شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی ۱۹۲۲-۲۷۸۳

تمدن حقوقی

دوره ۸ - شماره ۲۶ - زمستان ۱۴۰۴

egal Civilization
Vol. 8, No. 26, Winter 2026
Pages: 477-502
Article Type: Original Research
https://www.pzhfars.ir/article_238746.html
doi: 10.22034/lc.2026.570058.1727

تمدن حقوقی
دوره ۸، شماره ۲۶، زمستان ۱۴۰۴
صفحات: ۵۰۲-۴۷۷
نوع مقاله: پژوهشی

Commitment to Data Security as a Commitment to Result or a Commitment to Means in Private Law

Sayyed Amirhasan Mostafavi
Master of Science in Private Law, Faculty of Humanities, Islamic Azad University, Hamadan Branch, Hamadan, Iran

تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد به نتیجه یا تعهد به وسیله در حقوق خصوصی

سیدامیرحسن مصطفوی
کارشناس ارشد حقوق خصوصی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد همدان، همدان، ایران
seyedamirmostafavi@gmail.com

Abstract

The expansion of the digital economy and the pivotal role of data in private relationships have transformed the commitment to data security into one of the most significant obligations for individuals and legal entities. Data security breaches not only lead to financial losses but also damage privacy and public trust. However, in private law, a fundamental ambiguity persists regarding the nature of this commitment: Is the commitment to data security a commitment to means or a commitment to result? The central question of this research is, from the perspective of private law, what is the nature of the commitment to data security, and what is the criterion for determining it? Consequently, how can the implications of each of these two interpretations be analyzed regarding the civil liability of the obligor? The aim of this article is to clarify the legal nature of the commitment to data security, analyze the consequences of each of the two approaches—commitment to means and commitment to result—and provide an efficient model that aligns with technological developments and protective needs. The present research has been conducted using a descriptive-analytical method and drawing upon library resources, domestic laws, legal doctrines, and comparative law approaches. Considering this commitment absolutely as a commitment to means or result does not address the technical and legal complexities of the data field. Accordingly, the article arrives at a mixed and dynamic model in which the type of data, the professional status of the obligor, and the level of risk play a fundamental role in determining the nature of the commitment. In conclusion, adopting this approach can, while strengthening the protection of data subjects, create an appropriate balance between civil liability and the development of digital activities.

Keywords: Data Security, Commitment to Means, Commitment to Result, Private Law, Information Security.

چکیده

گسترش اقتصاد دیجیتال و نقش محوری داده‌ها در روابط خصوصی، تعهد به ایمن‌سازی داده‌ها را به یکی از مهم‌ترین تعهدات اشخاص حقیقی و حقوقی تبدیل کرده است. نقض امنیت داده‌ها نه‌تنها خسارات مالی، بلکه لطمه به حریم خصوصی و اعتماد عمومی را به دنبال دارد. بااین‌حال، در حقوق خصوصی همچنان ابهام اساسی درباره ماهیت این تعهد وجود دارد: آیا تعهد به ایمن‌سازی داده‌ها تعهد به وسیله است یا تعهد به نتیجه؟ مسئله اصلی این پژوهش آن است که تعهد ایمن‌سازی داده‌ها از منظر حقوق خصوصی چه ماهیتی دارد و معیار تشخیص آن چیست؟ و به‌تبع آن، آثار هریک از این دو تلقی بر مسئولیت مدنی متعهد چگونه قابل تحلیل است؟ هدف این پژوهش تبیین ماهیت حقوقی تعهد به ایمن‌سازی داده‌ها، تحلیل پیامدهای هریک از دو رویکرد تعهد وسیله و تعهد نتیجه و ارائه الگویی کارآمد و منطبق با تحولات فناوری و نیازهای حمایتی است. پژوهش حاضر با روش توصیفی-تحلیلی و با بهره‌گیری از منابع کتابخانه‌ای، قوانین داخلی، دکترین حقوقی و رویکردهای حقوق تطبیقی انجام شده است. تلقی مطلق این تعهد به‌عنوان تعهد وسیله یا نتیجه، پاسخگوی پیچیدگی‌های فنی و حقوقی حوزه داده نیست. بر این اساس، پژوهش به الگوی مختلط و پویا دست می‌یابد که در آن، نوع داده، جایگاه حرفه‌ای متعهد و سطح خطر، در تعیین ماهیت تعهد نقش اساسی دارند. نتیجه آن‌که پذیرش این رویکرد می‌تواند ضمن تقویت حمایت از اشخاص موضوع داده، تعادل مناسبی میان مسئولیت مدنی و توسعه فعالیت‌های دیجیتال ایجاد کند.

واژگان کلیدی: ایمن‌سازی داده‌ها، تعهد به وسیله، تعهد به نتیجه، حقوق خصوصی، امنیت اطلاعات.

دریافت مقاله: ۱۴۰۴/۱۰/۱۰ –بازنگری مقاله: ۱۴۰۴/۱۱/۲۱ –پذیرش مقاله: ۱۴۰۴/۱۲/۲۵

Received: 2025/12/31 - Review: 2026/02/10 - Accepted: 2026/03/16

ارجاع:
مصطفوی، سیدامیرحسن؛ (۱۴۰۴)، تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد به نتیجه یا تعهد به وسیله در حقوق خصوصی، تمدن حقوقی، شماره ۲۶.

مقدمه

تحولات شتابان فناوری اطلاعات و گسترش روابط مبتنی‌بر داده، چهره سنتی روابط حقوق خصوصی را به‌طور بنیادین دگرگون ساخته است. امروزه داده‌ها، به‌ویژه داده‌های شخصی، نه‌تنها به‌عنوان یک منبع اقتصادی ارزشمند، بلکه به‌مثابه عنصری تعیین‌کننده در شکل‌گیری اعتماد، حریم خصوصی و امنیت اشخاص در بستر دیجیتال مطرح‌اند. اشخاص حقیقی و حقوقی در جریان فعالیت‌های اقتصادی، قراردادی و حتی غیرقراردادی، حجم گسترده‌ای از داده‌ها را جمع‌آوری، پردازش و ذخیره می‌کنند؛ امری که به‌طور اجتناب‌ناپذیر، تعهد به ایمن‌سازی داده‌ها را به یکی از اساسی‌ترین تعهدات ناشی از این روابط بدل ساخته است. افزایش روزافزون حملات سایبری، نشت داده‌ها و سوءاستفاده از اطلاعات شخصی، اهمیت این تعهد و آثار حقوقی نقض آن را دوچندان کرده و پرسش‌های بنیادینی را در حوزه مسئولیت مدنی و حقوق خصوصی پدید آورده است.

با وجود این اهمیت، ماهیت حقوقی تعهد به ایمن‌سازی داده‌ها همچنان با ابهام جدی مواجه است. در حقوق خصوصی، تمایز میان «تعهد به وسیله» و «تعهد به نتیجه» نقشی تعیین‌کننده در تعیین بار اثبات، گستره مسئولیت و حدود ضمانت‌اجراها ایفاء می‌کند. اگر ایمن‌سازی داده‌ها تعهدی به وسیله

تلقی شود، متعهد صرفاً مکلف به به‌کارگیری مراقبت متعارف و اقدامات معقول خواهد بود و اثبات تقصیر بر عهده زیان‌دیده قرار می‌گیرد. در مقابل، اگر این تعهد از نوع تعهد نتیجه دانسته شود، صرف نقض امنیت داده‌ها می‌تواند موجب تحقق مسئولیت متعهد گردد، مگر آن‌که وی وجود عوامل خارجی یا قوه قاهره را اثبات کند. این دو تلقی متفاوت، آثار حقوقی و عملی کاملاً متمایزی دارند و انتخاب هریک، می‌تواند توازن میان حمایت از اشخاص موضوع داده و آزادی فعالیت‌های اقتصادی را به‌طور جدی تحت تأثیر قرار دهد.

ازاین‌رو، مسئله اصلی پژوهش حاضر آن است که تعهد به ایمن‌سازی داده‌ها در حقوق خصوصی چه ماهیتی دارد؟ آیا می‌توان آن را تعهدی به وسیله یا تعهدی به نتیجه دانست، یا آن‌که نیازمند رویکردی متفاوت و منعطف است؟ همچنین این پرسش مطرح می‌شود که معیارهای تشخیص ماهیت این تعهد چیست و هریک از این رویکردها چه پیامدهایی برای مسئولیت مدنی متعهدان داده به همراه دارد. هدف اصلی این پژوهش، تبیین دقیق ماهیت حقوقی تعهد به ایمن‌سازی داده‌ها و تحلیل انتقادی رویکردهای موجود درباره تعهد وسیله و تعهد نتیجه است. پژوهش در پی آن است که ضمن بررسی مبانی نظری هریک از این دو تلقی، آثار و کاستی‌های آن‌ها را در بستر روابط مبتنی‌بر داده روشن سازد و در نهایت، الگویی کارآمد و منطبق با واقعیت‌های فنی و حقوقی عصر دیجیتال ارائه دهد. هدف نهایی، دستیابی به راهکاری است که بتواند هم‌زمان از حقوق اشخاص موضوع داده حمایت مؤثر به عمل آورد و از تحمیل مسئولیت نامتناسب بر فعالان اقتصادی و ارائه‌دهندگان خدمات دیجیتال جلوگیری کند.

روش تحقیق در این پژوهش، توصیفی–تحلیلی است و با بهره‌گیری از منابع کتابخانه‌ای، شامل کتب، مقالات علمی، قوانین و مقررات داخلی و اسناد حقوق تطبیقی انجام شده است. افزون بر این، از تحلیل مفهومی و استدلال حقوقی برای تبیین تمایز میان تعهد وسیله و نتیجه و تطبیق آن با تعهد ایمن‌سازی داده‌ها استفاده شده است. در بخش تطبیقی، رویکردهای منتخب حقوق خارجی، به‌ویژه حقوق اتحادیه اروپا و حقوق فرانسه، مورد توجه قرار گرفته‌اند تا از رهگذر آن‌ها، امکان ارائه راه‌حلی

متوازن‌تر فراهم شود. جنبه نوآورانه این پژوهش در آن است که به‌جای تقلیل تعهد ایمن‌سازی داده‌ها به یکی از دو قالب سنتی تعهد وسیله یا نتیجه، مدلی انعطاف‌پذیر و چندمعیاره پیشنهاد می‌کند که با تحولات فناوری و نیازهای حمایتی معاصر همخوانی دارد. این رویکرد می‌تواند مبنایی برای تفسیر قضایی، توسعه دکترین حقوقی و حتی اصلاحات تقنینی در حوزه حمایت از داده‌ها فراهم آورد.

تلقی مطلق تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد وسیله یا تعهد نتیجه، پاسخگوی پیچیدگی‌های فنی، تنوع داده‌ها و تفاوت موقعیت متعهدان نیست. در عمل، سطح خطر، نوع داده[1]، جایگاه حرفه‌ای متعهد و انتظارات مشروع اشخاص موضوع داده، نقش تعیین‌کننده‌ای در ارزیابی این تعهد ایفاء می‌کنند. بر این اساس، پژوهش به این نتیجه می‌رسد که یک رویکرد مختلط و پویا که در آن ماهیت تعهد بر اساس اوضاع و احوال هر مورد تعیین شود، از کارآمدی و انصاف بیشتری برخوردار است. بازاندیشی در ماهیت تعهد به ایمن‌سازی داده‌ها و پذیرش رویکردی منعطف، نه‌تنها به تقویت حمایت از حقوق اشخاص و افزایش اعتماد عمومی در فضای دیجیتال می‌انجامد، بلکه زمینه‌ساز تعادل مطلوب میان مسئولیت مدنی و پویایی فعالیت‌های اقتصادی در حقوق خصوصی خواهد بود.

۱- مفهوم داده در حقوق خصوصی

«داده»[2] در معنای عام، مجموعه‌ای از اطلاعات خام، نشانه‌ها یا علائم قابل پردازش است که به‌تنهایی یا در کنار داده‌های دیگر معنا پیدا می‌کند. بااین‌حال، در حقوق خصوصی، داده صرفاً یک مفهوم فنی یا رایانه‌ای نیست، بلکه موضوع روابط حقوقی، منافع اقتصادی و گاه حقوق بنیادین اشخاص قرار می‌گیرد. از همین رو، تعریف داده در این حوزه نیازمند نگاهی کارکردی و هنجاری است، نه صرفاً توصیفی. داده به‌عنوان «هر نوع اطلاعات مرتبط با شخص حقیقی یا حقوقی که قابلیت‌شناسایی مستقیم یا غیرمستقیم داشته باشد» تعریف شده است. این تعریف که در اسناد بین‌المللی و حقوق تطبیقی،

۱- عادی یا حساس

2- Data

به‌ویژه مقررات عمومی حفاظت از داده اتحادیه اروپا[3]، مورد پذیرش قرار گرفته، بر پیوند میان داده و شخصیت حقوقی یا حقیقی تأکید دارد (Protection,2018,4). در حقوق خصوصی، همین پیوند است که داده را از یک «شیء بی‌جان» به موضوع حمایت حقوقی تبدیل می‌کند.

در حقوق ایران، هرچند تعریف مستقلی از «داده» در قوانین مدنی ارائه نشده است، اما قوانین خاص، به‌ویژه قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون تجارت الکترونیکی مصوب ۱۳۸۲، به‌طور ضمنی به مفهوم داده پرداخته‌اند. مطابق ماده اول قانون جرایم رایانه‌ای، «داده» به هر نوع نماد، علامت، نوشته، تصویر یا صوت اطلاق می‌شود که به‌صورت الکترونیکی، نوری یا فناوری‌های جدید اطلاعاتی تولید، ارسال، دریافت یا ذخیره می‌شود. این تعریف، اگرچه فنی به نظر می‌رسد، اما مبنای‌شناسایی داده به‌عنوان موضوع حق و تکلیف در روابط خصوصی قرار گرفته است (عطازاده و انصاری، ۱۴۰۰، ۱۱۲).

داده در حقوق خصوصی واجد دو ویژگی اساسی است: نخست، قابلیت انتساب؛ بدین معنا که داده غالباً به شخص معینی قابل انتساب است و همین امر زمینه‌سازشناسایی حقوق و تعهدات متقابل می‌شود. دوم، ارزش اقتصادی و غیرمالی؛ داده‌ها علاوه بر ارزش تجاری، می‌توانند با حقوق شخصیتی همچون حریم خصوصی و کرامت انسانی گره بخورند. دکترین حقوقی بر این نکته تأکید دارد که داده، هرچند عین مادی نیست، اما می‌تواند در قالب «مال غیرمادی» یا «منفعت مورد حمایت قانون» تحلیل شود (پیشنماز و رکنی، ۱۴۰۲، ۴۷۲). البته این طور می‌توان گفت که داده نه موضوع حق مالکیت کلاسیک، بلکه موضوع نوعی «حق کنترلی» است؛ حقی که به شخص اجازه می‌دهد بر جمع‌آوری، پردازش و استفاده از داده‌های مربوط به خود نظارت داشته باشد (یشنماز و رکنی، ۱۴۰۲، ۴۷۳). این تحلیل، به‌ویژه در حقوق خصوصی نوین، اهمیت فراوان دارد؛ زیرا مبنای تعهدات ناشی از نگهداری و ایمن‌سازی داده‌ها را فراهم می‌کند.

از دیدگاه نگارنده، داده در حقوق خصوصی مفهومی چندبعدی است که در تقاطع حقوق اموال،

3- GDPR

حقوق شخصیت و مسئولیت مدنی قرار می‌گیرد. درک دقیق این مفهوم، پیش‌نیاز تحلیل تعهدات ناشی از پردازش و ایمن‌سازی داده‌ها است و بدون آن، تعیین ماهیت و حدود تعهدات متعهدان داده ممکن نخواهد بود.

۱-۱- مفهوم تعهد در حقوق خصوصی

«تعهد» یکی از بنیادی‌ترین مفاهیم حقوق خصوصی است که ساختار اصلی روابط حقوقی میان اشخاص را شکل می‌دهد. در معنای کلاسیک، تعهد رابطه‌ای حقوقی است که به موجب آن، شخصی[۴] مکلف می‌شود عملی را انجام دهد یا از انجام عملی خودداری کند و شخص دیگر[۵] حق مطالبه آن را دارد. این تعریف که ریشه در حقوق روم دارد، همچنان مبنای تحلیل تعهد در نظام‌های حقوقی معاصر به شمار می‌آید (Cabrol,2018,179).

قانون مدنی تعریف مستقلی از تعهد ارائه نکرده است، اما از مجموع ماده‌های ۱۸۳، ۱۸۴ و ۲۱۹ قانون مدنی می‌توان چنین استنباط کرد که تعهد، اثر مستقیم رابطه قراردادی یا الزامی است که ضمانت اجرای قانونی دارد. یکی از حقوقدانان، تعهد را «رابطه‌ای حقوقی که به موجب آن، شخصی مکلف به انجام یا ترک کاری در برابر شخص دیگر می‌شود» تعریف می‌کند و بر عنصر «الزام حقوقی» به‌عنوان ویژگی متمایز تعهد از تکلیف اخلاقی تأکید دارد (کاتوزیان، ۱۴۰۴، ۵۵). این الزام حقوقی است که امکان مراجعه به دادگاه و اعمال ضمانت اجرا را فراهم می‌سازد.

تعهد واجد سه رکن اساسی است: متعهد، متعهدله و موضوع تعهد. موضوع تعهد ممکن است انجام فعل، ترک فعل یا انتقال حق باشد. در حقوق خصوصی مدرن، دامنه موضوع تعهد گسترش یافته و صرفاً به اعمال مادی محدود نمی‌شود، بلکه رفتارهای فنی، حرفه‌ای و حتی تعهدات مرتبط با مدیریت ریسک را نیز دربرمی‌گیرد. به همین دلیل، دکترین حقوقی بر لزوم تفسیر پویا از مفهوم

۴- متعهد

۵- متعهدله

تعهد تأکید کرده است (Buffelan-Lanore,2016,43).

یکی از مهم‌ترین تحولات نظری در مفهوم تعهد، تقسیم آن به «تعهد به وسیله» و «تعهد به نتیجه» است. این تقسیم‌بندی که نخستین‌بار در حقوق فرانسه مطرح شد، ناظر بر شدت الزام متعهد و نحوه تحقق مسئولیت مدنی است. در تعهد به وسیله، متعهد مکلف به به‌کارگیری کوشش متعارف و رفتار متناسب با استانداردهای حرفه‌ای است، درحالی‌که در تعهد به نتیجه، تحقق نتیجه مشخص، خود موضوع تعهد محسوب می‌شود (Tancelin,1978,841). این تمایز، نقش اساسی در توزیع بار اثبات و تعیین حدود مسئولیت دارد و امروزه به یکی از ابزارهای تحلیلی مهم در حقوق خصوصی بدل شده است. اگرچه این تقسیم‌بندی به‌صورت صریح در قانون مدنی پیش‌بینی نشده، اما دکترین حقوقی و رویه قضایی به‌طور ضمنی آن را پذیرفته‌اند. یکی از حقوقدانان با استناد به قواعد عمومی مسئولیت مدنی، امکان استنباط این دو نوع تعهد را از نظام حقوقی ایران تأیید می‌کند و آن را برای تحلیل تعهدات نوظهور، به‌ویژه تعهدات حرفه‌ای، ضروری می‌داند (کاتوزیان، ۱۴۰۴، ۲۳۳).

از دیدگاه نگارنده، تعهد در حقوق خصوصی مفهومی ایستا و محدود به الگوهای سنتی نیست، بلکه نهادی پویا است که باید متناسب با تحولات اجتماعی، اقتصادی و فناورانه تفسیر شود. کارکرد اصلی تعهد، ایجاد تعادل میان آزادی اشخاص و حمایت از اعتماد مشروع طرف مقابل است. بر این اساس، تحلیل تعهدات نوین از جمله تعهدات مرتبط با داده و فناوری مستلزم عبور از تعریف صرفاً صوری تعهد و توجه به کارکرد، هدف و آثار آن در نظام مسئولیت مدنی است. چنین رویکردی می‌تواند از تحمیل مسئولیت‌های نامتناسب جلوگیری کرده و درعین‌حال، حمایت مؤثر از حقوق اشخاص را تضمین کند.

۱-۲- ایمن‌سازی داده‌ها به‌عنوان یک تعهد حقوقی

ایمن‌سازی داده‌ها در حقوق خصوصی صرفاً یک الزام فنی یا توصیه مدیریتی نیست، بلکه تعهدی حقوقی است که از منابع مختلف، اعم از قانون، قرارداد و عرف حرفه‌ای، نشئت می‌گیرد. این تعهد

ناظر بر اتخاذ تدابیر معقول و متناسب برای جلوگیری از دسترسی غیرمجاز، افشاء، تغییر یا از بین رفتن داده‌ها است و به‌طور مستقیم با حقوق و منافع اشخاص مرتبط می‌شود. در واقع، ایمن‌سازی داده‌ها پاسخی حقوقی به خطراتی است که پردازش داده در بستر دیجیتال ایجاد می‌کند. مبنای اصلی تعهد به ایمن‌سازی داده‌ها را می‌توان در قاعده لزوم جبران خسارت ناشی از تقصیر و نقض اعتماد مشروع جست‌وجو کرد. هنگامی که شخصی داده‌های دیگری را جمع‌آوری یا پردازش می‌کند، وضعیتی از اعتماد حقوقی ایجاد می‌شود که به‌موجب آن، متعهد باید از داده‌ها به‌نحوی مراقبت کند که خطرات قابل پیش‌بینی به حداقل برسد. همان‌گونه که «سولیو»[۶] اشاره می‌کند، امنیت داده بخشی جدایی‌ناپذیر از حمایت مؤثر از حریم خصوصی است و فقدان آن، خود نوعی رفتار زیان‌بار محسوب می‌شود (Solove,2010,112).

از نظر نگارنده، ایمن‌سازی داده‌ها در حقوق خصوصی باید به‌عنوان یک تعهد حقوقی مستقل و قابل ارزیابی تلقی شود که نه به امنیت مطلق فروکاسته می‌شود و نه به توصیه‌ای اخلاقی یا فنی تقلیل می‌یابد. ماهیت این تعهد تابعی از خطر، نوع داده و جایگاه متعهد است و ارزیابی آن باید بر مبنای استانداردهای متعارف حرفه‌ای و انتظار مشروع اشخاص صورت گیرد. چنین تحلیلی، امکان اعمال مسئولیت منصفانه را فراهم کرده و از یک‌سو مانع بی‌حمایتی زیان‌دیدگان و از سوی دیگر مانع تحمیل مسئولیت نامتناسب بر متعهدان داده می‌شود.

۲- تعهد به ایمن‌سازی داده‌ها در قالب تعهد به وسیله

با توجه به ماهیت فنی و پیچیده فرایندهای مرتبط با امنیت اطلاعات و عدم امکان تحقق امنیت مطلق در فضای دیجیتال، یکی از رویکردهای مهم در تحلیل ماهیت تعهد به ایمن‌سازی داده‌ها، تلقی آن در قالب تعهد به وسیله است. این دیدگاه که ریشه در دکترین سنتی حقوق خصوصی دارد، بر این فرض استوار است که متعهد صرفاً مکلف به به‌کارگیری تلاش متعارف، رعایت استانداردهای حرفه‌ای و

6- Solove

اتخاذ تدابیر معقول برای حفاظت از داده‌ها است، نه تضمین نتیجه‌ای قطعی مبنی بر عدم نقض امنیت. بررسی این رویکرد مستلزم تحلیل مبانی نظری پذیرش تعهد وسیله بودن ایمن‌سازی داده‌ها، تبیین آثار حقوقی آن در حوزه مسئولیت مدنی و در نهایت ارزیابی انتقادی کارآمدی این تلقی در حمایت از اشخاص موضوع داده است.

۲-۱- پذیرش تعهد به وسیله بودن ایمن‌سازی داده‌ها

پذیرش تعهد به ایمن‌سازی داده‌ها در قالب تعهد به وسیله مبتنی‌بر این پیش‌فرض اساسی است که امنیت داده‌ها ماهیتی نسبی، پویا و غیرقطعی دارد و تحقق کامل آن همواره در کنترل متعهد نیست. در فضای دیجیتال، حتی با به‌کارگیری پیشرفته‌ترین تدابیر فنی و سازمانی، امکان وقوع نفوذ، حملات سایبری یا افشای غیرمجاز داده‌ها به‌طور کامل منتفی نمی‌شود. همین ویژگی، نخستین و مهم‌ترین مبنای نظری برای تحلیل ایمن‌سازی داده‌ها به‌عنوان تعهد وسیله به شمار می‌آید. در دکترین کلاسیک حقوق تعهدات، تعهد وسیله ناظر بر مواردی است که نتیجه مورد انتظار به عوامل متعدد و گاه خارج از اراده متعهد وابسته است و ازاین‌رو، متعهد تنها مکلف به به‌کارگیری «مراقبت متعارف» و رفتار منطبق با استانداردهای حرفه‌ای است (Tancelin,1978,841). امنیت داده‌ها نیز دقیقاً در همین وضعیت قرار دارد؛ زیرا متعهد، هرچند مسئول طراحی و اجرای نظام‌های امنیتی است، اما همواره در معرض تهدیدهای نوظهور، آسیب‌پذیری‌های ناشناخته و رفتارهای مجرمانه اشخاص ثالث قرار دارد. به همین دلیل، تضمین عدم نقض داده‌ها به‌عنوان نتیجه‌ای قطعی، با منطق حقوقی تعهدات سازگار تلقی نمی‌شود.

در حقوق ایران نیز، هرچند قانون‌گذار صراحتاً از تعهد وسیله یا نتیجه سخن نگفته است، اما قواعد عمومی مسئولیت مدنی و تحلیل دکترین حقوقی، امکان‌پذیرش این رویکرد را فراهم می‌کند. یکی از حقوقدانان تأکید می‌کند که در تعهداتی که موضوع آن‌ها ماهیت تخصصی و پرخطر دارد، احراز مسئولیت متعهد مستلزم اثبات تقصیر و عدم رعایت معیار رفتار متعارف است (کاتوزیان، ۱۴۰۴، ۲۳۴). با تطبیق این تحلیل بر ایمن‌سازی داده‌ها، می‌توان گفت متعهد زمانی مسئول شناخته می‌شود که ثابت

گردد تدابیر لازم و متعارف را اتخاذ نکرده یا از استانداردهای فنی رایج عدول کرده است. افزون بر این، رویه عملی شرکت‌ها و سازمان‌ها نیز نشان می‌دهد که امنیت داده‌ها غالباً بر اساس مدیریت ریسک و کاهش احتمال خسارت تعریف می‌شود، نه تضمین نتیجه‌ای مطلق.

به دیدگاه نگارنده، پذیرش تعهد وسیله بودن ایمن‌سازی داده‌ها از حیث واقع‌گرایی فنی و انطباق با منطق سنتی حقوق تعهدات قابل دفاع است، اما این پذیرش باید با تفسیر مضیق همراه باشد. تعهد وسیله در این حوزه نباید به حدی تضعیف شود که هرگونه نقض داده، بدون بررسی دقیق رفتار متعهد، موجه جلوه کند. معیار «مراقبت متعارف» باید به‌صورت پویا و متناسب با سطح خطر، نوع داده و جایگاه حرفه‌ای متعهد تفسیر شود؛ در غیر این صورت، تعهد وسیله بودن ایمن‌سازی داده‌ها می‌تواند به ابزاری برای فرار از مسئولیت بدل شود، نه سازوکاری منصفانه برای توزیع آن.

۲-۲- آثار حقوقی تعهد به وسیله بودن

تلقی تعهد به ایمن‌سازی داده‌ها در قالب تعهد به وسیله آثار حقوقی مشخص و قابل توجهی در حوزه مسئولیت مدنی و روابط قراردادی به همراه دارد که مهم‌ترین آن‌ها به نحوه تحقق مسئولیت، توزیع بار اثبات و معیار ارزیابی رفتار متعهد بازمی‌گردد. این آثار، نقش تعیین‌کننده‌ای در میزان حمایت از اشخاص موضوع داده و حدود مسئولیت متعهدان ایفاء می‌کنند.

نخستین و بنیادی‌ترین اثر تعهد وسیله بودن، لزوم اثبات تقصیر متعهد است. در این نوع تعهد، صرف وقوع خسارت یا نقض امنیت داده‌ها برای تحقق مسئولیت کافی نیست، بلکه زیان‌دیده باید اثبات کند که متعهد از به‌کارگیری مراقبت متعارف یا رعایت استانداردهای حرفه‌ای خودداری کرده است. این قاعده که در دکترین حقوقی به‌عنوان ویژگی اصلی تعهد وسیله شناخته می‌شود، به‌وضوح در آثار حقوقی کلاسیک مورد تأکید قرار گرفته است (Tancelin,1978,841). در نتیجه، در دعاوی ناشی از نقض داده، تمرکز رسیدگی قضایی از «نتیجه» به «رفتار متعهد» منتقل می‌شود.

اثر دوم، تغییر معیار ارزیابی مسئولیت از نتیجه به رفتار متعارف است. در تعهد وسیله، قاضی

مکلف است رفتار متعهد را با معیار شخص متعارف یا، در موارد حرفه‌ای، با معیار «حرفه‌ای متعارف» مقایسه کند. در حوزه ایمن‌سازی داده‌ها، این امر به معنای بررسی سطح تدابیر فنی، سازمانی و مدیریتی اتخاذشده در زمان وقوع نقض داده است، نه صرف امکان جلوگیری از آن (Chantepie,2016,125).

اثر سوم تعهد وسیله بودن، سنگین شدن بار اثبات برای زیان‌دیده است. اثبات قصور در حوزه امنیت داده‌ها غالباً نیازمند دسترسی به اطلاعات فنی، اسناد داخلی و فرآیندهای امنیتی متعهد است؛ امری که معمولاً خارج از دسترس اشخاص موضوع داده قرار دارد. این وضعیت، به‌ویژه در روابط نامتوازن میان کاربران و پلتفرم‌های دیجیتال، می‌تواند به کاهش کارآمدی حمایت حقوقی منجر شود. در ادبیات حقوقی اروپایی نیز به این چالش اشاره شده است و برخی نویسندگان آن را از پیامدهای منفی تحلیل تعهد امنیت داده به‌عنوان تعهد وسیله دانسته‌اند (De Hert&Papakonstantinou,2016,193).

اثر چهارم، امکان گسترده‌تر استناد متعهد به عوامل خارجی است. در تعهد وسیله، متعهد می‌تواند با اثبات وقوع حملات پیشرفته، رفتار مجرمانه اشخاص ثالث یا نقص‌های غیرقابل پیش‌بینی فناوری، از مسئولیت رهایی یابد، مشروط بر آن‌که نشان دهد تدابیر متعارف را رعایت کرده است. این امر، دامنه مسئولیت متعهد را محدود و انعطاف‌پذیر می‌سازد و با منطق مدیریت ریسک در حوزه فناوری اطلاعات سازگار است (Protection,2018,4).

به دیدگاه نگارنده، آثار حقوقی تعهد وسیله بودن ایمن‌سازی داده‌ها هرچند با واقعیت‌های فنی و پیچیدگی‌های امنیت سایبری سازگار است، اما در عمل می‌تواند به عدم توازن در حمایت از اشخاص موضوع داده بینجامد. انتقال بار اثبات به زیان‌دیده و تمرکز بر رفتار متعهد، بدون پیش‌بینی سازوکارهای جبرانی، خطر تضعیف کارآمدی مسئولیت مدنی را به همراه دارد. ازاین‌رو، به نظر می‌رسد پذیرش تعهد وسیله بودن تنها در صورتی قابل دفاع است که با معیارهای سخت‌گیرانه ارزیابی رفتار حرفه‌ای و تسهیل اثبات تقصیر، به‌ویژه در روابط نامتوازن، همراه شود.

۲-۳- نقد دیدگاه تعهد به وسیله

با وجود دلایل فنی و نظری که برای تحلیل ایمن‌سازی داده‌ها در قالب تعهد به وسیله ارائه شده است، این دیدگاه با انتقادات جدی حقوقی مواجه است که عمدتاً ناظر بر کارآمدی حمایت از اشخاص موضوع داده و انطباق این رویکرد با تحولات ساختاری حقوق خصوصی معاصر است. یکی از مهم‌ترین نقدها به این دیدگاه، ناسازگاری آن با ماهیت قدرت و عدم تقارن اطلاعاتی در روابط داده‌محور است. پردازش‌کنندگان داده، به‌ویژه پلتفرم‌ها و شرکت‌های فناوری، در موقعیتی کاملاً برتر از حیث دانش فنی، کنترل زیرساخت و دسترسی به اطلاعات و ادله قرار دارند. تحلیل ایمن‌سازی داده‌ها به‌عنوان تعهد وسیله، با تحمیل بار اثبات تقصیر بر زیان‌دیده، عملاً این عدم تقارن را تشدید می‌کند و کارکرد حمایتی مسئولیت مدنی را تضعیف می‌سازد (Bygrave,2014,146).

از سوی دیگر، این رویکرد با تحول مفهوم تعهدات حرفه‌ای در حقوق خصوصی نوین نیز در تعارض است. در بسیاری از تعهدات حرفه‌ای، مرزهای سنتی میان تعهد وسیله و تعهد نتیجه کمرنگ شده و استانداردهای سخت‌گیرانه‌تر جایگزین شده‌اند. در حوزه ایمن‌سازی داده‌ها که ماهیتی آشکارا حرفه‌ای دارد، تحلیل این تعهد به‌صورت تعهد وسیله کلاسیک نوعی عقب‌گرد مفهومی محسوب می‌شود و ممکن است منطق مسئولیت حرفه‌ای مدرن را نادیده بگیرد (Zimmermann,1990,1023).

این دیدگاه همچنین با منطق پیشگیرانه مسئولیت مدنی نیز تناسب ندارد. مسئولیت مدنی در حقوق نوین، بخشی از کارکرد خود را به ایجاد انگیزه برای پیشگیری از ورود ضرر اختصاص داده است. هنگامی که متعهد بداند رعایت حداقل مراقبت، او را از مسئولیت رهایی می‌بخشد، انگیزه‌ای برای سرمایه‌گذاری مستمر در ارتقای امنیت داده‌ها باقی نمی‌ماند. برخی حقوقدانان اروپایی تأکید کرده‌اند که امنیت داده‌ها باید به‌عنوان بخشی از «حاکمیت داده» تلقی شود و نه صرفاً یک تعهد رفتاری حداقلی (Kuner,2013,89).

از نظر نگارنده، مهم‌ترین ایراد دیدگاه تعهد وسیله بودن ایمن‌سازی داده‌ها آن است که این رویکرد بیش از حد بر محدودیت‌های فنی تمرکز می‌کند و از کارکرد حمایتی و پیشگیرانه حقوق

خصوصی غفلت می‌ورزد. امنیت داده‌ها در روابط معاصر صرفاً یک رفتار فنی نیست، بلکه بخشی از تعهد حرفه‌ای و اعتمادساز متعهد است. بنابراین، تحلیل این تعهد در قالب تعهد وسیله سنتی، پاسخگوی نیازهای عدالت‌محور و پیشگیرانه حقوق خصوصی نیست و لازم است جای خود را به رویکردی سخت‌گیرانه‌تر و متناسب با عدم تقارن قدرت بدهد.

۳- تعهد به ایمن‌سازی داده‌ها در قالب تعهد به نتیجه

با توجه به اهمیت حفاظت از داده‌ها و نقش حیاتی آن در حفظ حقوق و منافع اشخاص، تحلیل تعهد به ایمن‌سازی داده‌ها در قالب تعهد به نتیجه یکی از رویکردهای حقوقی مطرح است. در این دیدگاه، متعهد موظف است نتیجه‌ای مشخص، یعنی امنیت داده‌ها، را محقق سازد و صرف به‌کارگیری تدابیر متعارف کفایت نمی‌کند. بررسی این رویکرد مستلزم تبیین مبانی نظری پذیرش تعهد نتیجه بودن، تحلیل آثار حقوقی آن در حوزه مسئولیت مدنی و روابط قراردادی وشناسایی چالش‌ها و انتقادات مربوط به عملیاتی‌کردن این نوع تعهد است.

۳-۱- پذیرش تعهد به نتیجه بودن

تلقی تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد نتیجه بر این اصل استوار است که متعهد مسئول تحقق یک نتیجه مشخص و قابل سنجش است و صرف به‌کارگیری تلاش متعارف برای حفاظت از داده‌ها کفایت نمی‌کند. این دیدگاه به‌ویژه در مواقعی که داده‌ها حساس، حیاتی یا مربوط به حقوق بنیادین اشخاص است، اهمیت پیدا می‌کند، چرا که خسارت ناشی از نقض امنیت داده‌ها می‌تواند تبعات مالی و شخصیتی جدی داشته باشد و انتظار جامعه و مقررات از متعهد، تضمین امنیت واقعی است. در حقوق تطبیقی، برخی قواعد و رویه‌ها حمایت از این دیدگاه را نشان می‌دهند. به‌طورمثال، در فرانسه، دکترین معاصر بر این باور است که در برخی تعهدات حرفه‌ای و قراردادی، خصوصاً در زمینه خدمات اطلاعاتی و فناوری، متعهد به تحقق نتیجه مشخصی است و مسئولیت او بدون نیاز به اثبات تقصیر برقرار می‌شود (Poulain,2007,995). این تحلیل به‌ویژه

برای خدماتی که داده‌های حساس مانند اطلاعات پزشکی یا مالی را پردازش می‌کنند، کاربرد دارد و منطق «اعتماد مشروع» را تقویت می‌کند.

از دیدگاه نگارنده، پذیرش تعهد نتیجه بودن ایمن‌سازی داده‌ها، به‌ویژه در حوزه داده‌های حساس یا در روابط نامتوازن، رویکردی منطقی و عدالت‌محور است. این دیدگاه، الزام متعهد به تأمین امنیت واقعی داده‌ها را برجسته می‌کند و از انتقال غیرمنصفانه ریسک به زیان‌دیده جلوگیری می‌کند. بااین‌حال، اعمال آن نیازمند استانداردهای روشن و معیارهای فنی قابل سنجش است تا از تحمیل مسئولیت غیرمتعارف بر متعهدان جلوگیری شود و هم‌زمان حمایت مؤثر از اشخاص موضوع داده تضمین گردد.

۳-۲- آثار حقوقی تعهد به نتیجه بودن

تحلیل تعهد به ایمن‌سازی داده‌ها در قالب تعهد نتیجه پیامدهای حقوقی متمایزی نسبت به تعهد وسیله دارد که بر ساختار مسئولیت مدنی و روابط قراردادی تأثیر مستقیم می‌گذارد. یکی از برجسته‌ترین آثار این رویکرد، ایجاد مسئولیت بدون نیاز به اثبات تقصیر است. در این وضعیت، صرف عدم تحقق نتیجه مورد انتظار، یعنی نقض امنیت داده‌ها، برای استناد به مسئولیت متعهد کافی است و زیان‌دیده نیازی به اثبات قصور متعهد ندارد. در نتیجه، بار اثبات بر رابطه علیت میان رفتار متعهد و خسارت متمرکز می‌شود و این ویژگی سطح بالایی از حمایت حقوقی برای افراد داده‌محور ایجاد می‌کند و اعتماد عمومی به خدمات دیجیتال را افزایش می‌دهد (Schlechtriem&Butler,2009,412).

این رویکرد باعث تشدید استانداردهای حرفه‌ای و فنی برای متعهدان داده‌ها می‌شود. متعهد در چهارچوب تعهد نتیجه ناگزیر است تدابیر پیشگیرانه فراتر از حداقل مراقبت متعارف اتخاذ کند، زیرا مسئولیت او مستقیماً معطوف به تحقق امنیت داده‌ها است. برخلاف تعهد وسیله که رعایت استانداردهای معمول کافی است، در تعهد نتیجه، متعهد موظف به بهره‌گیری از تمامی ابزارها و روش‌های قابل دستیابی برای محافظت از داده‌ها است، امری که نقش پیشگیرانه مسئولیت مدنی را

پررنگ می‌کند و به ارتقای سطح امنیت دیجیتال کمک می‌کند (Weber,2017,67).

تعهد به نتیجه همچنین توزیع منصفانه‌تر ریسک میان متعهد و زیان‌دیده را فراهم می‌آورد. در روابط داده‌محور که عدم تقارن اطلاعاتی شدید وجود دارد، پذیرش این نوع تعهد زیان‌دیده را از موقعیت ضعف خود نجات می‌دهد و تضمین می‌کند که متعهد مسئول جبران خسارت ناشی از نقض امنیت باشد، حتی اگر اثبات تقصیر عملی دشوار باشد. این امر با اصول عدالت قراردادی و حمایت از طرف ضعیف در قراردادهای الکترونیکی همخوانی دارد (Wessel,2015,418). از سوی دیگر، تعهد به نتیجه باعث تقویت انگیزه برای نوآوری و ارتقای فناوری‌های حفاظتی می‌شود. متعهد برای کاهش احتمال مسئولیت، به سرمایه‌گذاری در فناوری‌های نوین، آموزش نیروهای انسانی و ارتقای سیستم‌های امنیتی تشویق می‌شود. این اثر مثبت بر کیفیت خدمات و حفاظت از داده‌ها، یکی از مزایای شاخص تحلیل تعهد به نتیجه در حقوق فناوری است.

نگارنده بر این باور است که تعهد به نتیجه بودن ایمن‌سازی داده‌ها، به‌ویژه در زمینه داده‌های حساس یا خدمات ارائه‌شده به کاربران فاقد توان فنی، نه‌تنها منطقی بلکه عدالت‌محور است. این رویکرد مسئولیت متعهد را به سطحی ارتقاء می‌دهد که حفاظت واقعی از داده‌ها تضمین شود و انگیزه متعهد برای رعایت حداکثر استانداردهای امنیتی افزایش یابد. بااین‌حال، اعمال چنین تعهدی نیازمند تعیین معیارهای فنی روشن و سازوکارهای منطقی ارزیابی است تا از تحمیل مسئولیت‌های غیرمنطقی یا فراتر از توان متعهد جلوگیری شود.

۳-۳- چالش‌ها و انتقادات

با وجود مزایای قابل توجه تحلیل تعهد به ایمن‌سازی داده‌ها در قالب تعهد نتیجه، این رویکرد با چالش‌ها و انتقادات حقوقی مهمی مواجه است که بخش عمده آن‌ها ناشی از محدودیت‌های عملی و ماهیت پیچیده داده‌ها است. یکی از اصلی‌ترین انتقادات، مشکل تحقق امنیت مطلق است. داده‌ها به‌ویژه در فضای دیجیتال، همواره در معرض تهدیدهای نوظهور، آسیب‌پذیری‌های فناوری و

رفتارهای مجرمانه اشخاص ثالث قرار دارند. الزام متعهد به تحقق نتیجه مطلق، می‌تواند منجر به ایجاد مسئولیت غیرقابل مدیریت و نامتناسب با توان عملی متعهد شود (ضیایی، ۱۴۰۴، ۶۳۲). افزون بر این، تحلیل تعهد نتیجه باعث افزایش چشمگیر هزینه‌های اجرایی و فنی برای متعهدان داده‌ها می‌شود. برای تحقق نتیجه، متعهد باید تدابیر بسیار پیشرفته و سرمایه‌گذاری‌های مداوم در فناوری‌های امنیتی انجام دهد. این امر نه‌تنها می‌تواند به افزایش هزینه خدمات منجر شود، بلکه ممکن است کسب‌وکارهای کوچک و متوسط را از ارائه خدمات دیجیتال بازدارد. برخی محققان حقوقی ایران بر این باورند که این مسئله می‌تواند منطق اقتصادی قراردادها و دسترسی عمومی به خدمات دیجیتال را تحت تأثیر قرار دهد (السان، ۱۴۰۲، ۱۴۲).

مسئله دیگری که مطرح می‌شود، دشواری اثبات و سنجش مسئولیت است. در تعهد نتیجه، زیان‌دیده نیازی به اثبات تقصیر ندارد، اما باید نشان دهد که نتیجه مورد انتظار محقق نشده و خسارت متوجه او شده است. با توجه به پیچیدگی‌های فنی و محدودیت دسترسی به اطلاعات داخلی متعهد، اثبات نقض امنیت داده‌ها و ارتباط مستقیم آن با خسارت، می‌تواند دشوار باشد و فرآیند قضایی را پیچیده کند (باقری و نوشادی، ۱۳۹۶، ۲۳۶). همچنین، الزام به نتیجه مطلق می‌تواند با استانداردهای متعارف حرفه‌ای و واقع‌گرایی فنی در تعارض باشد. متعهد ممکن است به جای تمرکز بر مدیریت ریسک و اتخاذ اقدامات متناسب با خطر، به دنبال تضمین غیرواقع‌بینانه امنیت داده‌ها باشد. این رویکرد نه‌تنها عملیاتی نیست، بلکه می‌تواند انگیزه نوآوری و توسعه خدمات را محدود کند (نعمتی، ۱۳۹۶، ۱۶۴).

نگارنده بر این باور است که تحلیل تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد نتیجه، اگرچه از نظر عدالت و حمایت از اشخاص موضوع داده جذاب و منطقی است، اما بدون معیارهای روشن فنی، محدودیت‌های عملی و سازوکارهای متعادل ارزیابی، می‌تواند منجر به مسئولیت غیرمنطقی و فشار بی‌مورد بر متعهدان شود. بهترین راهکار ترکیب تحلیل تعهد نتیجه با استانداردهای مدیریت ریسک و توجه به توان عملی متعهد است تا هم امنیت داده‌ها تضمین شود و هم مسئولیت‌ها متناسب و عملیاتی باقی بمانند.

۴- رویکردهای تطبیقی و ارائه الگوی مطلوب

حفاظت از داده‌ها و تضمین امنیت آن‌ها به‌عنوان یکی از موضوعات حیاتی در حقوق خصوصی معاصر، نیازمند بررسی تطبیقی وشناسایی بهترین شیوه‌های حقوقی است. در این راستا، تحلیل رویکردهای تطبیقی می‌تواند هم نقاط قوت و ضعف نظام‌های حقوقی مختلف را روشن سازد و هم زمینه لازم برای طراحی یک الگوی مؤثر و کارآمد فراهم آورد. مبحث حاضر با تمرکز بر رویکرد حقوق ایران، مقررات اتحادیه اروپا و حقوق فرانسه، ضمن مقایسه سازوکارهای حقوقی، به ارائه الگوی مختلط و پویا می‌پردازد که بتواند هم پاسخگوی نیازهای فنی و عملی باشد و هم عدالت و حمایت از اشخاص موضوع داده را تضمین کند. این بررسی با هدف ارائه چهارچوبی عملی و قابل اجرا برای تنظیم تعهدات ایمن‌سازی داده‌ها طراحی شده است.

۴-۱- رویکرد حقوق ایران

در حقوق ایران، تعهد به ایمن‌سازی داده‌ها به‌صورت مستقیم و صریح مورد اشاره قرار نگرفته است، اما تحلیل قوانین موجود و قواعد مسئولیت مدنی امکان‌شناسایی چنین تعهدی را فراهم می‌کند. قوانین مرتبط، به‌ویژه قانون تجارت الکترونیکی مصوب ۱۳۸۲ و قانون جرایم رایانه‌ای مصوب ۱۳۸۸، چهارچوبی ابتدایی برای الزام پردازش‌کنندگان داده به اتخاذ تدابیر حفاظتی ارائه می‌دهند. به‌طور مثال، ماده دهم قانون تجارت الکترونیکی، صراحتاً تأمین امنیت داده‌ها و اطلاعات کاربران را به‌عنوان یکی از وظایف متعهدان خدمات الکترونیکی معرفی می‌کند، درحالی‌که ماده اول قانون جرایم رایانه‌ای با جرم‌انگاری دسترسی غیرمجاز به داده‌ها، به‌طور ضمنی توجه قانون‌گذار به اهمیت حفاظت از داده‌ها را نشان می‌دهد (عطازاده و انصاری، ۱۴۰۰، ۱۱۲).

تحلیل مقررات و دکترین حقوق خصوصی ایران نشان می‌دهد که نگهدارنده یا پردازش‌کننده داده، در صورتی که از استانداردهای متعارف حفاظت از داده‌ها عدول کند، مسئول جبران خسارت خواهد بود. یکی از حقوقدانان در تحلیل قواعد عمومی قراردادها و مسئولیت مدنی تأکید می‌کند که

هرگاه موضوع قرارداد یا عمل حرفه‌ای دارای ریسک ذاتی و پیچیدگی فنی باشد، مسئولیت متعهد تابع اثبات قصور و عدم رعایت معیار رفتار متعارف خواهد بود (کاتوزیان، ۱۴۰۴، ۲۳۴). با تطبیق این اصول با حوزه داده‌ها، می‌توان گفت که پذیرش تعهد وسیله بودن ایمن‌سازی داده‌ها در ایران از منظر حقوقی قابل توجیه است، هرچند هنوز معیارهای فنی و عملیاتی مشخص و مستند به قوانین برای تعیین حداقل استانداردها وجود ندارد. رویکرد قضایی نیز به شکل محدود، نشان‌دهنده پذیرش مسئولیت متعهدان داده در صورت وقوع خسارت است. برخی آراء قضایی، در پرونده‌های مرتبط با نقض امنیت اطلاعات و افشای داده‌ها، متعهد را مکلف به جبران خسارت کرده‌اند، حتی در مواردی که تقصیر مستقیم متعهد به اثبات رسیده است. این رویه ضمن حمایت از طرف ضعیف‌تر، ضرورت تعریف معیارهای روشن و دقیق برای اندازه‌گیری رفتار متعارف متعهد را برجسته می‌کند.

نگارنده بر این باور است که رویکرد حقوق ایران به تعهد ایمن‌سازی داده‌ها، اگرچه از منظر اصول مسئولیت مدنی و قواعد قراردادها قابل توجیه است، اما هنوز محدودیت‌های عملی و فنی زیادی دارد. برای ارتقای کارآمدی این تعهد، لازم است قوانین و مقررات با استانداردهای فنی و حرفه‌ای روز هماهنگ شوند و معیارهای مشخصی برای تعیین حداقل تدابیر حفاظتی تدوین گردد. این امر، علاوه بر افزایش امنیت داده‌ها، امکان اعمال مسئولیت متناسب و عدالت‌محور را فراهم می‌کند.

۴-۲- رویکرد اتحادیه اروپا و حقوق فرانسه

رویکرد اتحادیه اروپا به تعهد ایمن‌سازی داده‌ها عمدتاً از طریق مقررات عمومی حفاظت از داده‌ها[7] تعریف می‌شود که از سال ۲۰۱۸ میلادی لازم‌الاجرا شد. مقررات عمومی حفاظت از داده‌ها چهارچوبی جامع برای حفاظت از داده‌های شخصی ایجاد کرده و برای پردازش‌کنندگان داده تکالیف مشخصی در نظر گرفته است. ماده سی و دوم این مقرره متعهدان داده را ملزم می‌کند که اقدامات فنی و سازمانی مناسب برای تضمین سطح امنیت متناسب با خطر را اتخاذ کنند. این اقدامات

7- GDPR

شامل رمزگذاری، حفظ محرمانگی و یکپارچگی داده‌ها، تضمین توان بازیابی و تست منظم سیستم‌های امنیتی است (Chantepie,2016,160).

نکته مهم آن است که مقررات عمومی حفاظت از داده‌ها ضمن تأکید بر اقدامات پیشگیرانه، اصول حاکمیت داده و پاسخگویی را نیز برقرار می‌کند؛ بدین معنا که سازمان‌ها باید مستندسازی کنند که چه تدابیری برای حفاظت از داده‌ها اتخاذ شده و در صورت نقض، اقدامات اصلاحی سریع انجام دهند. این ترکیب الزامات، نوعی مسئولیت مبتنی‌بر تعهد وسیله و نتیجه ترکیبی ایجاد می‌کند، زیرا رعایت اقدامات متعارف کافی است، اما در صورت نقض داده‌ها، سازمان ممکن است مسئولیت جبران خسارت داشته باشد، حتی اگر اقدامات متعارف را رعایت کرده باشد.

در حقوق فرانسه، رویکرد نسبت به ایمن‌سازی داده‌ها با تأکید بر مسئولیت حرفه‌ای و استانداردهای حرفه‌ای شکل گرفته است. ماده ۱۲۴۰ قانون مدنی فرانسه مسئولیت مدنی ناشی از اعمال زیان‌بار را به‌طور کلی تعیین کرده و دکترین معاصر، پردازش‌کنندگان داده را موظف به رعایت استانداردهای فنی و سازمانی متعارف در محافظت از داده‌ها می‌داند (Dautieu,2018,49). همچنین، کمیسیون ملی فناوری اطلاعات و آزادی‌ها[8] مجموعه‌ای از راهنماها و دستورالعمل‌های عملیاتی برای حفاظت از داده‌ها منتشر کرده است که هم الزامات مقررات عمومی حفاظت از داده‌ها را پیاده‌سازی می‌کند و هم استانداردهای حرفه‌ای فرانسوی را تقویت می‌نماید. این دستورالعمل‌ها شامل ارزیابی ریسک، تست‌های نفوذ، مدیریت دسترسی و آموزش کارکنان است.

یکی از ویژگی‌های مهم رویکرد فرانسه، تمرکز بر مسئولیت متعهد در رابطه با کاربران نهایی است. در این چهارچوب، حتی در صورتی که متعهد اقدامات فنی متعارف را اتخاذ کرده باشد، در صورت وقوع نقض داده‌ها، مسئولیت او می‌تواند بر اساس تحلیل رابطه علیت و اعتماد مشروع تعیین شود؛ بنابراین، رویکرد فرانسوی از نظر عملی، به سمت یک ترکیب تعهد وسیله همراه با مسئولیت

8- Commission Nationale de l’Informatique et des Libertés (CNIL)

نتیجه محدود حرکت می‌کند و درعین‌حال، شفافیت و مستندسازی اقدامات حفاظتی را ضروری می‌داند. در مجموع، رویکرد اتحادیه اروپا و حقوق فرانسه هر دو بر اهمیت اقدامات پیشگیرانه، مدیریت ریسک و پاسخگویی تأکید دارند، اما مقررات عمومی حفاظت از داده‌ها چهارچوب قانونی گسترده‌تری ارائه می‌دهد که الزامات اجرایی و مکانیسم‌های نظارتی مشخص دارد، درحالی‌که رویکرد فرانسه، بیشتر بر استانداردهای حرفه‌ای، تحلیل مسئولیت و شفافیت عملکرد متعهدان تمرکز می‌کند. این تفاوت‌ها، زمینه مهمی برای طراحی الگوی تطبیقی و کارآمد در سایر نظام‌های حقوقی، از جمله ایران، فراهم می‌آورد.

از دیدگاه نگارنده ترکیب رویکرد اتحادیه اروپا و فرانسه، با توجه به تمرکز مقررات عمومی حفاظت از داده‌ها بر الزامات قانونی و کمیسیون ملی فناوری اطلاعات و آزادی‌ها بر استانداردهای حرفه‌ای، بهترین مسیر برای ایجاد چهارچوبی پویا و قابل اجرا در حوزه ایمن‌سازی داده‌ها است. چنین چهارچوبی می‌تواند امنیت واقعی داده‌ها را تضمین کند، نقش پیشگیرانه مسئولیت مدنی را تقویت نماید و هم‌زمان استانداردهای عملیاتی و حرفه‌ای متناسب با محیط فناوری را رعایت کند.

۴-۳- ارائه الگوی مختلط و پویا

با توجه به تحلیل تطبیقی رویکردهای حقوق ایران، اتحادیه اروپا و حقوق فرانسه، روشن می‌شود که هیچ یک از این رویکردها به تنهایی قادر به پوشش کامل ابعاد فنی، عملی و حقوقی ایمن‌سازی داده‌ها نمی‌باشند. حقوق ایران عمدتاً بر تعهد وسیله مبتنی‌بر رعایت استانداردهای متعارف و اثبات قصور متکی است، درحالی‌که مقررات عمومی حفاظت از داده‌ها و حقوق فرانسه، ترکیبی از الزامات پیشگیرانه و مسئولیت محدود نتیجه را ارائه می‌دهند. ازاین رو طراحی یک الگوی مختلط و پویا که عناصر تعهد وسیله و تعهد نتیجه را ترکیب کند، می‌تواند چهارچوبی جامع و عملی ارائه دهد و هم امنیت واقعی داده‌ها را تضمین کند و هم مسئولیت متعهدان را با واقعیت‌های فناوری هماهنگ سازد (شریفی کیا و شعبانی جهرمی، ۱۴۰۱، ۲۳۳).

در این الگو، بخش وسیله تعهد، تمرکز بر رعایت اقدامات پیشگیرانه، استانداردهای حرفه‌ای و مدیریت ریسک دارد. متعهد موظف است کلیه تدابیر فنی، سازمانی و مدیریتی متعارف برای حفاظت از داده‌ها را اتخاذ کند، از جمله رمزگذاری داده‌ها، مدیریت دسترسی، مستندسازی اقدامات حفاظتی، آموزش پرسنل و تست منظم سیستم‌ها (Brkan,2016,324). این بخش از تعهد، تضمین می‌کند که متعهد با معیارهای فنی و عملی متناسب با سطح ریسک هماهنگ باشد و انعطاف‌پذیری لازم برای مواجهه با تهدیدهای غیرقابل پیش‌بینی حفظ شود. به بیان دیگر، تعهد وسیله، مسئولیت متعهد را با توان عملی و محدودیت‌های فنی تطبیق می‌دهد و از اعمال مسئولیت غیرواقعی جلوگیری می‌کند.

در کنار آن، بخشی از تعهد به‌صورت تعهد نتیجه محدود تعریف می‌شود تا امنیت واقعی داده‌ها تضمین شود، به‌ویژه در مورد داده‌های حساس و حیاتی مانند اطلاعات مالی، پزشکی یا هویتی کاربران. در این حالت، متعهد مسئول تحقق نتیجه مشخصی، یعنی حفاظت کامل داده‌ها است و در صورت وقوع نقض داده‌ها، حتی اگر اقدامات پیشگیرانه متعارف را رعایت کرده باشد، مسئولیت جبران خسارت خواهد داشت (Zeller,2000,79). این ترکیب، انگیزه متعهد را برای سرمایه‌گذاری مستمر در فناوری‌های نوین امنیتی افزایش می‌دهد و بهبود مستمر سیستم‌های حفاظتی را تضمین می‌کند. ویژگی دیگر این الگو پویا بودن آن است؛ به این معنا که معیارها و الزامات آن بسته به نوع داده، حساسیت آن، جایگاه حرفه‌ای متعهد و تغییرات فناوری قابل تنظیم و اصلاح است. به‌عنوان مثال، در محیط‌هایی با ریسک بسیار بالا، بخش تعهد نتیجه پررنگ‌تر شده و فشار مسئولیت افزایش می‌یابد، درحالی‌که در محیط‌های با ریسک محدود، تمرکز بر رعایت استانداردهای حرفه‌ای و اقدامات متعارف برای مدیریت ریسک کافی خواهد بود (رحمانی، ۱۳۹۴، ۷۸). این انعطاف‌پذیری موجب می‌شود که الگو هم عدالت محور باشد و هم با واقعیت‌های عملی و فنی همخوانی داشته باشد.

از نظر نگارنده، الگوی مختلط و پویا بهترین چهارچوب برای اعمال تعهد ایمن‌سازی داده‌ها در نظام حقوقی ایران و سایر کشورها است. این مدل نه‌تنها امنیت واقعی داده‌ها را تضمین می‌کند، بلکه

انگیزه پیشگیری، نوآوری و ارتقای استانداردهای حرفه‌ای را تقویت می‌نماید و هم‌زمان امکان اعمال مسئولیت متناسب، عادلانه و عملیاتی را فراهم می‌آورد. ترکیب عناصر تعهد وسیله و نتیجه، ضمن انعطاف‌پذیری، عدالت و حمایت از کاربران را با واقعیت‌های فناوری دیجیتال همسو می‌کند و نقطه تلاقی میان منطق پیشگیرانه و پاسخگویی حقوقی را ایجاد می‌نماید.

نتیجه

تلقی تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد صرفاً به وسیله، هرچند با ماهیت غیرقطعی امنیت سایبری و نسبی بودن امکان پیشگیری از نقض داده‌ها سازگار به نظر می‌رسد، اما در عمل به تضعیف حمایت از اشخاص موضوع داده و انتقال بار سنگین اثبات تقصیر به زیان‌دیده منجر می‌شود. این رویکرد، به‌ویژه در شرایطی که متعهد از جایگاه حرفه‌ای، توان فنی و اطلاعات برتر برخوردار است، با اصول انصاف و عدالت قراردادی هم‌خوانی کامل ندارد و می‌تواند به کاهش انگیزه متعهدان برای اتخاذ تدابیر مؤثر امنیتی بینجامد. از سوی دیگر، پذیرش مطلق تعهد نتیجه بودن ایمن‌سازی داده‌ها نیز با چالش‌های جدی مواجه است؛ چراکه تحمیل مسئولیت صرف در تمامی موارد نقض امنیت داده، بدون توجه به ماهیت تهدیدات سایبری و عوامل خارج از کنترل متعهد، می‌تواند منجر به مسئولیت نامتناسب، افزایش هزینه‌های فعالیت اقتصادی و حتی محدود شدن نوآوری در فضای دیجیتال شود.

تعهد به ایمن‌سازی داده‌ها نه تعهدی ذاتاً به وسیله است و نه تعهدی ذاتاً به نتیجه، بلکه ماهیتی انعطاف‌پذیر و وابسته به اوضاع و احوال دارد. معیارهای تعیین‌کننده در این خصوص شامل نوع داده، میزان حساسیت آن، جایگاه حرفه‌ای متعهد، سطح خطرات متعارف، استانداردهای فنی رایج و انتظارات مشروع اشخاص موضوع داده است. در مواردی که داده‌ها از اهمیت و حساسیت بالاتری برخوردارند یا متعهد به‌عنوان یک ارائه‌دهنده حرفه‌ای خدمات دیجیتال فعالیت می‌کند، انتظار تحقق سطح بالاتری از امنیت منطقی است و تعهد به ایمن‌سازی داده‌ها به تعهد نتیجه نزدیک می‌شود. در

مقابل، در روابطی که سطح خطر پایین‌تر یا کنترل متعهد محدودتر است، تحلیل این تعهد در قالب تعهد وسیله تقویت‌شده قابل توجیه خواهد بود. رویکرد مختلط و پویا، علاوه بر انطباق با واقعیت‌های فنی، از حیث حقوقی نیز با اصول مسئولیت مدنی و حمایت از حقوق اشخاص سازگارتر است. این رویکرد امکان توزیع منصفانه‌تر بار اثبات، ارزیابی دقیق‌تر رفتار متعهد و جلوگیری از افراط و تفریط در اعمال مسئولیت را فراهم می‌آورد. بدین‌ترتیب، نه زیان‌دیده در معرض بی‌حمایتی قرار می‌گیرد و نه متعهد با مسئولیتی فراتر از توان متعارف خود مواجه می‌شود.

پذیرش چنین رویکردی می‌تواند به ارتقای سطح مراقبت در ایمن‌سازی داده‌ها و افزایش اعتماد عمومی به خدمات دیجیتال منجر شود. همچنین این الگو ظرفیت آن را دارد که در تفسیر قضایی و تدوین قواعد تقنینی آینده مورد استفاده قرار گیرد و به شکل‌گیری رویه‌ای منسجم در مواجهه با دعاوی ناشی از نقض امنیت داده‌ها کمک کند. تأکید بر معیارهای چندگانه و ارزیابی موردی، امکان سازگاری حقوق خصوصی با تحولات پرشتاب فناوری را افزایش داده و از ایستایی مفاهیم سنتی تعهد جلوگیری می‌کند. در نهایت، پاسخ به پرسش ماهیت تعهد به ایمن‌سازی داده‌ها، نه در انتخاب یکی از دو قالب سنتی، بلکه در بازتعریف انعطاف‌پذیر آن‌ها نهفته است. چنین بازتعریفی می‌تواند زمینه‌ساز تعادلی پایدار میان حمایت مؤثر از حقوق اشخاص موضوع داده و حفظ کارایی و پویایی روابط حقوق خصوصی در عصر دیجیتال باشد.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

فارسی

ـ السان، مصطفی، ۱۴۰۲، **حقوق تجارت الکترونیکی**، چاپ دهم، تهران، انتشارات سمت.

ـ باقری، محمود و نوشادی، ابراهیم، ۱۳۹۶، چالش‌های تعیین صلاحیت قضایی و قانون حاکم بر قراردادهای الکترونیکی بین‌المللی، **مجله حقوقی دادگستری**، شماره ۱۰۰.

ـ پیشنماز، سیدامین و رکنی، امیرعباس، ۱۴۰۲، تعطیلی پلتفرم‌های مجازی؛ ضرورت تحلیل نظام حاکم بر داده‌های شخصی از منظر حقوق اموال، **فصلنامه پژوهش‌های حقوقی**، شماره ۵۳.

ـ رحمانی، هادی، ۱۳۹۴، **مسئولیت مدنی رسا در حقوق تجارت الکترونیکی**، چاپ اول، تهران، انتشارات مجد.

ـ شریفی کیا، محمدعلی و شعبانی جهرمی، فریده، ۱۴۰۱، شرط شخصی تلقی شدن داده‌ها در فضای سایبر بررسی تطبیقی مقررات عمومی اروپایی حفاظت از داده و حقوق ایران، **دوفصلنامه حقوق خصوصی**، شماره ۱.

ـ ضیایی، جلال، ۱۴۰۴، بررسی فقهی و حقوقی حریم خصوصی در عصر دیجیتال و ارائه راهکارهای حفاظت از آن، **کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق**.

ـ عطازاده، سعید و انصاری، جلال، ۱۴۰۰، **حقوق جزای اختصاصی**، چاپ دوم، تهران، انتشارات میزان.

ـ کاتوزیان، ناصر، ۱۴۰۴، **قواعد عمومی قراردادها**، جلد اول، چاپ یازدهم، تهران، انتشارات گنج دانش.

ـ نعمتی، نبی الله، ۱۳۹۶، بررسی مسئولیت مدنی ناشی از نقض امنیت داده در تهدیدات سایبری، **فصلنامه پژوهش‌های حفاظتی و امنیتی**، شماره ۲۳.

لاتین

- Brkan, Maja, 2016, Data protection and conflict-of-laws: A challenging relationship, Eur. Data Prot. L. Rev. 2.

- Bygrave, Lee Andrew, 2014, Data privacy law: an international perspective. Oxford University Press.
- Buffelan-Lanore, Yvaine, Virginie Larribau-Terneyre, 2016, Droit civil: les obligations, Vol. 2. Sirey: Dalloz.
- Cabrol, Pierre, Monique Ribeyrol, 2018, Leçons de Droit des obligations.
- Chantepie, Gaël, Mathias Latina, 2016, La réforme du droit des obligations, Commentaire théorique et pratique dans l'ordre du Code civil. Dalloz.
- Dautieu, Thomas, 2018, La Commission nationale de l'informatique et des libertés, régulateur des données de santé, Les Tribunes de la santé 58.1
- De Hert, Paul, Vagelis Papakonstantinou, 2016, The new General Data Protection Regulation: Still a sound system for the protection of individuals?, Computer law & security review 32.2.
- Kuner, Christopher, 2013, Transborder data flows and data privacy law. Oxford University Press.
- Poulain, Michèle, 2007, Bibliographie systématique des ouvrages et articles en langue française, Annuaire Français de Droit International 53.1
- Protection, Formerly Data, 2018, General data protection regulation (GDPR), Intersoft Consulting.
- Schlechtriem, Peter, Petra Butler, 2009, UN Law on international sales: The UN Convention on the international sale of goods. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Solove, Daniel J, 2010, Understanding privacy. Harvard university press.
- Tancelin, Maurice, 1978, Traité de droit civil, sous la direction de Jacques GHESTIN,

Introduction générale par Jacques GHESTIN et Gilles GOUBEAUX, Paris, LGDJ, Les Cahiers de droit 19.3.

- Weber, Rolf H, 2017, Data Protection in the Termination of Contract. Nomos Verlagsgesellschaft mbH & Co. KG.

- Wessel, Ramses A, 2015, Towards EU cybersecurity law: regulating a new policy field, Research handbook on international law and cyberspace. Edward Elgar Publishing.

- Zeller, Bruno, 2000, The UN Convention on Contracts for the International Sale of Goods (CISG) -A Leap Forward towards Unified International Sales Law, Pace Int'l L. Rev. 12.

- Zimmermann, Reinhard, 1990, The law of obligations: Roman foundations of the civilian tradition. Juta and Company Ltd.

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.26- Winter 2026