran's E-commerce Law Art. 59, and Draft Law Art. 8) appears to contradict binding contracts. However, the research suggests data contracts might be permissible ("ja'iz") rather than strictly binding, aligning with privacy rights and preventing misuse.

- "Gharari" (Uncertainty): The "right to be forgotten" (RtbF) (GDPR Art. 17, Iran's Draft Law Art. 9) introduces uncertainty as data can be deleted. However, the research posits that data's utility often lies in extracted insights,

which are not subject to RtbF, and uncertainty is present in other permissible contracts without invalidating them.

Ultimately, the study contends that classical contract rules are not immutable, and emerging contract types often necessitate specific regulations. Given that such contracts serve to regulate people's livelihoods and economic affairs, they should be recognized and accommodated through specialized laws. Notably, Iran's draft "Personal Data Protection Law" (Articles 13 and 26) implicitly allows for commercial exploitation of data by processors under specific conditions.

4. Conclusion

The landscape of contracts is undergoing a profound transformation driven by technological advancements, necessitating adaptation in legal frameworks. Personal data exchange uniquely intersects human rights (privacy) and contract law (exchange), prompting a search for a balanced approach. While some advocate for absolute privacy protection and others prioritize uninhibited economic use, the EU exemplifies a middle ground, adopting a human rights-centric approach while prudently allowing for restricted data exchange, acknowledging the undeniable economic imperatives of the data economy and the dual nature of certain data types.

In Iran, despite progress with the E-commerce Law and the draft "Personal Data Protection Law," the specifics of data exchange remain ambiguous. Therefore, there is a pressing need for comprehensive, specialized regulations in Iran that adopt a combined human rights and contract law approach. Such regulations should meticulously delineate the processes of contract formation, validity conditions (including the right to be forgotten and precise data scope), and various forms of data exchange. Absent such specific legislation, the research concludes that, based on the economic value of personal data and its general compatibility with overarching contract principles, personal data exchange is legitimate and lawful within the existing Iranian legal framework.

Funding

There is no funding support.

Authors' Contribution

Authors contributed equally to the conceptualization and writing of the article. All of the authors approved the content of the manuscript and agreed on all aspects of the work

Conflict of Interest

Authors declared no conflict of interest.

Acknowledgments

We are grateful to all the persons for scientific consulting in this paper.



مبانی حقوقی تبادل داده‌های شخصی

(مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)

محسن اسماعیلی

دانشیار دانشکده حقوق و علوم سیاسی دانشگاه تهران
esmaeili1344@ut.ac.ir

مهدی نریمانپور (نویسنده مسئول)

دانشجوی دکتری فقه و حقوق خصوصی دانشگاه شهید مطهری
narimanpourm99@gmail.com



Citation Mohsen Esmaeili, mahdi narimanpour. [Legal Basis of Personal Data Exchange (Comparative Study of EU General Data Protection Regulations and Iranian Law) (Persian)]. *Islamic Law (A Quarterly Journal of Law)*. 2024; 21 (82): 131-176

doi [10.22034/ilaw.2023.708599](https://doi.org/10.22034/ilaw.2023.708599)

تاریخ دریافت: ۱۴۰۲/۰۶/۰۶، تاریخ پذیرش: ۱۴۰۲/۰۶/۰۴

چکیده

امروزه داده‌های شخصی از یک طرف در اقتصاد دیجیتال، ثروت محسوب می‌شود و از طرف دیگر نگرانی‌های جدی نسبت به نقض حریم خصوصی اشخاص حقیقی وجود دارد. این دوگانگی در نحوه استفاده از داده‌های شخصی، موجب ظهور مباحث حقوقی متعددی گردیده است؛ مشروعیت یا عدم مشروعیت مبادله داده‌های شخصی یکی از این مباحث حقوقی است. در این پژوهش بر آن هستیم تا با مطالعه تطبیقی میان حقوق اروپا و ایران و با استناد به منابع کتابخانه‌ای، امکان قانونی مبادله و معامله داده‌های شخصی مورد بررسی قرار گیرد. این پژوهش نشان می‌دهد که وجود رویکردهای مبتنی بر بازار، امکان مبادله قانونی و به تبع امکان انعقاد قرارداد حول داده شخصی را تسهیل می‌بخشد، در مقابل رویکردهای حقوق بشری امکان چنین مبادله‌ای را محدود می‌کند. در مقررات عمومی حفاظت از داده اتحادیه اروپا، اتخاذ رویکرد حقوق بشری، مبادله داده‌ها را بسیار مضیق گردانده است؛ در مقابل در حقوق ایران، با توجه به نبود سازوکارهای تضییعی اتحادیه اروپا در قوانین و عدم مخالفت جدی آن با قواعد حقوقی، امکان مبادله وسیع آن وجود دارد.

واژگان کلیدی

داده شخصی، مبادله، رویکرد مالکیت محور، رویکرد حقوق بشری، رضایت



مقدمه

«داده‌های شخصی» به معنای هرگونه اطلاعات مربوط به یک شخص حقیقی شناخته شده یا قابل شناسایی («موضوع داده‌ها») است. یک شخص حقیقی قابل شناسایی شخصی است که می‌توان به‌طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به یک شناسه مانند نام، شماره شناسایی، داده‌های مکان، شناسه آنالین یا یک یا چند ویژگی خاص فیزیکی، فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی، شناسایی کرد (GDPR, Art.4).

استفاده از این داده‌ها مزایا و معایب خاص خود را دارد. از یک طرف، امروزه نقش داده‌های شخصی در تثبیت اقتصاد و توسعه آن غیرقابل انکار است؛ به طوری که در اقتصاد داده، این تمایل وجود دارد که داده‌ها به‌عنوان ابزاری برای پرداخت هزینه در تراکنش‌هایی که خدمات یا محتوای دیجیتال ارائه می‌شود، تلقی شوند و در نتیجه با این کار، مصرف‌کنندگان بهایی پرداخت نمی‌کنند، بلکه داده‌های خود را مانند آدرس‌های IP، مکان‌ها، مشخصات ایمیل، آدرس صفحات مجازی و غیره را به‌عنوان پول در اختیار تولیدکنندگان قرار می‌دهند.

این تمایل پول‌انگاری در اقتصاد دیجیتال، به قدری روبه‌فزونی است که عده‌ای

گفته‌اند: «داده‌های شخصی ارزش جدید هستند» (Gates, 2014, p.105-106)

این‌گونه تعامل با داده‌های شخصی از این ناشی می‌شود که کسب‌وکارها از این مجموعه داده‌های شخصی به روش‌های مختلف درآمدزایی می‌کنند. به‌عنوان مثال، بسیاری از این کسب‌وکارها این اطلاعات را از طریق تجزیه و تحلیل داده‌ها و به‌تبع پیش‌بینی‌های ناشی از نتایج آن، علایق و سلایق مصرف‌کننده را شناسایی می‌کنند که به‌واقع وسیله‌ای در جهت تولید درآمد است (Rose, 2021, p.521). علاوه بر این، شرکت‌های هستند که این داده‌های شخصی را جمع‌آوری می‌کنند و این داده‌ها را به

تبلیغ کنندگان و کسب و کارها می‌فروشند و تبلیغ کنندگان و کسب و کارها نیز از آن جهت که این گونه تعامل با داده‌های شخصی در مقایسه با تکنیک‌های بازاریابی ساده گذشته، کارآمدتر هستند، تمایل زیادی به خرید داده‌های شخصی پردازش شده از این گونه شرکت‌ها دارند (Bedir, 2020, p.349). از طرف دیگر، با وجود اینکه داده‌های کاربران مزایای بسیاری را برای مشاغل و مصرف کنندگان به‌طور یکسان فراهم می‌کند، اما نقض داده‌های اخیر توسط شرکت‌های بزرگ و سوءاستفاده از آن و افشای حریم خصوصی، هم کاربران و هم مشاغل را آشفته و در معرض خطرات مختلف قرار داده است. این دوگانگی در نحوه استفاده از داده‌های شخصی - یعنی ایجاد فرصت‌های اقتصادی و زمینه‌های دخل و تصرف در حریم خصوصی اشخاص حقیقی - قانون‌گذاران را به تکاپو برای تقنین و تنظیم قواعد و مقررات داده شخصی کرده است؛ به طوری که بسیاری از کشورها قوانین تحت عنوان «مقررات عمومی حفاظت از داده‌های شخصی» و یا با عبارات کم‌وبیش شبیه، به تصویب رسانده‌اند.

قوانین مذکور بیشتر با تغلیب حفظ حریم خصوصی بر منافع اقتصادی، تبادل داده‌های شخصی را از ذیل حقوق قراردادها دور کرده‌اند و ذیل قواعد حفاظت از داده‌ها قرار داده‌اند و این دو قانون کاملاً همسو نیستند. این تباعد میان حقوق قراردادها و قانون حفاظت از داده شخصی این بحث را مطرح کرده است که آیا داده‌های شخصی، تحت قوانین حفاظت از داده‌های شخصی، قابل مبادله در قبال مواردی همچون ارائه خدمات است یا نه؟ آیا با وجود رویکرد حقوق بشری و حقوق اساسی نسبت به داده‌های شخصی، همچنان امکان مبادله آن وجود دارد؟ مبادله داده‌های شخصی از منظر مقررات حفاظت از داده‌های شخصی اتحادیه اروپا و قوانین ایران با چه چالش‌های مواجه است؟ آیا مبادله داده‌های شخصی با قواعد عمومی قراردادها سازگار است؟

باتوجه به افزایش روزافزون مبادله داده‌های شخصی - خصوصاً در بستر فضای مجازی - به پرسش‌های مذکور باید پاسخ‌های حقوقی مناسب ارائه داد.

در این پژوهش در ضمن پاسخ به سؤالات و چالش‌های مذکور، این مسئله روشن خواهد شد که مبادله داده‌های شخصی از منظر فقهی و حقوقی امکان‌پذیر است.

در این پژوهش، ابتدا به بیان رویکردهای متعدد نسبت به وضعیت حقوقی داده شخصی خواهیم پرداخت؛ چراکه این رویکردها نقش کلیدی در اتخاذ امکان تبادل داده شخصی به‌نحو موسع و مضیق دارد، سپس رویکرد مقررات عمومی حفاظت از داده شخصی اتحادیه اروپا - مصوب ۲۰۱۶ - نسبت به قانونی بودن مبادله داده‌های شخصی مورد مذاقه قرار می‌گیرد و در آخر امکان قانونی مبادله داده شخصی در حقوق ایران بررسی خواهد شد. با جست‌وجو در پایگاه‌هایی همچون نور مگز، روشن گردید که به زبان فارسی در این زمینه پژوهشی صورت نگرفته است؛ گرچه مقالاتی همچون «تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا»، به نویسندگی خانم مهدیه لطیف‌زاده، سید محمدمهدی قبولی درافشان، سعید محسنی و محمد عابدی، حول مقررات حفاظت از داده شخصی اتحادیه اروپا نوشته شده است، لکن در این پژوهش‌ها به بررسی مشروعیت تبادل داده‌های شخصی پرداخته نشده است. برعکس این وضعیت پژوهشی در فضای فقهی و حقوقی ایران (یعنی فقر منابع به زبان فارسی) پژوهش‌های قابل توجهی به زبان انگلیسی در اروپا و آمریکا انجام گرفته است که در ارجاعات این پژوهش بخشی‌های از آن را می‌توان مشاهده کرد.

۱. رویکردهای متعدد نسبت به داده‌های شخصی

تعیین نسبت میان داده و اشخاص حقیقی و به‌تبع چگونگی مدیریت آن

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)

از حیث حفظ حریم خصوصی و یا نقض آن منجر به ظهور طیف وسیعی از نظریات و رویکردهای مختلف شده است (Abraham, 2015, p.9)؛ به گونه‌ای که در بسیاری از موارد قابل جمع نیستند. با وجود این، می‌توان این آراء و نظریات مختلف را ذیل دو رویکرد کلی گنجانند: ۱. رویکرد مالکیت محور؛ برخی از اندیشمندان داده شخصی را دارایی اشخاص حقیقی می‌دانند و اشخاص حقیقی را مالک این داده‌ها معرفی می‌کنند (Purtova, 2009, p.1)؛ ۲. رویکرد حقوق بشری؛ در مقابل رویکرد مالکیت محوری، بسیاری از اندیشمندان، خصوصاً در اروپا، از رویکرد حقوق بشری حمایت می‌کنند و معتقد هستند که حفاظت از داده شخصی یک حق اساسی است (Rodota, 2009, p.77).

اتخاذ هر کدام از این رویکردها نقش کلیدی در توسعه و تضییق امکان قانونی تبادل داده شخصی ایفا می‌کند؛ لذا در این بخش به بررسی ادله و نقدهای این دو رویکرد خواهیم پرداخت.

۱-۱. رویکرد مالکیت محور نسبت به داده‌های شخصی

مطابق این رویکرد، افراد مالک داده‌های شخصی خودشان هستند؛ به عبارت دیگر داده‌های شخصی دارایی افراد است؛ گرچه در کیفیت تفسیر این مالکیت اختلاف نظر جدی وجود دارد: برخی آن را از قبیل مالکیت معنوی دانسته‌اند (Glancy. 2016. P.1) و برخی دیگر آن را جزء اسرار تجاری دانسته‌اند و بدین طریق تا ذیل قوانین تجاری مورد بحث قرار گیرد (Maria Bottis, 2017, p.207)؛ عده‌ای نیز داده شخصی را شهادت‌ارایی معرفی کرده‌اند (Lauren Henry Scholz, 2016, p.1113).

خاستگاه این رویکرد ایالت متحده آمریکا است و محققان ایالات متحده از اوایل دهه 1970 در مورد اینکه آیا اطلاعات شخصی باید به عنوان دارایی تلقی شود یا خیر بحث می‌کردند و از اوایل ۱۹۹۰ به بعد و به خصوص در سال‌های اخیر اقبال به این رویکرد بسیار افزایش یافته است (Purtova, 2009, p.1).

507, P. 2009)؛ لکن فزونی اقبال به این نظریه، در میان بسیاری از محققین آمریکا، قانون‌گذار را متقاعد به اخذ این رویکرد نکرده است.

منشأ ایده مالکیت اطلاعات شخصی در ایالات متحده عمدتاً در ناتوانی قانون حفاظت از داده‌های آمریکا در پاسخگویی مناسب به چالش‌های انقلاب اطلاعات، نهفته است (Purtova, 2009, p.508).

کسانی که از این نظریه پیروی می‌کنند، استدلال‌ها و تحلیل‌های متنوعی ارائه می‌کنند. برخی بر این عقیده هستند که رویکرد مالکیت‌محور به داده‌های شخصی مبادله بازار را تسهیل می‌کند و هزینه‌های جاری معاملات را کم می‌کند و به‌گونه‌ای میان ارزش داده‌های شخصی برای شرکت‌ها و ارزش داده‌های شخصی برای افراد و ارزش اجتماعی حفاظت از اطلاعات تعادل ایجاد می‌کند.

عده‌ای نیز سعی کرده‌اند با بیان طیفی از مزایای ایده مالکیت داده، جذابیت بیشتر آن را نمایان سازند، از جمله اینکه گفته‌اند: یک مدل حقوق مالکیت، شرکت‌ها را مجبور می‌کند تا برخی از هزینه‌هایی را که اشخاص حقیقی از جمع‌آوری و استفاده گسترده از داده‌های شخصی متحمل می‌شوند، درونی کنند. با درونی‌سازی این هزینه‌ها، شرکت‌ها ممکن است تصمیمات بهتری در مورد اینکه چه داده‌هایی جمع‌آوری کنند و چه استفاده‌هایی از داده‌ها انجام دهند، اتخاذ کنند (Samuelson, 1995, p. 8).

توضیح مطلب اینکه باتوجه به اینکه داده شخصی کالایی است که در دسترس همگان قرار دارد؛ لذا زمینه‌های تراژدی منابع مشترک (Tragedy Of The Commons) فراهم می‌شود.

تراژدی منابع مشترک به حالتی اشاره دارد که افراد بیشترین استفاده را از منبع مشترک خواهند داشت و استفاده پیش از حد، زمینه‌های سوءاستفاده، از جمله گسیل تعداد فزاینده پیام‌ها از سوی تبلیغ‌کنندگان، کلاه‌برداری و آسیب‌های مالی، جسمی و روانی را فراهم می‌آورد.

اعطای مالکیت به صاحبان داده‌ها به او کمک خواهد کرد تا با حداکثرسازی ارزش داده خود، در موقعیت مناسب جهت تعیین قیمت داده‌ها قرار بگیرد؛ در نتیجه جمع‌کنندگان داده مجبور خواهند شد هزینه‌های جمع‌آوری و استفاده از داده‌های شخصی را «داخلی» کنند و به تبع داده‌های کمتری را جمع‌آوری و استفاده خواهند کرد (YING, 2021, p.189). رویکرد حقوق مالکیت ممکن است به‌ویژه برای انطباق با ترجیحات مختلف افراد در مورد استفاده از داده‌های شخصی مفید باشد. اگرچه برخی از افراد ممکن است برای حفظ حریم خصوصی آن‌قدر ارزش قائل شوند که ترجیح دهند در معاملات بازار در مورد داده‌های شخصی خود شرکت نکنند ولی برخی دیگر ممکن است کاملاً مایل باشند که داده‌های شخصی خود را به شرکت‌های متعدد بفروشند (Samuelson, 1995, p.8).

همچنین برخی از صاحب‌نظران، سعی کرده‌اند با ارائه تحلیل‌هایی اقتصادی و نشان دادن ضعف‌های سیستم‌های دیگر به‌نوعی از رویکرد مالکیت دفاع کند. از جمله تحلیل‌های اقتصادی در دفاع از رویکرد مالکیت، تحلیل ورا برگلسون است. وی استدلال می‌کند که رژیم مالکیت ضعف‌های سیستم فعلی جرائم حریم خصوصی (رژیم جرم‌انگاری از جمله رژیم‌های است که ایالت متحده برای جلوگیری از نقض حریم خصوصی استفاده می‌کند) را جبران می‌کند. وی استدلال می‌کند که انتخاب بین رژیم جرم و رژیم دارایی (مالکیت) برای حفاظت از اطلاعات شخصی به معنای انتخاب بین قوانین مالکیت و قوانین مسئولیت است که توسط کالابرسی و ملامد تعریف شده است. مطابق نظریه کالابرسی و ملامد، حق توسط قانون مالکیت تا جایی محافظت می‌شود که کسی که مایل است حق دیگر را به دست آورد، باید آن را از او در یک معامله رضایت‌مندانه خریداری کند که در آن ارزش این حق با فروشنده توافق شده است. براساس قانون مسئولیت، دارندگان باید هر زمان که این حق بدون رضایت آن‌ها سلب می‌شود،

گرامت دریافت کنند و مطابق قانون مسئولیت، ارزش این حق توسط برخی از ارگان‌های دولتی تعیین می‌شود نه توسط خود طرفین. بنابراین در صورت ترجیح رژیم جرم‌انگاری دو مشکل عمده ایجاد خواهد شد: اول اینکه اولویت‌دهی به رژیم جرم‌انگاری، به این معنی است که حق فرد بر اطلاعات باید به‌طور انحصاری توسط دادرس به رسمیت شناخته شود که خود شامل هزینه‌های قابل توجهی است، ثانیاً: شاکی باید خسارات واقعی را اثبات کند که به احتمال زیاد ناچیز خواهد بود. این امر به‌خودی‌خود مردم را از طرح دعوا علیه افرادی که حقوق آن‌ها را در اطلاعات شخصی نقض می‌کنند، منصرف می‌کند و در نتیجه این قانون را ناکارآمد می‌کند. محصل این تحلیل این است که رژیم مالکیت حقوق افراد را به شکل بهتری محافظت می‌کند. (Bergelson, 2005, p.417)

مطابق نظر وی، رژیم مالکیت‌محور، به فرد حداکثر کنترل بر اطلاعات شخصی را می‌دهد و به همه طرف‌های ذینفع اجازه می‌دهد تا بدون محدود کردن منابع ارزشمند اجتماعی وارد معاملات قابل قبول دوجانبه شوند، بالعکس رژیم جرم‌انگاری که در آن زمینه‌های بیشتر جمع‌آوری اطلاعات شخصی فراهم می‌شود (Bergelson, 2005, p.419).

برخی دیگر از نویسندگان نیز با پیش‌فرض «داده‌های شخصی دارایی هستند» روی این مسئله بحث کرده‌اند که مالک این دارایی چه کسانی هستند؟ موضوع داده یا گردآوری‌کنندگان داده‌ها یا هر دو؟ و در چهارچوب این سؤال به‌نفع مالکیت موضوع داده‌ها استدلال کرده‌اند که در واقع به‌گونه‌ای در قالب مالکیت از حریم خصوصی دفاع می‌کنند. ازجمله این نویسندگان مورفی است. مطابق دیدگاه مورفی، بسته به اینکه حق مالکیت در ابتدا به چه کسی واگذار می‌شود: یک فرد یا یک گردآورنده داده، دو نوع قانون پیش‌فرض متمایز وجود دارد: عدم افشا (قانون حفظ حریم خصوصی) و افشا (قانون عدم حفظ حریم خصوصی). براساس قانون

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران) ■

حریم خصوصی، کنترل بر داده شخصی به موضوع داده اعطا می‌شود و فرد می‌تواند انتشار اطلاعاتی را که «خصوصی» تلقی می‌کند، کنترل کند، اما در سایر اطلاعاتی که خصوصی تلقی نمی‌کند، چنین کنترلی ندارد ولی بر اساس قانون افشا، کنترل بر داده‌های شخصی ابتدا به یک گردآورنده داده اختصاص داده می‌شود، در نتیجه به خود اجازه خواهد داد به هر نوع داده‌ای دسترسی داشته باشد و این آغازی خواهد برای نگرانی‌های گسترده (Murphy, 1996, pp.2383 -84).

۱-۱-۱. انتقادات وارد شده نسبت به رویکرد مالکیتی

برخی از پژوهشگران نسبت به سودمندی تجاری‌سازی داده (تبادل) اظهار تردید کرده‌اند. یکی از این نقدها این است که بازار حریم خصوصی شکست خورده است (Privacy Market Failur).

یکی از جلوه‌های شکست بازار حریم خصوصی ناتوانی شرکت‌های پردازش‌کننده اطلاعات در «تبعیض قیمت حریم خصوصی» است (privacy price discrimination). به عبارت دیگر، یک بازار کارآمد حفظ حریم خصوصی به افراد اجازه می‌دهد تا داده‌های خود را به میزان ارزشی که حریم خصوصی‌شان برایشان دارد، بفروشند؛ حال آنکه در بیشتر موارد، افراد زمانی که قصد فروش داده‌های شخصی‌شان را دارند، یک انتخاب باینری دارند: یا به قیمت موردنظر شرکت می‌فروشند یا نمی‌فروشند و در نتیجه میان افرادی که به حریم خصوصی خود اهمیت زیادی قائل هستند و کسانی که چنین نیستند، تفاوتی قائل نمی‌شوند (Schwartz, 2004, p.2077).

عده‌ای نیز رویکرد مالکیت‌محور را در تضاد با اصل «آزادی قابلیت انتقال» (Free Alienability) دانسته‌اند. اصل آزادی قابلیت انتقال به این معناست که مالک در انتقال مالکیت اموال خود بدون محدودیت است. این قابلیت در حریم خصوصی محدود است؛ چراکه ممکن است صاحبان داده‌ها، در جهت استفاده خاصی، به شرکت‌های پردازش‌کننده به فروش برسانند؛ به طوری که

اجازه استفاده در جهات دیگر به شرکت ندهد یا اینکه به شرکت اجازه فروش داده‌ها به شخص ثالث را ندهد (Samuelson, 2000, p.11).

برخی دیگر اظهار داشته‌اند که کاربران به‌وضوح ارزش نهایی داده‌های شخصی خود را نمی‌دانند و بنابراین به‌طور کامل درک نمی‌کنند که تا چه حد داده‌های شخصی خود را در ازای محصولات/خدمات «رایگان» یا سایر مشوق‌ها ارائه می‌کنند. برای مثال، ارزش داده‌های شخصی آن‌ها ممکن است از ارزش محصول/خدمتی که «رایگان» دریافت می‌کنند بیشتر باشد. علاوه بر این، افراد ممکن است از نحوه استفاده از داده‌های شخصی خود آگاه نباشند و یا درک کاملی از آن نداشته باشند. مضافاً اینکه، عدم تقارن اطلاعاتی مابین کاربر و پردازشگر، با استفاده از تکنیک‌های سوگیری روان‌شناختی کاربران که آن‌ها را به سمت انتخاب‌های مزاحم حریم خصوصی و یا به اشتراک گذاشتن داده‌های شخصی خود سوق می‌دهد، تشدید می‌شود (Galli, 2021/Athey. 2017. p. 7).

همچنین ادعا می‌شود که تجاری‌سازی داده‌ها ممکن است باعث دسترسی ناعادلانه به حریم خصوصی و رفتار تبعیض‌آمیز شوند. در واقع، حریم خصوصی می‌تواند به‌طور بالقوه به یک کالای لوکس تبدیل شود که فقط برای کسانی که توانایی پرداخت هزینه را دارند، در دسترس است، در حالی که کاربران کم‌درآمد می‌پذیرند که خود را در معرض افزایش جمع‌آوری داده‌ها، چه برای تخفیف، چه مزایا یا پاداش، قرار دهند (Elvy, pp.1400 - 1406).

۱-۲. رویکرد حقوق بشری نسبت به داده‌های شخصی

یکی دیگر از رویکردهای عمده در حفاظت از داده‌های شخصی، رویکرد حقوق بشری در این زمینه است؛ گرچه در ادبیات حقوقی با تعابیر متعددی آمده است و لکن این عبارات متعدد به‌نظر می‌رسد به‌لحاظ مفهومی و مصداقی با حقوق بشر هم‌پوشانی دارد.

یکی از این تعبیری که در سطح کلان زمینه مناقشات را فراهم کرده است، تعبیر به حق اساسی است. در اتحادیه اروپا، حق حفاظت از داده‌ها به عنوان یک حق اساسی در نظر گرفته شده است و از تعبیر به حقوق طبیعی و حقوق بشر امتناع می‌شود.

بند ۱ ماده ۸ منشور حقوق اساسی اتحادیه اروپا - مصوب ۲۰۰۰ - مقرر می‌دارد: «هرکس حق دارد از اطلاعات شخصی خود حفاظت کند». منشور حقوق اساسی اتحادیه اروپا طیفی از حقوق اساسی را به رسمیت شناخته است، از جمله حق حفاظت از داده‌های شخصی؛ همچنان که در مقدمه مقررات عمومی حفاظت از داده اتحادیه اروپا - مصوب ۲۰۱۶ - آمده است: «حفاظت از اشخاص حقیقی در ارتباط با پردازش داده‌های شخصی، یک حق اساسی است». همچنین در دستورالعمل - ۷۷۰/۲۰۱۹ - آمده است: «داده‌های شخصی را نمی‌توان به عنوان یک کالا در نظر گرفت» (این جمله به واقع اشاره به حق اساسی بودن حفاظت از داده دارد).

به نظر می‌رسد با وجود اصرار اتحادیه اروپا بر به کارگیری «حق اساسی» به جای «حقوق بشری»، این دو مفهوم، مستقل از هم نیستند (Sloot, 2017, pp. 12-13)؛ چراکه اولاً: در برخی از اسناد اتحادیه اروپا حقوق بشر و حقوق اساسی معادل هم انگاشته شده و به جای یکدیگر به کار رفته است؛ ثانیاً استدلال‌هایی که به نفع این رویکرد شده است، استدلال‌های از جنس حقوق بشر هستند که در ادامه خواهد آمد.

به هر روی چه حقوق اساسی را معادل حقوق بشری بدانیم یا نه، کسانی که حفاظت از داده شخصی را یک حق اساسی می‌دانند، استدلال‌های فراتر از استناد به پاره‌ای از حقوق بشر ندارند. به عبارت دیگر این گروه، مجموعه‌ای از حقوق (بشری) را زیربنای رویکرد خود قرار داده‌اند.

یکی از این حقوق، حفظ استقلال فردی (autonomy of the individual) است. این مبنا در حقوق فرانسه مورد توجه قرار گرفته است و

در دادگاه‌ها اعمال حقوق حفاظت از داده‌ها به‌عنوان جزئی از حق آزادی (استقلال فردی) مطرح شده است (McDermott, 2017, p.3). بند ۷ GDPR در این زمینه اشاره می‌کند: «افراد حقیقی باید کنترل داده‌های شخصی خود را داشته باشند».

علاوه بر این، تمرکز بر رضایت در حق حفاظت از داده‌ها نیز - به‌عنوان یکی از مبانی قانونی پردازش داده‌ها - در راستای استقلال فردی است. به‌واقع رضایت موجود در مقررات عمومی حفاظت از داده‌ها با اصطلاح «نظریه اراده» در حقوق مطابقت دارد. طرفداران تئوری اراده، کارکرد حقوق را اعطای کنترل به دارندگان حقوق می‌داند تا دیگران را تحت تکلیف احترام به آن حقوق قرار دهند (Stanford, 2020).

اصل کرامت یکی دیگر از مفاهیم ارزشی است که زیربنای رویکرد حقوق بشری در نظر گرفته شده است. این اصل در آلمان به‌عنوان مبانی «خودتعیینی اطلاعاتی» مطرح شده است (McDermott, 2017, p.2). این اصل مورد تصریح ماده ۸۸ GDPR است.

یکی دیگر از مفاهیم اصلی شفافیت است. طبق ماده ۷ GDPR هرگونه درخواست رضایت باید قابل فهم، در دسترس و به زبانی روشن و واضح باشد. بند ۵۸ GDPR به‌صراحت این الزام را به «اصل شفافیت» مرتبط می‌کند؛ لذا مقررات مذکور افشای اطلاعات در مورد انتقال و استفاده از داده‌ها را الزامی می‌داند.

یکی دیگر از اصول، اصل عدم تبعیض است. مطابق GDPR جمع‌آوری و پردازش داده‌ها باید به‌گونه‌ای انجام شود که از اثرات تبعیض‌آمیز بر افراد بر اساس منشأ نژادی یا قومی، عقاید سیاسی، مذهب یا عقاید جلوگیری شود (McDermott, 2017, p.3).

محصل استدلال کسانی که بر مبنای اصول و مفاهیم حقوق بشری به حفاظت از داده‌های شخصی می‌نگرند، این است که آزادی مدنی، استقلال،

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران) ■

کرامت و آزادی فردی در یک جامعه مدنی دموکراتیک ضروری است و قانون حفاظت از داده‌های شخصی برای تضمین حمایت از این منافع است و تجاری‌سازی داده‌های شخصی منافع مذکور و به تبع دموکراسی را تهدید می‌کند (Schwartz, 2004, p.2087).

۱-۲-۱. انتقادات وارد شده نسبت به رویکرد حقوق بشری

این رویکرد نیز از انتقادات مصون نمانده است. برخی از نویسندگان حق اساسی دانستن حفاظت از داده‌های شخصی را مورد مناقشه قرار داده‌اند. از جمله اینکه در مقررات عمومی حفاظت از داده‌ها دو طیف از داده‌ها وجود دارد: برخی از این داده‌ها حاوی ویژگی‌های حق اساسی است، از جمله داده‌های حساس، داده‌های شخصی با منشأ نژادی یا قومیتی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی، عضویت در اتحادیه‌های کارگری، داده‌های ژنتیکی، داده‌های بیومتریک که صرفاً برای شناسایی یک انسان پردازش می‌شوند، داده‌های مرتبط با سلامت، داده‌های مربوط به زندگی جنسی یا گرایش جنسی یک فرد (Article 4(13), (14) and (15), Article 9 and Recitals (51) to GDPR of (56));؛ برخی دیگر از داده‌های شخصی وجود دارد که حاوی ویژگی‌های حق اساسی نیست. به عنوان مثال عکس گرفتن از دیگران در یک مهمانی و ارسال آن‌ها در اینترنت بدون رضایت آن‌ها نقض قوانین حفاظت از داده‌ها، شمرده می‌شوند، حال اینکه، داده‌های با این مقدار اهمیت، تحت قلمرو حقوق اساسی (بشر)، همچون منع شکنجه، تحت محاکمه عادلانه قرار گیرند، محل شک و تردید است (Sloot, 2017, p.15).

همچنین عملکرد مقررات حفاظت از داده‌ها، با عملکرد حقوق بشر متفاوت است؛ مقررات حفاظت از داده‌ها از ارزشی محافظت می‌کند که کاملاً متفاوت با ارزش‌هایی است که حقوق بشر از آن حمایت می‌کند. هدف از دستورالعمل‌ها، مقررات و قوانین حفاظت از داده‌ها، حفاظت از دو ارزش کاملاً متضاد، یعنی منافع افراد برای حفاظت از داده‌های شخصی

خود و منافع کنترل‌کنندگان داده‌ها برای پردازش داده‌ها است؛ حال آنکه حقوق بشر عمدتاً بر منافع افراد متمرکز است، حتی اگر برخی از آن‌ها تحت شرایط خاصی محدود شوند. بنابراین به نظر می‌رسد که کارکرد حق حفاظت از داده‌ها با کارکرد بسیاری از حقوق (بشری) متفاوت است (Sloot, 2017, p.16).

۲. داده‌های شخصی؛ عملکردی دوگانه

همان‌طوری که روشن گردید، رویکرد مالکیت امکان قانونی دادوستد داده‌های شخصی را فراهم می‌آورد و می‌توان در قالب این رویکرد، اقدام به خرید و فروش داده‌های شخصی و انعقاد سایر قراردادها کرد، ولی اتخاذ رویکرد حقوق بشری به‌نحو مطلق، سدی محکم در امکان مبادله داده‌ها است؛ چراکه این‌گونه حقوق، حقوق طبیعی هستند نه از قبیل حقوق وضعی.

با وجود این، مشاهده می‌شود که برخی از قوانینی که رویکرد حقوق بشری اتخاذ کرده‌اند - به‌رغم اینکه صراحتاً داده شخصی را از قبیل حقوق (بشر) می‌دانند - یا امکان تبادل داده شخصی را مسکوت گذاشته‌اند یا اینکه به‌نحو محدود پذیرفته‌اند (از جمله مقررات حفاظت از داده اتحادیه عمومی و لایحه صیانت و حفاظت از داده‌های شخصی ایران)؛ در نتیجه می‌توان گفت یا این قوانین امکان مبادله برخی از این‌گونه حقوق (بشر) را پذیرفته‌اند یا اینکه قائل هستند که برخی از داده‌های شخصی جزء حقوق بشر به حساب نمی‌آیند.

گزینه اول بسیار بعید به نظر می‌رسد؛ چراکه حقوق بشر جزء حقوق طبیعی و اولیه است که باید به رسمیت شناخته شوند، نه اینکه وضع شوند و قابل معاوضه نیست. لذا می‌توان ادعا کرد - همان‌طوری که برخی از نویسندگان اذعان کرده‌اند - دودسته از داده‌های شخصی وجود دارند:

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)

داده‌های حساس (داده‌های با منشأ قومی، نژادی و غیره) و داده‌هایی که اهمیت چندانی ندارند، همچون بسیاری از عکس‌ها و فیلم‌های شخصی یا صفحات مجازی و غیره. داده‌های اخیر دارای عملکردی دوگانه هستند: عملکردی اقتصادی: این عملکرد، به‌واقع عملکردی است که طرفداران رویکرد مالکیت، همچون اقتصاددانان، بسیار روی آن تأکید دارند و عملکردی غیراقتصادی (نقض حریم خصوصی که ممکن است زمینه‌های سوءاستفاده از این داده‌ها را فراهم کند) که طرفداران رویکرد حقوق بشری بدان اهتمام دارند.

به نظر می‌رسد بسیاری از قوانینی که رویکرد حقوق بشری نسبت به داده‌های شخصی دارند و امکان تبادل داده شخصی را مسکوت گذاشته‌اند یا اینکه به‌نحو محدود پذیرفته‌اند، تفصیل اخیر را اخذ کرده‌اند، گرچه صراحتاً بدان اشاره‌ای نشده است، بلکه تحلیل کلی مواد قانونی این تفصیل را نشان می‌دهد.

۳. مبادله داده‌های شخصی در مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)

به‌رغم اینکه امکان مبادله قانونی داده‌های شخصی صراحتاً در مقررات عمومی حفاظت از داده اتحادیه اروپا مطرح نشده است؛ عده‌ای از صاحب‌نظران، با استناد به برخی از مبانی پردازش داده‌های شخصی، مبادله این‌گونه داده‌ها را قانونی دانسته‌اند.

توضیح مطلب اینکه ماده (۶) مقررات مذکور، شش مبنای قانونی برای پردازش داده‌ها مطرح کرده است؛ به‌طوری‌که شخصی که به‌دنبال پردازش داده شخصی است، باید یکی از شش مبنای قانونی را جهت مشروعیت پردازش انتخاب کند. از میان این مبانی، بسیاری از محققین رضایت را (Consent) (Article 6(1)(a) GDPR) به‌عنوان یک زمینه قانونی کلیدی

برای پردازش داده‌های شخصی اشخاص حقیقی برای تعهدات متقابل مطرح کرده‌اند (Taştan, 2021, p.18).

رضایت موضوع داده به معنای «هرگونه اشاره آزادانه، مشخص، آگاهانه و بدون ابهام از خواسته‌های او با بیانیه یا یک اقدام مثبت واضح است که به معنای موافقت با پردازش داده‌های شخصی مربوط به او است» (Art 4(11) GDPR).

همان‌طوری که روشن است، قانون‌گذار، در این تعریف، طیفی از ویژگی‌های را برای رضایت مطرح می‌کند که در صورت احراز این ویژگی‌ها رضایت موضوع داده‌های شخصی معتبر تلقی خواهد شد (Bojana. 2017, p.217).

یکی از این ویژگی‌ها، اصطلاح «آزادانه داده‌شده» (freely given) است. این اصطلاح گرچه در مقررات مذکور، به‌صراحت تعریف نشده است، اما کارگروه ماده (۲۹) اقدام به تفسیر این اصطلاح کرده است. مطابق نظر این کارگروه، «آزادانه داده می‌شود» به معنای انتخاب و کنترل واقعی موضوع داده بر داده‌های خود است. به این معنا که اگر موضوع داده انتخاب واقعی نداشته باشد، احساس کند مجبور به رضایت می‌شود یا در صورت عدم رضایت عواقب منفی را متحمل می‌شود، رضایت معتبر نخواهد بود. بر این اساس، در صورتی که موضوع داده قادر به امتناع یا پس گرفتن رضایت خود بدون ضرر نباشد، رضایت آزاد تلقی نخواهد شد (WP29, 2017, p.5). همچنین کارگروه مذکور، در ادامه می‌نویسد: رضایت تنها در صورتی معتبر است که موضوع داده بتواند یک انتخاب واقعی را اعمال کند و خطر فریب، ارباب، اجبار یا پیامدهای منفی قابل توجهی (مثلاً هزینه‌های اضافی قابل توجه) وجود ندارد. در مواردی که عنصر اجبار، فشار یا ناتوانی در اعمال اختیار وجود داشته باشد، رضایت آزاد نخواهد بود (WP29, 2017, p.7).

همین تفسیر از بند (۴۲) مقررات مذکور، قابل استنباط است؛ چراکه

عبارات اخیر بند مذکور به صراحت مقرر می‌دارد که اگر موضوع داده هیچ انتخاب واقعی یا آزادانه‌ای نداشته باشد یا قادر به رد یا پس گرفتن رضایت بدون ضرر نباشد، نباید به عنوان رضایت آزادانه تلقی شود.

برای احراز رضایت آزادانه، بند (۴) ماده (۷) معیاری را مطرح می‌کند که به واقع ارتباط مستقیمی با امکان تبادل داده دارد، در این بند آمده است: «هنگام ارزیابی اینکه آیا رضایت آزادانه داده می‌شود یا خیر، باید ملاحظه کرد که آیا، مواردی از قبیل اجرای یک قرارداد و ارائه خدمات، منوط به رضایت به پردازش داده‌های شخصی‌ای است که برای اجرای آن قرارداد ضروری نیست؟»؛ همچنان که بند (۴۳) نیز مقرر می‌دارد: «فرض می‌شود که رضایت آزادانه داده نمی‌شود [...] اگر اجرای یک قرارداد، از جمله ارائه خدمات، وابسته به رضایت باشد، با وجود اینکه این رضایت برای چنین قراردادی ضروری نیست» مطابق دو بند مذکور، درجایی که اجرای قرارداد یا ارائه خدمات منوط به رضایت به پردازش داده‌هایی باشد که برای اجرای قرارداد یا ارائه خدمات ضروری نیست، رضایت آزادانه نیست و در نتیجه مطابق مقررات، رضایت معتبر نخواهد بود.

لذا وضعیت بند (۴) ماده (۷) گاهی اوقات «باندلینگ» نامیده می‌شود؛ زیرا کنترل‌کننده رضایت را برای مقاصد «ضروری» همراه با رضایت برای آن دسته از فرآیندهایی که ممکن است «غیر ضروری» در نظر گرفته شوند، جمع می‌کند (Bojana, 2017, p.218).

نمونه‌ای از «وضعیت باندلینگ» می‌تواند این باشد که فردی قصد خرید آنلاین بلیت هواپیما را داشته باشد و ممکن است بنابر درخواست شرکت‌های هواپیمایی، نه تنها با به اشتراک گذاشتن داده‌های شخصی که برای این تراکنش ضروری است، بلکه همچنین اجازه استفاده از آن را برای اهداف تبلیغاتی بدهد، حال اینکه پردازش‌های اضافی داده برای اجرای قرارداد ضروری نیست.

همچنین درخواست رضایت برای تراکنش‌های آنلاین همراه با اهداف بازاریابی و وابسته کردن خرید به این رضایت، به احتمال زیاد منجر به این نتیجه می‌شود که رضایت «آزادانه داده نمی‌شود» (Bojana, 2017, p.218). همچنین درجایی که برنامه‌های تلفن همراه برای ویرایش عکس، از کاربران درخواست می‌کند تا GPS خود را برای استفاده از خدمات فعال کنند، درحالی که برای ویرایش عکس نیازی به این گونه اطلاعات نیست. همچنین در برخی از موارد، این گونه برنامه‌ها به کاربران خود می‌گوید که از داده‌های جمع‌آوری شده برای اهداف تبلیغاتی استفاده خواهد کرد، درحالی که برای ارائه خدمات ویرایش عکس ضروری نیست و فراتر از ارائه خدمات اصلی ارائه شده است. از آنجایی که کاربران نمی‌توانند بدون رضایت به این اهداف از برنامه استفاده کنند، رضایت را نمی‌توان آزادانه در نظر گرفت (WP29, 2017, p.5).

همچنین یک بانک از مشتریان رضایت می‌خواهد تا به اشخاص ثالث اجازه دهند تا از جزئیات پرداخت خود برای اهداف بازاریابی مستقیم استفاده کنند. این فعالیت پردازشی برای اجرای قرارداد با مشتری و ارائه خدمات عادی حساب بانکی ضروری نیست. اگر امتناع مشتری از رضایت از این هدف پردازشی منجر به عدم ارائه خدمات بانکی، بسته شدن حساب بانکی یا حسب مورد افزایش کارمزد شود، رضایت آزادانه نخواهد بود (WP29, 2017, p.9).

به‌هرروی، این وضعیت را می‌توان مکانیزمی برای «اجبار کردن» موضوع داده‌ها به رضایت و اجازه استفاده از داده‌ها برای مقاصد غیر از مواردی که برای اجرای قرارداد ضروری است در نظر گرفت (Bojana, 2017, p. 218). بند (۴) ماده (۷) به شدت مورد مناقشه واقع شده است؛ به طوری که رویکردها و نظرات متفاوتی ارائه شده است؛ از تفسیرهای مطلق‌انگارانه تا تفسیرهای منعطف. برخی این بند را به نحو مطلق تفسیر کرده‌اند، از جمله

دیوان عالی اتریش که در ۳۰ آگوست ۲۰۱۸ اعلام کرد که ممنوعیت رضایت مشروط ماهیتاً مطلق است و جایی برای استثنا وجود ندارد. مطابق این تفسیر امکان مبادله داده اصلاً وجود ندارد.

عده‌ای نیز، از جمله کارگروه ماده (۲۹)، با اینکه دیدگاه ممنوعیت مطلق تبادل را اتخاذ نکرده‌اند، لکن تفسیر بسیاری محدودی ارائه داده‌اند. این کارگروه اعلام می‌کند که به واسطه اعمال این بند، GDPR تضمین می‌کند که پردازش داده‌های شخصی که برای آن رضایت درخواست شده است، نمی‌تواند به‌طور مستقیم یا غیرمستقیم به تعهد متقابل قراردادی تبدیل شود (WP29, 2017, p.8)؛ و از آنجایی که بند (۴) ماده (۷) به‌طور مطلق تفسیر نشده است؛ ممکن است موارد نادری باشد که مشروط کردن رضایت، موجب بی‌اعتباری رضایت نشود و کلمه «فرض می‌شود» (pre-sumed) در بند (۴۳) نشان می‌دهد که چنین مواردی استثنایی خواهد بود و در این صورت (در موارد نادر)، بار اثبات بند (۴) بر عهده کنترل‌کننده خواهد بود و کنترل‌کننده می‌تواند ثابت کند که مجموعه وی انتخاب واقعی به موضوع داده ارائه کرده، با این وجود اثبات این مسئله دشوار خواهد بود (WP29, 2017, pp.8-9).

به‌زبان ساده این کارگروه اعلام می‌کند در جایی که داده شخصی در مقام ایفای تعهد متقابل است، اصل بر این است که رضایت آزادانه نیست، مگر اینکه پردازشگر ثابت کند که رضایت آزادانه است. با این تفسیر عملاً می‌توان ادعا کرد اصل عدم صحت تبادل داده شخصی است، مگر اینکه خلافش ثابت شود.

در مقابل این دو رویکرد سخت‌گیرانه، برخی از صاحب‌نظران رویکرد منعطفی را اتخاذ و سعی کرده‌اند تفسیر موسعی از این بند ارائه کنند. رویکردی که امکان توسعه تبادل داده‌های شخصی را در مقابل ارائه خدمات یا ارائه تخفیف و یا اعطای جوایز آسان‌تر می‌کند (Metzger, 2017, p.4).

لذا در این راستا، برخی عبارت کارگروه ماده (۲۹): «پردازش داده‌های شخصی که برای آن رضایت درخواست شده است، نمی‌تواند به‌طور مستقیم یا غیرمستقیم به تعهد متقابل قراردادی تبدیل شود» را این‌گونه تفسیر کرده‌اند که مقصود از آن این است که در همه حال، رضایت به پردازش داده‌های شخصی غیرضروری به معنای اجباری بودن رضایت در مقابل ارائه خدمات نیست؛ به عبارت دیگر این‌گونه نیست که این‌گونه رضایت (به داده غیرضروری) همیشه و در همه حال از باب اجبار و الزام پردازش‌کننده است؛ در نتیجه رضایت به پردازش داده‌ها می‌تواند مشوق باشد و همچنان آزاد در نظر گرفته شود. بنابراین، موضوع تمایز بین انگیزه غیرمجاز و مجاز است که به افراد امکان می‌دهد در ازای داده‌های شخصی خود خدمات «رایگان» یا تخفیف یا پاداش دریافت کنند.

توضیح مطلب اینکه گفته شد رضایت آزادانه به معنای انتخاب واقعی (داشتن جایگزین واقعی) است؛ انتخاب واقعی به سه صورت قابل تصویر است: گاهی شخصی در ازای ارائه خدمات، خواهان داده‌های غیرضروری است ولی حاضر است در ازای پول نیز خدمات موردنظر را ارائه دهد؛ لذا کاربر می‌تواند به جای ارائه داده شخصی، در ازای ارائه خدمات پول پردازد؛ در نتیجه پول یک جایگزین واقعی برای داده شخصی است، لذا رضایت آزادانه است؛ گاهی جایگزین داده شخصی (به غیر از پول)، صرفاً از طرف ارائه‌کننده خدمات، ارائه نشده است، بلکه در بازار جایگزین‌های وجود دارد که کاربر می‌تواند آن‌ها را انتخاب کند، لذا اگر ارائه‌کننده خدمات، جایگزینی برای داده شخصی ارائه ندهد، رضایت همچنان معتبر است؛ چراکه توسط اشخاص دیگر در بازار جایگزین ارائه شده است و کاربر می‌تواند از آن‌ها استفاده کند و اجباری ندارد که حتماً از یک ارائه‌کننده خدماتی که انحصاراً در ازای داده شخصی، خدمات ارائه می‌دهد، مطالبه خدمات داشته باشد؛ گاهی جایگزین داده شخصی توسط خود ارائه‌کننده خدمات نیز ارائه می‌شود. کارگروه ماده

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران) ■

(۲۹) بند (۴) را محدود به قسم سوم دانسته، لذا اگر ارائه‌کننده خدمات، جایگزین معرفی نکند (با وجود اینکه ارائه‌کننده جایگزین نیز هست)، حتی اگر جایگزین پول داشته باشد یا در بازار جایگزین داشته باشد، همچنان رضایت نامعتبر است.

در مقابل برخی از نویسندگان نیز هر سه قسم را مصداق انتخاب واقعی دانسته‌اند. لذا کسانی که بند (۴) را محدود به قسم سوم کرده‌اند یا اینکه هر سه قسم را مصداق انتخاب واقعی دانسته‌اند، تفسیر بسیار موسع از بند (۴) ارائه داده‌اند.

به‌هرروی آنچه محرز است، در اتحادیه اروپا هنوز به وحدت نظر در رابطه با تبادل موسع داده‌ها نرسیده‌اند، گرچه به نظر می‌رسد اکثریت - قدر متیقن - تفسیر مضیق را پذیرفته‌اند و تمایلی به ممنوعیت مطلق وجود ندارد.

۴. رویکرد نظام حقوقی ایران و فقه امامیه؛ چالش‌ها و راه‌حل‌ها

در نظام حقوقی ایران، قانون‌گذاری در خصوص داده‌های شخصی به‌صورت مستقل صورت نگرفته است، بلکه در ضمن برخی از قوانین خاص به‌صورت جزئی به این موضوع اشاره شده است (لطیف‌زاده و همکاران، ۱۴۰۰، ص ۴۶۱). لذا با توجه به اینکه از یک طرف سند مستقلی در حوزه داده‌های شخصی هنوز به تصویب نرسیده، برای بررسی مشروعیت و قانونی بودن تجاری‌سازی داده شخصی لازم است به قواعد عمومی قراردادها و برخی از قوانین خاصی که به‌صورت جزئی به داده‌های شخصی پرداخته‌اند، رجوع کرد.

بررسی قوانین نشان می‌دهد که قانون‌گذار در حقوق ایران نسبت به تجاری‌سازی داده‌های شخصی صراحتاً موضعی اتخاذ نکرده است؛ نه در رد امکان تجاری‌سازی و نه در پذیرش؛ به‌عنوان مثال قانون تجارت الکترونیکی - که می‌توان گفت بارزترین و مهم‌ترین قانون مشتمل بر داده‌های شخصی

است - در ذیل فصل سوم - حمایت از «داده‌پیام‌های شخصی» اشاره‌ای به اینکه داده‌های شخصی دارای ارزش اقتصادی هستند و یا اینکه می‌تواند مورد عقد واقع شود، نکرده است؛ گرچه در صورت نقض داده‌های شخصی مجازات در نظر گرفته است، لکن همان‌طوری که روشن است، تشریح این‌گونه مجازات بیشتر در مقام حفظ حقوق صاحبان داده‌ها و حفظ حریم خصوصی است نه به‌خاطر اینکه داده‌های شخصی را دارای ارزش اقتصادی می‌داند.

بنابراین باتوجه به نبود قوانین مصرح در این زمینه، برای تعیین مشروعیت یا عدم مشروعیت تبادل داده شخصی در حقوق ایران باید به قواعد و قوانین عام رجوع کرد. از لحاظ قواعد عمومی قرارداد داده‌های شخصی با طیفی از چالش‌های حقوقی و فقهی مواجه است و در صورتی که بتوان بدان پاسخ مناسبی داد، در این صورت از نظر حقوق ایران، این‌گونه قراردادها را باید بلامانع دید. در ادامه به بررسی چالش‌های مذکور خواهیم پرداخت:

۴-۱. مالیت داشتن داده‌های شخصی

از منظر قواعد عمومی، مهم‌ترین مانع در زمینه تبادل داده، مالیت یا عدم مالیت داده شخصی است؛ لذا باید به بررسی مفهوم مالیت و انطباق آن با داده شخصی پرداخت. فقها و حقوق‌دانان تعاریف متعددی از مال کرده‌اند؛ برخی در تعریف مال آورده‌اند که مال چیزی است که دارای ارزش اقتصادی است و مفهوم نسبی دارد و تابع شرایط و اوضاع خاص است (شهیدی، ۱۳۸۷، ص ۵)؛ برخی دیگر گفته‌اند: مال در اصطلاح حقوقی به چیزی گفته می‌شود که بتواند مورد دادوستد قرار گیرد و از نظر اقتصادی ارزش مبادله را داشته باشد (امامی، ۱۳۷۷، ج ۱، ص ۱۹)؛ عده‌ای نیز گفته‌اند: مال چیزی است که بتوان با آن دادوستد کرد و برای آن تقاضا مطرح باشد و بتوان آن را به پول ارزیابی کرد؛ در تعریف دیگر آمده است: مال چیزی است که مردم نسبت بدان رغبت دارند و در زندگی مردم دخیل است (بجنوردی، ۱۳۸۹،

ج ۲، ص ۲۰۹)؛ همچنین گفته‌اند: مال چیزی است که دارای منافع حلال باشد (خویی، بی‌تا، ج ۲، ص ۴)؛ برخی دیگر آورده‌اند: هر جنسی که در نزد عرف مال محسوب شود، مالیت دارد، اعم از اینکه اصلش مباح باشد یا نه (طوسی، ۱۳۸۷، ج ۸، ص ۲۰)؛ برخی دیگر نیز آورده‌اند: مال چیزی است که عرفاً مردم برای به دست آوردن آن رقابت می‌کنند و معاوضه آن سفهی نیست (مظفر، بی‌تا، ج ۱، ص ۱۵۸).

از مجموعه این تعاریف می‌توان استنباط کرد که مال دارای دو شاخصه است: داشتن ارزش اقتصادی و رغبت و نیاز مردمان بدان؛ بنابراین در صورتی که ارزش اقتصادی نداشته باشد یا مردمان رغبتی بدان نشان ندهند، آن شیء مالیت ندارد، لذا بسیاری از فقها در صورت قلت منافع شیء، بیع آن شیء را جایز نمی‌دانند (انصاری، ۱۴۱۵، ج ۴، ص ۹).

این دیدگاه مورد انتقاد برخی از فقهای معاصر گردیده است و در نقد این رویکرد آورده‌اند که اینکه مالیت شرط صحت بیع باشد، صحیح نیست؛ چراکه چه بسا چیزی مالیت نداشته باشد ولی برخی از افراد برای خرید آن تمایل داشته باشند، به عنوان مثال ممکن است نامه پدر بزرگ شخصی برای مردمان ارزش اقتصادی نداشته باشد، ولی برای شخص بسیار ارزشمند باشد و حاضر باشد پول هنگفتی بابت آن پردازد (خویی، بی‌تا، ج ۵، ص ۱۲۰/امام خمینی، ۱۴۲۱، ج ۳، ص ۸).

به نظر می‌رسد با توجه به اینکه امروزه داده‌های شخصی دارای ارزش اقتصادی هستند و بسیاری از کسب و کارها در ازای رضایت به پردازش داده‌های شخصی، به ارائه خدمات می‌پردازند؛ تعاریف مذکور بر داده‌های شخصی نیز صدق می‌کند؛ چراکه از یک طرف بنابر تعاریفی که بر ارزش اقتصادی شیء تکیه دارند، صدق مالیت بر داده‌های شخصی روشن است و بنابر تعاریفی که بر رغبت و حاجات مردم تکیه دارند، وجه صدق مال از آن جهت است که مردمان به واسطه آن (همان طوری که در مقدمه اشاره شد

امروزه داده به عنوان پول استفاده می شود) نیازهای خود را تأمین می کنند و از طرف دیگر، اگر هم کسی قائل به مالیت داده های شخصی نباشد، مطابق نظر برخی از فقهای معاصر، مالیت شرط صحت معامله نیست؛ چرا که انگیزه ها و اغراض اشخاص در خرید متفاوت است، چه بسا مالی باشد که کسی به آن وقعی نهد، حال آنکه دیگری حاضر باشد هزینه هنگفتی بابت آن بپردازد؛ لذا چه قائل به مالیت داده شخصی باشیم یا نه مانعی از تبادل داده شخصی نیست.

۴-۲. غیر قابل انتقال بودن داده شخصی

یکی دیگر از موانع حقوقی را می توان در نوع رویکرد به داده های شخصی مشاهده کرد. همان طوری که گفته شد، دو نوع رویکرد به داده های شخصی وجود دارد: رویکرد حقوق بشری و رویکرد اقتصادی. مطابق رویکرد بشری، حفاظت از داده های شخصی چون یکی از مصادیق حقوق بشر است، قابل مبادله و نقل و انتقال نیست. توضیح مطلب اینکه صاحب نظران طیفی از ویژگی ها را برای حقوق بشر مطرح می کنند از جمله جهان شمولی، سلب ناپذیری و تساوی. یکی از این ویژگی ها عدم قابلیت نقل و انتقال حقوق بشر است؛ زیرا حقوق بشر، جزء حق های ذاتی و طبیعی افراد است و حقی که از چنین خصایصی (ذاتی و طبیعی بودن) برخوردار باشد، کسی صلاحیت نقل و انتقال آن را ندارد (محسنی، ۱۳۹۴، ص ۴۴۴).

و از طرف دیگر بی شک نظام فقهی و حقوقی ما رویکرد حقوق بشری نسبت به داده های شخصی دارند؛ چون در برخی از مواد قانونی به نحو مجبیه جزئی از جمله اصل ۲۵ قانون اساسی و یا به نحو مجبیه کلیه از جمله ماده ۷۲۹ قانون مجازات اسلامی، ماده ۶ و ۱۴ قانون دسترسی و انتشار آزاد اطلاعات، داده های شخصی از حقوق اساسی افراد و حریم خصوصی افراد شمرده شده است (فاطمه قناد و سایر همکاران، ۱۴۰۰، ص ۱۴ به بعد) و از طرف دیگر بسیاری از صاحب نظران نیز بدان اذعان دارند (نوری، ۱۳۸۴، ص ۳۴).

در تأیید این نظر می‌توان به رویکرد لایحه «صیانت و حفاظت از داده‌های شخصی» اشاره کرد. در این لایحه در ماده (۱) (بخش یکم: هدف قانون) آمده است: «هدف اصلی این قانون صیانت از حیثیت و کرامت اشخاص موضوع داده‌ها از راه‌های ذیل است که قواعد و احکام آن‌ها در بخش‌های مربوط آمده است: الف) تبیین حقوق اشخاص موضوع داده‌ها، به‌ویژه در تعامل با سایر حق‌های مشروع؛ ...»، این ماده به‌وضوح هدف قانون را صیانت از حیثیت و کرامت اشخاص موضوع داده‌ها معرفی می‌کند؛ لذا از این حیث روشن می‌شود که تمایل قانون‌گذار به رویکرد حقوق اساسی است و رویکرد مالکیتی نسبت به داده‌های شخصی ندارد؛ همچنان که در مقدمه توجیهی، ارجاعات صورت گرفته، خصوصاً عمل به فتوای رهبری نسبت به حرمت نقض حریم خصوصی به‌خوبی این مسئله را نمایان می‌کند. در پاسخ به چالش مذکور پاسخ‌های متعددی داده شده است. برخی در پاسخ بدان گفته‌اند: داده‌های شخصی ذی‌الوجهین است؛ هم ارزش اقتصادی دارد و هم بخشی از حریم خصوصی افراد است و آنچه مورد تبادل و نقل و انتقال قرار می‌گیرد، ارزش اقتصادی آن است؛ گرچه به‌تبع آن ممکن است حریم خصوصی افراد نیز در دسترس قرار بگیرد؛ خصوصاً اینکه حریم خصوصی افراد نیز ممنوعیت مطلق ندارد، بلکه شخص می‌تواند با رضای خود آن را در معرض دیگران قرار دهد. (نگاه کنید به بخش نقد رویکرد حقوق مالکیتی و حقوق بشری)

۴-۳. مخالفت با اصل لزوم قراردادها

یکی دیگر از موانعی که ممکن است مخالفین مبادله داده‌های شخصی بدان متمسک شوند، مخالفت آن با اصل لزوم قراردادها است. مطابق اصل مذکور، اصل غیرقابل انحلال بودن قراردادها و لزوم اجرای مفاد قراردادهاست جز در موارد استثنایی همچون فسخ، اقاله و حکم قانون. اصل لزوم در مقابل جواز قرار دارد که به معنای انحلال عقد به اراده، فوت و

حجر است (شهیدی، ۱۳۹۶، ج ۲، ص ۲۵۳). این اصل مورد تصریح قانون مدنی ایران (ماده ۲۱۹) و فقه اسلامی است.

وجه مخالفت مبادله داده‌های شخصی را باید، در بازپس‌گیری رضایت عمومی حفاظت از داده‌های شخصی طیف وسیعی از مبانی قانونی برای مشروعیت پردازش در نظر گرفته است (ماده ۶ مقررات عمومی حفاظت از داده شخصی اتحادیه اروپا و ماده ۴ و ۵ لایحه صیانت و حفاظت از داده‌های شخصی). یکی از این مبانی رضایت موضوع داده است (بند یک ماده ۶ مقررات عمومی حفاظت از داده شخصی اتحادیه اروپا و ماده ۴ لایحه صیانت و حفاظت از داده‌های شخصی). در حالی که رضایت یکی از چندین زمینه قانونی موجود برای پردازش داده‌های شخصی تحت تمام مقررات حفاظت از داده‌ها است، بدون شک جهانی‌ترین استاندارد مشروعیت است و باعث ایجاد اعتماد کاربر می‌شود (Edwards, 2016, p.31).

اما این مبنا به گونه‌ای نیست که غیرقابل پس‌گیری باشد، بلکه کاربر می‌تواند رضایت خود را پس بگیرد؛ چراکه هنگامی که به افراد فرصت داده می‌شود تا با استفاده و بهره‌گیری از اطلاعات شخصی آن‌ها - به‌عنوان ابزار اصلی برای اعمال استقلال خود و حفاظت از حریم خصوصی خود - موافقت کنند، منطقی است که گزینه مربوطه برای پس‌گرفتن و لغو رضایت یا برای ایجاد تغییرات بعدی در آن رضایت وجود داشته باشد (Curren, 2010, p.273).

از این حق به‌عنوان حق «بازپس‌گیری رضایت» (right to withdraw) یاد می‌کنند (Curren, 2010, p.273) که در بند ۳ ماده ۷ GDPR بدان تصریح شده است؛ همچنان‌که بند «ه» ماده ۵۹ قانون تجارت الکترونیکی نیز از امکان حق محو داده‌های شخصی سخن می‌راند. گرچه این بند مربوط به محو داده‌های شخصی است، نه انصراف از رضایت ولی به‌هرروی

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)

متضمن مفهوم بازپس‌گیری رضایت نیز است. همچنین این حق در ماده ۸ لایحه صیانت و حفاظت از داده‌های شخصی شناسایی شده است. بند ۳ ماده ۷ مقرر می‌دارد: «۳. موضوع داده حق دارد تا هر زمان که می‌خواهد، رضایت خود را پس گیرد.» و ماده ۸ نیز مقرر می‌دارد: «شخص موضوع داده حق دارد هر زمان، پردازش یا عدم پردازش همه یا بخشی از داده‌ها را از کنترل‌گر بخواهد، مشروط بر آنکه: الف) داده‌ها یا نتایج حاصل از آنها نادرست باشد؛ ب) داده‌های یا پردازش آنها خارج از محدوده رضایت وی باشد».

بر طبق آنچه ذکر شد، وجه تباین در مقررات عمومی حفاظت از داده‌های شخصی اتحادیه اروپا روشن است؛ چراکه همان‌طوری که گفته شد، اگر فردی داده‌های شخصی خود را، خواه به‌عنوان عوض؛ یعنی در ازای ارائه محتوا یا خدمات دیجیتال ارائه دهد، خواه به‌عنوان معوض؛ یعنی مورد معامله و در جایگاه مژمن قرار گیرد، طبق ماده ۷ (۳) GDPR او حق دارد در هر زمان رضایت خود را پس بگیرد؛ بنابراین، اگر هیچ مبنای دیگری به‌غیر از رضایت (از میان مبنای پیش‌بینی‌شده در ماده ۶) برای جمع‌آوری و پردازش داده‌های شخصی فرد موردنظر وجود نداشته باشد، پردازش و جمع‌آوری باید متوقف شود. از طرف دیگر مطابق مقررات مذکور، حق بازپس‌گیری رضایت یک حق اساسی است؛ بنابراین، (در قالب شرط ضمن عقد) موضوع داده‌ها را نمی‌توان از پس گرفتن رضایت خود منع کرد، به‌تبع قانون‌گذار به ارائه‌دهنده خدمات یا محتوای دیجیتال حقی برای ادعای خسارت بر اساس نقض قرارداد نمی‌دهد (Langhanke, 2015, p.222).
بنابر آنچه گفته شد، این واقعیت که موضوع داده‌ها حق دارد رضایت خود را پس بگیرد با ماهیت الزام‌آور یک تعهد و قرارداد در تضاد است (Langhanke, 2015, p.221).

ممکن است گفته شود که در ادامه بند مذکور تصریح شده است که اثر این

بازپس‌گیری نسبت به ماسبق است نه مال‌حق: «بازپس‌گیری رضایت هیچ تأثیری بر روی قانونی‌بودن پردازش بر اساس رضایت، پیش از بازپس‌گیری ندارد»؛ لکن این تصریح نیز منافاتی با آنچه گفته شد، ندارد؛ چراکه اولاً اثربخشی حق مذکور نسبت به پردازش آینده با اصل لزوم قراردادهای سازگار نیست و ثانیاً کارگروه ماده ۲۹ بیان می‌کند که اگر دلایل قانونی دیگری برای توجیه استفاده و ذخیره‌سازی بیشتر از داده‌های موردنظر، وجود نداشته باشد باید توسط کنترل‌کننده داده حذف شود، لذا در صورت نبود دلایل قانونی دیگر و به تبع حذف داده‌ها از پایگاه‌ها، حتی آثار این حق نسبت به گذشته نیز سرایت پیدا می‌کند (Bedir, 2020, p.359).

در پاسخ به چالش مذکور باتوجه به مبانی فقهی و حقوقی می‌توان از تفاسیری که برخی از حقوق‌دانان از اصل لزوم قراردادهای ارائه کرده‌اند، بهره برد. برخی از حقوق‌دانان برای تبیین معیار لزوم و جواز در قراردادهای بر این عقیده هستند که وجود مصلحت‌کامنه در قراردادهای و عقود نشان می‌دهد که آیا آن عقد جایز است یا نه؟ مطابق این دیدگاه هر عقدی دارای مصالحی است که طبیعت آن عقد بر آن استوار است و این مصلحت نمایانگر وجهه الزام‌آور بودن یا نبودن عقود است. به‌عنوان مثال مقتضای مصلحت‌کامنه عقد بیع و معاوضه لازم بودن آن است (لنگرودی، ۱۳۸۷، ج ۴، ص ۱۳۷۹). با این نظریه، دیگر اصل الزام‌آور بودن عقود را نباید از احکامی دانست که از طرف شارع یا مقنن وضع شده است، بلکه باید در اعماق ماهیتی عقود جست. بنابر آنچه گفته شد، در مسئله موردنظر ما نیز جایز بودن قرارداد داده‌های شخصی را باید در مصلحت‌کامنه آن دانست؛ بدین نحو که داده‌های شخصی باتوجه به اینکه مربوط به حریم خصوصی و شخصیت افراد است، اقتضا می‌کند که با جایزشمردن آن از موارد سوءاستفاده افراد یا به‌خاطر افتادن اغراض و اهداف شخصی افراد جلوگیری کرد. به عبارت دیگر با جایزشمردن آن بخشی از نگرانی‌های کسانی

که به شدت نگران حریم خصوصی افراد هستند و بدین جهت سخت با تجاری‌سازی داده‌های شخصی مخالف هستند، تأمین می‌شود. از طرف دیگر بنابر مبنای برخی از فقها اصل جواز عقود است و لااقل بر مبنای این فقهیان مبادله داده‌های شخصی ناسازگار با قواعد عمومی قراردادها نیست (عاملی حسینی، بی‌تا، ج ۴، ص ۵۳۸).

۴-۴. مخالفت با اصل آزادی اراده

مخالفت با اصل آزادی اراده و حاکمیت آن یکی دیگر از جلوه‌های مخالفت مبادله داده شخصی با قواعد عمومی قراردادهاست. وجه مخالفت مذکور را باید در کاهش قدرت چانه‌زنی موضوع داده شخصی دانست؛ چراکه به واسطه نابرابری در قدرت چانه‌زنی طرف قوی قرارداد با تحمیل شرایط خود بر طرف ضعیف اراده، اراده طرف ضعیف را تحت تأثیر قرار می‌دهد (کاتوزیان، ۱۳۹۸، ج ۱، ص ۱۸۹).

در قرارداد داده‌های شخصی، عدم توازن در قدرت چانه‌زنی میان صاحب داده و پردازشگر مشاهده می‌شود؛ زیرا هنگامی که حق حریم خصوصی شخص موضوع داده نقض شود، این امر بر آزادی انتخاب موضوع داده در مورد اینکه چه قراردادهایی را منعقد کند و با چه شرایطی، تحت تأثیر قرار می‌گیرد که در نهایت استقلال طرف را تضعیف می‌کند (Bedir, 2020, p.360).

نبود قدرت چانه‌زنی به نوبه خود موضوع داده را در شرایط دوگانه قرار می‌دهد؛ از یک طرف نیاز به کالا و خدماتی دارد که پردازشگر قصد ارائه آن را دارد و از طرف دیگر در قبال این کالاها و خدمات ملزم به ارائه داده‌های شخصی است؛ لذا در میانه عدم افشای داده‌های شخصی و برطرف کردن نیازهای خود قرار می‌گیرد و ناچار است یا از نیازمندیهای خود بگذرد یا از داده‌های شخصی.

در پاسخ به این چالش نیز می‌توان گفت که بالعکس آنچه ادعا می‌شود،

قانون‌گذار با اعطای برخی از حقوق ویژه به موضوع داده و جانب‌داری عملی از وی قدرت چانه‌زنی موضوع داده را بیشتر کرده است و شناسایی حق انصراف از رضایت و یا حق بر فراموشی، موضوع داده را در موضع برتر و یا حداقل مساوی با پردازشگر قرار می‌دهد.

۴-۵. غرری بودن قرارداد داده‌های شخصی

یکی دیگر از مواردی که قرارداد داده‌های شخصی را با چالش جدی مواجه می‌سازد، غرری بودن مبادله داده‌های شخصی است. جلوه‌های غرری بودن این‌گونه قراردادها را می‌توان در حق موسوم به «حق بر فراموشی» مشاهده کرد.

امروزه ظرفیت رایانه‌های مدرن برای ذخیره همه‌چیز و هرگز فراموش کردن، همیشه به‌عنوان یک ویژگی خواستنی در نظر گرفته شده است. با این وجود تحقیقات گسترده نشان می‌دهد این ویژگی همیشه مطلوب نیست؛ چراکه سیستم‌های دیجیتالی که همه چیز را به‌یاد می‌آورند امروزه به تهدیدی جدی برای هویت بشر مبدل شده‌اند (Burkell, 2016, p.2). در این رابطه سولو می‌نویسد: «اطلاعاتی که زمانی پراکنده، فراموش‌شدنی و محلی شده بودند دائمی و قابل جستجو می‌شوند. از قضا، جریان آزاد اطلاعات تهدیدی برای تضعیف آزادی ما در آینده است. این دگرگونی‌ها تهدیدی برای کنترل افراد بر شهرت و توانایی آن‌ها برای تبدیل شدن به آن چیزی است که می‌خواهند باشند. هرچه افراد آزادی بیشتری برای انتشار اطلاعات آنلاین داشته باشند، احتمال بیشتری وجود دارد که اسرار خصوصی افراد به‌گونه‌ای فاش شود که مانع از فرصت‌های آن‌ها در آینده شود.» . (Solove, 2007, p.4) آسیب‌های مذکور نشان می‌دهد در فراموشی و فراموش شدن ارزش و نیاز وجود دارد. بنابراین، در زمینه سیستم‌های اطلاعاتی، ما باید فراموشی را به‌عنوان یک ویژگی در نظر بگیریم و از این رو، سعی کنیم از فناوری برای تقویت فراموشی در تعامل انسان و رایانه استفاده کنیم.

نگرانی‌ها و آسیب‌های مذکور و به تبع اهمیت روزافزون فراموشی، لزوم شناسایی حق بر فراموشی را فراهم کرد. به موجب حق فراموشی - که به طور اختصار (Rtbf) نامیده می‌شود - به فرد اجازه داده می‌شود تا داده‌های شخصی فرد بنا به درخواست او، از همه مکان‌های موجود که ممکن است منتشر شده باشند، پاک شوند (Politou, 2018, p.1).

این حق در بسیاری از مقررات مرتبط با داده‌ها و اطلاعات به طور ضمنی یا صریح شناسایی گردیده است؛ از جمله در بند ۱ ماده ۱۷ GDPR که مقرر می‌دارد: «۱. موضوع داده حق دارد تا از کنترل‌کننده بخواهد که داده‌های شخصی مربوط به خود را بدون هیچ‌گونه تأخیر غیرمنطقی پاک کند و کنترل‌کننده نیز ملزم است تا داده‌های شخصی را در صورتی که یکی از موارد زیر مصداق داشته باشد، بدون تأخیر غیرمعقول پاک کند...».

در حقوق ایران نیز، حق بر فراموشی در قوانین فعلی مورد تصریح قرار نگرفته است؛ لکن برخی از نویسندگان با استنباط از ماده ۵۸ و ۵۹ قانون تجارت الکترونیکی چنین حقی را در حقوق ایران پیش‌بینی کرده‌اند (درافشان و سایر همکاران، ۱۳۵۹، ص ۲۴).

باین وجود در ماده (۹) پیش‌نویس لایحه صیانت و حفاظت از داده شخصی این حق به صراحت پیش‌بینی است: «درخواست انجام یا توقف پردازش داده‌های شخصی می‌تواند با هدف فراموشی مطرح شود، مشروط بر آنکه ذی‌نفع دیگری نباشد.»

وجه غرری بودن باتوجه به حق بر فراموشی این است که با اعطای حق فراموشی به موضوع داده، هر آن ممکن است وی این حق را اعمال کند؛ در نتیجه طرف مقابل عقد مابه‌ازای معامله را از دست بدهد. بنابراین درجایی که داده شخصی در مقام عوض باشد، وی عوض را از دست می‌دهد و درجایی که در مقام معوض باشد، به‌واقع میباید از دست می‌دهد. از این حیث، مسئله مورد نظر می‌توان به موردی که متعاقدين جعل خیار می‌کنند

ولی مدت خیار مجهول باشد، تشبیه کرد. در صورتی که مدت خیار تعیین نشده باشد، فقها، آن را غرری و معامله را باطل می‌دانند.

به نظر می‌رسد با توجه به کارکردهای داده شخصی غرری بودن این گونه معاملات مضر نیست؛ چراکه کارکرد عمده داده‌های شخصی برای تبلیغات و شناسایی ذائقه افراد است و با ارائه داده‌های شخصی به اشخاص حقیقی و حقوقی، نیازهای مورد نظر آن‌ها از جمله ذائقه افراد را تأمین می‌کنند؛ در نتیجه ولو اینکه صاحب داده از حق فراموشی خود استفاده کند، این حق بر فراموشی شامل اطلاعات استخراجی از این گونه داده‌ها نمی‌شود.

به عنوان مثال، فرض کنید شرکتی از بانوان داده‌های شخصی آن‌ها را می‌خرد و آن‌ها نیز موافقت می‌کنند تا بفروشند، در این صورت این گونه شرکت‌ها ذائقه بانوان را مثلاً در نوع پوشش خود به دست می‌آورند و دیگر اصلاً نیازی به داده‌های بانوان ندارند؛ چراکه هدف آن‌ها شناسایی ذائقه بانوان است و داده‌ها بالأصله هدف اصلی نیست.

از طرف دیگر اشکال مذکور در همه عقود جایز نیز وارد است؛ به عنوان مثال عقد مضاربه که عامل با درخواست صاحب سرمایه اقدام به تجارت می‌کنند، هر آن در معرض فسخ عقد از طرف صاحب سرمایه است، باین وجود کسی در جواز و مشروعیت این عقد مناقشه نکرده است.

۴-۶. عدم صدق مبیع بر داده‌های شخصی

ممکن است که برخی اشکال کنند که برحسب ماده ۳۸۸ قانون مدنی که مقرر می‌دارد: «بیع عبارت است از تملیک عین به عوض معلوم»، عین باید معین باشد؛ همچنان که برخی از فقها با استناد به تعریف عرفی بیع، صحت و تبادر سلب (انصاری، ۱۴۱۵، ج ۳، ص ۷/خویی، بی تا، ج ۲، ص ۱۱) بر لزوم عین بودن مبیع در بیع تأکید دارند. داده‌های شخصی نیز با توجه به اینکه جزء اعیان شمرده نمی‌شوند، در نتیجه نمی‌توان آن‌ها را به خرید و فروش رساند.

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)

در پاسخ به این اشکال می‌توان که اولاً بسیاری از فقہیان معاصر این دیدگاه را رد کرده‌اند (امام خمینی (ره)، ۱۴۲۱، صص ۳۱-۳۲)، ثانیاً با فرض پذیرش، این اشکال منحصر در بیع خواهد بود ولی نسبت به سایر قراردادها نافذ نخواهد بود.

۴-۷. پاسخ کلی به چالش‌های مذکور؛ چالش قواعد عمومی قراردادهای کلاسیک و قراردادهای نوظهور

وجود طیف گسترده از قراردادها یکی از عمده مشکلاتی است که فقہا و حقوق‌دانان با آن مواجه هستند؛ چراکه بخش قابل توجهی از احکام و شرایط این‌گونه قراردادها با قواعد عمومی قراردادها سازگار نیستند. چالش مذکور صرفاً در زمان حاضر نبوده، بلکه در زمان‌های گذشته نیز بوده است.

به‌عنوان مثال موارد متعددی را می‌توان مشاهده کرد که با وجود غرری بودن، فقہیان آن را جایز شمرده‌اند، مانند عقد قبالة که در آن مجموع میوه تخمین زده می‌شود و شریک با توجه به تخمین مذکور، این میوه‌های تخمینی را در مقابل عوضی معین از شریک خود می‌ستاند (شهید ثانی، بی‌تا، ج ۳، ص ۳۶۸) یا همچنان که در دوره معاصر بیمه باوجود غرری بودن و حکم به بطلان آن از طرف برخی از صاحب‌نظران، مشهور صاحب‌نظران آن را پذیرفته‌اند (مسجدسرای، ۱۳۹۲، ص ۱۴۴).

یا همچنان که در قانون قراردادهای کار، شورای نگهبان، با استناد به اینکه برخی از شروط قانون کار مانند ساعت کاری معین، میزان دستمزد معین، بیمه کارگر و موارد دیگر، خلاف آزادی اراده متعاقدین است، قانون کار را غیرشرعی تشخیص می‌دهد و در آخر نیز با قید مصلحت توسط مجمع تشخیص مصلحت نظام به تصویب رسید (آهنگری، ۱۲، ص ۳۱۴).

بنابر آنچه گفته شد، روشن است که نباید به قواعد عمومی قراردادهای به‌عنوان امری ثابت و لایزال نگاه کرد، بلکه چه‌بسا به‌مرور زمان قراردادهایی با شرایط ویژه‌ای به‌وجود بیاید که نتوان آن را در قالب قواعد عمومی قراردادها

گنجانند، بلکه نیازمند تدوین قوانین خاص است؛ لذا معمول و مرسوم است که در کنار قوانین مادر قوانینی خاصی همچون قانون قرارداد کار یا قانون بیمه و غیره تدوین و تصویب می‌شود و یا همچنان که برای عقود معین شرایط و مقررات منحصری نوشته می‌شود و یا همچنان که بسیاری از فقیهان برخی از قراردادها را به‌عنوان استثناء بر قواعد عمومی پذیرفته‌اند. ریشه پذیرش قوانین خاص و استثنا بر قواعد عمومی قراردادها را باید در فلسفه معاملات جست. بنابر نظر مشهور فقیهان معاملات از قبیل امور اعتباری و عقلایی است؛ لذا برخی از فقیهان صراحتاً تنظیم امور معیشتی مردم را از اهداف معاملات دانسته‌اند. به‌عنوان مثال شهید اول می‌فرماید: کل حکم شرعی یکون الغرض الأهم منه الدنيا ... یسمی معامله... (شهید اول، بی‌تا، ج ۱، ۳۵). یا همچنان که علامه بحرالعلوم در مصابیح الأحكام می‌نویسد: «لأن المعاملات شرعت لنظام أمر المعاش المطلوب لذاته، و لتوقف أمر المعاد علیه، و هی مشار الاختلاف، و منشأ النزاع و التراجع» (مصابیح الاحکام، نسخه خطی، موجود در کتابخانه مجلس، شماره برگه: ۱۱۷، قابل دانلود از کتاب بديا). یا همچنان که جناب مامقانی در غایه‌الآمال می‌نویسد: «کون المعاملات قد شرعت لنظام أمر المعاشی المطلوب لنفسه و توقف أمر المعاد علیه و لما كانت منشأ الاختلاف و التنازع و الترافع و جب ضبطها بالأمر» (ج ۲، ص ۲۳۴).

بنابر آنچه گفته شد، غرض عقلای عالم از جعل احکام معاملی تنظیم امور معیشتی و دنیوی مردمان است، لذا اگر قراردادهای نوظهوری که در جهت تنظیم امور معیشتی و دنیوی است، به‌وجود بیاید، به‌صرف مخالفت آن با قواعد عمومی قراردادها نباید نامشروع دانست، بلکه شایسته است با حفظ شرایط آن قرارداد و تدوین قوانین ویژه و انسجام‌دهی به آن به‌مانند بسیاری از قوانین خاص و استثنایی، آن را به‌رسمیت شناخت.

بنابر آنچه گفته شد، سزاوار است، قراردادهای داده‌های شخصی نیز در

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران) ■

این فضای انعطاف‌پذیر دیده شود و از آن جهت که وجود داده‌های شخصی برای توسعه اقتصادی و معیشتی مردمان ضروری است و از این حیث در جهت اهداف تشریع معاملات حرکت می‌کند، لذا مشروعیت‌دهی به آن موجه است.

بنابر آنچه گفته شد، به نظر می‌رسد مبادله داده‌های شخصی از منظر حقوق قراردادهای ایران و فقه اسلامی امکان‌پذیر است. در تأیید این نظر می‌توان به موضع‌گیری لایحه حفاظت و صیانت از داده‌های شخصی اشاره کرد.

ماده (۱۳) لایحه، پردازشگران را با حفظ شرایطی مالک داده‌ها معرفی می‌کند، به تبع امکان تبادل برای آن‌ها فراهم است. این ماده مقرر می‌دارد: «بهره‌برداری مالکانه از داده‌های شخصی، بدون رضایت شخص موضوع آن‌ها در صورتی بلامانع است که: الف) گمنامی وی حفظ شود؛ ب) عرفاً زیان مادی یا معنوی برای وی نداشته باشد؛ پ) جلب رضایت وی عملاً امکان‌پذیر نباشد.»

در این ماده به صراحت بهره‌برداری مالکانه و به تبع تجاری‌سازی را با حفظ شروط سه‌گانه به پردازش‌کنندگان داده است؛ لذا این شرکت‌ها با حفظ این شروط می‌توانند این داده‌ها را به دیگران بفروشند یا سایر معاملات را انجام دهند؛ همچنان که در ماده (۲۶) لایحه آمده است که پردازشگر باید اهداف پردازش را به موضوع داده ارائه دهد، یکی از اهدافی که در این ماده پیش‌بینی شده است، اهداف اقتصادی است؛ لذا با توجه به دو ماده شکی باقی نمی‌ماند که پردازشگران امکان تبادل تجاری داده‌ها را دارند.

باین حال، به نظر می‌رسد سکوت قانون‌گذار نسبت به امکان قانونی مبادله تجاری از طرف موضوع داده، مانعی برای امکان تبادل داده برای صاحب داده نباشد؛ چراکه از یک طرف منش قانون‌گذار ایران در تدوین این

لایحه منطبق با GDPR است؛ همچنان که در بسیاری از کشورها دیده می‌شود و از طرف دیگر محدودیت‌هایی از قبیل «ضروری برای آزادی قرارداد» و «رضایت آزادانه» - که در GDPR ملاحظه می‌شود - تشریح نشده است و آزادی اراده بسیاری به صاحب داده‌های شخصی داده است؛ لذا موضوع داده می‌تواند، با اعطای رضایت به پردازش داده (مواد ۴ تا ۷)، در ازای ارائه خدمات، داده‌های خود را در اختیار پردازشگران قرار دهد.

نتیجه

امروزه جهان قراردادها با توسعه فناوری و اطلاعات متحول می‌شود و ساحت‌های گوناگونی را تجربه می‌کند؛ همگام نشدن با این تحولات و واقعیات، خواه به خاطر عدم پذیرش ما باشد یا به خاطر سایر جهات باشد، به زودی ما رو مجبور به پذیرش خود خواهد شد و نتیجتاً چیزی جزء ایجاد مشکلات ناشی از همگام نشدن با این تحولات عاید ما نخواهد شد.

مسئله مبادله داده‌های شخصی را نیز باید در راستای تحولات قراردادها تحلیل کرد و باید این واقعیت را بپذیریم که مبادله داده‌های شخصی در بسترهای متعدد - خصوصاً در بستر فضای مجازی - واقع می‌شود. به عنوان مثال ساده‌ترین جلوه تبادل را باید در تخفیفات در قبال داده شخصی دانست که به وفور در معاملات بستر فضای مجازی دیده می‌شود.

مبادله داده‌های شخصی بستری برای دوشاخه از علم حقوق است: حقوق بشر و حقوق قرارداد؛ بستر حقوق بشری آن ناظر بر حریم خصوصی است و بستر حقوق قراردادی آن ناظر بر مبادله است؛ در کشاکش این دوشاخه، برخی با افراط در نگرانی‌های به حق در حوزه حریم خصوصی، علی‌الاطلاق جانب حقوق بشر را گرفته است و برخی با نگاه صرف و افراطی اقتصادی به داده‌های شخصی که بی‌شک عاملی بسیار حیاتی در توسعه اقتصاد است، جانب حقوق قراردادها را گرفته‌اند، بدون اینکه نگران حریم خصوصی افراد

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)

باشند و یا اهمیتی بدان دهند. در کشاکش این دعوا برخی راه میانه گرفته‌اند؛ گرچه همچنان نگاه حقوق بشری را غالب می‌دانند. اتحادیه اروپا را می‌توان نمونه بارز دیدگاه اخیر دانست. در مقررات عمومی حفاظت از داده اتحادیه اروپا رویکرد کالا محوری نسبت به داده‌های شخصی ممنوع شده است، چراکه رویکرد اتحادیه اروپا به داده شخصی حقوق بشری است، لکن با وجود چنین رویکردی، امکان تبادل داده‌های شخصی به صورت مضیق فراهم شده است. امکان تبادل داده شخصی در این مقررات نشان می‌دهد که قانون‌گذار اروپا نتوانسته است ضرورت اقتصاد داده را انکار کند و به نوعی با اعطای تبادل مضیق خواسته است که خود را با ضرورت‌های اقتصادی جهان هماهنگ سازد و به واقع عملاً به عملکرد دوگانه (عملکرد اقتصادی و غیراقتصادی) در برخی از داده‌ها (داده‌های غیر حساس) اذعان و از مطلق‌انگاری در این حوزه پرهیز کرده است.

در حقوق ایران نیز، گرچه با تصویب قانون تجارت الکترونیکی و تدوین پیش‌نویس لایحه «حفاظت از داده‌های شخصی» گام‌های برداشته شده است، ولی هم در قانون تجارت الکترونیکی تکلیف مبادله داده شخصی روشن نشده است و هم در لایحه مذکور جوانب مسئله به خوبی روشن نگشته است. لذا با توجه به اهمیت مبادله داده‌های شخصی در بستر فضای مجازی لازم است مقررات ویژه‌ای با رویکرد ترکیبی به حقوق بشر و حقوق قراردادها تدوین و تصویب شود. این مقررات ویژه باید شامل مراحل چگونگی انعقاد قرارداد (شامل ایجاب و قبول و ضوابط آن) و شرایط صحت آن (از جمله وجود حق فراموشی یا انصراف از رضایت، تعیین دقیق محدوده داده‌های شخصی) در حوزه مبادله داده شخصی موضوع داده با شرکت‌های پردازشگر و مبادله داده شخصی میان موضوع داده شخصی و سایر اشخاص حقوقی و مبادله داده شخصی میان اشخاص حقیقی باشد.

حال با توجه به نبود مقررات وافی و کافی در حقوق ایران، لاجرم باید به

سراغ قواعد عمومی قراردادها رفت. به نظر می‌رسد باتوجه به مالیت داشتن داده‌های شخصی و عدم مخالفت آن با سایر قواعد عمومی قراردادها این مبادله مشروع و قانونی است.

حامی مالی

بنا به اظهار نویسنده مسئول، این مقاله حامی مالی نداشته است.

سهام نویسندگان در پژوهش

تمام نویسندگان در نگارش مقاله مشارکت یکسان داشته‌اند و محتوای آن را تأیید میکنند.

تضاد منافع

نویسنده (نویسندگان) اعلام می‌دارند که هیچ تضاد منافی در رابطه با نویسندگی و یا انتشار این مقاله ندارند.

منابع

- آهنگری، احسان، مومنی، عابدین؛ «مبانی فقهی الزامات خارج از توافق در قرارداد کار»، پژوهشنامه حقوقی اسلامی، ش ۵۴، پاییز و زمستان ۱۴۰۰، ص ۳۱۳-۳۳۶.
- امامی، سیدحسین؛ حقوق مدنی؛ ج ۱، چ ۲، تهران: انتشارات کتاب فروشی اسلامیة، ۱۳۷۷ ش.
- انصاری دزفولی، شیخ مرتضی بن محمد امین؛ کتاب المکاسب؛ ج ۴، چ ۱، قم: کنگره جهانی بزرگداشت شیخ اعظم انصاری، ۱۴۱۵ ق.
- ایروانی، علی بن عبدالحسین نجفی؛ حاشیة المکاسب؛ ج ۱، تهران: وزارت فرهنگ و ارشاد اسلامی، ۱۴۰۶ ق.
- بجنوردی، سید میرزا حسن؛ القواعد الفقهیه؛ ج ۲؛ چ ۱، قم: دارالکتب العلمیه، ۱۳۸۹ ق.
- بحر العلوم، سید محمد مهدی؛ مصابیح الاحکام؛ نسخه خطی، موجود در کتابخانه مجلس (قابل دانلود از کتاب بدیا).
- جعفری لنگرودی، محمدجعفر؛ الفارق؛ تهران: گنج دانش، ۱۳۷۹ ش.
- خمینی، سید روح الله؛ کتاب البیع؛ ج ۳، چ ۱، تهران: مؤسسه تنظیم و نشر آثار امام خمینی، ۱۴۲۱ ق.
- خویی، ابوالقاسم؛ مصباح الفقاهة؛ ج ۲ و ۵، چ ۱، بی‌جا، بی‌تا.
- شهید اول، محمد بن مکی؛ القواعد والفوائد؛ ج ۱، قم: کتابفروشی مفید، بی‌تا.

مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)

- شهید ثانی، زین الدین؛ *الروضه البهیه فی شرح المععه الدمشقیه*؛ بی جا، بی تا.
- شهیدی، مهدی؛ *اصول قراردادها و تعهدات*؛ ج ۷، تهران: مجد، ۱۳۹۶ ش.
- شهیدی، مهدی؛ *حقوق مدنی ۳- تعهدات*؛ ج ۲، تهران: انتشارات مجد، ۱۳۸۷ ش.
- طوسی، ابوجعفر محمد بن حسن؛ *المبسوط فی فقه الامامیه*؛ ج ۸، چ ۱، تهران: مکتب المرتضویه لاحیاء الآثار الجعفریه، ۱۳۸۷ ق.
- عاملی حسینی، سیدجواد؛ *مفتاح الکرامه (طبع قدیم)*؛ ج ۴، چ ۱، بیروت: دار احیاء التراث العربی، بی تا.
- قبولی درافشان، سید محمد هادی، بختیاروند، مصطفی و خوانساری، سمانه؛ «حق شهرت مطالعه در حقوق آمریکا، کوشش برای شناسایی در فقه امامیه و ساماندهی آن در حقوق ایران»؛ *مطالعات حقوق خصوصی*، ۴۸ (۱)، بهار ۱۳۹۷، ۱۳۳-۱۵۱.
- کاتوزیان، ناصر؛ *قواعد عمومی قراردادها*، ج ۱، چ ۲؛ تهران: گنج دانش، ۱۳۹۸ ش.
- لطیف زاده مهدیه، قبولی درافشان سید محمد مهدی، محسنی سعید، عابدی محمد؛ «تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا»؛ *پژوهشنامه پردازش و مدیریت اطلاعات*، ۳۷ (۲)، زمستان ۱۴۰۰، ص ۴۳۹-۴۷۲.
- مامقانی، محمدحسن؛ *غایة الآمال فی شرح کتاب المکاسب*؛ ج ۱، قم: مجمع الذخائر الاسلامیه، ۱۳۱۶ ق.
- محسنی؛ محمدسالم؛ «نقد و بررسی ویژگی‌های حقوق بشر»؛ *همایش علوم انسانی اسلامی*، ۱۳۹۴، ص ۴۳۱-۴۵۴.
- محقق داماد، سیدمصطفی؛ *قواعد فقه*؛ ج ۴، چ ۲، تهران: مرکز نشر علوم اسلامی، ۱۴۰۶ ق.
- مسجدسرابی، حمید؛ «تحلی فقهی حقوقی مبنای غرر در بیمه»؛ *پژوهش‌های فقه و حقوق اسلامی*، ش ۳۳، پاییز ۱۳۹۲، ۱۳۱-۱۴۴.
- مظفر، محمدرضا؛ *حاشیة المظفر علی المکاسب*؛ ج ۱، چ ۲، قم: حبیب، بی تا.
- میرشکاری، عباس؛ «بهره برداری تجاری از شهرت ورزشکاران در نظام های حقوقی آمریکا، انگلستان و ایران»؛ *دیدگاه‌های حقوق قضایی*، ۲۴ (۸۸)، زمستان ۱۳۹۸، ص ۱۴۱-۱۶۴.
- نوری، محمد علی؛ *حقوق حمایت داده‌ها*، تهران: گنج دانش، ۱۳۸۴ ش.
- Abraham, Tony. (2015). Consumers as Data Brokers: Should They Sell Their Own Personal Data?
- Article 29 Working Party, Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018.
- Bedir, Cemre. (2020). Contract Law in the Age of Big Data. European Review of Contract Law Volume 16 Issue 3. Retrieved from. <https://www.degruyter.com/document/doi/10.1515/ercl-2020-0020/html>.

- Bojana Kostic; Emmanuel Vargas Penagos (2017). the freely given consent and the “bundling” provision under the GDPR.
- Bottis, M. and Bouchagiar, G. (2018). Personal Data v. Big Data: Challenges of Commodification of Personal Data. *Open Journal of Philosophy*, 8, 206-215. Doi: 10.4236/ojpp.2018.83015.
- Burkell, Jacquelyn A., “Remembering Me: Big Data, Individual Identity, and the Psychological Necessity of Forgetting” (2016). FIMS Publications.
- Carleton Athey, Susan and Catalini, Christian and Tucker, Catherine E. (April 8, 2018). The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. MIT Sloan Research Paper No. 5196-17, Stanford University Graduate School of Business Research Paper No. 17-14, Available at SSRN: <https://ssrn.com/abstract=2916489> or <http://dx.doi.org/10.2139/ssrn.2916489>.
- Carmen Langhanke, M. Schmidt-Kessel. (2015). Consumer Data as Consideration. *Journal of European Consumer and Market law*.
- Curren L, Kaye J. Revoking consent: a ‘blind spot’ in data protection law? *Comp L & Sec Rev* 2010; 26:273–83.
- Dorothy J. Glancy. (2016). Personal Information as Intellectual Property. Retrieved from. https://www.law.berkeley.edu/files/bclt_IPSC2010_Glancy2.pdf.
- Edwards L. Privacy, security and data protection in smart cities: a critical eu law perspective. *Eur Data Prot L Rev* 2016; 2:28.
- Elvy, Stacy-Ann. (October 25, 2017) Paying for Privacy and the Personal Data Economy. *Columbia Law Review*, Vol. 117, No. 6, Available at SSRN: <https://ssrn.com/abstract=3058835>.
- Eugenia Politou and others, Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, *Journal of Cybersecurity*, Volume 4, Issue 1, 2018, ty001, <https://doi.org/10.1093/cybsec/ty001>.
- Galli, Ermes. (2021). The commodification of our digital identity. Retrieved from. https://www.filodiritto.com/commodification-our-digital-identity#_ftn47.
- Gates, Carrie; Matthews, Peter. (2014)..Data Is the New Currency. Retrieved from. <https://www.nspw.org/papers/2014/nspw2014-gates.pdf>.
- Hart, HLA. (1955). Are there any natural rights? *The Philosophical Review* 64(2): 175–191.
- Jerry, Kang. (2004). Information Privacy in Cyberspace Transactions. Avail-

able at SSRN: <https://ssrn.com/abstract=631723>.

Lauren Henry Scholz. (2016). Privacy as Quasi-Property, 101 Iowa L. Rev. 1113, Available at: <https://ir.law.fsu.edu/articles/418>.

McDermott, Yvonne. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society* January-June 2017: 1-7. Retrieved from: <https://journals.sagepub.com/doi/full/10.1177/2053951716686994#bibr212053951716686994>.

Metzger, Axel. (2017). Data as Counter-Performance: What Rights and Duties do Parties Have, 8 JIPITEC 2 para 1.

Murphy, R. S. (1996). "Property Rights in Personal Information: An Economic Defence of Privacy" *Geo. L.J.* 2381, pp. 2383-84

Purtova, Nadezhda. (October 25, 2009). Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation. *European Journal of Legal Studies* 2:3, 2010, Available at SSRN: <https://ssrn.com/abstract=2363634>.

Purtova, Nadezhda. Property Rights in Personal Data: Learning from the American Discourse (February 17, 2010). *Computer Law & Security Review*, Vol. 25, No. 6, pp. 507-521, 2009, Available at SSRN: <https://ssrn.com/abstract=1554341>.

Rodotà, S. (2009). Data Protection as a Fundamental Right. In: Gutwirth, S., Pouillet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) *Reinventing Data Protection?*. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-9498-9_3.

Rose, Blaire. (2021). The commodification of personal data and the road to consumer autonomy through the CCPA, 15 *Brook. J. Corp. Fin. & Com. L.* 521.

Samuelson, Pamela. (2000). Privacy As Intellectual Property? *Stanford Law Review* Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm?, pp. 1125-1173.

Schwartz, Paul M. Property, Privacy, and Personal Data. Available at SSRN: <https://ssrn.com/abstract=721642>.

Solove DJ. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. Yale University Press, 2007.

Stanford Encyclopedia of Philosophy (2020). Rights. Retrieved from: <https://plato.stanford.edu/entries/rights/>.

Taştan, Furkan Güven. (2021). The (im)possibility of personal data as an object of contracts: An analysis of the GDPR and the Digital Content Directive. Master's Degree Programme Law and Technology.

Van der Sloot, Bart. (2017). Legal fundamentalism: Is data protection really a fundamental right. *Data protection and privacy: (In) visibilities and infrastructure*. Editor / Ronald Leenes; Rosamunde van Brakel; Serge Gutwirth; Paul De Hert. Dordrecht: Springer. pp. 3-30 (Law, Governance and Technology Series). (Issues in Privacy and Data Protection).

Vera, Bergelson.2003)). It's Personal But is it Mine? Toward Property Rights in Personal Information. *UC Davis Law Review*, Vol. 37, No. 379, Available at SSRN: <https://ssrn.com/abstract=870070>.

ying, HU. (2021).Private and Common Property Rights in Personal Data. (173-201).