



University of Tabriz

Contemporary Comparative Legal Studies

Online ISSN: 2821-0514

Volume: 17 Issue: 42

Spring 2026

Article Type: Research Article

Pages: 149-185

A Study on the Conflict Between the Right to Personal Data and the Right to Trade Secrets

Amir Mohammad Ghorbannia¹ | Zahra Shakeri²

1. PhD Candidate in International Trade and Investment Law, Shahid Beheshti University, Tehran, Iran
amir.ghorbannia@ut.ac.ir
2. Associate Professor, Department of Law, University of Tehran, Iran (Corresponding Author)
zshakeri@ut.ac.ir

Abstract

With the growing use of personal data in commercial processes, the conflict between individuals' rights to their personal data and the rights of trade secret holders has emerged as a novel challenge in the field of technology and data law. In many cases, personal data, such as customer lists, behavioral preferences, or purchase histories, are treated as strategic assets within the framework of corporate trade secrets. On the other hand, data subjects enjoy rights such as access, portability, and erasure of their data, which may conflict with confidentiality obligations and the competitive interests of companies. This raises a fundamental legal question: in cases of conflict between the right to personal data and the right to protect trade secrets, how can a fair and balanced legal solution be achieved? This article adopts a descriptive-analytical approach based on library sources to explore this tension. It analyzes relevant domestic and international regulations and seeks to propose solutions for balancing data transparency with commercial confidentiality. The findings suggest that neither right takes absolute precedence over the other, and that mechanisms such as data pseudonymization, limited access, and case-by-case assessments may provide practical grounds for resolving these conflicts.

Keywords: Contrast Between Transparency and Confidentiality, Data Subjects Rights, Personal Data, Privacy, Trade Secrets.

Received: 2025/08/18 Received in revised form: 2026/05/10 Accepted: 2026/06/01 Published: 2026/06/10

DOI: 10.22034/LAW.2026.68716.3521

Publisher: University of Tabriz

law@tabrizu.ac.ir





جستاری در تعارض میان حق بر داده‌های شخصی و حق بر اسرار تجاری

امیرمحمد قربان‌نیا^۱ | زهرا شاکری^۲

amir.ghorbannia@ut.ac.ir
zshakeri@ut.ac.ir

۱. دانشجوی دکتری حقوق تجارت و سرمایه‌گذاری بین‌المللی، دانشگاه شهید بهشتی، تهران، ایران
۲. دانشیار گروه حقوق، دانشگاه تهران، ایران (نویسنده مسئول)

چکیده

با گسترش روزافزون استفاده از داده‌های شخصی در فرایندهای تجاری، تقابل میان حقوق اشخاص بر داده‌های خود و حقوق دارندگان اسرار تجاری، به یکی از چالش‌های نوپدید در عرصه حقوق فناوری و داده تبدیل شده است. در بسیاری از موارد، داده‌های شخصی مانند فهرست مشتریان، ترجیحات رفتاری یا اطلاعات خرید، به‌مثابه دارایی‌های راهبردی در نظام اسرار تجاری شرکت‌ها تلقی می‌شوند. از سوی دیگر، اشخاص موضوع داده از حقوقی همچون دسترسی، انتقال و حذف داده‌ها برخوردارند که ممکن است با الزامات محرمانگی و منافع رقابتی شرکت‌ها در تضاد قرار گیرد. در چنین وضعیتی، این پرسش اساسی مطرح می‌شود که در صورت تعارض میان حق افراد بر داده‌های شخصی خود و حق شرکت‌ها بر حفظ اسرار تجاری، چگونه می‌توان به توازن حقوقی و منصفانه دست یافت؟ نگارندگان مقاله حاضر با روش توصیفی-تحلیلی و بر پایه منابع کتابخانه‌ای، به بررسی این تعارض می‌پردازند و ضمن تحلیل مقررات مرتبط در اسناد داخلی و بین‌المللی، تلاش می‌کنند راهکارهایی برای موازنه میان شفافیت داده‌ای و محرمانگی تجاری ارائه دهند. یافته‌های تحقیق نشان می‌دهد که هیچ‌یک از این دو حق به‌صورت مطلق مقدم بر دیگری نیست و راه‌حلی هم‌چون مستعارسازی داده‌ها، دسترسی محدود و ارزیابی موردی می‌تواند در عمل، مبنایی برای رفع این تعارض‌ها فراهم سازد.

واژگان کلیدی: اسرار تجاری، تقابل شفافیت و محرمانگی، حریم خصوصی، حقوق اشخاص موضوع داده، داده‌های شخصی.

تاریخ دریافت: ۱۴۰۴/۰۵/۲۷ تاریخ بازنگری: ۱۴۰۵/۰۲/۲۰ تاریخ پذیرش: ۱۴۰۵/۰۳/۱۱ تاریخ انتشار: ۱۴۰۵/۰۳/۲۰

DOI: 10.22034/LAW.2026.68716.3521



law@tabrizu.ac.ir

ناشر: دانشگاه تبریز

مقدمه

در عصر داده‌محور کنونی، اطلاعات شخصی افراد به یکی از مهم‌ترین دارایی‌های نامشهود شرکت‌ها تبدیل شده است. استفاده از داده‌های شخصی در فرایندهای اقتصادی، به‌ویژه در قالب تحلیل‌های رفتاری، پیش‌بینی ترجیحات مشتریان و شخصی‌سازی خدمات، موجب شده است تا مرز میان داده‌های فردی و اطلاعات تجاری روزبه‌روز مبهم‌تر شود. در بسیاری از موارد، داده‌های متعلق به اشخاص، نظیر فهرست مشتریان، سوابق خرید، اطلاعات تماس یا تحلیل‌های مبتنی بر الگوهای رفتاری، نه تنها نقش کلیدی در موفقیت تجاری شرکت‌ها دارند، بلکه در چارچوب حقوق اسرار تجاری نیز به عنوان اطلاعات محرمانه دارای ارزش اقتصادی مشمول حمایت قرار می‌گیرند.

این درهم‌تنیدگی داده‌های شخصی با دارایی‌های اطلاعاتی شرکت‌ها، زمینه‌ساز بروز چالش‌های حقوقی تازه‌ای شده است؛ به‌ویژه آنگاه که افراد در چارچوب مقررات مربوط به حمایت از داده‌های شخصی، خواستار اعمال حقوق خود، از جمله دسترسی، اصلاح، حذف یا انتقال داده می‌شوند، اما شرکت‌ها با استناد به ضرورت حفظ محرمانگی و رقابت‌پذیری، از افشای این داده‌ها خودداری می‌کنند.

اهمیت پرداختن به این مسئله در این است که از یک سو، حمایت از داده‌های شخصی مبتنی بر حقوق بشر، با کرامت انسانی، حریم خصوصی و آزادی‌های بنیادین افراد در پیوند مستقیم است؛ و از سوی دیگر، حمایت از اسرار تجاری نیز سنگ بنای رقابت سالم و نوآوری در محیط اقتصادی به‌شمار می‌رود. ناتوانی در تبیین مرزهای دقیق این دو حوزه می‌تواند به تضعیف حقوق اشخاص یا اخلال در منافع مشروع شرکت‌ها منجر شود و اعتماد عمومی به نظام‌های حقوقی را خدشه‌دار سازد. افزون بر این، مقررات مختلف در نظام‌های حقوقی گوناگون، به‌ویژه در اسناد بین‌المللی یا منطقه‌ای نظیر مقررات عمومی حفاظت از داده‌های اتحادیه اروپا و دستورالعمل اسرار تجاری اتحادیه اروپا یا قانون اسرار تجاری امریکا، چارچوب‌های مبهم، تفسیرپذیر، متفاوت و گاه متعارضی را در این زمینه پیش‌بینی کرده‌اند؛ امری که تحلیل تطبیقی و نظری را ضروری‌تر می‌سازد.

در این مقاله، تلاش خواهد شد تا ضمن بررسی مفهومی و تحلیلی هریک از این دو حق، ابعاد حقوقی ناظر بر تلاقی آن‌ها مورد ارزیابی قرار گیرد. پرسش اصلی آن است که در صورت بروز تقابل میان حق اشخاص نسبت به داده‌های شخصی خود و حق شرکت‌ها نسبت به اطلاعات محرمانه‌شان، کدام راهکارهای حقوقی می‌تواند ضمن حفظ توازن، به اجرای هم‌زمان این دو دسته از حقوق کمک کند؟ آیا می‌توان معیارهایی برای تقدم نسبی یکی از این دو حق در شرایط خاص ارائه داد؟

از منظر ساختاری، مقاله حاضر در دو بخش اصلی سامان یافته است. در بخش نخست، مفاهیم بنیادین مورد بررسی قرار می‌گیرند تا زمینه نظری لازم برای تحلیل تعارض فراهم شود. به این ترتیب، ابتدا مفهوم داده‌های شخصی در حقوق داخلی و بین‌المللی تبیین می‌شود و سپس به تعریف اسرار تجاری و مؤلفه‌های اساسی آن پرداخته خواهد شد. در بخش دوم، به‌صورت دقیق‌تر تقابل میان حقوق ناظر بر داده‌های شخصی و حمایت از اسرار تجاری تحلیل می‌شود. ابتدا نحوه حمایت از اسرار تجاری در نظام‌های حقوقی مختلف بررسی و سپس با تمرکز بر یکی از مهم‌ترین مصادیق تعارض، یعنی اطلاعات و فهرست مشتریان، ابعاد حقوقی شناسایی آن به‌عنوان سرّ تجاری تحلیل خواهد شد. در ادامه، به مطالعه موارد تعارض میان حقوق اشخاص و الزامات محرمانگی شرکت‌ها پرداخته، در نهایت، راهکارهایی برای اعمال هم‌زمان این دو دسته از حقوق، پیشنهاد می‌شود.

با اینکه در آثار متعددی به بررسی نظام حقوقی حمایت از اسرار تجاری در حقوق ایران و مقایسه آن با استانداردهای بین‌المللی پرداخته شده، موضوع تحدید قلمرو حق بر اسرار تجاری با استناد به حق بر داده‌های شخصی، تاکنون به‌طور مستقیم محل توجه قرار نگرفته است. تنها مورد مشابه، مقاله‌ای (شاگری، زهرا، ۱۳۹۴) است که به بررسی محدودیت‌های حق بر اسرار تجاری و دفاعیات قابل طرح در دعاوی نقض این اسرار پرداخته است؛ ازجمله دفاع بر مبنای منافع عمومی، استفاده منصفانه و مهندسی معکوس. با این حال، در این اثر نیز بحث حقوق اشخاص موضوع داده و ارتباط آن با تحدید حق بر اسرار تجاری دیده نمی‌شود.

توجه به این نکته ضروری است که هرچند بر اساس اکثر قوانین حوزه اسرار تجاری، ازجمله دستورالعمل اسرار تجاری اتحادیه اروپا، دارنده اسرار تجاری می‌تواند هر شخص حقیقی یا حقوقی



باشد، اما در این مقاله تمرکز بر موقعیت‌هایی است که تعارض میان حق بر داده‌های شخصی اشخاص موضوع داده و حق بر اسرار تجاری بروز می‌کند. با توجه به اینکه در عمل، گردآوری و پردازش گسترده داده‌های شخصی عمدتاً از سوی شرکت‌ها انجام می‌شود، مصادیق مورد بحث در این نوشتار بر اسرار تجاری شرکت‌ها متمرکز شده، اصطلاح «دارنده اسرار تجاری» در این چارچوب، برای سهولت بیان، معادل «شرکت» به کار رفته است.

۱. آشنایی با مفاهیم اصلی

برای ورود به بحث، آشنایی با دو مفهوم اصلی پژوهش، یعنی داده‌های شخصی و اسرار تجاری، ضرورت دارد. لذا در این بخش به تعریف این مفاهیم می‌پردازیم.

۱.۱. تعریف داده‌های شخصی

داده‌های شخصی^۱، به‌عنوان نخستین سطح از طبقه‌بندی داده‌های کاربران، نقطه آغاز اغلب مقررات مربوط به حمایت از اطلاعات به‌شمار می‌رود. در بیشتر نظام‌های حقوقی، همین ویژگی شخصی‌بودن، کفایت می‌کند تا داده‌ها مشمول مجموعه‌ای از الزامات قانونی، ازجمله در زمینه جمع‌آوری، پردازش و انتقال شوند. گرچه شدت حمایت از داده‌های شخصی در مقایسه با داده‌های حساس یا اطلاعات مشمول حقوق مالکیت فکری کمتر است، اما دامنه شمول آن‌ها گسترده‌تر بوده، افراد بیشتری را دربر می‌گیرد.

در سطح بین‌المللی، یکی از جامع‌ترین تعاریف در بند نخست ماده ۴ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا^۲ ارائه شده است. مطابق آن، داده شخصی به هرگونه اطلاعاتی اطلاق می‌شود که به شخص حقیقی شناسایی شده یا قابل شناسایی مربوط باشد. شناسایی فرد می‌تواند مستقیم یا غیرمستقیم، از طریق عناصری مانند نام، شناسه‌ها، داده‌های مکانی، یا ویژگی‌های فیزیکی، روانی، اقتصادی یا اجتماعی انجام گیرد. اغلب نظام‌های حقوقی، ازجمله قانون

1. Personal Data

2. European Parliament and Council. (2016). 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 GDPR), art 4(1).

بریتانیای^۳ پس از برگزیت، چین^۴، آلمان^۵ و هند^۶ نیز از همین تعریف یا تعاریف مشابهی بهره برده‌اند.

در ایالات متحده، با وجود فقدان یک قانون فدرال جامع، قوانین بخشی مانند قانون قابلیت انتقال و مسئولیت‌پذیری بیمه‌های درمانی^۷، داده‌های درمانی قابل‌شناسایی را به‌عنوان داده شخصی شناسایی کرده‌اند. همچنین، قوانین ایالتی مانند قانون حریم خصوصی مصرف‌کنندگان کالیفرنیا^۸ و قانون داده‌های مصرف‌کنندگان ویرجینیا^۹ اطلاعات شخصی را به داده‌هایی تعریف می‌کنند که به‌طور مستقیم یا غیرمستقیم با یک فرد یا خانوار مرتبط باشند، مگر آنکه این داده‌ها شناس یا عمومی باشند.

در حقوق ایران، تعاریف پراکنده‌ای از داده‌های شخصی وجود دارد. برابر بند «ب» ماده ۱ قانون انتشار و دسترسی آزاد به اطلاعات، اطلاعات فردی شامل نام، نشانی، عادات شخصی، اطلاعات خانوادگی، بیماری‌ها و اطلاعات مالی است. در قانون تجارت الکترونیکی نیز داده‌پیام‌های شخصی به پیام‌هایی اطلاق شده که به فرد مشخصی مربوط می‌شوند. علاوه بر آن، شیوه‌نامه تفکیک اطلاعات شخصی از عمومی و نیز پیش‌نویس لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی، تعاریف گسترده‌تری از داده‌های شخصی به‌دست داده‌اند. در ماده ۱ این پیش‌نویس، داده شخصی به داده‌ای اطلاق شده است که «به‌تنهایی یا در ترکیب با داده‌های دیگر بتوان از آن برای شناسایی شخص استفاده کرد». طرح الزام به انتشار داده‌ها (۱۴۰۳) و طرح حفاظت از داده‌های شخصی (۱۴۰۳) نیز تعاریف مشابهی با تأکید بر امکان شناسایی مستقیم یا غیرمستقیم فرد، ارائه کرده‌اند.

تعاریف یادشده نشان می‌دهند که معیار شناسایی، نه صرفاً داده منفرد، بلکه قابلیت ترکیب‌پذیری داده‌ها در بسترهای تحلیلی و فناورانه است. حتی داده‌هایی که به‌ظاهر فاقد عنصر

3. UK Data Protection Act 2018.

4. Personal Information Protection Law PIPL, 2021

5. Bundesdatenschutzgesetz BDSG 2018

6. Digital Personal Data Protection Act, 2023

7. Health Insurance Portability and Accountability act of 1996 (HIPAA), CFR §160.103 45: Protected Health Information (PHI)

8. California Consumer Privacy act 2019, 1798.140 Section.

9. Virginia Consumer Data Protection act 2021, 575-59.1 Section.

هویتی‌اند، ممکن است در کنار داده‌های دیگر، هویت فرد را آشکار کنند. پژوهش‌ها نشان داده‌اند که تلفیق داده‌هایی مانند جنسیت، تاریخ تولد و کد پستی، می‌تواند برای شناسایی بخش عمده‌ای از جمعیت کافی باشد.^{۱۰}

این قابلیتِ بازشناسایی، به‌ویژه در محیط‌های داده‌محور امروزی، با توسعه فناوری‌هایی چون یادگیری ماشین و تحلیل‌های آماری، برجسته‌تر شده است. بر این اساس، مفهوم داده شخصی مفهومی نسبی است که بسته به بافت، نوع داده و توانایی‌های فنی، در بازشناسایی افراد تغییر می‌کند.

۲.۱. اسرار تجاری

در کنار شناسایی تعریف و عناصر قانونی یک سرّ تجاری، آشنایی با دامنه و انواع آن، می‌تواند به حصول نگاهی جامع نسبت به این مفهوم کمک کند. لذا در این بخش در کنار تعریف اسرار تجاری، گستره شمول آن نیز بررسی خواهد شد.

۱.۲.۱. تعریف اسرار تجاری

مفهوم اسرار تجاری^{۱۱} در زبان عمومی و عرف بازار گاه بسیار گسترده به‌کار می‌رود و هرگونه اطلاعات محرمانه‌ای که شرکت ترجیح می‌دهد از دید عموم پنهان بماند، ذیل این عنوان قرار می‌گیرد. در چنین برداشت‌های غیررسمی، صرف تمایل بنگاه به محرمانه نگه‌داشتن اطلاعات، برای اطلاق عنوان سرّ تجاری کافی تلقی می‌شود. اما در نظام‌های حقوقی، شناسایی اسرار تجاری به الزامات دقیق‌تری نیاز دارد که هم شامل ویژگی‌های ماهوی اطلاعات و هم رعایت شرایط شکلی مشخص در قوانین موضوعه است.^{۱۲}

مطابق رویه پذیرفته‌شده در حقوق بین‌الملل، اطلاعات زمانی مشمول حمایت به‌عنوان اسرار تجاری می‌شوند که:

10. Sweeney, L., "k-Anonymity: A Model for Protecting Privacy", *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, 10, (2002), p. 3.

11. Trade Secrets

12. White, Nancy & Sanney, Kenneth, "FOIA and Trade Secrets: Managing the Risks of FOIA-able Trade Secrets", *SSRN Electronic Journal*, (2010), p. 12.

(۱) به شکل معقول از دسترس عموم خارج باشند؛

(۲) ارزش اقتصادی خود را از همین وضعیت محرمانه بودن کسب کرده باشند؛ و

(۳) دارنده اطلاعات، اقدامات منطقی را برای حفاظت از محرمانگی آن انجام داده باشد.

این سه شرط، که نخستین بار به صورت منسجم در ماده ۳۹ موافقت‌نامه جنبه‌های تجاری حقوق مالکیت فکری^{۱۳} تبیین شد، در اسناد معتبر دیگر همچون دستورالعمل ۲۰۱۶ اتحادیه اروپا^{۱۴} نیز به عنوان معیارهای هسته‌ای شناسایی اسرار تجاری تکرار شده‌اند.

در ایالات متحده نیز قوانین متعددی، از جمله قانون نمونه یکنواخت اسرار تجاری^{۱۵} و قانون جاسوسی اقتصادی ۱۹۹۶^{۱۶}، همین ساختار را مبنا قرار داده‌اند.^{۱۷} قانون اخیر با افزودن ضمانت‌های اجرای کیفری، افشای غیرمجاز یا بهره‌برداری ناعادلانه از اسرار تجاری را در سطح فدرال جرم‌انگاری کرده است.

در سطح داخلی، نخستین تعریف رسمی از اسرار تجاری در ماده ۶۵ قانون تجارت الکترونیکی (۱۳۸۲) ارائه شده که بیشتر بر داده‌های دیجیتال متمرکز است. در این ماده، اطلاعات، فرمول‌ها، الگوها، نرم‌افزارها و برنامه‌ها، ابزارها و روش‌ها، تکنیک‌ها و فرایندها، تألیفات منتشرنشده، روش‌های انجام تجارت و دادوستد، فنون، نقشه‌ها و فراگردها، اطلاعات

13. World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), art 39.

14. Directive (EU) 2016/943 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure is a Directive of the European Parliament and the European Council Which was Adopted by the European Council on 27 May 2016, Following an Agreement Reached with the European Parliament on 15 December 2015, and Amendment by the Parliament on 14 March 2016.

15. Uniform Trade Secrets Act 1979 with 1985 Amendments

16. Economic Espionage act 1996 (EEA)

۱۷. در نظام حقوقی ایالات متحده آمریکا، حفاظت از اسرار تجاری ساختارمند و چندلایه است. نخستین گام مهم در این زمینه، تصویب «قانون متحدالشکل اسرار تجاری» (Uniform Trade Secrets Act - UTSA) در سال ۱۹۷۹ بود که در سال ۱۹۸۵ اصلاح شد. این قانون به عنوان یک الگوی پیشنهادی (Model Law) از سوی اغلب ایالت‌های آمریکا به صورت کامل یا با اندکی تغییر به تصویب رسید و به تدریج به زیربنای واحدی برای تبیین اسرار تجاری در سطح ایالتی تبدیل شد. با وجود این انسجام نسبی در سطح ایالت‌ها، خلأهایی در سطح فدرال برای حمایت از اسرار تجاری باقی بود. به همین منظور، در سال ۲۰۱۶ «قانون دفاع از اسرار تجاری» (Defend Trade Secrets Act - DTSA) به تصویب رسید که نقطه عطفی در توسعه این نظام حقوقی محسوب می‌شود. این قانون، برای نخستین بار، حمایت از اسرار تجاری را به صراحت در صلاحیت دادگاه‌های فدرال قرار داد و به صاحبان اسرار اجازه داد تا در صورت نقض حقوق خود، مستقیماً در دادگاه‌های فدرال طرح دعوا کنند.

مالی، فهرست مشتریان، طرح‌های تجاری و امثال این‌ها که به‌طور مستقل دارای ارزش اقتصادی بوده، در دسترس عموم قرار ندارد و تلاش‌های معقولانه‌ای برای حفظ و حراست از آن‌ها انجام شده است، به‌عنوان اسرار تجاری شناخته می‌شوند. این تعریف، با رعایت همان سه معیار بین‌المللی، در بستری محدود به فضای الکترونیکی ارائه شده است.

با تصویب قانون حمایت از مالکیت صنعتی در سال ۱۴۰۳، تعریف جامع‌تری از اسرار تجاری در ماده ۱۲۲ این قانون آمده است. بر اساس آن، هر نوع اطلاعات تجاری که دارای ارزش اقتصادی مستقل بالقوه یا بالفعل یا ارزش رقابتی باشد و به سبب آنکه عموماً ناشناخته است و به‌سادگی و از طرق قانونی قابل دستیابی یا احراز نیست، و دارنده قانونی تدابیر متعارفی را برای حفظ محرمانگی آن‌ها ترتیب داده باشد، در زمره اسرار تجاری قرار می‌گیرد. این تعریف ضمن آنکه به ویژگی‌های ماهوی توجه دارد، بر عنصر پنهان‌ماندگی قانونی و نقش اقتصادی اطلاعات تأکید می‌کند.

در جمع‌بندی، می‌توان گفت شناسایی حقوقی یک اطلاعات به‌عنوان سر تجاری، صرفاً بر اساس اراده شرکت امکان‌پذیر نیست، بلکه مستلزم احراز معیارهایی است که هم در سطح اسناد بین‌المللی و هم در قوانین داخلی مورد تأکید قرار گرفته‌اند. این معیارها، یعنی محرمانگی واقعی، ارزش اقتصادی و تدابیر حفاظتی معقول، بنیان حمایت‌های حقوقی در این زمینه را تشکیل می‌دهند و مبنایی برای تفکیک اطلاعات عادی از دارایی‌های اطلاعاتی راهبردی محسوب می‌شوند.

۲.۲.۱. دامنه و انواع اسرار تجاری

پس از بررسی تعاریف قانونی ارائه‌شده در زمینه اسرار تجاری، می‌توان به دسته‌بندی مفهومی آن‌ها در قالب تفکیک درون‌گروهی پرداخت. در یک برداشت محدودتر و تخصصی‌تر، اسرار تجاری را می‌توان به‌صورت کلی در دو رده اصلی جای داد:

نخست، اسرار فنی^{۱۸} که معمولاً شامل دانش تخصصی، فرمول‌های علمی، فرایندهای صنعتی، نقشه‌های طراحی، روش‌های تولید یا برنامه‌نویسی می‌شود.

دوم، اسرار مرتبط با حوزه کسب و کار^{۱۹}، که دربرگیرنده اطلاعاتی نظیر استراتژی‌های بازاریابی، طرح‌های کلان تجاری، و مهم‌تر از همه، فهرست مشتریان است؛ فهرستی که ممکن است حاوی داده‌هایی با ماهیت شخصی، ازجمله نام، محل سکونت، شماره تماس یا تاریخچه تراکنش‌های افراد باشد. دقیقاً در همین نقطه است که تلاقی یا گاه تداخل میان حقوق مشتریان در زمینه حفظ حریم خصوصی از یک سو، و منافع شرکت در حمایت از اسرار تجاری خود از سوی دیگر، آشکار می‌گردد؛ به‌ویژه در مواردی که اطلاعات یادشده به‌عنوان بخشی از دارایی‌های نامشهود شرکت‌ها، موضوع انتقال یا تحلیل‌های تجاری قرار می‌گیرد. البته در مورد فهرست مشتریان بحث‌هایی قابل طرح است که در بخش‌های بعدی مطرح خواهند شد.^{۲۰}

نکته دیگر آن است که شماری از صاحب‌نظران، تفاوتی مفهومی میان اصطلاح اسرار تجاری و عنوان گسترده‌تر اطلاعات محرمانه تجاری^{۲۱} قائل شده‌اند. از این منظر، اطلاعات محرمانه تجاری دامنه‌ای فراگیرتر دارد و علاوه بر اسرار تجاری، شامل انواع داده‌های شغلی، تخصصی و حتی اطلاعات شخصی^{۲۲} نیز می‌شود. بر این اساس، اسرار تجاری و دانش فنی^{۲۳} تنها بخشی از یک طیف وسیع‌تر از داده‌های محرمانه به‌شمار می‌روند.^{۲۴}

همچنین در چارچوب تحلیل تعارض بین حمایت از داده‌های شخصی و حقوق مربوط به اسرار تجاری، دیدگاهی وجود دارد که مقررات ناظر بر اسرار تجاری را تنها ناظر بر اطلاعات پردازش‌شده با ارزش تجاری می‌داند، نه داده‌های خام و اولیه. بر پایه این دیدگاه، صرف برخورداری یک داده از ماهیت شخصی برای قرار گرفتن در قلمرو اسرار تجاری کفایت نمی‌کند، بلکه این اطلاعات باید در نتیجه تحلیل، پردازش و ترکیب، واجد نوعی ارزش اقتصادی عینی شوند. در نتیجه، داده‌های اولیه مرتبط با مشتریان که به‌تنهایی حاوی معنای تجاری نیستند، از نگاه این تحلیل، در چارچوب اسرار تجاری قرار نمی‌گیرند.^{۲۵} از همین رو، این رویکرد بر آن است که میان حمایت از داده‌های شخصی و قواعد ناظر بر اسرار تجاری تضادی ماهوی وجود ندارد. با

19. Business Secrets

۲۰. باقر انصاری، «حمایت از اسرار تجاری در برابر افشای غیرمجاز»، پژوهش حقوق خصوصی، ش ۴۱ (۱۴۰۱)، ص ۴۵.

21. Confidential Information

22. Business Information, Professional Information and Personal Information

23. Know-How

24. Radoń, Barbara Anna, Trade Secrets Protection for 'Big Data': Personal Data as Trade Secrets in the European Union. Master Thesis, MIPLC, Munich, 2015, p. 31.

25. Drexler, J., "Designing Competitive Markets for Industrial Data – Between Propertisation and Access", JIPITEC, 8, (2017), p. 263.



وجود این، تحولات اخیر در اسناد حقوقی بین‌المللی، به‌ویژه در حوزه مقررات نوین، حفاظت از داده‌ها، این تمایز را چندان موجه نمی‌دانند. در نظام‌های قدیمی‌تر، مرز روشنی میان داده‌های شخصی خام و اطلاعات تجاری پردازش‌شده وجود داشت؛ اما در رویکردهای جدیدتر، این مرزبندی دستخوش تغییر شده، مرز میان داده و اطلاعات تدریجاً تضعیف گشته است.^{۲۶} بر همین اساس، حمایت از داده‌های مشتریان می‌تواند در عمل با حمایت از اطلاعات دارای ارزش اقتصادی تلاقی یابد؛ بدین‌سان، مفهوم اطلاعات شخصی در برخی موارد می‌تواند هم‌زمان در زمره دارایی‌های تجاری نیز قرار گیرد.^{۲۷}

به‌دلیل همین تداخل‌ها و پیچیدگی‌های مفهومی، بررسی دقیق‌تر هم‌پوشانی‌ها، تعارض‌ها و راهکارهای توأمان‌سازی حمایت از داده‌ها و اسرار تجاری، در بخش‌های بعدی مقاله به‌طور مبسوط دنبال خواهد شد.

۲. تقابل حمایت از اسرار تجاری و حقوق ناظر بر داده‌های شخصی

به‌نتیجه رسیدن بحث اصلی پژوهش حاضر، ناظر بر تقابل میان شفافیت و محرمانگی ناشی از اعمال هم‌زمان حق بر داده‌های شخصی و حق بر اسرار تجاری، پس از تعریف مفاهیم، نیازمند بررسی نحوه حمایت از داده‌های شخصی و حقوق مربوط به آن و همچنین نظام حمایت از اسرار تجاری است. لذا در این بخش ضمن بررسی این موارد، در نهایت، تعارضات احتمالی ارزیابی و راهکارهایی برای رفع آن‌ها ارائه می‌شود.

۱.۲. نحوه حمایت از اسرار تجاری

چارچوب‌های حقوقی حمایت از اسرار تجاری در کشورهای مختلف، به‌ویژه اتحادیه اروپا، از تنوع زیادی برخوردار است. پیش از دستورالعمل ۲۰۱۶ اتحادیه، این حمایت‌ها یکپارچه نبود: در

۲۶. امروزه در بسیاری از صنایع، داده‌های خام شخصی نیز می‌توانند واجد ارزش اقتصادی و مزیت رقابتی باشند و در قالب اسرار تجاری حفاظت شوند. برای مثال، یک شرکت ارائه‌دهنده خدمات پوشیدنی‌های هوشمند (wearables) ممکن است داده‌های خام مربوط به ضربان قلب یا الگوی خواب کاربران را ذخیره کند. این داده‌ها، حتی بدون پردازش تحلیلی، می‌توانند خود، بسترساز الگوریتم‌های پیش‌بینی بیماری یا طراحی محصولات اختصاصی شوند. به همین ترتیب، شرکت‌های تجارت الکترونیک گاه داده‌های خام جست‌وجو یا کلیک کاربران را پیش از هرگونه پردازش، به‌عنوان دارایی محرمانه خود نگه می‌دارند، زیرا افشای آن‌ها می‌تواند استراتژی‌های بازاریابی رقبا را تقویت کند.

27. Mylly, U. M., "Trade Secrets and the Data Act" *JIC*, 55, (2024), p. 373.

سوئد مقررات موقت و ناپایدار حاکم بود؛ آلمان، اتریش، لهستان و اسپانیا آن را ذیل مفاهیم رقابت ناعادلانه قرار می‌دادند و افشای غیرمجاز را قابل تعقیب مدنی یا کیفری می‌دانستند؛ هلند و لوکزامبورگ قواعد مسئولیت مدنی را مبنا قرار داده بودند؛ بریتانیا، ایرلند و مالت بر نقض تعهد محرمانگی^{۲۸} تکیه داشتند؛ و ایتالیا، پرتغال و تا حدی فرانسه آن را ذیل مالکیت فکری طبقه‌بندی و به‌عنوان اموال دارای ارزش اقتصادی مشابه اختراع یا علامت تجاری شناسایی می‌کردند.^{۲۹} در دستورالعمل ۲۰۱۶، هدف، ایجاد نظام الزام‌آور واحد نبود، بلکه حداقل سطح حمایت را تعیین می‌کرد تا ضمن حفظ تنوع ملی، هماهنگی نسبی حاصل شود. اعضا می‌توانند حمایت گسترده‌تری پیش‌بینی کنند، مشروط به رعایت استانداردهای مشترک در اجرای حقوق، جبران خسارت و استثناهای^{۳۰}. این رویکرد انعطاف‌پذیر، میان یکپارچگی حداقلی و استقلال ملی تعادل برقرار می‌کند.^{۳۱}

در سطح بین‌المللی، چالش اصلی جایگاه اسرار تجاری در نسبت با مالکیت و آزادی رقابت است. برخلاف اختراعات یا علائم تجاری که تحت مالکیت صنعتی با حقوق انحصاری مشخص تعریف می‌شوند، بیشتر نظام‌های حقوقی از اعطای وصف مالکانه به اسرار تجاری خودداری کرده، صرفاً از آن‌ها در برابر دسترسی یا بهره‌برداری بدون مجوز حمایت می‌کنند.^{۳۲} این حمایت ماهیتی رفتاری دارد و بر بی‌صدافتی، فریب یا نقض الزامات رقابت منصفانه متمرکز است، نه خلایق یا ابتکار.^{۳۳} تمایز اصلی با سایر حقوق مالکیت فکری در این است که معیار حمایت، نه آفرینش فکری، بلکه نحوه حفظ محرمانگی است و برخلاف حمایت‌های مدت‌دار و انحصاری مالکیت فکری، اسرار تجاری فقط در صورت تحصیل یا افشای غیرقانونی قابل استنادند.^{۳۴} بنابراین، این

28. Breach of Confidentiality

29. Baker & McKenzie, Study on Trade Secrets and Confidential Business Information in the Internal Market, Available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_-final-study_en.pdf.

30. Recital 10 and Article 1 of the Trade Secrets Directive.

31. Banterle, F., "The Interface Between Data Protection and IP Law: The Case of Trade Secrets and Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis", in Bakhoum, M. et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (2016), p. 6-8.

32. Aplin, Tanya F., "A Critical Evaluation of the Proposed EU Trade Secrets Directive", *King's College London Law School Research Paper*, 25 (2014), p 15.

33. Recitals 14 and 16.

۳۴. محسن اسماعیلی و همکاران، «حل چالش‌های عمده در دعاوی اسرار تجاری با رفع تزاخم دو حق: دادخواهی منصفانه و حفظ محرمانگی اطلاعات»، *مطالعات حقوق تطبیقی معاصر*، ش ۱۶ (۱۳۹۷)، ص ۳.

نظام بیش از آنکه حق مطلق ایجاد کند، بر جلوگیری از سوءاستفاده و نقض اعتماد تأکید دارد. البته گرچه اسرار تجاری از حیث مینا و شیوه حمایت با سایر مصادیق مالکیت فکری تفاوت دارد، اما کارکرد آن غالباً مکمل نظام مالکیت فکری است. در مواردی که ایده، فرمول یا فرایند، قابلیت ثبت به‌عنوان اختراع یا اثر ادبی- هنری را ندارد یا مالک به افشای آن در فرایند ثبت تمایلی ندارد، حمایت از آن در قالب اسرار تجاری، خلأهای حمایتی نظام مالکیت فکری را پر می‌کند و به حفظ مزیت رقابتی کمک می‌نماید.^{۳۵}

۲.۲. شناسایی فهرست و اطلاعات مشتریان به‌عنوان سرّ تجاری

در خصوص اسرار تجاری شرکت‌ها، دو سناریوی اصلی قابل تصور است. نخست آنکه اطلاعات بنیادین شکل‌دهنده اسرار تجاری، مستقیماً در بستر فعالیت‌های داخلی شرکت یا از سوی کارکنان آن تولید شده باشند. در این وضعیت، شرکت از لحظه ایجاد داده‌ها، مالکیت آن‌ها را در اختیار دارد و در صورتی که این اطلاعات دارای ارزش اقتصادی مستقل، محرمانگی واقعی و همچنین مشمول تدابیر معقول حفاظتی باشند، به‌روشنی در دایره حمایت نظام حقوقی اسرار تجاری جای می‌گیرند. اما حالت دوم هنگامی است که اسرار تجاری بر مبنای داده‌هایی شکل گرفته باشند که از طریق گردآوری اطلاعات مربوط به کاربران یا مشتریان به‌دست آمده‌اند. در چنین مواردی، این پرسش مطرح می‌شود که در صورت تعارض میان حقوق داده‌ای اشخاص از یک سو و منافع شرکت در حفاظت از اطلاعات تجاری از سوی دیگر، نظام حقوقی چگونه باید واکنش نشان دهد.

در این میان، فهرست مشتریان به‌عنوان یکی از نمونه‌های رایج اسرار حرفه‌ای جمع‌آوری شده از کاربران، همواره محل بحث بوده است. مسئله این است که آیا چنین فهرستی به‌تنهایی می‌تواند شرایط لازم برای برخورداری از حمایت به‌عنوان سرّ تجاری را دارا باشد یا خیر؟ هرچند برخی منابع اتحادیه اروپا آن را مصداق از اسرار تجاری دانسته‌اند، ولی نه استدلال روشنی برای این ادعا ارائه شده و نه رویه قضایی منسجمی در سطح اتحادیه شکل گرفته است. با این حال، نظام قضایی ایتالیا در این خصوص برخوردی پیشرو دارد. برای مثال، دادگاه ونیز در رأی در سال

۳۵. باقر انصاری، پیشین، ص ۴۲-۴۵.

۲۰۱۵^{۳۶} اعلام کرده که فهرست مشتریان ممکن است مشمول حمایت اسرار تجاری بشود؛ حتی در فرضی که برخی اطلاعات آن از طریق حضور رقبا در مجامع عمومی یا نمایشگاه‌ها قابل شناسایی باشد. از نگاه این دادگاه، امکان بالقوه کشف برخی داده‌ها از سوی دیگران، مانعی برای برخورداری از حمایت قانونی محسوب نمی‌شود. چنانچه اطلاعات یادشده از طریق فرایندی هدفمند گردآوری شده باشد، ساختاری منسجم و مزیتی رقابتی برای شرکت فراهم کند، و نیز اقدامات معقولی برای محرمانه نگه‌داشتن آن‌ها صورت گرفته باشد، شایسته برخورداری از حمایت به‌عنوان سرّ تجاری خواهد بود. این تفسیر، بیانگر نگاهی منعطف و تطبیقی در حقوق ایتالیاست که قابلیت اثرگذاری بر تفسیرهای حقوقی سایر کشورها را نیز دارد. نمونه‌های دیگری از این رویکرد در نظام قضایی ایتالیا دیده می‌شود. در آرای صادره از دادگاه ونیز در همان سال^{۳۷}، و همچنین دادگاه پروجا در سال ۲۰۰۸^{۳۸}، تصریح شده که بهره‌برداری یا افشای فهرست مشتریان، شامل مشخصات فردی، داده‌های حساس، اطلاعات قراردادی و وضعیت تعاملات تجاری، مصداق روشنی از نقض حقوق ناشی از اسرار تجاری است. دادگاه مودنا در رأی ۲۰ آوریل ۲۰۰۵^{۳۹} نیز اعلام کرد که حتی اگر دسترسی به برخی داده‌های مشتریان از طریق بررسی بازار ممکن باشد، این موضوع از شمول حمایت قانونی نمی‌کاهد؛ مشروط بر آنکه این داده‌ها ساختاریافته و دربرگیرنده ارزش اقتصادی ویژه‌ای باشند. رویه دادگاه تجدیدنظر فلورانس در سال ۲۰۱۱^{۴۰} نیز مؤید همین دیدگاه است. این دادگاه تأکید کرده است که ارزش فهرست مشتریان، نه صرفاً به محتوا، بلکه به هدفمندی و انسجام آن بستگی دارد. برای نمونه، حتی فهرستی شامل ایمیل‌هایی از مخاطبان علاقه‌مند به محصولات یا خدمات خاص، اگر به‌طور هدفمند گردآوری شده باشد، می‌تواند دارایی تجاری محسوب شود. این امر به‌ویژه زمانی تقویت می‌شود که گردآوری چنین اطلاعاتی نیازمند سرمایه‌گذاری قابل‌توجه زمانی، انسانی و مالی باشد. به همین ترتیب، دادگاه برسیا در سال ۲۰۰۴^{۴۱} اعلام کرد که رویه‌های مرتبط با داده‌های مشتریان، واجد ارزش اقتصادی بالفعل اند و در اختیار داشتن آن‌ها می‌تواند موجب صرفه‌جویی در هزینه‌های بازاریابی، کاهش مراحل آزمایشی و تسریع در توسعه بازار گردد. در همین راستا، دادگاه میلان در

36. Court of Venice, Judgment of 16 July 2015, Riv. Dir. Ind., 2015, 437.

37. Court of Venice, Judgment of 16 July 2015.

38. Court of Perugia, Judgment of 23 January 2008, Giur. ann. dir. ind., 2008, 1, 675.

39. Court of Modena, Judgment of 20 April 2005, Giur. ann. dir. ind., 2005, 861.

40. Florence Court of Appeal, Judgment of 9 May 2011, No. 635, Iusexplorer.

41. Court of Brescia, Judgment of 29 April 2004, in Giur. ann. dir. ind., 2004, 1079.

رای سال ۲۰۱۲^{۴۲} معیارهایی نظیر میزان تلاش، زمان و منابع صرف‌شده در تهیه و تحلیل اطلاعات مشتریان را به‌عنوان مؤلفه‌های تعیین‌کننده ارزش تجاری آن‌ها در نظر گرفته است. از منظر این دادگاه، ارزش داده‌های تجاری، نه صرفاً در محتوای خام آن‌ها، بلکه در فرایند تولید، پالایش و ساختاردهی‌شان نهفته است.^{۴۳}

ارزیابی انتقادی این آرا نشان می‌دهد که رویکرد دادگاه‌های ایتالیایی در شناسایی فهرست مشتریان به‌عنوان سرّ تجاری، بر یک معیار سه‌جانبه استوار است: ۱- هدفمندی و انسجام گردآوری اطلاعات؛ ۲- ارزش اقتصادی مستقل ناشی از محرمانگی؛ و ۳- تلاش‌های معقول برای حفظ اطلاعات. نکته اساسی این است که این دادگاه‌ها تصریح کرده‌اند که قابلیت کشف داده‌ها از طریق تحقیق عمومی مانع شناسایی آن‌ها به‌عنوان سرّ تجاری نیست؛ مشروط بر آنکه گردآوری سازمان‌یافته آن‌ها برای رقبا دشوار باشد. این معیار ارزشمند است زیرا میان در دسترس بودن بالقوه داده‌ها و قابل بهره‌برداری بودن آن‌ها تمایز می‌گذارد. با این حال، این رویکرد در تعارض با حقوق داده‌های شخصی پرسش‌برانگیز است: چگونه می‌توان اطلاعاتی را که اشخاص حق دسترسی به آن را دارند، هم‌زمان به‌عنوان دارایی محرمانه شرکت حفاظت کرد؟ این چالش نیازمند رویکردی متوازن است که در بخش‌های بعدی بررسی خواهد شد.

مجموعه این آرا، بر جایگاه فهرست مشتریان به‌عنوان یک دارایی اطلاعاتی راهبردی تأکید دارد و رویکرد سرمایه‌محور نظام حقوقی ایتالیا نسبت به چنین داده‌هایی را نشان می‌دهد. در این رویکرد که در سراسر اتحادیه اروپا نیز در عمل مشاهده می‌شود، داده‌های مربوط به مشتریان، نه صرفاً ابزارهای اجرایی، بلکه عناصر حیاتی رقابت‌پذیر تلقی می‌شوند. با این توصیف، مسئله نحوه بهره‌برداری تجاری از این فهرست‌ها، به‌ویژه زمانی که داده‌ها مشتمل بر اطلاعات شخصی باشند، مستلزم تبیین حقوقی دقیق‌تری است؛ چراکه در این نقطه، مرز میان حمایت از اسرار تجاری و احترام به حقوق داده‌ای افراد، باریک‌تر از همیشه خواهد بود و توازن میان این دو نیازمند بررسی جدی است.

42. Court of Milan, Judgment of 14 February, Giur. ann. dir. ind., 2012, 5859.

43. Banterle, F., "The Interface Between Data Protection and IP Law: The Case of Trade Secrets and Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis", in Bakhoum, M. et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (2016), p. 6-8.

۳.۲. ارزیابی تعارضات میان حقوق اشخاص مرتبط با اسرار تجاری

برای تحلیل دقیق سطح تعارض میان حقوق اشخاص نسبت به داده‌های شخصی و حقوق شرکت‌ها در بهره‌برداری از اسرار تجاری، ابتدا باید انواع حقوق در معرض تضاد را شناسایی کرد.

در رأس این حقوق، حق بنیادین اشخاص نسبت به حریم خصوصی قرار دارد که مستلزم شفاف‌سازی و أخذ رضایت آگاهانه پیش از هرگونه پردازش یا انتقال داده‌های شخصی است. حق‌هایی نظیر دسترسی به داده‌ها، حق حذف، و حق انتقال‌پذیری نیز در نظام‌های نوین حمایت از داده‌ها شناسایی شده‌اند. با این حال، اعمال این حقوق ممکن است در تضاد با منافع شرکت‌ها برای حفظ محرمانگی و بهره‌برداری انحصاری از اطلاعات تجاری مانند فهرست مشتریان یا داده‌های تحلیلی قرار گیرد؛ چراکه افشا یا حذف این داده‌ها می‌تواند مزیت رقابتی شرکت را تضعیف کند. برای نمونه، در یک بانک اطلاعاتی دیجیتال، اطلاعاتی چون تاریخچه تراکنش‌ها و الگوهای رفتاری مشتریان ممکن است با الگوریتم‌های خاصی مورد پردازش قرار گیرد. شرکت مدعی است که تحلیل‌های صورت‌گرفته و شیوه طبقه‌بندی مشتریان بخشی از مدل کسب‌وکار و اسرار تجاری آن است که باید محرمانه بماند. در مقابل، کاربران خواهان اطلاع از منطق تصمیم‌گیری‌های خودکار درباره اعطای خدمات یا رتبه‌بندی اعتباری‌شان، و گاه خواستار حذف یا انتقال داده‌های خود هستند. در این وضعیت، تعارض میان دو دسته حق، یکی بر داده‌های شخصی و دیگری بر اطلاعات طبقه‌بندی و پردازش‌شده دارای ارزش تجاری، ضرورت تبیین مرزها و ایجاد توازن حقوقی میان آن‌ها را آشکار می‌سازد.

معیارهای پیشنهادی برای تعیین تقدم حقوق در این تعارض عبارت‌اند از: ۱- معیار ضرورت و تناسب: آیا محدودسازی حق بر داده‌های شخصی برای حمایت از اسرار تجاری ضروری است و آیا این محدودیت متناسب با هدف است؟ ۲- معیار تفکیک‌پذیری: در صورت امکان جداسازی داده‌های شخصی از اسرار تجاری، محدودسازی حقوق اشخاص موجه نیست؛ ۳- معیار ماهیت داده: داده‌های حساس (سلامت، مالی، عقیدتی و ...) از حمایت قوی‌تری برخوردارند و اسرار تجاری نمی‌توانند دسترسی به آن‌ها را کاملاً منتفی کنند؛ ۴- معیار رضایت آگاهانه: هر جا که داده‌ها با رضایت آگاهانه فرد نسبت به ماهیت و هدف پردازش جمع‌آوری شده‌اند، حق شرکت بر آن‌ها اصولاً مقدم است؛ ۵- معیار هدف پردازش: داده‌هایی که صرفاً برای اهداف تجاری پردازش

می‌شوند، اما نه با اطلاع و رضایت مشخص فرد، نمی‌توانند به‌سادگی زیر چتر اسرار تجاری جای گیرند. این چارچوب پنج‌گانه، ابزاری است برای ارزیابی موردی تعارضات، به‌جای تعیین اولویت مطلق یکی از حقوق.

از منظر تحلیل انتقادی، تعارض میان حق بر داده‌های شخصی و حق بر اسرار تجاری را می‌توان در چارچوب یک مدل دوگانه تبیین کرد: از یک سو، حقوق داده‌محور برآمده از کرامت انسانی که ماهیتی بنیادین دارند؛ و از سوی دیگر، اسرار تجاری که از نظر حقوقی، نه مالکیت مطلق، که حمایتی رفتاری- رقابتی شمرده می‌شوند. این تمایز ماهوی پیامد مهمی دارد: در تعارض میان این دو، نمی‌توان به‌صرف وجود ادعای محرمانگی، حقوق بنیادین فرد را محدود کرد؛ از این رو، معیار تهدید جدی و مشخص به منافع تجاری که در رویه اتحادیه اروپا نیز منعکس شده، معیاری متوازن‌تر برای تعیین حدود تقدم هریک از این حقوق است. اسرار تجاری تنها آنگاه می‌توانند حقوق داده‌ای را محدود کنند که افشای داده‌ها به‌طور مستقیم، مشخص و اثبات‌پذیر به ارزش اقتصادی راز تجاری لطمه وارد نماید.

فارغ از این‌ها، برخی کشورها برای رفع تعارض میان حقوق داده‌ای افراد و اسرار تجاری شرکت‌ها، استثناهای هدفمند و قابل‌کنترلی درنظر گرفته‌اند. در مقابل، در کشورهایی فاقد چنین مقررات، مشروعیت پردازش یا اعمال حقوق راجع به اسرار تجاری نسبت به داده‌ها ممکن است مبهم باقی بماند. برای نمونه، قانون حفاظت از داده‌های شخصی در ایتالیا مقرر کرده است که اگر پردازش یا انتقال داده‌ها در چارچوب فعالیت‌هایی صورت گیرد که تحت قواعد اسرار تجاری و صنعتی هستند، أخذ رضایت قبلی افراد ممکن است الزامی نباشد.^{۴۴} البته این معافیت تنها شامل داده‌هایی است که دارای ارزش تجاری باشند و در مورد داده‌های صرفاً شخصی همچنان قواعد عمومی حفاظت از داده‌ها حاکم است. با این حال، حتی در این موارد، افراد می‌توانند به استناد دلایل خاص مرتبط با وضعیت شخصی خود به پردازش داده‌ها اعتراض کنند. در انگلستان نیز قانون حفاظت از داده‌ها تصریح می‌کند که افراد حق دارند از منطق تصمیم‌گیری خودکار مطلع شوند؛ اما اگر این افشا به افشای اسرار تجاری منجر شود، این حق قابل محدودسازی است. این

44. Codice in Materia di Protezione dei dati Personali (Decreto Legislativo 30 Giugno 2003, n. 196), Modificato dal Decreto Legislativo 10 Agosto 2018, n. 101, Articoli 24 e 25.

معافیت صرفاً به جنبه‌های الگوریتمی پردازش مربوط می‌شود و سایر حقوق مانند حذف یا انتقال داده‌ها را شامل نمی‌شود. مقررات مشابهی نیز در ایرلند وجود دارد که به شرکت‌ها اجازه می‌دهد در شرایط خاص، اعمال حقوق داده‌ای را به دلیل ملاحظات محرمانگی تجاری محدود کنند.^{۴۵} این نمونه‌ها نشان می‌دهند که برخی نظام‌های حقوقی، به‌منظور برقراری توازن میان حریم خصوصی و منافع تجاری، معافیت‌هایی محدود و غیرمطلق را در نظر گرفته‌اند. برای درک بهتر این تعارض، بررسی آرای قضایی در حوزه‌های مرتبط می‌تواند مفید واقع شود.

در یک پرونده مطرح در سال ۲۰۱۱،^{۴۶} فیسبوک از ارائه کامل داده‌های درخواستی کاربران خودداری کرد و تنها بخشی از آن‌ها را در اختیار گذاشت؛ زیرا مدعی شد بخش‌هایی از این اطلاعات پردازشی جزء اسرار تجاری هستند و مشمول حق دسترسی کاربران نمی‌شوند. دادگاه نیز با پذیرش این استدلال، رأی را به نفع فیسبوک صادر کرد. این حکم نشان‌دهنده آن است که در برخی نظام‌ها، اسرار تجاری می‌توانند به‌عنوان مبنایی برای محدودسازی حقوق اطلاعاتی افراد، به‌ویژه در خصوص داده‌های تحلیل‌شده یا الگوریتمی، به کار روند.^{۴۷}

در پرونده‌ای دیگر^{۴۸}، کارمندی که طی اشتغال در شرکت خدمات موبایلی، صفحه‌ای در شبکه‌های اجتماعی با نام شرکت راه‌اندازی کرده بود، پس از قطع همکاری با شرکت، ادعای مالکیت شخصی آن صفحه را بر این مبنای که گاهی از خود و از محیط زندگی، تصاویر و اطلاعاتی را (هرچند در راستای نمایش حرفه خویش) در این صفحه منتشر می‌نمود، مطرح کرد. اما دادگاه با توجه به ماهیت حرفه‌ای محتوا و اطلاعات تجاری موجود در آن صفحه و اینکه ممکن بود مطالب منتشرشده در صفحه یادشده از سوی کارمند، متضمن اسرار تجاری و نمایش نحوه و جزئیات فعالیت‌های تجاری شرکت باشد، مالکیت صفحه را به نفع شرکت تشخیص داد. این حکم بر نقش داده‌های شرکتی در تعیین حقوق بهره‌برداری و مالکیت نیز تأکید دارد و نمونه‌ای از برتری حق بر اسرار تجاری نسبت به حق اشخاص بر داده‌های شخصی است.^{۴۹}

45. Malgieri, Gianclaudio, "Trade Secrets v Personal Data: A Possible Solution for Balancing Rights", *International Data Privacy Law*, 6, (2016), pp. 4-5.

46. Schrems vs Facebook 2011

47. Schrems v. Facebook, Available at: http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf.

48. Phonedog v. Kravitz, Dist. Court, ND California 2011.

49. PhoneDog v. Kravitz, No. C 11-03474 MEJ, Available at: https://scholar.google.com/scholar_case?case=9890904231170613660.



ارزیابی انتقادی این دو رأی ایجاب می‌کند فراتر از گزارش نتایج آن‌ها، مبانی استدلالی و سازگاری‌شان با اصول حقوق داده را بسنجیم. در پرونده فیسبوک، پذیرش استدلال لزوم حمایت از اسرار تجاری برای محدود کردن حق دسترسی با یادآوری شماره ۶۳ مقررات عمومی حفاظت از داده‌ها که وجود اسرار تجاری نمی‌تواند توجیهی برای محروم کردن کامل فرد از حق دسترسی باشد در تعارض است. این حکم در واقع نشان‌دهنده یک خلأ حقوقی دوره قبل از تصویب مقرره اتحادیه اروپا بود که در حقوق کنونی اروپا قابل قبول نیست. در پرونده فون‌داگ، دادگاه اگرچه ماهیت تجاری محتوا را مبنای تصمیم قرار داد، اما از این پرسش بنیادین‌تر غافل ماند که آیا اشتراک اطلاعات شخصی کارمند در صفحه‌ای که با نام شرکت ایجاد شده است، می‌تواند به‌طور خودکار همه آن اطلاعات را به اسرار تجاری شرکت تبدیل کند؟ از منظر حقوق ایران، هیچ‌یک از این آرا مستقیماً قابل اعمال نیستند، اما مفهوم کلی آن‌ها که ماهیت اطلاعات، نه مالکیت رسانه، تعیین‌کننده است، می‌تواند در تفسیر ماده ۶۵ قانون تجارت الکترونیکی و نیز ماده ۱۲۲ قانون مالکیت صنعتی ۱۴۰۳ مفید باشد.

با این حال، در سطح نظری، حق اشخاص بر داده‌های شخصی خود معمولاً برتر از حقوق مبتنی بر اسرار تجاری تلقی می‌شود؛ هرچند این برتری مطلق نیست. برای نمونه، در قانون داده‌های سلامت ایالت واشینگتن^{۵۰}، حتی اگر داده‌های شخصی با اسرار تجاری ترکیب شده باشند، مصرف‌کننده حق دسترسی کامل دارد؛ شامل داده‌های خام، پردازش‌شده و اطلاعات مربوط به اشخاص ثالثی که داده‌ها به آن‌ها منتقل شده‌اند. همچنین، فرد حق دارد درخواست حذف داده‌ها را بدهد، و شرکت موظف است نه تنها داده‌ها را حذف کند، بلکه حذف آن‌ها نزد تمام دریافت‌کنندگان ثالث را نیز تضمین نماید^{۵۱}. این نمونه بیانگر آن است که در حوزه داده‌های حساس مانند سلامت، حقوق فردی بر داده‌ها مطلق تلقی شده، حتی بر اسرار تجاری اولویت دارد.

در حقوق اتحادیه اروپا، هرچند صراحتی مشابه برخی نظام‌های ملی درباره اولویت‌بندی میان داده‌های شخصی و اسرار تجاری وجود ندارد، اما مقررات عمومی حفاظت از داده‌ها و دستورالعمل

50. My Health My Data (MHMD) act 2023.

51. Colgate, Jenny, Why Privacy and Trade Secret Law Are on A Collision Course, Available at: <https://www.jdsupra.com/legalnews/why-privacy-and-trade-secret-law-are-on-6821298/>.

۲۰۱۶ درباره اسرار تجاری تلاش کرده‌اند نوعی توازن میان این دو دسته از حقوق برقرار نمایند. مقررات عمومی حفاظت از داده‌ها در مواد ۱۵ و ۲۰ و یادآوری شماره ۶۳ به صورت محدود به این تعارض پرداخته‌اند. ماده ۱۵^{۵۲} که حق دسترسی را تبیین می‌کند، تصریح دارد که اعمال این حق نباید به نقض حقوق و آزادی‌های دیگران، از جمله اسرار تجاری شرکت‌ها منجر شود. همین قید در ماده ۲۰ (مربوط به حق انتقال داده‌ها)^{۵۳} نیز آمده است. با این حال، چنین محدودیت‌هایی درباره برخی حقوق دیگر از جمله حق حذف یا انصراف از رضایت به روشنی پیش‌بینی نشده‌اند و لذا ابهامات باقی می‌مانند. حق دسترسی در ماده ۱۵ شامل سه بخش اصلی است: (۱) حق دریافت تأییدیه درباره پردازش داده‌ها؛ (۲) حق دسترسی به داده‌ها و دریافت نسخه‌ای از آن‌ها؛ و (۳) حق دریافت اطلاعات درباره هدف، منبع و منطق پردازش.

شرکت‌ها نمی‌توانند صرفاً با استناد به اسرار تجاری از ارائه این اطلاعات خودداری کنند، مگر آنکه داده‌های شخصی به گونه‌ای در دل اطلاعات محرمانه تنیده شده باشند که تفکیک آن‌ها ممکن نباشد و افشای آن موجب آسیب به منافع تجاری شود. در چنین شرایطی شرکت موظف است: ۱- داده‌های قابل تفکیک را ارائه کند؛ ۲- وجود پردازش را تأیید نماید؛ ۳. اطلاعات پایه درباره پردازش را اعلام کند؛ ۴- در صورت عدم امکان تفکیک، امکان مشاهده تحت نظارت داده‌ها را برای فرد یا نماینده‌اش فراهم سازد.

این رویکرد نشان می‌دهد که محدودسازی حق دسترسی تنها در چارچوب دقیق و محدود، و نه به صورت مطلق، پذیرفته شده است. برای نمونه، اگر داده‌های پردازش شده از سوی شرکت در یک دعوای قضایی مرتبط با شخص موضوع داده نقش کلیدی داشته، تفکیک آن‌ها از اسرار تجاری ممکن نباشد، شرکت موظف است امکان مشاهده این اطلاعات را برای دادگاه و نمایندگان طرفین فراهم کند؛ هرچند می‌تواند از ارائه نسخه کپی آن خودداری نماید.

بر پایه یادآوری شماره ۶۳ مقررات عمومی حفاظت از داده‌ها^{۵۴}، افراد باید دسترسی منظم و آسان به داده‌های شخصی خود داشته باشند تا بتوانند مشروعیت پردازش را بررسی کرده، در صورت نیاز، آن را به چالش بکشند. این حق شامل داده‌های حساس، مانند اطلاعات پزشکی نیز

52. GDPR, art 15.

53. GDPR, art 20.

54. GDPR, Recital 63.

می‌شود. افراد باید بتوانند از هدف پردازش، مدت نگهداری، گیرندگان داده، منطق تصمیم‌گیری خودکار و آثار آن آگاه شوند. شرکت‌ها نیز در صورت امکان، باید سامانه‌ای امن برای دسترسی مستقیم به داده‌ها فراهم کنند. با این حال، اعمال این حق نباید به گونه‌ای باشد که به حقوق و آزادی‌های دیگران، از جمله اسرار تجاری یا حقوق مالکیت فکری (مانند حقوق نرم‌افزار) آسیب برساند. ولی در عین حال، همین یادآوری تصریح می‌کند که وجود اسرار تجاری نمی‌تواند دلیلی برای محروم کردن کامل فرد از حق دسترسی باشد. این دیدگاه بر سه استدلال تفسیری مبتنی است:

۱. برخلاف دستورالعمل سال ۱۹۹۵، در مقررات عمومی حفاظت از داده‌ها تأکید شده است که اسرار تجاری مانع کلی برای دسترسی نیستند.

۲. کارگروه ماده ۲۹، قید مربوط به لطمه به اسرار تجاری را نیازمند تفسیر مضیق دانسته است.

۳. همین کارگروه تأکید دارد که صرف ادعای وجود اسرار تجاری نمی‌تواند توجیهی برای امتناع از ارائه اطلاعات باشد.^{۵۵}

در نتیجه، هرچند مقررات عمومی اتحادیه اروپا در تعارض میان داده‌های شخصی و اسرار تجاری رویکردی محتاطانه را در پیش گرفته است، تفسیر غالب حقوقی، بر اولویت نسبی حق دسترسی افراد دلالت دارد؛ مگر در مواردی استثنایی که افشای داده‌ها به‌طور جدی و مشخص منافع تجاری مشروع را تهدید کند.^{۵۶}

در یادآوری شماره ۶۳ مقررات عمومی حفاظت از داده‌ها، توصیه شده است که سازمان‌ها باید امکان دسترسی مستقیم افراد را از راه دور به اطلاعات شخصی‌شان فراهم کنند. با این حال، دفتر کمیسر اطلاعات اتحادیه بریتانیا تأکید کرده است که چنین دسترسی‌ای نباید شامل اسرار

55. Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (wp251rev.01), Available at: <https://ec.europa.eu/newsroom/-article29/items/612053/en>.

56. La Diega Noto, Guido & Sappa, Cristiana, "The Internet of Things at the Intersection of Data Protection and Trade Secrets, Non-Conventional Paths to Counter Data Appropriation and Empower Consumers", *Revue Européenne de Droit de la Consommation, European Journal of Consumer Law*, 3, (2020), p. 24.

تجاری بشود، زیرا ارائه خودکار و بی‌قید و شرط اطلاعات، با ضرورت حفظ محرمانگی اطلاعات تجاری^{۵۷} ناسازگار است.^{۵۸} بنابراین، قید موجود در یادآوری پیش‌گفته مبنی بر اینکه اعمال حق دسترسی نباید به اسرار تجاری لطمه بزند، باید به‌عنوان یک محدودیت تفسیری در برابر دسترسی خودکار و عمومی تلقی شود، و نه مانعی کلی برای حق دسترسی. در عوض، شرکت‌ها ملزم‌اند به‌صورت موردی و در پاسخ به درخواست مشخص، امکان دسترسی فرد به داده‌های شخصی‌اش را فراهم آورند. شرکت‌ها باید میان داده‌هایی که افشای آن‌ها لطمه‌ای به اسرار تجاری نمی‌زند و داده‌هایی که بخشی از اطلاعات تجاری محرمانه‌اند، تمایز بگذارند. در صورت وجود تعارض، دادگاه‌ها می‌توانند تدابیری همچون محدود کردن دامنه افشا یا ممنوع کردن انتشار ثانویه را برای حفظ ارزش اقتصادی اسرار تجاری اعمال نمایند. چنین تدابیری تضمین می‌کنند که اجرای حق دسترسی، موجب نقض یا حذف کامل حمایت‌های قانونی از اسرار تجاری نشود. در نهایت، یادآوری شماره ۶۳، اسرار تجاری را تنها یکی از مواردی می‌داند که در اعمال حق دسترسی باید حقوق اشخاص ثالث در آنها مورد ملاحظه قرار گیرد.^{۵۹}

در کنار حق دسترسی، تنها حق دیگری که ممکن است در تعارض با اسرار تجاری قرار گیرد، حق انتقال داده‌هاست که در ماده ۲۰ مقررات عمومی حفاظت از داده‌ها پیش‌بینی شده است. این حق به افراد اجازه می‌دهد داده‌های شخصی خود را در قالبی ساختارمند و قابل خواندن از ماشین دریافت کرده، به کنترل‌کننده دیگری منتقل کنند. با این حال، وجود اسرار تجاری نباید مانعی کلی برای چنین انتقالی ایجاد کند. در سیاست‌های حفظ حریم خصوصی شرکت‌هایی مانند آمازون نیز آمده است که کاربران می‌توانند مطابق با قوانین قابل اجرا، درخواست انتقال داده‌هایشان را ثبت کنند.^{۶۰} این اشاره به قانون قابل اجرا به‌طور منطقی شامل بند ۴ ماده ۲۰ می‌شود که تأکید دارد حق انتقال نباید به حقوق و آزادی‌های دیگران لطمه بزند. کارگروه ماده

57. Trade Secret Directive, art 2(1)(c).

58. ICO, Guide to the General Data Protection Regulation, Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>.

59. Di Martino, M., "Personal Information Leakage by Abusing the GDPR "Right of Access"", Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19), (2019), p. 371-375.

60. Amazon Inc, Privacy Notice, Available at: <https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ>.



۲۹ این بند را ناظر بر حفاظت از داده‌های شخصی اشخاص ثالث می‌داند، نه اسرار تجاری^{۶۱} با این حال، حتی در فرض تعارض با اسرار تجاری نیز مقررات تصریح می‌کنند که این تعارض نباید به انکار کامل ارائه داده‌ها به شخص موضوع داده منجر شود. شرکت‌ها موظف‌اند ملاحظات فنی و حقوقی لازم را برای تحقق این حق، بدون آسیب به محرمانگی اطلاعات تجاری، به کار گیرند.

پس از تحلیل مقررات عمومی حفاظت از داده‌ها، لازم است دستورالعمل اسرار تجاری اتحادیه اروپا نیز از منظر تعارض میان حقوق مربوط به اسرار تجاری و داده‌های شخصی بررسی شود. یادآوری شماره ۲۱ این دستورالعمل^{۶۲} بر اصل تناسب تأکید دارد؛ به این معنا که اقدامات حفاظتی در قبال اسرار تجاری، در عین جلوگیری از تحصیل، استفاده یا افشای غیرقانونی، نباید مانع تحقق اهداف بنیادین بازار داخلی نظیر تحقیق و نوآوری بشوند و همچنین به حقوق اساسی افراد یا منافع عمومی نظیر سلامت، امنیت و حقوق مصرف‌کننده لطمه بزنند. بر همین اساس، مقامات قضایی موظف‌اند در رسیدگی‌ها عواملی مانند ارزش اقتصادی راز تجاری، شدت نقض و آثار عملی آن را در کنار منافع طرفین و حتی اشخاص ثالث مانند مصرف‌کنندگان ارزیابی کنند. این رویکرد، توازنی میان منافع دارنده اسرار و سایر ذی‌نفعان برقرار می‌سازد. یادآوری شماره ۳۴ نیز بر هماهنگی این دستورالعمل با حقوق بنیادین مندرج در منشور حقوق اساسی اتحادیه اروپا تأکید دارد؛ ازجمله حق بر حریم خصوصی، حفاظت از داده‌ها، آزادی بیان، مالکیت، دادرسی منصفانه و جبران خسارت^{۶۳}. به این ترتیب، حمایت از اسرار تجاری نباید به پوششی برای محدودسازی غیرقانونی سایر حقوق تبدیل شود. در نهایت، یادآوری شماره ۳۵ تصریح می‌کند که در صورت پردازش داده‌های شخصی در جریان حفاظت از اسرار تجاری یا دادرسی‌های مربوطه، رعایت الزامات قانونی مربوط به حفاظت از داده‌ها لازم است. بنابراین، اقدامات حفاظتی شرکت‌ها باید با ملاحظات حریم خصوصی افراد سازگار باشند^{۶۴}.

با وجود این، در دستورالعمل اسرار تجاری اتحادیه اروپا، بند ۴ ماده ۹ و یادآوری شماره ۳۵^{۶۵}، از مهم‌ترین مقررات دستورالعمل در ارتباط با حفاظت از داده‌های شخصی هستند (یادآوری‌ها

61. Article 29 Working Party, Guidelines on the Right to Data Portability 16/EN WP 242 rev.01, 2017, Available at: <https://ec.europa.eu/newsroom/article29/items/611233/en>.

62. Trade Secrets Directive, Recital 21.

63. Trade Secrets Directive, Recital 34.

64. Trade Secrets Directive, Recital 35.

65. Trade Secrets Directive, art 9(4), Recital 35.

جنبه تفسیری و مشورتی دارند، نه الزام‌آور). بند ۴ ماده ۹ تصریح می‌کند که همه پردازش‌های داده‌های شخصی باید با مقررات حفاظت از داده‌ها کاملاً منطبق باشند. یادآوری شماره ۳۵ نیز تأکید می‌کند که حمایت از اسرار تجاری نباید حقوق و تعهدات ناشی از مقررات حفاظت از داده‌های شخصی، از جمله حقوق دسترسی، اصلاح و حذف داده‌ها را تحت تأثیر قرار دهد. با این حال، محدود بودن قلمرو بند ۴ ماده ۹، به معنای معافیت سایر پردازش‌های مرتبط با اسرار تجاری از مقررات حفاظت از داده‌های شخصی نیست. اما از یک سو، اصول کلی دستورالعمل و تأکید بر احترام به حقوق اساسی، از جمله حفظ داده‌ها، ایجاب می‌کند کلیه پردازش‌های مربوط به اسرار تجاری نیز با مقررات حفاظت از داده‌ها هماهنگ باشد. به عبارت دیگر، دارنده راز تجاری ملزم به رعایت استانداردهای پردازش داده‌های شخصی است، حتی اگر در متون الزام‌آور به‌صراحت ذکر نشده باشد. از سوی دیگر، از میان حقوق ناظر بر داده‌ها، فقط حق دسترسی و حق انتقال ممکن است در صورت تعارض با منافع دیگران محدود شود. بنابراین، اسرار تجاری نباید مبنایی برای محدود کردن سایر حقوق بنیادین داده‌محور مانند حق اطلاع‌رسانی، اصلاح، حذف، محدودسازی پردازش، اعتراض یا مصونیت از تصمیم‌گیری خودکار باشد؛ به‌ویژه حق اطلاع‌رسانی و حق عدم تبعیت از تصمیمات خودکار، اهمیت فراوانی در حمایت از مصرف‌کنندگانی دارد که داده‌های آن‌ها به شکل پنهان تخصیص داده یا حتی فروخته می‌شود.

حق اطلاع‌رسانی تجلی اصل شفافیت است که در مقررات عمومی حفاظت از داده‌ها به‌عنوان یکی از اصول بنیادین پردازش قانونی، منصفانه و شفاف داده‌ها مطرح شده است. این اصل مقابله با پنهان‌کاری است و ایجاب می‌کند که پردازش‌کنندگان داده‌ها به‌صورت صادقانه، دقیق و قابل فهم به افراد اطلاع دهند که چگونه، چرا و از سوی چه نهادی داده‌های آن‌ها پردازش می‌شود. شفافیت در سه محور اصلی تحقق می‌یابد: (۱) اطلاع درباره نوع داده‌های جمع‌آوری شده و روش پردازش یا انتقال آن‌ها؛ (۲) آگاهی از حقوق قانونی افراد موضوع داده؛ (۳) توضیح روش‌های اعمال این حقوق از جانب افراد. تعهد به اطلاع‌رسانی تنها در مواردی که داده‌ها از منابعی به غیر از خود فرد (مثل فروشندگان یا واسطه‌ها) به‌دست آمده‌اند، می‌تواند مستثنی شود؛ مشروط بر اینکه کاربر قبلاً مطلع شده باشد، اطلاع‌رسانی ناممکن یا پرهزینه باشد، اطلاع‌رسانی مانع تحقق اهداف پردازش شود، پردازش بر اساس الزام قانونی انجام شود، یا داده‌ها تحت تعهدات محرمانگی حرفه‌ای قرار داشته باشند. نکته مهم این است که استثنای مربوط به اسرار حرفه‌ای به‌صراحت



ذکر شده، اما این استثنا شامل اسرار تجاری به معنای کلی نمی‌شود. بنابراین، شرکت‌ها حتی در فرایند انتقال اسرار تجاری، اصولاً باید تعهدات شفاف‌سازی و اطلاع‌رسانی را رعایت کنند.^{۶۶} با این حال، ممکن است شرکت‌ها ادعا کنند که افشای اطلاعات به کاربران، تحقق اهداف معامله را مختل می‌کند؛ اما این ادعا مستلزم اثبات دقیق و قابل قبول است و به‌تنهایی موجب معافیت نمی‌شود.^{۶۷} اگرچه افشای اسرار تجاری ممکن است اهداف پردازشی را تحت تأثیر قرار دهد، اما دسترسی یا استخراج داده‌های شخصی مرتبط با آن‌ها لزوماً چنین تأثیری ندارد.

در وضعیت فعلی، حق بر اسرار تجاری به‌عنوان مبنای مستقل مشروعیت پردازش و انتقال داده‌های شخصی شناخته نشده و افراد همچنان می‌توانند حقوق خود را نسبت به داده‌هایشان در چارچوب اسرار تجاری اعمال کنند، مگر آنکه قانون استثنایی مقرر کرده باشد. بنابراین، پردازش، فروش فهرست مشتریان و داده‌های مرتبط بدون رعایت مقررات حفاظت از داده‌ها مجاز نیست و شرکت‌ها باید تدابیر لازم برای حفظ حریم خصوصی و اخذ رضایت معتبر را به‌اجرا گذارند، حتی اگر مالک اسرار تجاری باشند. قوانین حفاظت از داده‌ها، حمایت گسترده‌ای از داده‌های شخصی فراهم می‌کنند و حتی در صورت رضایت قبلی برای استفاده داده‌ها در الگوریتم‌های اختصاصی، هرگونه پردازش یا انتقال داده‌ها به دلیل تغییر هدف، نیازمند رضایت جداگانه است. تنها محدودیت کلی موجود، رعایت حقوق و آزادی‌های مشروع دیگران است که غالباً نیازمند ارزیابی موردی برای تعیین تقدم یکی از حقوق است.

۴.۲. راهکارهای اعمال هم‌زمان حقوق اشخاص مرتبط با اسرار تجاری

در شرایطی که قوانین اجرایی از شفافیت کافی برخوردار نیستند و حدود دقیق حقوق مرتبط با اسرار تجاری به‌عنوان عاملی محدودکننده در برابر حقوق اشخاص موضوع داده به‌روشنی تبیین نشده‌اند، اتخاذ تدابیر احتیاطی و ساختاریافته در حوزه‌های حقوقی و فنی می‌تواند نقش مؤثری در کاهش زمینه‌های تعارض ایفا کند.

66. Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, 2018/WP260 rev.01, 2017, Available at: <https://ec.europa.eu/newsroom/article29/items/622227/en>.

67. Chris J. Hoofnagle, "Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement", 29 N.C. J. Int'l L., 595, (2017), p. 595-600.

۱) یکی از راهکارهای عملی در این زمینه آن است که شرکت‌ها هنگام مواجهه با درخواست‌های افراد برای دسترسی به اطلاعات، این دسترسی را منوط به انعقاد قراردادهای مشخص عدم افشا^{۶۸} با متقاضیان نمایند. علاوه بر این، قراردادهای عدم افشا دو کارکرد هم‌زمان دارند: از یک سو به حفظ محرمانگی اطلاعات تجاری شرکت در قالبی که بیان شد، کمک می‌کند؛ و از سوی دیگر امکان اعمال کنترل مؤثر بر نحوه افشای اطلاعات به اشخاص ثالث را در راستای صیانت از حقوق کاربران فراهم می‌آورد. همچنین در صورت نقض تعهدات قراردادی، امکان استناد به ضمانت‌های اجرای پیش‌بینی‌شده در قرارداد نیز از جمله الزام به حذف اطلاعات و جلوگیری از افشای بیشتر یا حتی جبران خسارات وارده نیز فراهم می‌شود. بنابراین نکته‌ای که نباید مغفول بماند آن است که قرارداد عدم افشا صرفاً ابزاری در راستای تأمین منافع بنگاه‌ها نیست، بلکه می‌تواند به مثابه یکی از سازوکارهای حمایتی برای حقوق اشخاص موضوع داده نیز به کار گرفته شود. افزون بر این، ارائه داده‌ها در پاسخ به چنین درخواست‌هایی باید صرفاً تحت مدیریت مستقیم شرکت صورت پذیرد و با بهره‌گیری از سازوکارهای امنیتی مناسب، به گونه‌ای انجام شود که ضمن پاسخگویی به الزامات قانونی یا قراردادی، با منافع اقتصادی و راهبردی شرکت نیز هماهنگ باشد.

۲) از منظر حقوقی، شرکت‌ها قادرند با تکیه بر مالکیت یا کنترل خود بر اسرار تجاری، این اطلاعات را در قالب‌هایی نظیر واگذاری، اعطای مجوز بهره‌برداری (لیسانس)، یا قراردادهای فرانشیز، منتقل کنند^{۶۹}. در تمامی اشکال انتقال یا صدور مجوز، برای حفظ حریم محرمانگی، استفاده از ابزارهایی چون شروط عدم رقابت، ممنوعیت ترغیب مشتریان، و تعهدات رازداری، نقشی اساسی ایفا می‌کند^{۷۰}؛ به‌ویژه در مواردی که اسرار تجاری مورد انتقال شامل داده‌های شخصی نیز می‌شود، اعم از اینکه انتقال با استناد به حقوق شرکت یا با اتکای به رضایت آگاهانه افراد صورت گیرد، ضروری است که شرکت‌ها پیش از هرگونه افشا، اقدام به انعقاد قراردادهای

68. NDA

۶۹. ابراهیم رهبری، حقوق اسرار تجاری، ج ۱، (تهران: سمت، چ ۴، ۱۳۹۷)، ص ۱۴۹-۱۵۴.

۷۰. ابراهیم رهبری، «نقش قراردادهای محدودکننده در حمایت از اسرار تجاری؛ مطالعه در حقوق آمریکا، انگلستان، فرانسه و ایران»، تحقیقات حقوقی، ش ۵۰ (۱۳۸۸)، ص ۵۴۶.

شفاف، صریح و الزام‌آور در زمینه حفظ محرمانگی با طرف مقابل نمایند.^{۷۱}

حتی در مواردی که صرفاً اجازه بهره‌برداری محدود از اسرار تجاری از طریق قرارداد لیسانس اعطا شده، ولی مالکیت اطلاعات منتقل نمی‌شود، شرکت می‌تواند با درج شروط دقیق و الزام‌آور در متن قرارداد، سازوکارهای رازداری و حفاظت از اطلاعات را تحکیم بخشد. این شروط، امکان کنترل دقیق بر نحوه استفاده و میزان دسترسی به داده‌ها را فراهم می‌سازند و در صورت نقض، مستند حقوقی لازم برای پیگیری را فراهم می‌کنند.^{۷۲}

۳) در کنار این تدابیر قراردادی، طراحی و پیاده‌سازی برنامه‌های پیشرفته برای مدیریت رخدادهای امنیتی^{۷۳} به‌عنوان یک ابزار مکمل فنی، ضرورتی انکارناپذیر است. چنین برنامه‌هایی باید قادر باشند به‌صورت پیشگیرانه و واکنشی، در برابر رخدادهایی نظیر دسترسی غیرمجاز، افشای اطلاعات یا بهره‌برداری غیرقانونی از اسرار تجاری حاوی داده‌های شخصی، وارد عمل شوند. همچنین لازم است این سامانه‌های پاسخگویی امنیتی به‌گونه‌ای طراحی شوند که امکان واکنش سریع، هوشمند و هدفمند را برای صیانت از تمامیت و محرمانگی داده‌ها فراهم سازند.^{۷۴}

۴) افزون بر راهکارهای قراردادی و فنی، بهره‌گیری از تکنیک‌هایی نظیر مستعارسازی^{۷۵} یا ناشناس‌سازی^{۷۶} داده‌های شخصی که به‌عنوان بخشی از محتوای اسرار تجاری تلقی می‌شوند، می‌تواند ابزار مؤثری برای تقویت حریم خصوصی و کاهش خطرهای حقوقی در فرایند پردازش، انتقال، فروش یا واگذاری این اطلاعات باشد. این رویکردهای فنی با کاهش قابلیت شناسایی افراد، احتمال بروز تعارض میان منافع تجاری شرکت‌ها و حقوق اشخاص موضوع داده را تا حد زیادی کاهش می‌دهند.

71. Fawcett, James J. & Torremans, Paul, *Intellectual Property and Private International Law*, (England: Oxford University Press, 1998), p. 75.

۷۲. محمدحسن صادقی مقدم و همکاران، «کاربست نظریه نقض اساسی در قراردادهای لیسانس فناوری»، *مطالعات حقوق تطبیقی معاصر*، (۱۴۰۴)، ص ۲.

73. Security Incident Response Plan

74. Kohel, Matthew & Strin, Austin, (2024), Where Trade Secrets and Data Privacy Strategies Overlap, Available at: <https://ipwatchdog.com/2024/01/31/trade-secrets-data-privacy-strategies-overlap/id=172502/>, Visited 2024/06/06.

75. Pseudonymization

76. Anonymization

با این حال، در بستر حقوق اسرار تجاری، باید به این نکته توجه داشت که دسترسی به اطلاعات محرمانه صرفاً زمانی غیرقانونی تلقی می‌شود که برخلاف هنجارهای منصفانه و مشروع باشد، و یکی از استثنای مهم در این زمینه، استفاده از مهندسی معکوس^{۷۷} است. این روش به‌عنوان یکی از شیوه‌های مشروع دستیابی به اطلاعات، در دو موقعیت حقوقی قابل تصور است: نخست، در شرایطی که کالا، خدمت یا اطلاعاتی به‌صورت عمومی در بازار عرضه و منتشر شده است و در نتیجه امکان تحلیل و استنتاج ویژگی‌های فنی آن از طریق بررسی مستقل وجود دارد؛ و دوم، در وضعیتی که شرکت اطلاعاتی را در چارچوب قراردادی خاص در اختیار گیرنده معین قرار داده، به‌گونه‌ای که این اطلاعات، هرچند محرمانه، به‌طور هدفمند به مخاطب خاص انتقال یافته‌اند. در حالت دوم، یعنی زمانی که اسرار تجاری حاوی داده‌های شخصی مستعار یا ناشناس هستند، خطر بازشناسایی افراد از طریق اعمال روش‌های مهندسی معکوس وجود دارد. برای پیشگیری از این خطر و تضمین رعایت هم‌زمان حقوق شرکت و حریم خصوصی افراد، شرکت‌ها باید در تنظیم قراردادهای با گیرندگان اطلاعات، به‌صراحت شرطی مبنی بر منع هرگونه تلاش برای بازشناسایی داده‌ها از طریق مهندسی معکوس درج نمایند. چنین شروطی باید به‌گونه‌ای تدوین شوند که دامنه آن‌ها تمامی اشکال تحلیل فنی، استنتاج الگوریتمی یا بازیابی هویت فردی را نیز دربر گیرد. در واقع، پیش‌بینی صریح چنین ممنوعیتی، بخشی از الزامات مکمل برای حمایت توأمان از منافع تجاری بنگاه و حقوق اطلاعاتی اشخاص موضوع داده تلقی می‌شود. از منظر حقوقی، این شروط نقش تعیین‌کننده‌ای در تحکیم مرزهای مسئولیت طرف دریافت‌کننده دارند و مانعی جدی در برابر استفاده‌های ثانوی و غیرمجاز از اطلاعات مستعارشده یا ناشناس‌سازی‌شده خواهند بود.^{۷۸}

۵) یکی دیگر از مؤثرترین شیوه‌ها برای تحقق توأمان حقوق اشخاص موضوع داده و منافع دارندگان اسرار تجاری، استفاده از رویکردی موسوم به تفکیک و محتوایابی^{۷۹} است. مطابق این رهیافت، اعمال حقوق داده‌ای اشخاص، نظیر حق دسترسی، تصحیح یا حذف اطلاعات، صرفاً

77. Reverse Engineering

۷۸. زهرا شاکری، «خوانشی بر تحدید قلمرو حقوق اسرار تجاری؛ با نگاهی به دفاعیات خوانندگان دعاوی نقض»، تحقیقات حقوقی، ش ۷۰ (۱۳۹۴)، ص ۲۰۹.

79. Segregation and Content-depletion



نسبت به داده‌های اولیه و خامی امکان‌پذیر است که فرد ذی‌ربط با رضایت آگاهانه خود در اختیار شرکت قرار داده است. این حقوق، به‌هیچ‌وجه شامل نتایج حاصل از تحلیل، الگوریتم‌های استخراج‌شده، فرایندهای دسته‌بندی، یا دانش فنی ایجادشده از طریق تجميع داده‌ها در قالب پایگاه‌های اطلاعاتی یا سامانه‌های کلان‌داده نمی‌شود. در پاسخ به درخواست‌های ناظر بر اعمال حقوق داده‌ای، شرکت باید ابتدا با بهره‌گیری از روش‌های محتوایابی، مرز مشخصی میان داده‌های خام و اطلاعات حاصل از پردازش ایجاد کرده، صرفاً داده‌های اولیه را، آن‌هم در سطحی که فاقد ارزش تجاری و غیرمرتبط با اسرار شرکتی باشد، در اختیار فرد قرار دهد. این تفکیک ساختاری، زمینه‌ساز نوعی تعادل کارآمد میان حفظ حریم خصوصی افراد و صیانت از دارایی‌های اطلاعاتی شرکت است. چنین تمایزی میان داده‌های شخصی به‌عنوان دارایی‌های اطلاعاتی فردی و اطلاعات پردازش‌شده به‌عنوان سرمایه فکری شرکت، امکان اعمال مستقل حقوق هر طرف را بدون بروز تراحم یا نقض فراهم می‌سازد.^{۸۰} در فرایندهایی نظیر فروش یا واگذاری اسرار تجاری نیز این منطق کاربرد مؤثری دارد. با حذف یا بی‌نام‌سازی داده‌های شناسایی‌پذیر از درون اسرار مورد انتقال، می‌توان صرفاً برون‌داد تحلیلی، الگوریتم‌ها یا فرآورده‌های اطلاعاتی حاصل از داده‌ها را به انتقال‌گیرنده تحویل داد، بی‌آنکه داده‌های خام یا قابل انتساب به افراد در معرض افشا قرار گیرند. این راهبرد، نه‌تنها به شرکت اجازه می‌دهد مزیت رقابتی خود را حفظ کند، بلکه مانع از نقض حقوق اطلاعاتی اشخاص ثالث نیز خواهد شد.

با این همه، چالش اصلی در بهره‌گیری از این مدل، ترسیم دقیق حدود حقوق مشروع هریک از طرفین است. حقوق حریم خصوصی نباید چنان گسترده تفسیر شود که ابتکارات فناورانه یا بهره‌برداری مشروع از داده‌ها را با اختلال مواجه سازد؛ به همان میزان نیز نباید به اسرار تجاری اجازه داد که پوششی برای سلب یا تحدید حقوق بنیادین اشخاص نسبت به داده‌های خود شوند. نظام‌های حقوقی پیشرو، از طریق طراحی برخی استثنایات، الزام به شفاف‌سازی و مکانیزم‌های جبران خسارت، تلاش کرده‌اند این تعارض ذاتی را در سطحی منطقی و قابل مدیریت نگه دارند.

ارزیابی کلی پژوهش در پرتو مباحث مطرح‌شده نشان می‌دهد که راه‌حل توازن‌یافته برای این تعارض، نه در تقدم مطلق یکی از حقوق، بلکه در یک مدل تحلیلی «حداقل تقييدِ ضروری»^{۸۱}

80. Malgieri, Gianclaudio, *op. cit.* p. 102-107.

81. Minimum Necessary Restriction

نهفته است. بر اساس این مدل، نظام حقوقی باید: الف) فرض اولیه را بر حاکمیت حق اشخاص بر داده‌های خود قرار دهد؛ ب) استثنا بر این حق، یعنی حق بر اسرار تجاری، باید از سوی شرکت به صورت دقیق، مستند و محدود اثبات شود؛ ج) جایی که تفکیک داده‌های شخصی از اسرار تجاری ممکن است، این تفکیک اجباری است؛ د) جایی که تفکیک ممکن نیست، دسترسی محدود^{۸۲} به جای انکار کامل دسترسی ترجیح دارد. این مدل با رویه اتحادیه اروپا، به ویژه تفسیر کارگروه ماده ۲۹ از یادآوری شماره ۶۳ مقررات عمومی حفاظت از داده‌ها، همخوانی دارد و می‌تواند در نظام حقوقی ایران نیز به عنوان چارچوب تفسیری پیشنهادی مورد استفاده قرار گیرد.

از منظر راهکارهای حقوقی و تقنینی، فراتر از تدابیر قراردادی و فنی، سه دسته راهکار کلان قابل پیشنهاد است: اول، راهکارهای تقنینی: تصویب قانون جامع حفاظت از داده‌های شخصی در ایران برای تنظیم صریح رابطه میان حقوق داده‌ای و اسرار تجاری، درج ماده‌ای با الهام از رویکرد یادآوری شماره ۳۵ دستورالعمل اسرار تجاری اتحادیه اروپا که تمام پردازش‌های مربوط به اسرار تجاری را به رعایت مقررات حفاظت از داده‌ها ملزم کند و نیز تعریف دقیق استثنای اسرار تجاری با محدوده مشخص و قابل کنترل قضایی. دوم، راهکارهای تنظیمی: ایجاد یک نهاد تنظیمی مستقل برای حل اختلاف در موارد تعارض میان حقوق داده‌ای و اسرار تجاری، طراحی سازوکار ارزیابی اثر حریم خصوصی برای موارد پردازش داده‌ها در قالب اسرار تجاری، و تدوین دستورالعمل‌های اجرایی برای شرکت‌ها در مورد نحوه تفکیک داده‌های شخصی از اسرار تجاری. سوم، راهکارهای قضایی: تدوین رویه یکپارچه قضایی برای رسیدگی به دعاوی تعارض حق داده‌ای و اسرار تجاری، بهره‌گیری از کارشناس مستقل فنی - حقوقی در دعاوی مربوطه و اعمال اصل تناسب در صدور دستورات موقت در این حوزه.

ارتباط این راهکارها به نظام حقوقی ایران در بخش نهایی به صورت مستقل بررسی می‌شود.

نتیجه

با گسترش کاربرد داده‌های شخصی در فعالیت‌های تجاری و فناوری، تعارض میان حق افراد بر داده‌های شخصی و حق دارنده اسرار تجاری به موضوعی پیچیده و مهم در حوزه حقوق

فناوری و حفاظت از حریم خصوصی تبدیل شده است. تحلیل مقررات بین‌المللی از جمله مقررات عمومی حفاظت از داده‌های اتحادیه اروپا و دستورالعمل اسرار تجاری نشان می‌دهد که این دو حق، هرچند گاهی در تعارض قرار می‌گیرند، اما هیچ‌یک نباید به صورت مطلق بر دیگری ارجحیت یابد. توازن حقوقی عادلانه و مؤثر تنها از طریق اتخاذ راهکارهای فنی و حقوقی هوشمندانه امکان‌پذیر است.

راهکارهای کلیدی در این زمینه، شامل تفکیک و جداسازی داده‌های شخصی از اسرار تجاری، مستعارسازی و ناشناس‌سازی داده‌ها، ایجاد سازوکارهای دسترسی کنترل‌شده به داده‌ها و عقد قراردادهای محرمانگی میان طرفین ذی‌ربط است. همچنین، اجرای ارزیابی‌های موردی و فنی از سوی مراجع ذی‌صلاح برای تعیین مرزهای تعارض و تنظیم شرایط دسترسی و انتقال داده‌ها، می‌تواند نقش بسزایی در حل اختلافات داشته باشد.

در حقوق ایران، نبود قانون جامع و مشخص در حوزه حمایت از داده‌های شخصی و تعیین چارچوب حقوقی تعارضات با اسرار تجاری، خلأ قابل‌توجهی ایجاد کرده که به سردرگمی و نااطمینانی در روابط تجاری و فناورانه منجر شده است. از این رو، تصویب قانون مدون و جامع حفاظت از داده‌های شخصی با توجه به واقعیت‌های فناورانه و حقوقی کشور، امری ضروری است تا ضمن حفظ حقوق فردی، از منافع مشروع دارنده اسرار تجاری نیز محافظت شود.

با نگاهی دقیق‌تر به وضعیت حقوق ایران، می‌توان سه لایه قانونی مرتبط را تشخیص داد:

لایه نخست، حقوق اسرار تجاری که در ماده ۶۵ قانون تجارت الکترونیکی (۱۳۸۲) و ماده ۱۲۲ قانون مالکیت صنعتی (۱۴۰۳) تنظیم شده است.

لایه دوم، مقررات پراکنده حمایت از داده‌های شخصی در قانون انتشار و دسترسی آزاد به اطلاعات، قانون تجارت الکترونیکی و پیش‌نویس‌های لایحه حمایت از داده‌ها.

لایه سوم، اصول کلی حقوقی ناظر بر حریم خصوصی برگرفته از قانون اساسی، به‌ویژه اصول ۲۲ و ۲۵.

نبود ارتباط صریح قانونی میان این لایه‌ها، اصلی‌ترین چالش نظام حقوقی ایران در این زمینه است. برای نمونه، اگر شرکتی در ایران با استناد به ماده ۱۲۲ قانون مالکیت صنعتی مانع

دسترسی فرد به داده‌های شخصی‌اش شود، هیچ ضابطه قانونی روشنی برای ارزیابی مشروعیت این اقدام وجود ندارد. این خلأ تقنینی بزرگ‌ترین تفاوت نظام حقوقی ایران با حقوق اتحادیه اروپاست که در آن، مقررات عمومی حفاظت از داده‌ها و دستورالعمل اسرار تجاری به‌طور صریح برای همزیستی طراحی شده‌اند.

پیامدهای عملی این یافته‌ها برای نظام حقوقی ایران را می‌توان در چند محور خلاصه کرد:

نخست، در دعاوی حقوقی جاری. دادگاه‌های ایران در غیاب قانون خاص، می‌توانند با تکیه بر اصل ۲۲ قانون اساسی (حمایت از حیثیت و حریم خصوصی) و اصول و قواعد کلی حقوق (چون اصل عدم اضرار به غیر) و نیز در قرائت مضیق از مفهوم اسرار تجاری در ماده ۶۵ قانون تجارت الکترونیکی، به‌گونه‌ای تفسیر کنند که حقوق داده‌ای اشخاص کمتر محدود شود.

دوم، در سیاست‌گذاری. تصویب قانون جامع حمایت از داده‌های شخصی، گامی ضروری است و این قانون باید به‌صراحت ماده‌ای برای تنظیم تعارض با اسرار تجاری در خود داشته باشد (مشابه ماده پیشنهادی در این بخش).

سوم، برای شرکت‌های فعال در ایران. تا زمان تصویب قانون جامع، شرکت‌ها باید به‌صورت داوطلبانه سیاست‌های حفاظت از داده‌ها را متناسب با استانداردهای بین‌المللی اجرا کنند، به‌ویژه اگر با شرکای اروپایی یا تحت پوشش مقررات عمومی حفاظت از داده‌ها فعالیت می‌کنند.

در این خصوص چند پیشنهاد عملی قابل ارائه است:

۱- تفکیک و طبقه‌بندی داده‌ها. تدوین استانداردهای مشخص برای تشخیص داده‌های شخصی و اسرار تجاری و مرزهای تفکیک آنها در سطح فنی و حقوقی.

۲- ایجاد سامانه‌های دسترسی کنترل‌شده. راه‌اندازی سامانه‌های امن مبتنی بر فناوری اطلاعات که دسترسی به داده‌های شخصی را تحت نظارت و محدودیت‌های حقوقی فراهم کند تا اسرار تجاری حفظ شود.

۳- ارزیابی موردی و متوازن‌سازی حقوق. تعیین فرایندهای حقوقی و قضایی ویژه برای بررسی مورد به مورد تعارضات بین حقوق داده‌ها و اسرار تجاری، با استفاده از کارشناس‌های فنی و حقوقی.

۴- آموزش و فرهنگ‌سازی. تقویت ظرفیت‌های حقوقی، فنی و اجرایی در بخش‌های خصوصی و دولتی برای مدیریت صحیح داده‌ها و اسرار تجاری.

همچنین باوجود تلاش‌های متعدد در حقوق ایران از طریق ارائه طرح‌ها و لوایح بی‌سرانجام، پیشنهاد می‌شود که با تصویب قانونی جامع در مورد حمایت از داده‌های شخصی، ماده‌ای مشابه با ماده پیشنهادی زیر در آن درج گردد:

(۱) در مواردی که داده‌های شخصی موضوع حق دسترسی، انتقال یا اصلاح، شامل اطلاعاتی باشد که به‌عنوان اسرار تجاری شناخته می‌شوند، باید به‌گونه‌ای اقدام کرد که حقوق و آزادی‌های فرد موضوع داده حفظ شود و در عین حال، منافع مشروع دارنده اسرار تجاری مورد حمایت قرار گیرد.

(۲) دارنده اسرار تجاری موظف است قبل از محدودسازی دسترسی به داده‌های شخصی، امکان تفکیک داده‌های شخصی قابل ارائه از اسرار تجاری را بررسی و به‌صورت مستند اعلام نماید.

(۳) در صورتی که تفکیک داده‌ها ممکن نباشد، دارنده اسرار تجاری باید دسترسی کنترل‌شده و تحت نظارت قانونی به داده‌های شخصی را فراهم نماید تا از افشای غیرمجاز اسرار تجاری جلوگیری شود.

(۴) انتقال داده‌های شخصی که با اسرار تجاری مرتبط است، منوط به رعایت شرایط زیر است:

الف) رضایت آگاهانه و صریح فرد موضوع داده برای انتقال، مگر آنکه قانون یا مراجع ذی‌صلاح شرایط دیگری را مقرر کرده باشند.

ب) اتخاذ تدابیر فنی و سازمانی برای حفظ محرمانگی اسرار تجاری در فرایند انتقال.

(۵) مراجع ذی‌صلاح موظف‌اند در موارد اختلاف، بر اساس ارزیابی کارشناسی، نسبت به تعیین توازن میان حقوق فرد موضوع داده و اسرار تجاری اقدام نمایند.

منابع و مأخذ

الف) منابع فارسی

کتاب

۱. رهبری، ابراهیم (۱۳۹۷). *حقوق اسرار تجاری*. تهران: سمت.

مقالات

۲. اسماعیلی، محسن و تقی‌زاده، ابراهیم و حیدری منور، حسین (۱۳۹۷). حل چالش‌های عمده در دعاوی اسرار تجاری با رفع تراحم دو حق؛ دادخواهی منصفانه و حفظ محرمانگی اطلاعات. *مطالعات حقوق تطبیقی معاصر*، ۹(۱۶)، ۱-۲۹. Doi: 10.22034/law.2018.8532
۳. انصاری، باقر (۱۴۰۱). حمایت از اسرار تجاری در برابر افشای غیرمجاز. *پژوهش حقوق خصوصی*، ۱۱(۴۱)، ۴۱-۸۲. Doi: 10.22054/jplr.2023.62445.2593
۴. رهبری، ابراهیم (۱۳۸۸). نقش قراردادهای محدود کننده در حمایت از اسرار تجاری مطالعه در حقوق آمریکا، انگلستان، فرانسه و ایران. *تحقیقات حقوقی*، ۱۲(۵۰)، ۵۳۱-۵۸۶.
۵. شاکری، زهرا (۱۳۹۴). خوانشی بر تحدید قلمرو حقوق اسرار تجاری؛ با نگاهی به دفاعیات خواندگان دعاوی نقض. *تحقیقات حقوقی*، ۱۸(۷۰)، ۱۹۷-۲۲۲.
۶. صادقی مقدم، محمدحسن؛ عرب‌زاده، رضا و شمس، آزاده (۱۴۰۴). کاربست نظریه نقض اساسی در قراردادهای لیسانس فناوری. *مطالعات حقوق تطبیقی معاصر*، ۱۶(۳۹)، ۹۳-۱۲۴. Doi: 10.22034/law.2025.63625.3418

ب) منابع انگلیسی

Books

7. Fawcett, James j, & Torremans, Paul (1998). *intellectual property and private international law*. Oxford University press, England.
8. Rahbari, Ebrahim, (1397). *Trade Secrets Law*, 4th ed., Samt, Tehran. [In Persian].

Thesis

9. Radoń, Barbara Anna (2015). Trade Secrets Protection for 'Big Data': Personal Data as Trade Secrets in the European Union, **Master Thesis**, MIPLC, Munich. Available at: SSRN: <http://ssrn.com/abstract=-3012525>.

Articles

10. Ansari, Bagher (1401). Protection of Trade Secrets against Unauthorized Disclosure, **Private Law Research**, 11(41), 41-82. [In Persian]. Doi: 10.22054/jplr.2023.62445.2593.
11. Aplin, Tanya F. (2014). A Critical Evaluation of the Proposed EU Trade Secrets Directive, **King's College London Law School Research Paper**, 25, Doi: 10.2139/ssrn.2467946.
12. Banterle, F. (2016). The Interface Between Data Protection and IP Law: The Case of Trade Secrets and Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis, in Bakhoum, M. et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*
13. Chris J. Hoofnagle (2017). Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. **J. Int'l L**, 595.
14. Di Martino, M. (2019). Personal Information Leakage by Abusing the GDPR "Right of Access", In Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19), USENIX Association, USA, 371-386.
15. Drexler, J. (2017). Designing Competitive Markets for Industrial Data between Propertisation and Access, **JIPITEC**, 8, 257-292. Doi: 10.2139/ssrn.2862975.
16. Esmaeili, Mohsen; Taghizadeh, Ebrahim; & Heydari Manvar, Hossein (1397). Solving Major Challenges in Trade Secret Disputes through Balancing Two Rights; Fair Trial and Confidentiality of Information, **Contemporary Comparative Law Studies**, 9(16), 1-29. [In Persian]. Doi: 10.22034/law.2018.8532.

17. La Diega Noto, Guido & Sappa, Cristiana (2020). The Internet of Things at the Intersection of Data Protection and Trade Secrets, Non-Conventional Paths to Counter Data Appropriation and Empower Consumers, *Revue Européenne de Droit de la Consommation, European Journal of Consumer Law*, 3, 419-458.
18. Malgieri, Gianclaudio (2016). Trade Secrets v Personal Data: A Possible Solution for Balancing Rights, *International Data Privacy Law*, 6(2), 102-116.
19. Mylly, U. M. (2024). Trade Secrets and the Data Act, IIC, 55, pp 368-393, Available at: <https://link.springer.com/article/10.1007/s40319-024-01432-0>.
20. Rahbari, Ebrahim (1388). The Role of Restrictive Contracts in Protecting Trade Secrets: A Study in the Laws of the United States, England, France, and Iran, *Legal Research Quarterly*, 12(50), 531-586. [In Persian].
21. Sadeghi Moghadam; Mohammad Hassan; Arabzadeh, Reza; & Shams, Azadeh (1404). Application of the Theory of Fundamental Breach in Technology License Contracts, *Contemporary Comparative Law Studies*. [In Persian]. Doi: 10.22034/law.2025.63625.3418.
22. Shakeri, Zahra (1394). A Reading on the Limitation of the Scope of Trade Secret Rights; With a View to Defenses of Defendants in Infringement Claims, *Legal Research Quarterly*, 18(70), 197-222. [In Persian].
23. Sweeney, L. (2002). K-Anonymity: a Model for Protecting Privacy, *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 557-570. Doi: 10.1142/S02184885020016
24. White, Nancy & Sanney, Kenneth (2010). FOIA and Trade Secrets: Managing the Risks of FOIA-Able Trade Secrets, *SSRN Electronic Journal*, Available at: <https://ssrn.com/abstract=1738409>.

Websites

25. Amazon Inc, Privacy Notice, Available at: <https://www.amazon.com/-gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ>.
26. Article 29 Working Party, Guidelines on Automated Individual

- Decision-Making and Profiling for the Purposes of Regulation 2016/679 (wp251rev.01), Available at: <<https://ec.europa.eu/newsroom/article29/items/612053/en>>.
27. Article 29 Working Party, Guidelines on the Right to Data Portability 16/EN WP 242 rev.01, 2017, Available at: <https://ec.europa.eu/newsroom/article29/items/611233/en>.
28. Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, 2018/WP260 rev.01, 2017, Available at: <https://ec.europa.eu/newsroom/article29/items/622227/en>.
29. Baker & McKenzie, Study on Trade Secrets and Confidential Business Information in the Internal Market, Available at: http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf.
30. Colgate, Jenny, Why Privacy and Trade Secret Law Are on A Collision Course, Available at: <https://www.jdsupra.com/legalnews/why-privacy-and-trade-secret-law-are-on-6821298/>.
31. ICO, Guide to the General Data Protection Regulation, Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>.
32. PhoneDog v. Kravitz, No. C 11-03474 MEJ, Available at: https://scholar.google.com/scholar_case?case=9890904231170613660.
33. Schrems v. Facebook, Available at: http://www.europe-v-facebook.-org/FB_E-Mails_28_9_11.pdf.
34. World Trade Organization, Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Available at: <https://www.wipo.int/wipolex/en/treaties/details/231>.