



University of Tabriz

Contemporary Comparative Legal Studies

Online ISSN: 2821-0514

Volum: 16 Issue: 41

Winter 2026

Article Type: Research Article

Pages: 105-139

Recognizing Data Loss as an Emerging Damage in the Civil Liability of Autonomous Vehicles: A Comparative Analysis of Iranian and EU Law

Hamid Hamidian¹| Zahra Bonjakhi²

1. Assistant Professor, Department of Private Law, University of Mazandaran, Iran (Corresponding Author)

h.hamidian@umz.ac.ir

2. Master in Private Law, Islamic Azad University, Sabzevar Branch, Iran

zahra.bonjakhi@iau.ir

Abstract

The rapid expansion of artificial intelligence (AI)-based technologies, particularly autonomous vehicles, has posed novel challenges to traditional structures of civil liability. In this context, data have emerged as a foundational element for safety assurance, algorithmic decision-making, and accident reconstruction. The loss or deletion of such data may significantly affect the establishment of causation and the allocation of technological risk. This study employs a descriptive-analytical method with a comparative approach to examine the legal status of “data loss” within the civil liability regimes governing autonomous vehicles under European Union and Iranian law. At the level of the European Union, instruments such as the Product Liability Directive, the General Data Protection Regulation, and the AI Liability Directive demonstrate that data loss is not recognized as an independent category of classical damage. Nevertheless, where the absence of data affects safety or results in demonstrable harm, compensation may be granted within existing liability frameworks. Moreover, certain mechanisms aimed at facilitating proof of causation (particularly in AI-related claims) have been introduced or proposed. Under Iranian law, despite the compensatory capacity of Articles 1 and 2 of the Civil Liability Act and the enactment of the National Data and Information Management Act, the explicit legal characterization of data as a compensable head of damage in the context of autonomous vehicle liability remains underdeveloped. The findings indicate that legislative clarification, either through the incorporation of a specific provision into the Civil Liability Act or the adoption of a dedicated statute addressing liability and safety in autonomous systems, would provide a more coherent framework for victim protection and a more equitable allocation of technological risk.

Keywords: Autonomous Vehicles, Data Loss, Emerging Damages, Civil Liability, European Union, Iran.

Received: 2025/08/25

Received in revised form: 2026/02/07

Accepted: 2026/02/23

Published: 2026/03/07

DOI: 10.22034/LAW.2026.68830.3526

Publisher: University of Tabriz

law@tabrizu.ac.ir





شناسایی از دست رفتن داده‌ها به عنوان خسارت نوین در مسئولیت مدنی خودروهای خودران: بررسی تطبیقی حقوق ایران و اتحادیه اروپا

حمید حمیدیان^۱ | زهرا بنجخی^۲

h.hamidian@umz.ac.ir

zahra.bonjakhi@iau.ir

۱. استادیار گروه حقوق خصوصی، دانشگاه مازندران، ایران (نویسنده مسئول)

۲. کارشناسی ارشد حقوق خصوصی، دانشگاه آزاد اسلامی، واحد سبزوار، ایران

چکیده

گسترش فناوری‌های مبتنی بر هوش مصنوعی، به‌ویژه خودروهای خودران، ساختارهای سنتی مسئولیت مدنی را با چالش‌های نوینی مواجه ساخته است. در این میان، داده‌ها به‌عنوان عنصر اساسی ایمنی، تصمیم‌گیری الگوریتمی و بازسازی حوادث، نقشی تعیین‌کننده یافته‌اند و فقدان یا حذف آنها می‌تواند آثار مهمی بر احراز رابطه سببیت و توزیع ریسک فناوریانه داشته باشد. این پژوهش با روش توصیفی-تحلیلی و رویکرد تطبیقی، جایگاه «از دست رفتن داده» را در مسئولیت مدنی خودروهای خودران در حقوق اتحادیه اروپا و ایران بررسی می‌کند. در سطح اتحادیه اروپا، مقرراتی همچون دستورالعمل مسئولیت ناشی از محصول، مقررۀ عمومی حفاظت از داده‌ها و دستورالعمل مسئولیت هوش مصنوعی نشان می‌دهد که فقدان داده به‌طور مستقل به‌عنوان خسارت کلاسیک شناسایی نشده، اما در صورت تأثیر بر ایمنی یا ورود ضرر قابل اثبات، در چارچوب‌های موجود قابل جبران است و در مواردی نیز سازوکارهای تسهیل اثبات رابطه سببیت پیش‌بینی شده است. در حقوق ایران، با وجود ظرفیت مواد ۱ و ۲ قانون مسئولیت مدنی و تصویب قانون مدیریت داده و اطلاعات ملی، جایگاه صریح داده به‌عنوان موضوع خسارت در مسئولیت مدنی خودروهای خودران تبیین نشده است. یافته‌ها حاکی از آن است که شفاف‌سازی تقنینی از طریق الحاق ماده‌ای به قانون مسئولیت مدنی یا تدوین قانون مستقل در حوزه مسئولیت و ایمنی سامانه‌های خودران می‌تواند چارچوبی منسجم‌تر برای حمایت از زیان‌دیدگان و تنظیم عادلانه توزیع ریسک فراهم سازد.

واژگان کلیدی: اتحادیه اروپا، خسارت از دست رفتن داده‌ها، خسارت نوین، خودروهای خودران، مسئولیت تولیدکننده، مسئولیت مدنی.

تاریخ انتشار: ۱۴۰۴/۱۲/۱۶

تاریخ پذیرش: ۱۴۰۴/۱۲/۰۴

تاریخ بازنگری: ۱۴۰۴/۱۱/۱۸

تاریخ دریافت: ۱۴۰۴/۰۶/۰۳

DOI: 10.22034/LAW.2026.68830.3526



law@tabrizu.ac.ir

ناشر: دانشگاه تبریز

مقدمه

تحولات سریع در عرصه فناوری، به‌ویژه در حوزه هوش مصنوعی^۱ و سیستم‌های خودکار، چشم‌اندازهای نوینی را در صنعت حمل‌ونقل رقم زده است. ادغام هوش مصنوعی در فناوری دیجیتال با سرعت در حال گسترش است و صنعت خودروسازی نیز شاهد افزایش علاقه به خودروهای متصل و خودران است.^۲ خودروهای خودران^۳ که با تکیه بر داده‌های پیچیده و پردازش لحظه‌ای اطلاعات محیطی و بدون دخالت انسانی هدایت می‌شوند، نمونه‌ای بارز از این دگرگونی فناورانه هستند. در واقع ما با تجهیزاتی روبه‌رو هستیم که ممکن است از جانب خود تصمیم بگیرند.^۴ در چنین سیستم‌هایی، داده^۵ نه تنها ابزاری کمکی، بلکه عنصر بنیادین تصمیم‌گیری و امنیت محسوب می‌شود. بنابراین، از بین رفتن، تخریب یا دست‌کاری داده‌ها می‌تواند به بروز حادثه، تضییع حقوق کاربران یا ناتوانی در تعیین مسئولیت حقوقی منجر شود؛ موضوعی که با عنوان خسارت ناشی از «از دست رفتن داده‌ها» یا «دیتا لاس»^۶ قابل بررسی است.

در ادبیات حقوقی ایران، پژوهش‌ها عمدتاً بر جنبه‌های سخت‌افزاری و نرم‌افزاری خودروهای خودران متمرکز بوده و توجه اصلی به شناسایی خطاهای سیستمی، نقائص نرم‌افزاری و عیوب فنی یا عملکردی این خودروها و مسئولیت تولیدکننده در قبال آنها بوده است. این مطالعات نشان می‌دهند که ضعف‌های نرم‌افزاری می‌توانند عامل مستقیم ایجاد خسارت باشند و در نتیجه، مسئولیت مدنی تولیدکننده را در معرض بررسی دقیق قرار دهند.^۷ علاوه بر این، پژوهشی دیگر بر اهمیت تحلیل معیارهای تشخیص عیب و نحوه تعیین مسئولیت در مواجهه با خسارات ناشی

1. Artificial Intelligence

2. Claudine Badue et al, «Self-Driving Cars: a Survey», *Expert Systems with Applications*, Vol. 165, (2021), p. 2.

3. Autonomous Vehicle

۴. اسماء جرفی و همکاران، «مسئولیت مدنی مالک کشتی‌های خودران ناشی از تصادم کشتی»، پژوهش‌های حقوق تطبیقی، ش ۲۸ (۱۴۰۳)، ص ۱۵.

5. Data

6. Data Loss

۷. حمید ابهری و همکاران، «مطالعه تطبیقی ضابطه‌های تشخیص عیب خودرو در حقوق ایران، انگلیس و امریکا»، مطالعات حقوق تطبیقی، ش ۱۲ (۱۴۰۰)، ص ۳۹۷.

از نقص‌های فنی و نرم‌افزاری تأکید کرده‌اند.^۸

با این حال، آنچه در ادبیات حقوقی ایران کمتر مورد توجه قرار گرفته، مفهوم نوپدید «ازدست رفتن داده» است؛ نوعی خسارت اطلاعاتی و فناورانه که می‌تواند در شرایط خاص نقش تعیین‌کننده‌ای در بروز حادثه یا ایجاد زیان ایفا کند. این مسئله اهمیت جدیدی به مسئولیت مدنی در خودروهای خودران می‌بخشد؛ چراکه فقدان یا تخریب داده‌های حیاتی ممکن است علاوه بر خطاهای سخت‌افزاری و نرم‌افزاری، به‌عنوان عامل مستقل ایجاد خسارت محسوب شود و چارچوب‌های موجود حقوقی را برای تعیین مسئولیت ناکافی کند.

در این مقاله، به روش توصیفی-تحلیلی و با اتکا بر داده‌های مبتنی بر تحلیل منابع کتابخانه‌ای، اسناد حقوقی، مقررات ملی و فراملی و نیز مقالات علمی داخلی و خارجی تلاش خواهد شد تا با نگاهی تطبیقی، مفهوم ازدست رفتن داده‌ها به‌عنوان نوعی خسارت نوین در بستر مسئولیت مدنی خودروهای خودران تعریف و تحلیل گردد. در این راستا، پس از بررسی جایگاه حقوقی این مفهوم در نظام مسئولیت مدنی ایران، مقررات و رویه‌های حقوقی اتحادیه اروپا، به‌ویژه دستورالعمل مسئولیت محصول^۹ و مقررات حفاظت از داده‌ها^{۱۰}، مورد واکاوی قرار خواهد گرفت. در پایان، پیشنهادهایی جهت اصلاح قوانین داخلی با هدف تطبیق با الزامات عصر داده‌محور ارائه خواهد شد. پرسش اصلی این پژوهش آن است که آیا می‌توان از بین رفتن داده‌ها را در خودروهای خودران، به‌عنوان خسارتی مستقل و قابل مطالبه در چارچوب مسئولیت مدنی شناسایی کرد؟ و در صورت مثبت بودن پاسخ، چه الزامات نظری و تقنینی برای پذیرش آن در نظام حقوقی ایران وجود دارد؟

۱. مفهوم داده و ازدست رفتن داده در خودروهای خودران

۱.۱. تعریف داده، تفاوت با اطلاعات

در خودروهای خودران، داده‌ها نقش حیاتی در تصمیم‌گیری، تحلیل محیط، مسیریابی،

۸. ناهید پارسا، «بررسی مسئولیت مدنی ناشی از نقص نرم‌افزار در خودروهای خودران با نگاهی به حقوق آمریکا»، *فقه و حقوق اسلامی*، ش ۱۵ (۱۴۰۳)، ص ۱۱۸.

9. Product Liability Directive

10. Data Protection Regulations

تشخیص موانع و حتی تعامل با زیرساخت‌ها ایفا می‌کنند. در چنین بسترهایی، داده نه تنها بخشی از فرایند فنی، بلکه عنصری دارای ارزش اقتصادی و حقوقی است که از بین رفتن آن می‌تواند به خطرهای جدی و مسئولیت قانونی بینجامد.

داده، اصطلاحی پیچیده است که ممکن است برای افراد مختلف و در زمینه‌های گوناگون، معانی متفاوتی داشته باشد.^{۱۱} واژه داده در علوم مختلف دارای معانی متعددی است، داده در ادبیات فناوری اطلاعات، ماده خامی است که قابلیت پردازش، تحلیل و استخراج معنا را دارد. طبق تعریف یکی از استانداردهای بین‌المللی سازمان ایزو و کمیسیون بین‌المللی الکتروتکنیک^{۱۲}، داده عبارت است از: «بازنمایی قابل تفسیر از اطلاعات به شکلی رسمی که برای ارتباط، تفسیر یا پردازش مناسب باشد»^{۱۳}.

داده و اطلاعات گرچه در اغلب موارد به صورت مترادف استعمال می‌شوند، با این حال از نظر مفهومی متفاوت‌اند.^{۱۴} به زبان ساده، داده‌ها عناصر خام و پردازش نشده هستند که به خودی خود معنای مشخصی ندارند، ولی می‌توانند ورودی پردازش‌های بعدی باشند.^{۱۵} برای مثال، عدد ۷۵ به تنهایی یک داده است که هیچ معنی خاصی ندارد. اما اگر بدانیم این عدد مربوط به سرعت یک خودرو است، معنای آن روشن و به اطلاعات تبدیل می‌شود.

اطلاعات، حاصل پردازش و تفسیر داده‌ها در یک زمینه مشخص است. در حقوق، اطلاعات زمانی ارزشمند می‌شود که در اثبات یا رد یک ادعا، تشخیص تقصیر، تعیین مسئولیت یا تحلیل قانونی مؤثر باشد. برای مثال، اگر از سرعت لحظه‌ای خودرو و تحلیل ویدئوی دوربین مشخص شود که خودرو خودران در لحظه تصادف به صورت خودکار تغییر مسیر داده و وارد مسیر مخالف

۱۱. محمد آوخ، درک مفهوم دیتا؛ دیتا دقیقاً چیست؟، <https://www.etemadonline.com/> بخش-اجتماعی-۵۵۵۱۴۳/۲۳-درک-مفهوم-دیتا-دیتا-دقیقاً-چیست.

12. ISO/IEC 2382:2015

13. ISO/IEC, ISO/IEC 2382:2015: Information technology — Vocabulary, International Organization for Standardization / International Electrotechnical Commission. <https://www.iso.org/standard/63598.-html>

۱۴. بهناز احمدوند و آرتین جهان‌شاهی، «بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی اتحادیه اروپا و ایران»، پژوهش‌های حقوقی تطبیقی، ش ۲۷ (۱۴۰۲)، ص ۱۱۰.

15. Ralph Stair & George Reynolds, Principles of Information Systems, (Cengage Learning, 13th ed, 2017), p. 4

شده است، این ترکیب تبدیل به اطلاعات حقوقی مهم برای تعیین مسئولیت در دعاوی می‌شود.

۲.۱. تعریف ازدست رفتن داده‌ها در بستر حقوقی

در منابع معتبر فنی همچون مؤسسه ملی استاندارد و فناوری ایالات متحده^{۱۶}، ازدست رفتن داده‌ها به‌عنوان «حذف، تخریب یا غیرقابل دسترس شدن ناخواسته داده‌ها به دلیل خطای انسانی، نقص فنی، حمله سایبری یا عوامل مشابه تعریف شده است». در ادبیات فناوری، ازدست رفتن داده‌ها به معنای از بین رفتن غیرقابل جبران اطلاعات دیجیتال به دلیل عوامل متعددی مانند خطای انسانی، نقص سخت‌افزاری، حملات سایبری یا مشکلات نرم‌افزاری تعریف می‌شود^{۱۷}. این تعریف گسترده زمینه مناسبی را برای طبقه‌بندی انواع ازدست رفتن داده‌ها در خودروه‌های خودران فراهم می‌آورد؛ ازجمله ازدست رفتن فیزیکی ناشی از آسیب سخت‌افزاری، نقص نرم‌افزاری، حملات سایبری، طراحی معیوب، حذف عمدی از سوی کاربران یا سازندگان، و اختلال در ارتباط داده‌ای با سرور یا سامانه پشتیبان. وجه مشترک تمام این موارد، تأثیر مستقیم بر ایمنی خودرو و کاهش قابلیت بازیابی اطلاعات حیاتی در هنگام حادثه است؛ عاملی که می‌تواند در تحلیل مسئولیت مدنی تولیدکنندگان یا ارائه‌دهندگان خدمات نرم‌افزاری نقش تعیین‌کننده‌ای ایفا کند. بنابراین، شناسایی دقیق انواع ازدست رفتن داده‌ها و منشأ آن نه‌تنها از منظر فنی، بلکه از دیدگاه حقوقی نیز ضرورتی انکارناپذیر است^{۱۸}.

می‌توان ازدست رفتن داده‌ها را با یک مثال ساده چنین توصیف کرد: فرض کنید یک دانش‌آموز هر روز در دفترچه‌ای یادداشت می‌کند که چه کارهایی انجام داده، تکالیفش چیست، و برنامه فردا چیست. حالا اگر این دفترچه گم شود یا خراب شود، دیگر به اطلاعات داخلش دسترسی ندارد. این یعنی ازدست رفتن داده‌ها یا همان دیتا لاس. در این مثال، گم‌شدن دفترچه ملاک تشخیص ما برای تعیین خسارت نیست، بلکه آنچه اهمیت دارد اطلاعات موجود در دفترچه است که می‌توان به علل مختلفی ازدست رفتن آن را متصور شد.

در بستر حقوقی، چنین مفهومی نیازمند بازتعریف است؛ چراکه داده صرفاً یک ابزار فناورانه

16. National Institute of Standards and Technology (NIST)

17. National Institute of Standards and Technology, "Computer Security Resource Center glossary", <https://csrc.nist.gov/glossary>

18. Hornetsecurity, "What is data loss?" <https://www.hornetsecurity.com/en/knowledge-base/data-loss/>

نیست، بلکه در بسیاری از موارد، واجد ارزش اقتصادی، عملکردی یا شخصی است که از بین رفتن آن می‌تواند موجب ورود ضرر گردد. در حوزه حقوق سنتی، مفهومی تحت عنوان «از دست رفتن داده‌ها» سابقه‌ای ندارد، چراکه حقوق کلاسیک عمدتاً بر اموال مادی و خسارات ملموس تمرکز داشته است. اما در نظام‌های حقوقی مدرن و با گسترش هوش مصنوعی، اینترنت اشیا و خودروهای خودران، لزوم شناسایی داده و از بین رفتن آن به عنوان یک منبع خسارت و مسئولیت حقوقی پدید آمده است.

۳.۱. تمایز از دست رفتن داده‌ها با مفاهیم مشابه

در نظام‌های حقوقی مرتبط با فناوری‌های نوین، به‌ویژه در زمینه خودروهای خودران، تمایز میان «نقص نرم‌افزار» و «از دست رفتن داده‌ها» از منظر اثبات مسئولیت و ارزیابی خسارت اهمیت بنیادین دارد. نقص نرم‌افزار به معنای وجود خطا، باگ^{۱۹} و یا عملکرد نادرست در برنامه‌نویسی یا الگوریتم‌هایی است که باعث می‌شود نرم‌افزار برخلاف آنچه طراحی یا وعده داده شده است، عمل کند. این نقص ممکن است به عملکرد غیرمنتظره، اشتباه در تصمیم‌گیری، یا حتی توقف کامل عملکرد سیستم منجر شود. نرم‌افزار خودران زمانی معیوب است که ایمنی‌ای که عموم مردم انتظار دارند، ارائه نکند^{۲۰}؛ مانند حالتی که الگوریتم تشخیص علائم راهنمایی، تابلوی «ایست» را در شرایط نوری خاص شناسایی نکند و خودرو بدون توقف وارد تقاطع شده، تصادف کند. در مقابل، از دست رفتن داده‌ها یا دیتا لاس معمولاً به عنوان پدیده‌ای ثانویه پس از حادثه یا به صورت هم‌زمان رخ می‌دهد و ممکن است ناشی از آسیب به حافظه، اختلال در سیستم ذخیره‌سازی یا حملات سایبری باشد. اگرچه از دست رفتن داده‌ها مستقیماً علت حادثه نیست، اما از منظر حقوقی می‌تواند مانعی جدی در فرایند اثبات دعوا، تعیین تقصیر یا دفاع مؤثر طرفین باشد. بر این اساس، تحلیل افتراق میان این دو مفهوم برای تنظیم دقیق مسئولیت مدنی تولیدکنندگان و توسعه‌دهندگان فناوری‌های خودران ضروری است.

۱۹. باگ (Bug) به هرگونه اشتباه در طراحی، کدنویسی یا اجرای نرم‌افزار گفته می‌شود که منجر به بروز اختلال در عملکرد سیستم یا از دست رفتن داده‌ها می‌گردد. در زمینه خودروهای خودران، باگ ممکن است باعث شود داده‌های مربوط به سرعت، موقعیت یا شرایط محیطی به درستی ذخیره نشوند یا حذف شوند، بدون اینکه سخت‌افزار آسیبی دیده باشد.

۲۰. ناهید پارسا، پیشین، ص ۱۲۰.

در ادبیات امنیت سایبری، مفهوم ازدست رفتن داده‌ها متمایز از مفاهیمی چون «نقض داده»^{۲۱} یا «خرابی داده»^{۲۲} است. درحالی که نقض داده ناظر به دسترسی غیرمجاز اشخاص ثالث به اطلاعات محرمانه است^{۲۳} و خرابی داده به تغییر ناخواسته یا مخرب در محتوای داده اشاره دارد دارد که موجب اختلال در عملکرد آن می‌شود^{۲۴}، ازدست رفتن داده‌ها به فقدان کلی یا جزئی اطلاعات حیاتی اطلاق می‌گردد که به‌صورت دائمی ازدست رفته‌اند و امکان بازیابی آنها وجود ندارد^{۲۵}. در سامانه‌های خودران که تصمیم‌گیری‌ها به‌صورت آنی و بر پایه داده‌های ورودی از حسگرها، نقشه‌ها و الگوریتم‌های پیش‌بینی انجام می‌شود، ازدست رفتن داده‌ها می‌تواند به خطای تصمیم‌گیری، رفتار غیرایمن و بروز خسارات جانی یا مالی منجر شود. در چارچوب حقوق مسئولیت مدنی، چنین فقدان می‌تواند به طرح ادعاهایی علیه تولیدکنندگان، توسعه‌دهندگان نرم‌افزار یا ارائه‌دهندگان خدمات ذخیره‌سازی بینجامد؛ به‌ویژه در مواردی که فقدان داده مانع از بازسازی حادثه و احراز تقصیر یا نقص در محصول می‌شود. در حقوق اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها به‌صراحت از مسئولیت اشخاص نسبت به امنیت و حفظ داده‌های پردازش‌شده سخن گفته است^{۲۶} و در قانون هوش مصنوعی نیز تولیدکنندگان سامانه‌های پرخطر مانند خودروهای خودران، مکلف به طراحی ایمن و تضمین قابلیت ثبت و بازیابی داده‌های بحرانی شده‌اند^{۲۷}.

۲. نقش داده در خودروهای خودران و سناریوهای حقوقی

۱.۲. اهمیت داده در عملکرد و ایمنی

در سیستم‌های هوش مصنوعی به‌ویژه در خودروهای خودران، داده نقش بنیادین در فرایند تصمیم‌گیری ایفا می‌کند. خودروهای خودران برای تشخیص محیط اطراف خود از فناوری‌هایی

21. Data Breach

22. Data Corruption

23. European Union Agency for Cybersecurity (ENISA), "Threat Landscape 2021", <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.

24. National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems (FIPS Publication No. 199), U.S. Department of Commerce, 2004. <https://doi.org/10.6028/NIST.FIPS.199>.

25. "What is data loss?", *op. cit.*

26. General Data Protection Regulation, Arts. 5 & 32.

27. Artificial Intelligence Act. Regulation, Arts. 16 & 17.

همچون رادار^{۲۸}، لیدار^{۲۹}، سامانه موقعیت‌یاب جهانی^{۳۰}، کیلومترشمار و بینایی رایانه‌ای^{۳۱} استفاده می‌کنند. سیستم‌های کنترل پیشرفته، اطلاعات دریافتی از حسگرها را تفسیر می‌کنند تا مسیر مناسب، موانع و علائم مرتبط را شناسایی نمایند. این سیستم‌ها قادرند داده‌های حسگرها را پردازش کرده، میان خودروهای مختلف تمایز قائل شوند؛ موضوعی که در طراحی مسیر به مقصد بسیار مفید است^{۳۲}. هوش مصنوعی در خودروهای خودران نقش محوری در تبدیل داده‌های خام حاصل از انواع حسگرها به تصمیمات عملیاتی ایفا می‌کند. داده‌های ورودی از لیدار، رادار، دوربین‌ها، سامانه موقعیت‌یاب، واحد اندازه‌گیری اینرسی^{۳۳} و حسگرهای اولتراسونیک^{۳۴}، ابتدا از طریق الگوریتم‌های پیش‌پردازشی، فیلتر و یکپارچه‌سازی می‌شوند تا تصویری منسجم از محیط اطراف خودرو ایجاد گردد. سپس سامانه‌های هوش مصنوعی شامل شبکه‌های عصبی، یادگیری ماشین^{۳۵} و الگوریتم‌های بینایی رایانه‌ای این داده‌ها را تحلیل می‌کنند تا عناصر کلیدی مانند موانع ثابت و متحرک، خطوط جاده، علائم رانندگی، عابران پیاده، وسایل نقلیه دیگر و تغییرات ناگهانی محیط را تشخیص دهند. با مدل‌سازی محیط و پیش‌بینی رفتار سایر عناصر در ترافیک، سامانه تصمیم‌یار هوشمند، مسیر بهینه، سرعت مناسب و زمان دقیق برای اعمال فرمان، ترمز یا شتاب‌گیری را تعیین می‌کند. این سیستم همچنین قادر است در شرایط غیرقابل پیش‌بینی مانند عبور ناگهانی عابر یا تغییر مسیر خودروهای مجاور، واکنش مناسب را در زمان واقعی نشان دهد. به‌طور خلاصه، هوش مصنوعی مغز متفکر خودرو است که از داده‌های حسی برای بازسازی

۲۸. Radar (Radio Detection and Ranging). سامانه‌ای در خودروهای خودران که با ارسال و دریافت امواج رادیویی، فاصله، سرعت و موقعیت اجسام اطراف خودرو را شناسایی می‌کند و نقش مهمی در سیستم‌های کمک‌راننده و جلوگیری از تصادف دارد.

۲۹. Lidar (Light Detection and Ranging). فناوری سنسور از دور که با استفاده از پالس‌های نور لیزر، فاصله اجسام تا خودرو را اندازه‌گیری می‌کند؛ لیدار در خودروهای خودران برای تهیه نقشه سه‌بعدی از محیط و شناسایی موانع کاربرد دارد.

30. Global Positioning System (GPS)

۳۱. Computer Vision. شاخه‌ای از هوش مصنوعی که به سیستم‌ها امکان می‌دهد تصاویر و ویدئوها را تحلیل و تفسیر کنند؛ در خودروهای خودران برای شناسایی علائم راهنمایی، خطوط جاده، عابران پیاده و سایر وسایل نقلیه به کار می‌رود.

32. James M. Anderson, Autonomous Vehicle Technology: A Guide for Policymakers, RAND Corporation, Santa Monica, CA, 2014.

۳۳. IMU (Inertial Measurement Unit). واحد اندازه‌گیری اینرسی؛ حسگری متشکل از شتاب‌سنج وژیروسکوپ که شتاب، سرعت زاویه‌ای و جهت‌گیری خودرو را اندازه‌گیری می‌کند و در ناوبری و تثبیت حرکت خودروهای خودران کاربرد دارد.

۳۴. Ultrasonic Sensors. حسگرهایی که با ارسال و دریافت امواج فراصوت، فاصله تا اشیای اطراف را اندازه‌گیری می‌کنند؛ این حسگرها در خودروهای خودران برای شناسایی موانع نزدیک، کمک به پارک و جلوگیری از برخورد استفاده می‌شوند.

35. Machine Learning

محیط، پیش‌بینی خطر و تصمیم‌گیری خودکار استفاده می‌کند و به این ترتیب، امکان رانندگی ایمن، مستقل و هوشمند را فراهم می‌سازد. در واقع، داده‌ها همانند چشم و گوش خودروهای خودران عمل می‌کنند و بدون آنها امکان پردازش هوشمند و عملکرد ایمن وجود نخواهد داشت.

در خودروهای خودران، داده‌ها عنصر محوری در تضمین عملکرد صحیح و حفظ ایمنی به‌شمار می‌آیند. هرگونه اختلال در جمع‌آوری، تحلیل، انتقال یا ذخیره‌سازی داده‌ها می‌تواند به خطا در تصمیم‌گیری یا واکنش‌های تاخیری منجر شده، امنیت سرنشینان یا سایر کاربران جاده را به‌خطر اندازد. این موضوع با مسئولیت مدنی تولیدکننده یا ارائه‌دهنده خدمات نرم‌افزاری ارتباط مستقیم دارد. در حقوق اتحادیه اروپا، نقص داده‌پردازی یا عدم شفافیت الگوریتمی می‌تواند مبنای مسئولیت تولیدکننده باشد. اگر رفتار سامانه هوش مصنوعی معیوب تلقی شود و میان این عیب و ورود خسارت رابطه سببیت احراز گردد، تولیدکننده می‌تواند مسئول شناخته شود.^{۳۶} افزون بر این، تولیدکنندگان مکلف‌اند ایمنی محصولات نرم‌افزارمحور را در شرایط عادی یا قابل پیش‌بینی تضمین کنند.^{۳۷} بنابراین، در مورد سامانه‌های هوش مصنوعی، تعهد به ایمنی تنها به اجزای فیزیکی محدود نیست و عملکرد نرم‌افزار و الگوریتم نیز در ارزیابی ایمنی نقش تعیین‌کننده دارد.

در حقوق ایران نیز بر اساس مواد ۱ و ۲ قانون مسئولیت مدنی، هر شخص یا نهادی که در نتیجه بی‌احتیاطی یا بی‌مبالاتی موجب ورود ضرر به غیر شود، مسئول جبران آن خواهد بود؛ حکمی که در خصوص خسارات ناشی از نقص داده‌پردازی در خودروهای خودران نیز قابل اعمال است. افزون بر این، وجود داده‌های دقیق و قابل بازیابی، مطابق اصل بار اثبات در دعوای مدنی^{۳۸}، برای اثبات تقصیر، اثبات وجود عیب یا دفاع مؤثر تولیدکننده، ضروری تلقی می‌شود. بر این اساس، داده‌ها نه‌تنها بنیان عملکرد ایمن خودروهای خودران را شکل می‌دهند، بلکه رکن اساسی در تحلیل حقوقی حوادث نیز محسوب می‌شوند.

۲.۲. طبقه‌بندی ازدست رفتن داده‌ها

در نظام‌های فناورانه خودروهای خودران، ازدست رفتن داده‌ها می‌تواند در قالب‌های متنوعی بروز کرده، آثار فنی و حقوقی متفاوتی به‌جای گذارد. این پدیده به‌طور کلی در شش دسته قابل

36. Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), Art. 6

37. General Product Safety Regulation, Art. 4

۳۸. قانون مدنی، ماده ۱۲۵۷

طبقه‌بندی است: نخست، ازدست رفتن فیزیکی داده‌ها^{۳۹} که به سبب خرابی سخت‌افزاری مانند آسیب به حافظه داخلی خودرو بر اثر تصادف رخ می‌دهد؛ دوم، ازدست رفتن نرم‌افزاری داده‌ها^{۴۰} که ناشی از خطا در سیستم‌عامل یا باگ در فرایند ثبت داده‌هاست؛ سوم، ازدست‌رفتن داده‌ها ناشی از حمله سایبری^{۴۱} که در آن هکرها^{۴۲} با نفوذ به سامانه، داده‌ها را حذف یا رمزنگاری می‌کنند؛ چهارم، ازدست رفتن داده‌ها ناشی از طراحی معیوب^{۴۳} که به دلیل نبود پیش‌بینی‌های ایمن‌سازی و ذخیره‌سازی در طراحی اولیه نرم‌افزار یا سخت‌افزار پدید می‌آید؛ پنجم، ازدست رفتن داده‌ها ناشی از حذف عمدی یا غیرمجاز که ممکن است از سوی کاربران، تعمیرکاران یا حتی تولیدکنندگان صورت گیرد؛ و ششم، ازدست‌رفتن داده‌ها به‌طور موقت یا ناشی از اختلال ارتباطی که در اثر قطع اتصال میان خودرو و سامانه‌های پشتیبان یا سرور مرکزی حادث می‌شود. هریک از این انواع، بسته به منشأ و شرایط وقوع، می‌تواند در تعیین مسئولیت مدنی یا قابلیت استناد داده‌ها در محاکم، نقش کلیدی ایفا کند.^{۴۴}

در خودروهای خودران، انواع ازدست رفتن داده‌ها بخش مهمی از تحلیل مسئولیت مدنی محسوب می‌شوند و ترکیب منشأ فنی و ابعاد حقوقی آنها ضروری است. ازدست رفتن فنی داده‌ها هنگامی رخ می‌دهد که سخت‌افزارهای ذخیره‌سازی (مانند SSD یا HDD)^{۴۵} آسیب می‌بینند؛ برای مثال سقوط یا ضربه به خرابی هاردیسک^{۴۶} یا چیپ SSD منجر می‌شود که بازیابی داده‌ها

39. Physical Data Loss

40. Logical (or Software-Based) Data Loss

41. Cyber-Induced Data Loss

۴۲. هکر، فردی است که بدون مجوز یا برخلاف قوانین و استانداردهای امنیتی، به سیستم‌های اطلاعاتی دسترسی یافته، ممکن است داده‌ها را تغییر دهد، حذف کند یا از آنها سوءاستفاده نماید.

43. Design-Based Data Loss

44. Ryan Calo, "Robotics and the Lessons of Cyberlaw", California Law Review, No. 3 (2016), p. 538.
European Commission, "Directive 85/374/EEC on Liability for Defective Products (Consolidated Version with 2024 Amendments)", EUR-Lex, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31985L0374>.

۴۵. SSD (Solid State Drive)، درایو حالت جامد در خودروهای خودران برای ذخیره سریع داده‌های سنسورها، GPS، و دوربین‌ها بسیار مناسب است.

HDD (Hard Disk Drive)، هارد دیسک مکانیکی در خودروها معمولاً کمتر استفاده می‌شود، چون نسبت به لرزش حساس‌تر است، اما در برخی سامانه‌های پشتیبان ممکن است کاربرد داشته باشد.

۴۶. هد دیسک (Disk Head) یکی از بخش‌های کلیدی در هارد دیسک (HDD) است که وظیفه خواندن و نوشتن داده‌ها روی دیسک را برعهده دارد.

را غیرممکن می‌سازد.^{۴۷} ازدست رفتن نرم‌افزاری داده‌ها در نتیجه خطاهای نرم‌افزاری مانند باگ فایل سیستم، کرش و یا خطای انسانی در جایگزینی دیسک رخ می‌دهد و داده‌ها بدون هیچ آسیب فیزیکی حذف یا خراب می‌شوند.^{۴۸} از دست رفتن امنیتی داده‌ها ناشی از حملات سایبری، نفوذ یا دست‌کاری داده‌هاست که علاوه بر تهدید اقدام نسبت به داده، ممکن است حذف عمدی داده‌های بحرانی را نیز شامل شود و موجب اختلال در تحلیل حادثه گردد.^{۴۹} نهایتاً از دست رفتن حقوقی یا فرایندی داده‌ها زمانی اتفاق می‌افتد که داده‌های ضروری برای اثبات تقصیر یا پاسخ به نهادهای قانونی به درستی نگهداری یا ثبت نشده‌اند؛ موضوعی که به تضییع حق زیان‌دیده یا مختل شدن دادرسی می‌انجامد. شناخت دقیق این دسته‌ها با توجه به منشأ فنی و تأثیر حقوقی هریک برای تدوین سیاست‌های مسئولیت مدنی و بیمه‌ای خودروهای خودران ضروری است.

۳.۲. نمونه سناریوهای منجر به خسارت

سناریو ۱: حذف داده‌های ثبت‌شده حادثه در یک حادثه فرضی. خودروی خودرانی با اتوبوس برخورد می‌کند، اما داده‌های ذخیره‌شده در جعبه سیاه^{۵۰} خودرو که معمولاً برای بازسازی دقیق حادثه و تعیین مسئولیت حیاتی هستند، به دلیل نقص فنی یا پاک‌سازی عمدی قابل دسترسی نیستند. این فقدان اطلاعات مانع از تحلیل دقیق چگونگی وقوع تصادف می‌شود و به دنبال آن، زیان‌دیده با مشکل جدی در اثبات ادعای خود مواجه می‌شود. از منظر حقوقی، حذف یا عدم دسترسی به داده‌های جعبه سیاه، موجب تضییع حق و ایجاد ابهام در تعیین مسئولیت می‌گردد و روند دادرسی را دچار اختلال می‌کند. بنابراین، این مسئله ضرورت وضع مقررات و استانداردهای فنی و حقوقی سخت‌گیرانه‌تر برای حفظ و نگهداری داده‌های حادثه و همچنین اعمال ضمانت‌های اجرایی مؤثر را به شدت مطرح می‌سازد.

47. Riccardo Pincirolì, et al., "The Life and Death of SSDs and HDDs: Similarities, Differences, and Prediction Models", *Conference Paper* (2020), p. 6.

۴۸. مصطفی کیشانی و حسین اسدی، «ارزیابی اثر خطای انسانی بر اتکاپذیری سامانه‌های ذخیره‌سازی داده»، *علوم رایانش و فناوری اطلاعات*، ش ۱۸ (۱۳۹۹)، ص ۴۲.

49. Sai Varun Reddy Bhemavarapu, "Cybersecurity for Autonomous Vehicles", <https://arxiv.org/abs/2504.20180>.

۵۰. جعبه سیاه (Black Box) مفهومی است که در علوم مختلف مثل مهندسی، رایانه، هوافضا و حتی حقوق و فلسفه به کار می‌رود، اما در تعریف عمومی، جعبه سیاه سیستمی است که ورودی و خروجی آن برای ما قابل مشاهده یا اندازه‌گیری است، اما فرآیند داخلی آن ناشناخته یا غیرقابل مشاهده می‌ماند.

سناریو ۲: اختلال در سیستم موقعیت‌یاب جهانی یا نقشه دیجیتال. فرض کنید خودروی خودرانی به دلیل نقص در نرم‌افزار نقشه دیجیتال یا سیستم موقعیت‌یاب، به مسیر ممنوعه‌ای وارد شده، در آنجا دچار تصادف می‌شود. این مشکل ناشی از خطا یا نقص در داده‌های نقشه دیجیتال است که بخشی از عملکرد حیاتی خودروهای خودران محسوب می‌شود. در این حالت، تعیین مسئولیت میان تولیدکننده خودرو و ارائه‌دهنده سرویس نقشه دیجیتال محل اختلاف است؛ زیرا هر دو در هدایت اشتباه خودرو و در نتیجه بروز حادثه نقش داشته‌اند. بررسی رابطه قراردادی، میزان مراقبت و نقش طرفین در ایجاد نقص اهمیت فراوان دارد. این سناریو اهمیت تدوین قواعد دقیق و شفاف درباره مسئولیت مرتبط با داده‌ها و نرم‌افزارهای وابسته به خودروهای خودران را برجسته می‌سازد تا از تضییع حقوق کاربران و زیان دیدگان جلوگیری شود.

سناریو ۳: نشت اطلاعات کاربر از حافظه خودرو در سناریویی دیگر. داده‌های مربوط به مقصد سفرها و موقعیت مکانی لحظه‌ای کاربر خودرو خودران به دلیل نقص در حفاظت اطلاعات، به صورت ناخواسته به اشخاص ثالث غیرمجاز منتقل شده، در فضای عمومی منتشر می‌شود. این نشت اطلاعات حریم خصوصی فرد را به شدت نقض می‌کند و می‌تواند موجب ورود خسارات مادی و معنوی شود. شرکت‌های تولیدکننده یا توسعه‌دهنده نرم‌افزار خودروهای خودران مسئولیت دارند تا با اتخاذ تدابیر امنیتی مناسب، حفاظت از داده‌های کاربران را تضمین کنند و در صورت قصور، در معرض دعاوی حقوقی و جبران خسارت قرار گیرند. این مسئله بر ضرورت تقویت چارچوب‌های قانونی و استانداردهای امنیتی حفاظت داده‌ها در فناوری‌های نوین تأکید می‌کند و نقش کلیدی آن‌ها در حفظ اعتماد عمومی و امنیت حقوقی کاربران را نمایان می‌سازد.

سناریو ۴: حذف خودکار داده‌ها پس از وقوع خطا. در این سناریو، نرم‌افزار خودروهای خودران به گونه‌ای طراحی شده است که در صورت بروز خطا، داده‌های مربوط به حادثه به‌طور خودکار پاک می‌شوند؛ اقدامی که می‌تواند برای حفظ حریم خصوصی یا به‌منظور کاهش مسئولیت تولیدکننده صورت گیرد. چنین طراحی‌ای از منظر حقوقی بسیار بحث‌برانگیز است، زیرا می‌تواند به‌منزله سوءنیت و تلاش عمدی برای فرار از مسئولیت مدنی تلقی شود. حذف داده‌های مربوط به خطا روند اثبات وقوع خطا و مسئولیت تولیدکننده را مختل می‌سازد و اعتماد عمومی به شفافیت و ایمنی فناوری‌های خودران را خدشه‌دار می‌کند. در نتیجه، این موضوع ضرورت وضع

مقررات سخت‌گیرانه‌تر و الزام تولیدکنندگان به ثبت و حفظ داده‌های مرتبط با حوادث برای دوره‌های مشخص را به‌وضوح مطرح می‌کند تا حقوق زیان‌دیدگان حفظ و عدالت اجرا شود. همچنین، احتمال افزایش مسئولیت مدنی مضاعف برای تولیدکنندگان در چنین شرایطی وجود دارد.

با وجود سناریوهای مطرح‌شده، شناسایی «ازدست رفتن داده‌ها» به‌عنوان خسارت نوین، موجب می‌شود قوانین و مقررات به‌طور صریح به حفظ، مدیریت و جبران این نوع خسارت بپردازند و مسئولیت تولیدکنندگان و توسعه‌دهندگان فناوری را در قبال حفاظت داده‌ها مشخص نمایند. این رویکرد به ایجاد اعتماد عمومی نسبت به فناوری‌های نوین کمک کرده، امکان پیشگیری از سوءاستفاده و نقض حقوق را فراهم می‌آورد و زمینه اجرای عدالت و جبران خسارت‌های نوین را تقویت می‌کند.

۳. تحلیل تطبیقی با اتحادیه اروپا

۱.۳. توسعه مفهوم مسئولیت در چارچوب دستورالعمل مسئولیت محصول

خودروهای خودران به‌عنوان مصداق بارز سیستم‌های داده‌محور، وابسته به گردآوری، پردازش و ذخیره‌سازی لحظه‌ای داده‌ها هستند. در این بستر، ازدست رفتن داده‌ها می‌تواند نه‌تنها به بروز حادثه منجر شود، بلکه فرایند احراز تقصیر و ارزیابی مسئولیت را با دشواری مواجه سازد. حقوق اتحادیه اروپا در پاسخ به این چالش، اقدام به بازنگری ساختارهای سنتی مسئولیت مدنی کرده‌اند. دستورالعمل مسئولیت محصول اتحادیه اروپا در خصوص مسئولیت بدون تقصیر تولیدکنندگان نسبت به محصولات معیوب، از مهم‌ترین اسناد حقوقی در حوزه مسئولیت مدنی در سطح اتحادیه اروپا به‌شمار می‌رود. بر اساس این دستورالعمل، مسئولیت تولیدکننده ماهیت مبتنی بر تقصیر ندارد. مطابق مواد ۱ و ۴، برای تحقق مسئولیت، اثبات نقص محصول، ورود خسارت و رابطه سببیت کافی است.^{۵۱}

با پیشرفت فناوری و ظهور سامانه‌های هوشمند، کمیسیون اروپا در سال ۲۰۲۴ اصلاحیه‌ای بنیادین بر این دستورالعمل تصویب کرد. مطابق مواد ۲، ۶ و ۷ این اصلاحیه، داده‌ها، نرم‌افزار و

51. Product Liability Directive, Articles 1, 4.



به‌روزرسانی‌های الگوریتمی را رسماً بخشی از ماهیت محصول دانسته و مسئولیت تولیدکننده را در قبال نقص عملکرد این اجزا به رسمیت شناخته است. از این رو، اگر فقدان یا حذف داده به رفتار معیوب سیستم منجر شود یا مانع تحلیل حادثه گردد، محصول «معیوب» تلقی می‌شود.^{۵۲}

در همین راستا، در مطالعات جدید آمده است که اگر داده‌های عملکردی در سیستم‌های خودران به صورت ایمن، قابل ثبت و قابل تحلیل طراحی نشده باشند، این موضوع نه تنها موجب ضعف فنی، بلکه نقض صریح استانداردهای ایمنی و طراحی ایمن خواهد شد؛ زیرا تصمیم‌گیری‌های خودرو در شرایط بحرانی مبتنی بر این داده‌ها صورت می‌گیرد و حذف یا دست‌کاری آنها می‌تواند ایمنی سیستم را مختل کند.^{۵۳}

۲.۳. جایگاه فقدان داده در چارچوب مقررات عمومی حفاظت داده‌ها

مقررات عمومی حفاظت از داده‌ها، مهم‌ترین سند حقوقی در حوزه حفاظت از داده‌های شخصی در سطح اتحادیه اروپاست. به موجب ماده ۸۲، هرگونه نقض مقرر که به خسارت مادی یا غیرمادی بینجامد، مسئولیت جبران را برای مسئول یا کنترل‌کننده داده ایجاد می‌کند. بنابراین، از بین رفتن یا عدم دسترسی به داده‌های شخصی نیز می‌تواند مبنای مسئولیت باشد؛ حتی اگر خسارت مالی مستقیمی اثبات نشود. در بستر خودروهای خودران که داده‌هایی نظیر موقعیت مکانی، وضعیت فنی خودرو، مسیر حرکت، ترجیحات راننده و تعامل با زیرساخت‌ها جمع‌آوری می‌شود، از بین رفتن این داده‌ها ممکن است نقض این قانون تلقی شده، موجب مسئولیت گردد.

در پژوهشی مربوط به امنیت سایبری در سامانه‌های هوشمند آمده است که از بین رفتن داده‌های مربوط به عملکرد خودرو، به‌ویژه در شرایط بحرانی، موجب نابرابری اطلاعاتی میان زیان‌دیده و شرکت‌های تولیدکننده می‌شود و عملاً مانع از بازسازی دقیق حادثه خواهد شد.^{۵۴}

رای تاریخی دیوان دادگستری اتحادیه اروپا در پرونده گوگل علیه کوستخا گونزالس^{۵۵} نقطه عطفی در تحول مفهوم «کنترل داده‌ها» در حقوق اتحادیه اروپا به‌شمار می‌رود. موضوع پرونده از

52. New Product Liability Directive, Articles 2, 6, & 7.

53. Yao Xu, et al., "Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics", *World Electric Vehicle Journal*, Vol. 16, (2024), p. 8.

54. "What is Data Loss?", *op. cit.*

55. Google Spain SL, Google Inc. v. AEPD and Mario Costeja González (C-131/12)

آنجا آغاز شد که ماریو کوستخا گونزالس، شهروند اسپانیایی، علیه گوگل طرح دعوا کرد؛ زیرا هنگام جست‌وجوی نام وی، نتایجی شامل اخباری قدیمی درباره مشکلات مالی و حراج خانه‌اش ظاهر می‌شد. اگرچه این اطلاعات به‌صورت قانونی در روزنامه رسمی منتشر شده بود، اما وی استدلال کرد که استمرار نمایش آنها به حیثیت و زندگی خصوصی او لطمه می‌زند.

این رأی برای نخستین بار جایگاه موتورهای جست‌وجو را به‌عنوان «کنترل‌کننده داده‌ها» به‌رسمیت شناخت. دیوان دادگستری اتحادیه اروپا اعلام کرد که گوگل، صرف‌نظر از آنکه تولیدکننده محتوای اصلی نیست، به‌عنوان کنترل‌کننده داده‌ها شناخته می‌شود و مسئولیت فعالیت آنها را در قبال پردازش و حفظ داده‌های شخصی افراد مورد تأکید قرار داد.^{۵۶}

رأی یادشده^{۵۷}، گرچه ناظر به داده‌های شخصی بود، اما دارای بنیان مهم‌تری در حوزه فناوری است: مسئولیت کنترل و مدیریت داده‌ها نه‌تنها جنبه منفعل ندارد، بلکه فقدان، حذف یا مدیریت نادرست آنها می‌تواند مسئولیت‌آور تلقی شود.

در زمینه خودروهای خودران، داده‌ها جزئی از ساختار عملکردی محصول محسوب می‌شوند. اصلاحیه ۲۰۲۴ دستورالعمل مسئولیت محصول، معیار «عیب» را این چنین مشخص می‌کند: محصول باید ایمنی موجه موردانتظار مصرف‌کننده را فراهم کند و این ارزیابی شامل عملکرد، دستورالعمل‌ها، نگهداری و به‌روزرسانی‌های نرم‌افزاری است.^{۵۸} از این منظر، اگر خودرو به دلیل حذف یا عدم ثبت صحیح داده‌ها نتواند عملکرد ایمن خود را ارائه دهد، تولیدکننده مسئول محسوب می‌شود؛ ولو آنکه خودرو از نظر سخت‌افزاری سالم باشد.

به این ترتیب، این رأی مبنای حقوقی مهمی برای توسعه مسئولیت داده‌محور در فناوری‌های نوین، به‌ویژه در حوزه هوش مصنوعی و خودروهای خودران فراهم می‌سازد. با استناد به این

56. Court of Justice of the European Union (CJEU), Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>, paras. 34.

۵۷. دیوان در این رأی تصریح کرد که حتی اگر اطلاعات موردنظر در صفحات اینترنتی قانونی و منتشرشده باقی بماند، چنانچه بازایی و عرضه مجدد آنها از سوی موتور جست‌وجو به حریم خصوصی فرد لطمه وارد سازد، شخص می‌تواند خواهان حذف آن از نتایج جست‌وجو شود؛ حتی اگر آن اطلاعات زمانی مشروع بوده‌اند. این مبنا، تحت عنوان «حق فراموش‌شدن» وارد نظام حقوقی اتحادیه اروپا شد و متعاقباً در ماده ۱۷ مقررات عمومی حفاظت از داده‌ها نیز تثبیت گردید.

58. New Product Liability Directive, Article 6.



رأی، می‌توان استدلال کرد که شرکت‌های فناورانه، حتی در صورت عدم تقصیر در طراحی یا تولید، در برابر نحوه گردآوری، ذخیره‌سازی و ارائه داده‌های موردنیاز برای عملکرد ایمن سیستم مسئول هستند. بنابراین، مسئولیت مدنی در قبال داده‌ها نه تنها در حوزه افشای نادرست یا پردازش بیش از حد، بلکه در صورت فقدان یا حذف آنها نیز قابل استناد است. در حوادث ناشی از نقص در داده‌ها (اعم از حذف، خطا یا عدم ثبت مناسب)، مسئولیت مدنی تولیدکنندگان نه تنها قابل تصور، بلکه بر پایه اصول پذیرفته شده حقوق اتحادیه اروپا قابل اثبات است.

لیکن در حقوق اتحادیه اروپا، از دست رفتن داده‌ها فی‌نفسه به عنوان «خسارت مستقل» تلقی نمی‌شود، بلکه در چارچوب‌های مختلف حقوقی تحلیل متفاوتی می‌یابد. در نظام مسئولیت ناشی از محصول، فقدان داده‌های حیاتی ممکن است به عنوان یکی از مصادیق «نقص محصول» ارزیابی گردد، مشروط بر آنکه این نقص به ورود زیان جانی یا مالی منجر شود. در چارچوب مقررات حفاظت از داده‌ها نیز، تنها در صورتی که حذف یا تخریب داده‌ها موجب ورود خسارت مادی یا غیرمادی قابل اثبات گردد، حق مطالبه جبران ایجاد می‌شود. بنابراین، حقوق اتحادیه اروپا بیش از آنکه «فقدان داده» را به عنوان خسارت مستقل به معنای کلاسیک بشناسد، آن را به عنوان مبنای ایجاد مسئولیت یا عنصر تشکیل دهنده نقص تحلیل می‌کند.

۳.۳. الزامات طراحی ایمن و ثبت داده‌ها در قانون هوش مصنوعی

قانون هوش مصنوعی اتحادیه اروپا مصوب ۲۰۲۴^{۵۹}، خودروهای خودران را به عنوان سامانه‌های «پرریسک» تعریف کرده^{۶۰} و طراحی و بهره‌برداری از این فناوری‌ها را مشمول

59. Artificial Intelligence Act

۶۰. در مقررۀ هوش مصنوعی، سامانه‌های هوش مصنوعی بر اساس میزان ریسک، به چهار دسته تقسیم شده‌اند: ریسک غیرقابل قبول، ریسک بالا، ریسک محدود و ریسک حداقل. سامانه‌های دارای ریسک غیرقابل قبول به دلیل تهدید جدی برای حقوق بنیادین افراد (مانند امتیازدهی اجتماعی از سوی دولت‌ها یا شناسایی زیستی در زمان واقعی در اماکن عمومی) به طور کامل ممنوع شده‌اند. سامانه‌های ریسک بالا شامل کاربردهایی هستند که با ایمنی، سلامت یا حقوق اساسی افراد مرتبط‌اند (مانند استفاده در خودروهای خودران، زیرساخت‌های حیاتی، آموزش، استخدام، خدمات بانکی و قضایی) و مشمول الزامات سخت‌گیرانه‌ای مانند ثبت داده‌ها، شفافیت، مدیریت ریسک و نظارت انسانی هستند. سامانه‌های با ریسک محدود، مانند چت‌بات‌ها، باید الزامات شفافیت مانند اطلاع‌رسانی به کاربر درباره تعامل با یک سامانه هوش مصنوعی را رعایت کنند. در نهایت، سامانه‌های با ریسک حداقل که کمترین خطر را دارند (مانند فیلترهای اسپم یا توصیه‌گرهای کالا)، مشمول الزامات خاصی نیستند و استفاده از آنها آزاد است. این رویکرد مبتنی بر ریسک، هدفش توازن میان نوآوری و حفاظت از حقوق اساسی شهروندان اتحادیه اروپا است.

الزامات ایمنی و ثبت داده‌های دقیق دانسته است. بر اساس مواد ۱۶ و ۱۷ این قانون، توسعه‌دهندگان و تولیدکنندگان این سامانه‌ها موظف‌اند داده‌های مربوط به تصمیم‌گیری‌های الگوریتمی، خطاها، رخدادهای بحرانی و هرگونه اطلاعات مرتبط با عملکرد سامانه را به‌گونه‌ای ثبت و ذخیره کنند که در مواقع نیاز، امکان ارزیابی فنی و حقوقی دقیق فراهم شود. این الزام، تضمینی است برای شفافیت، قابل ردگیری بودن و امکان بررسی علل حادثه در فناوری‌های پیچیده مبتنی بر هوش مصنوعی.

برای نمونه، ماده ۱۶ این قانون تصریح می‌کند که سامانه‌های پریسک باید «قابلیت مستندسازی کامل و مداوم داده‌ها» را داشته باشند تا مسئولیت‌ها و تعهدات حقوقی مرتبط به‌درستی تعیین گردد. ماده ۱۷ نیز بر «الزام ثبت وقایع بحرانی و تصمیمات مهم» تأکید دارد و این داده‌ها را به‌عنوان بخش جدایی‌ناپذیر از مدیریت ریسک سامانه تلقی می‌کند.

با این حال، در بررسی‌های مفهومی و تحلیلی مقررات مربوط به خودروهای خودران در اروپا، نقایصی در تعاریف و چارچوب‌های قانونی مشاهده می‌شود. یکی از مهم‌ترین چالش‌ها، فقدان تعاریف واضح و یکپارچه از مفهوم «ریسک داده‌ای»^{۶۱} است. این خلأ موجب می‌شود که تنظیم‌گران، تولیدکنندگان و حتی مراجع قضایی در تفسیر و اجرای الزامات ایمنی دچار ناسازگاری و سردرگمی شوند. در چنین شرایطی، نبود زیرساخت‌های فنی و قانونی لازم برای ثبت، ذخیره و بازیابی داده‌ها عملاً به تضعیف ایمنی خودروهای خودران منجر می‌شود و از نظر حقوقی می‌تواند مصداق نقض تکالیف طراحی ایمن و مسئولیت مدنی تولیدکنندگان تلقی گردد.^{۶۲}

برای مثال، در صورت بروز تصادف ناشی از خودروی خودران، اگر داده‌های مربوط به تصمیمات لحظه‌ای الگوریتم‌ها، شرایط محیطی، و واکنش‌های سیستم به‌درستی ثبت نشده باشند، شاکی یا مقام قضایی ممکن است نتواند علت دقیق حادثه را مشخص کنند. در نتیجه، نبود این داده‌ها نه تنها مانع اثبات بی‌گناهی تولیدکننده می‌شود، بلکه می‌تواند دلیل فرضی برای قصور در طراحی ایمن تلقی گردد که با اصول کلی مسئولیت مدنی در مقررات اروپایی مطابقت دارد. به همین دلیل، مقررات ایمنی خودروهای خودران در اتحادیه اروپا بر ضرورت تدوین

61. Data Risk

62. Marcus Nolte et al, "A Review of Conceptualizations of Safety and Risk in Current Automated Driving Regulation", p. 4.

استانداردهای فنی مشخص برای «ثبت داده‌های ایمنی» و ایجاد سامانه‌های قابل اعتماد برای مستندسازی تأکید دارند تا خلأهای قانونی و فنی برطرف و از حقوق مصرف‌کنندگان و امنیت عمومی حفاظت شود.

۴.۳. فرض رابطه علیت در دستورالعمل مسئولیت هوش مصنوعی و نقش فقدان داده

در دستورالعمل مسئولیت مدنی هوش مصنوعی مصوب^{۶۳} ۲۰۲۴، ویژگی‌هایی مانند «مداخله در رابطه علت و معلولی» پیش‌بینی شده است تا چالش اثبات تقصیر در سامانه‌های خودران کاهش یابد. به‌ویژه در ماده ۴ این دستورالعمل، در صورت نقض وظیفه مراقبت مرتبط با کیفیت داده، شفافیت یا نظارت انسانی، و شرایطی که چنین تقصیری به‌طور معقولی خروجی یا عدم خروجی سامانه را تحت تأثیر قرار داده، منجر به زیان شده باشد، رابطه سببیت فرض می‌گردد؛ مگر خلاف آن ثابت شود. همچنین، ماده ۳ دادگاه را قادر می‌سازد در خصوص سامانه‌های با ریسک بالا، به درخواست شاکی، دستور افشای داده‌ها، مستندات فنی و لاگ‌ها را صادر نماید و در صورت امتناع، نبود یا حذف داده را نشانه‌ای از عیب سیستم تلقی کند^{۶۴}.

این مقررات در حوزه خودروهای خودران اهمیت مضاعف می‌یابند؛ چراکه شواهد و داده‌های ثبت‌شده مانند گزارش‌های حسگرها^{۶۵}، تصمیمات الگوریتمی، تاریخچه تعامل با محیط، و مستندات فنی هوش مصنوعی برای تحلیل عملکرد سامانه و تعیین علت حادثه، اساسی‌اند. اگر سامانه به هر دلیل فاقد قابلیت مستندسازی یا ثبت داده‌های محیطی و تصمیمی مرتبط با وقوع حادثه باشد، شاکی می‌تواند با استناد به نقض الزامات قانونی (نظیر شفافیت، ثبت تصمیم، یا ذخیره تاریخچه عملکرد) از سوی تولیدکننده یا بهره‌بردار، به استناد ماده ۴، رابطه سببیت میان این قصور و خسارت وارده را مفروض بگیرد. همچنین، دادگاه می‌تواند بر مبنای ماده ۳، دستور افشای داده‌های حذف‌شده یا ناقص را صادر کند. در صورت نبود داده، فرض بر آن خواهد بود که سیستم معیوب بوده است و این امر بار اثبات را به نفع زیان‌دیده کاهش می‌دهد.

63. Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), 2024.

64. Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), Articles 3 & 4.

65. Sensor Logs

در نتیجه، حتی در غیاب داده یا مستندات عملکرد سیستم خودران، بر اساس این دستورالعمل، فرض مسئولیت تولیدکننده یا توسعه‌دهنده قابل طرح است، مگر اینکه خلاف آن اثبات شود. این نوآوری حقوقی نقش کلیدی در حمایت از زیان‌دیدگان در بستر فناوری‌های پیچیده و مبتنی بر هوش مصنوعی ایفا می‌کند.

در چارچوب حقوق اتحادیه اروپا، تمایز میان داده خام و اطلاعات پردازش‌شده در ارزیابی نقص و خسارت اهمیت دارد. برای مثال، حذف داده‌های ثبت‌شده در خودرو ممکن است صرفاً نقص عملکرد فنی تلقی شود؛ اما اگر این داده‌ها پس از پردازش به اطلاعات ایمنی یا تصمیم‌گیری تبدیل شده باشند، از بین رفتن آنها می‌تواند به ورود خسارت جانی یا مالی منجر شود.

در تحلیلی از قابلیت‌های آزمون‌پذیری سیستم‌های هوش مصنوعی در خودروهای خودران آمده است که بدون ثبت تصمیمات الگوریتمی، امکان بازسازی دقیق فرایند تصمیم‌گیری خودرو وجود ندارد و در نتیجه اثبات بی‌تقصیری برای تولیدکننده دشوار خواهد بود. بنابراین، مستندسازی و ذخیره‌سازی داده‌ها نه تنها از منظر فنی، بلکه از نظر اخلاقی و حقوقی نیز یک ضرورت است.^{۶۶}

۴. تحلیل حقوقی خسارت به سبب ازدست رفتن داده در نظام حقوقی ایران

۴.۱. شناسایی ازدست رفتن داده به عنوان خسارت نوین

در نظام حقوقی ایران، مفهوم «ازدست رفتن داده‌ها» به طور مستقیم در قوانین سنتی پیش‌بینی نشده است، زیرا این نظام عمدتاً بر خسارات مادی و ملموس متمرکز بوده است. با این حال، توسعه فناوری‌های داده‌محور، به‌ویژه در خودروهای خودران، ضرورت شناسایی داده به عنوان دارایی مستقل و فقدان آن به عنوان خسارت را برجسته ساخته است. پرسش اصلی این است که آیا با تفسیر موسع از قوانین موجود، فقدان داده‌های حیاتی خودرو را ذیل مسئولیت مدنی می‌توان قابل جبران دانست؟

در نظام حقوقی ایران، «خسارت» به طور کلی به زیان‌هایی اطلاق می‌شود که در نتیجه فعل

66. David Fernandez Llorca, et al., "Testing autonomous Vehicles and AI: Perspectives and Challenges from Cybersecurity, Transparency, Robustness and Fairness", arXiv Preprint, (2024), p. 12.

یا ترک فعل زیان‌بار ایجادشده، باید جبران گردد. بر اساس ماده ۳۲۸ قانون مدنی، «هر کس مال غیر را تلف کند ضامن آن است». این تعریف سنتی، ناظر بر اتلاف مال مادی یا تسبیب در تلف آن است. ماده ۹ قانون مسئولیت مدنی نیز دامنه خسارت را به زیان‌های مادی و معنوی گسترش می‌دهد. با وجود این، در این چارچوب سنتی، داده به عنوان یک مصداق مستقل شناسایی نشده، زیرا در زمان تصویب این قوانین، داده به شکل امروزی آن مطرح نبوده است.

با آنکه داده‌های دیجیتال در زمره اموال مادی مشهود قرار نمی‌گیرند، برخی تحولات تقنینی جدید، ازجمله قانون مدیریت داده و اطلاعات ملی، اهمیت و ارزش راهبردی داده را در نظام حکمرانی به رسمیت شناخته‌اند، اما این قانون عمدتاً ناظر بر تنظیم، یکپارچه‌سازی و مدیریت داده در دستگاه‌های اجرایی و نهادهای عمومی است و متضمن شناسایی صریح «داده» به عنوان مال خصوصی یا دارایی مستقل در معنای مدنی نیست.

قوانین دیگری نیز به‌طور غیرمستقیم از داده‌ها حمایت می‌کنند. قانون تجارت الکترونیکی (۱۳۸۲) در ماده ۶۵ داده‌های دارای ارزش اقتصادی را در زمره «اسرار تجاری» قرار داده و در ماده ۶۷، محو یا توقف داده‌پیام را جرم‌انگاری کرده است. قانون جرایم رایانه‌ای (۱۳۸۸) در مواد ۳۲ و ۳۶ تا ۴۶، نگهداری داده‌ها و جلوگیری از تخریب آنها را الزام‌آور دانسته است. همچنین قانون انتشار و دسترسی آزاد به اطلاعات (۱۳۸۸) در مواد ۱ و ۵، حق دسترسی شهروندان به اطلاعات را تضمین و نهادها را مکلف به حفظ آنها کرده است. این مقررات، هرچند به حوزه خودروهای خودران تصریحی نداشته‌اند، اما مبنای حقوقی برای شناسایی و جبران خسارت ناشی از فقدان داده را فراهم می‌سازند.

با جمع‌بندی این مقررات، داده‌ها در حقوق ایران به عنوان دارایی اقتصادی، حق عمومی و منبع ملی با ارزش استراتژیک به رسمیت شناخته شده‌اند. این شناسایی، امکان بازتعریف «ازدست رفتن داده» را به عنوان یک نوع خسارت نوین فراهم می‌کند که گرچه در قالب سنتی خسارت‌های مادی و معنوی به صراحت نیامده است، اما با تفسیر موسع از مواد ۱ و ۳۲ قانون مسئولیت مدنی می‌توان آن را ذیل مسئولیت مدنی ناشی از تلف مال یا ورود ضرر به منفعت مشروع قرار داد و از بین رفتن آن را، نوعی «اتلاف مال غیرملموس» محسوب کرد. و آن را از محدوده اموال مادی به اموال و دارایی‌های غیرملموس مبتنی بر داده گسترش داد.

از این رو، برای تحلیل مسئولیت ناشی از اتلاف یا حذف داده در حقوق ایران، باید همچنان به قواعد عام مسئولیت مدنی، از جمله مواد ۱ و ۲ قانون پیش‌گفته و نیز مبانی فقهی همچون اتلاف و تسبیب رجوع کرد. به این ترتیب، خلأ تقنینی در خصوص تعریف صریح داده به‌عنوان مال مدنی همچنان وجود دارد و استناد به قانون مدیریت داده و اطلاعات ملی صرفاً می‌تواند مؤید اهمیت و ارزش اقتصادی و حاکمیتی داده باشد، نه دلیل قطعی بر شناسایی آن به‌عنوان دارایی خصوصی مستقل.

چنانچه داده را دارای ارزش اقتصادی و منفعت عقلایی بدانیم، حذف یا نابودی آن می‌تواند در حکم اتلاف مال غیر تلقی شود؛ حتی اگر مالیت آن غیرمادی باشد. در این تحلیل، تمرکز بر «نابودی منفعت قابل تقویم» است، نه لزوماً ماهیت مادی شیء.

قاعده لا ضرر نیز با نفی هرگونه حکم یا وضعیتی که مستلزم ورود ضرر به اشخاص باشد، می‌تواند مبنایی برای جبران زیان‌های ناشی از فقدان داده فراهم کند^{۶۷}؛ به‌ویژه در مواردی که از بین رفتن داده موجب تضییع فرصت‌های اقتصادی، محرومیت از اثبات حق یا تحمیل هزینه‌های بازیابی شود. در این چارچوب، حتی اگر داده به‌عنوان مال مستقل شناسایی نشده باشد، ورود ضرر عرفی و قابل احراز می‌تواند مبنای مسئولیت قرار گیرد.

به این ترتیب، ترکیب قواعد اتلاف، تسبیب و لا ضرر، امکان توسعه تفسیری نظام مسئولیت مدنی ایران را برای پوشش خسارات ناشی از نابودی داده‌های دیجیتال فراهم ساخت؛ هرچند خلأ تصریح تقنینی همچنان مشهود است.

در حقوق ایران نیز تمایز میان داده و اطلاعات در تحلیل قواعد اتلاف و لا ضرر مؤثر است. اتلاف داده خام ممکن است صرفاً موجب تحمیل هزینه فنی بازیابی شود، اما نابودی اطلاعاتی که دارای منفعت عقلایی، ارزش اقتصادی یا نقش اثباتی در دعاوی است، می‌تواند مصداق اتلاف مال یا ورود ضرر قابل مطالبه تلقی گردد. از این رو، تقویم خسارت ناشی از فقدان داده باید با توجه به ماهیت آن (خام یا پردازش‌شده) و میزان ارزش اقتصادی یا اثباتی آن صورت گیرد.

کاربرد این تحلیل در حوزه خودروهای خودران، اهمیت ویژه‌ای دارد. داده‌های تولیدشده از

۶۷. حسین، ولی‌زاده، «اثر قاعده لا ضرر در مسوولیت مدنی و نقش قاعده اقدام در اثر رافعیات آن»، *قانون‌یار*، ش ۱۰ (۱۳۹۸)، ص ۳۳۳.

سوی حسگرها، سیستم‌های ناوبری، و مازول‌های ثبت وقایع این خودروها، نه تنها ارزش عملیاتی و اقتصادی دارند، بلکه در فرایند اثبات علل حادثه، رسیدگی قضایی و حتی توسعه فناوری، نقش حیاتی ایفا می‌کنند. ازدست رفتن این داده‌ها می‌تواند مانع شناسایی علت دقیق حادثه و احقاق حق طرفین شده، موجب ازبین رفتن فرصت‌های تحقیق و توسعه یا تحلیل عملکرد شود، و به اختلال در ارائه خدمات پس از فروش یا تعمیر منجر گردد.

۲.۴. جایگاه ازدست رفتن داده در چارچوب مبنای مسئولیت مدنی

شناسایی ازدست رفتن داده‌ها در خودروهای خودران به عنوان خسارت نوین، مستلزم بررسی مبنای مسئولیت مدنی در حقوق ایران است. پرسش اساسی آن است که در فقدان داده‌های حیاتی خودرو بر چه مبنایی می‌توان تولیدکننده یا سایر بازیگران را مسئول شناخت. در این زمینه، چهار مبنای اصلی قابل طرح است:

الف) نظریه تقصیر: بر اساس ماده ۲ قانون مسئولیت مدنی: «هر کس عملی کند که موجب ورود ضرر به دیگری شود و آن عمل ناشی از تقصیر یا عمد باشد، مسئول جبران زیان است». همچنین ماده ۳ قانون مسئولیت مدنی بر مسئولیت ناشی از بی‌احتیاطی و اهمال تأکید دارد. در زمینه خودروهای خودران، اگر تولیدکننده یا ارائه‌دهنده خدمات نرم‌افزاری در طراحی سامانه ذخیره‌سازی داده بی‌مبالاتی کند یا در نگهداری داده‌های حیاتی کوتاهی نماید، می‌توان تقصیر او را مبنای مسئولیت دانست.^{۶۸} با این حال، در عمل اثبات تقصیر با دشواری‌های جدی مواجه خواهد بود؛ زیرا زیان دیده معمولاً به مستندات فنی دسترسی ندارد و نمی‌تواند بی‌احتیاطی تولیدکننده را به‌طور دقیق نشان دهد.

ب) مسئولیت ناشی از نقص محصول: تحولات اخیر حقوق تطبیقی، به‌ویژه در اتحادیه اروپا، نشان می‌دهد که نظریه خطر جای خود را به مسئولیت بدون تقصیر داده است. مطابق اصلحیه ۲۰۲۴ دستورالعمل مسئولیت محصول و دستورالعمل مسئولیت هوش مصنوعی، مسئولیت تولیدکننده بر مبنای مسئولیت بدون تقصیر است و زیان‌دیده نیازی به اثبات تقصیر ندارد، بلکه باید نقص، ورود خسارت و رابطه سببیت را اثبات کند. این نظام را نباید با «مسئولیت محض» به

۶۸. محمود حکمت‌نیا، مسئولیت مدنی در فقه امامیه: مبانی و ساختار، (تهران: پژوهشگاه علوم و فرهنگ اسلامی، ۱۳۸۶)، ص ۵۵.

معنای خاص آن در برخی نظام‌های ملی، مانند مسئولیت ویژه در حوزه دارویی در حقوق آلمان، یکسان دانست.

بر این اساس، فقدان داده‌های ایمنی یا ثبت ناقص اطلاعات می‌تواند در صورت کاهش سطح ایمنی موردانتظار، مصداق نقص محصول تلقی شود؛ با این حال، اثبات رابطه سببیت همچنان برعهده زیان‌دیده است.

تنها در چارچوب خاص قانون هوش مصنوعی، به‌ویژه ماده ۴، در شرایط معین و در صورت نقض تعهدات مرتبط با سامانه‌های هوش مصنوعی، دادگاه می‌تواند فرض قابل رد رابطه سببیت را بپذیرد. بنابراین، فرض سببیت در حقوق اتحادیه اروپا مطلق نبوده، به موارد تصریح‌شده تقنینی محدود است.

در حقوق ایران با تفسیر موسع از ماده ۱ قانون مسئولیت مدنی در حوزه خودروهای خودران، فقدان داده‌های حیاتی می‌تواند خود به‌عنوان یک عیب مستقل مطرح شود و مسئولیت بدون تقصیر تولیدکننده را فعال سازد؛ برای مثال، اگر جعبه سیاه خودرو به دلیل طراحی معیوب داده‌ها را ثبت نکند، همین نقص به‌تنهایی می‌تواند موجب مسئولیت شود؛ حتی اگر تقصیر مستقیم تولیدکننده اثبات نشود. فقدان داده پیامدهای حقوقی و عملی مهمی دارد: از یک سو، نبود داده‌های محیطی، حسگرها یا تصمیم‌های الگوریتمی، امکان اثبات علت حادثه و تعیین مسئولیت را برای زیان‌دیده محدود کرده، نابرابری اطلاعاتی میان او و تولیدکننده ایجاد می‌کند. از سوی دیگر، فقدان داده می‌تواند خود نوعی نقص محصول تلقی شود، به‌ویژه اگر داده‌ها برای عملکرد ایمن خودرو و بازسازی حوادث حیاتی باشند. بر این اساس، می‌توان با الهام از رویه‌ها و مقررات اتحادیه اروپا، مفهومی تحت عنوان فرض قانونی مسئولیت برای فقدان داده‌ها مطرح کرد؛ به‌گونه‌ای که تولیدکننده حتی در صورت عدم تقصیر مستقیم، نسبت به ثبت، نگهداری و ارائه داده‌های لازم پاسخگو باشد. این رویکرد توازن قدرت اطلاعاتی میان زیان‌دیده و تولیدکننده را بهبود می‌بخشد.

ج) مسئولیت ناشی از فعل غیر: بر اساس ماده ۳۳۲ قانون مدنی و قاعده فقهی تسبیب، اگر سامانه خودکار یا نرم‌افزار موجب ازبین رفتن داده‌ها شود، مسئولیت آن متوجه شخص حقیقی یا حقوقی طراح و ناظر خواهد بود. این تحلیل مشابه مسئولیت کارفرما نسبت به فعل کارگر است و

در فناوری‌های هوشمند می‌تواند در قالب «مسئولیت ناظر بر سامانه‌های خودکار» بازتعریف شود. علاوه بر آن، ماده ۱۲ قانون حمایت از مصرف‌کننده بر مسئولیت تولیدکننده در برابر هرگونه نقص محصول و ایجاد خسارت تأکید دارد که می‌تواند شامل داده‌های حیاتی خودرو باشد.

د) مسئولیت تضامنی در زنجیره فناوری: در خودروهای خودران، مجموعه‌ای از بازیگران در تولید، طراحی، توسعه نرم‌افزار و ارائه خدمات داده‌ای دخیل‌اند. در صورت ازدست‌رفتن داده‌های حیاتی، مسئولیت هریک از این افراد یا شرکت‌ها قابل تصور است و در برخی موارد می‌تواند به صورت تضامنی اعمال شود.^{۶۹} هرچند در قوانین ایران اصطلاح «زنجیره فناوری» وجود ندارد، اما می‌توان با استناد به مواد قانونی موجود، چنین مسئولیتی را تبیین کرد.

بر اساس ماده ۲۹۴ قانون مدنی، اگر چند نفر در ایجاد زیان نقش داشته باشند، هریک به نسبت دخالت خود مسئول است؛ مگر اینکه قانون مسئولیت تضامنی را مقرر کرده باشد. بنابراین، تولیدکننده سخت‌افزار و توسعه‌دهنده نرم‌افزار که هر دو در ایجاد نقص داده مؤثر بوده‌اند، می‌توانند به صورت تضامنی مسئول شناخته شوند. همچنین، ماده ۳۳۲ قانون مدنی تأکید می‌کند که اگر فعل یا ترک فعلی از سوی شخص حقیقی یا حقوقی موجب ورود ضرر به دیگری شود، مسئولیت متوجه وی خواهد بود؛ این قاعده می‌تواند در قالب «مسئولیت ناظر بر سامانه‌های خودکار» در خودروهای خودران بازتعریف شود. علاوه بر این، در چارچوب قراردادهای تجاری میان تولیدکنندگان، توسعه‌دهندگان نرم‌افزار و ارائه‌دهندگان خدمات ابری، ماده ۲۳۰ و ۲۳۱ قانون مدنی امکان اعمال مسئولیت تضامنی را فراهم می‌کند، زیرا هر متعهد که در اجرای یک تعهد مشترک کوتاهی کند، مسئول جبران خسارت خواهد بود.

در نتیجه، هرچند حقوق ایران فاقد مقررات صریح درباره مسئولیت تضامنی در زنجیره فناوری است، ترکیب این مواد قانونی و قواعد فقهی امکان حمایت از زیان‌دیده و اعمال مسئولیت تضامنی میان همه بازیگران دخیل را فراهم می‌کند. این رویکرد، ضمن همخوانی با ماده ۷ دستورالعمل مسئولیت محصول اتحادیه اروپا که مسئولیت مشترک را میان بازیگران فناوری پیش‌بینی کرده است، می‌تواند به عنوان چارچوبی عملی برای حل چالش‌های ناشی از

۶۹. حایه ذاکری‌نیا، «ماهیت و مبنای مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران و کشورهای اتحادیه اروپا»، حقوق خصوصی، ش ۲۰ (۱۴۰۲)، ص ۱۴۲.

فقدان داده‌ها در خودروهای خودران مورد استفاده قرار گیرد.

درمجموع می‌توان گفت، مبانی سنتی چون نظریه تقصیر به‌تنهایی پاسخگوی چالش‌های ناشی از فقدان داده‌ها نیستند. در شرایط پیچیده فناوری‌های داده‌محور، حرکت به سمت پذیرش مسئولیت بدون تقصیر در حقوق ایران منطقی‌تر و کارآمدتر است. این مبنا ضمن همسویی با استانداردهای اروپایی، امکان حمایت مؤثر از زبان‌دیدگان و پوشش زنجیره کامل بازیگران فناورانه را فراهم می‌آورد.

۳.۴. چالش‌های اثبات رابطه سببیت در فقدان داده‌ها

رابطه سببیت میان فعل زیان‌بار و خسارت وارده از ارکان اساسی مسئولیت مدنی است. در حوزه خودروهای خودران، اهمیت این رکن مضاعف است، زیرا فقدان یا حذف داده‌های حیاتی مانع از بازسازی حادثه و احراز مسئولیت می‌شود. در ادامه چالش‌های موجود در قالب سناریوها بررسی خواهد شد:

سناریو ۱: حذف یا از دست رفتن داده‌های جعبه سیاه

اگر داده‌های ذخیره‌شده در جعبه سیاه خودرو به دلیل نقص فنی یا حذف عمدی از دست بروند، امکان بازسازی حادثه و تعیین مسئولیت از بین می‌رود. ماده ۳۲ قانون جرایم رایانه‌ای تکلیف به نگهداری داده‌ها را مقرر کرده، حذف عمدی آنها را جرم می‌داند. همچنین، مطابق ماده ۱ قانون مسئولیت مدنی، هر ضرر مادی یا معنوی باید جبران شود و فقدان داده‌های حیاتی حادثه مصداق ورود ضرر است. بر این اساس، حذف عمدی داده‌های حادثه می‌تواند هم موجب مسئولیت کیفری (بر اساس قانون جرایم رایانه‌ای) و هم ایجاد مسئولیت مدنی (بر اساس قانون مسئولیت مدنی) شود. با این حال، مقرره خاصی که الزام صریح به ثبت و نگهداری داده‌های ایمنی خودروهای خودران را مقرر کند، وجود ندارد و همین امر اثبات تقصیر یا رابطه سببیت را با دشواری جدی مواجه می‌سازد.

بر مبنای اصل جبران کامل ضرر، در ماده ۴ قانون مسئولیت مدنی، زیان‌دیده حق مطالبه خسارت ناشی از فقدان داده‌ها را دارد. با این حال، فقدان داده‌های جعبه سیاه موجب می‌شود که وی قادر به ارائه ادله فنی کافی برای اثبات تقصیر یا نقص محصول نباشد. هرچند قوانین موجود

مانند قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای ارزش داده‌ها و لزوم حفاظت از آنها را تصریح کرده‌اند، اما مسئولیت خاص تولیدکننده خودروهای خودران در حفظ داده‌های حادثه را به روشنی مشخص نکرده‌اند. همین امر خلأ قانونی قابل توجهی در حمایت از زیان دیدگان ایجاد می‌کند.

در مقابل، در نظام حقوقی اتحادیه اروپا و بر اساس مصوبه ۲۰۱۹، مسئولیت محصول و مقررات هوش مصنوعی، تولیدکنندگان خودروهای خودران مکلف به ثبت و حفظ داده‌های مرتبط با حوادث هستند و فقدان داده‌های جعبه سیاه می‌تواند به عنوان «نقص محصول» تلقی شود. در چارچوب دستورالعمل اصلاحی مسئولیت ناشی از محصول، این فقدان داده گزینه‌ای به نفع زیان دیده محسوب می‌شود که بار اثبات را برعهده تولیدکننده می‌گذارد. علاوه بر این، مقررات حفاظت از داده‌ها و مواد ۱۶ و ۱۷ قانون هوش مصنوعی، الزام صریح به نگهداری داده‌های حیاتی برای شفافیت و ایمنی کاربران را مقرر کرده و در صورت عدم رعایت، امکان اعمال جریمه‌های سنگین و اقدامات نظارتی پیش‌بینی شده است.^{۷۰}

سناریو ۲: نقص در سیستم موقعیت‌یاب یا نقشه دیجیتال

مواد ۱ و ۲ قانون مسئولیت مدنی، مسئولیت ناشی از بی‌احتیاطی یا بی‌مبالاتی را مقرر می‌کنند و بر اساس قاعده فقهی تسبیب، هر کس با فعل یا ترک فعل خود سبب ورود خسارت شود، مسئول جبران آن است. در این فرض، ممکن است مسئولیت بین تولیدکننده سخت‌افزار خودرو و ارائه‌دهنده خدمات نقشه دیجیتال تقسیم شود، به‌ویژه اگر نقص داده‌ها یا خدمات ارائه‌شده نقش مستقیم در وقوع حادثه داشته باشد. با این حال، در قوانین ایران هیچ چارچوب مشخصی برای تعیین حدود و مرز مسئولیت میان ارائه‌دهندگان خدمات داده‌ای و تولیدکنندگان خودرو وجود ندارد. این ابهام می‌تواند موجب بروز اختلافات قضایی پیچیده شود و زیان دیده را در شناسایی دقیق طرف مسئول دچار مشکل کند.

این خلأ درحالی است که قوانین خاصی برای تعیین مسئولیت ارائه‌دهندگان داده‌های حیاتی مرتبط با عملکرد خودرو وجود ندارد و قراردادهای خصوصی نیز معمولاً فاقد ضمانت‌های اجرای

70. Artificial Intelligence Act, Articles 71, 72, and 73.

کافی در این زمینه هستند.

در اتحادیه اروپا، بر اساس ماده ۱۲ دستورالعمل اصلاحی مسئولیت ناشی از محصول، داده و نرم افزار به عنوان بخشی از محصول شناخته می شوند و هرگونه نقص در این اجزا می تواند به مسئولیت مستقیم تولیدکننده یا ارائه دهنده خدمات منجر شود. مهم تر آنکه این دستورالعمل امکان مسئولیت تضامنی میان تولیدکننده خودرو و ارائه دهنده خدمات داده را فراهم می کند، به نحوی که زیان دیده می تواند برای جبران خسارت علیه هریک از آنها طرح دعوی کند. این رویکرد، بار اثبات و پیچیدگی های حقوقی را برای زیان دیده به نحو چشمگیری کاهش می دهد.

سناریو ۳: نشت داده های کاربر از حافظه خودرو

در مواردی که داده های شخصی راننده یا مسیره های پیموده شده افشا شود، زیان دیده باید منبع افشا را شناسایی کند؛ امری که در عمل دشوار است. در حقوق ایران، قانون جرایم رایانه ای (مواد ۱۶ و ۱۷)، دسترسی غیرمجاز به داده ها و افشای آنها را جرم انگاری کرده است. همچنین مواد ۶۵ و ۶۷ قانون تجارت الکترونیکی، افشای غیرمجاز داده های دارای ارزش اقتصادی را ممنوع کرده است. ماده ۱ قانون جرایم رایانه ای، دسترسی غیرمجاز به داده ها را نیز جرم انگاری کرده و از منظر مدنی، ماده ۹ قانون مسئولیت مدنی امکان جبران خسارت معنوی ناشی از نشت داده ها را فراهم آورده است.

در این حوزه، خلأ اصلی در حقوق ایران، نبود الزام قانونی به رمزنگاری یا ایمن سازی داده های حیاتی خودرو است. این موضوع باعث می شود که حتی در صورت شناسایی مسئولیت، اثبات تقصیر و رابطه سببیت دشوار باشد و زیان دیده نتواند به طور کامل از حقوق خود بهره مند شود.

در اتحادیه اروپا، مقررات عمومی حفاظت از داده ها (مواد ۵، ۲۴، ۲۵، ۳۲) به طور صریح جبران خسارت مادی و غیرمادی ناشی از نقض داده را پیش بینی کرده و برای پردازشگران و کنترل کنندگان داده، تکالیف امنیتی مشخص مقرر کرده است. در صورت نقض این الزامات، زیان دیده حق دارد علیه مسئول پردازش داده اقامه دعوی کند و طبق ماده ۸۳ همین قانون، نهادهای نظارتی نیز می توانند جریمه های سنگین اعمال کنند. این چارچوب حمایتی قوی، امنیت

داده‌ها و حقوق کاربران را به شکل مؤثری تضمین می‌کند.

سناریو ۴: حذف خودکار داده‌ها پس از وقوع خطا

اگر نرم‌افزار خودرو به گونه‌ای طراحی شده باشد که داده‌های حادثه پس از بروز خطا به صورت خودکار حذف شوند، زیان دیده هیچ ابزاری برای اثبات مسئولیت نخواهد داشت. این وضعیت در حقوق ایران مصداق بارز قاعده تسبیب و ماده ۳۳۱ قانون مدنی است که ایجاد سبب زیان را بدون مباشرت مستقیماً موجب ضمان می‌دانند. علاوه بر این، در مواد ۳ و ۴ قانون مدیریت داده و اطلاعات ملی ۱۴۰۱، متولیان به حفاظت و بازپایی داده‌ها مکلف شده‌اند و حذف عمدی یا طراحی معیوب سامانه، نقض صریح این تکلیف قانونی است.

هرچند قانون مدیریت داده و اطلاعات ملی و قانون جرایم رایانه‌ای از منظر کلی حذف داده‌ها را ممنوع می‌دانند، اما مقررۀ خاصی وجود ندارد که حذف خودکار داده‌های ایمنی خودرو را به صراحت منع کند. در این زمینه، برخی، از ایجاد یک نهاد برای مدیریت و اداره داده‌ها در جهت تضمین حقوق اشخاص در برابر غول‌های فناوری سخن گفته‌اند^{۷۱}؛ این دیدگاه می‌تواند در بازپایی اطلاعاتی که تنها در اختیار تولیدکننده است کمک‌کننده باشد.

در اتحادیه اروپا، قانون هوش مصنوعی در مواد ۱۲ و ۱۹، الزام صریح به ثبت و نگهداری وقایع بحرانی را مقرر کرده است و حذف خودکار داده‌های مرتبط با ایمنی، نقض آشکار این الزام محسوب می‌شود. چنین نقضی می‌تواند مبنای مسئولیت بدون تقصیر علیه تولیدکننده باشد و نهادهای نظارتی نیز به اعمال جریمه‌های قابل توجه مجاز خواهند بود. این رویکرد، ازدست رفتن داده‌های حیاتی را به طور مؤثر محدود و مسئولیت تولیدکنندگان را به طور مستقیم تقویت می‌کند.

سناریوهای پیش گفته نشان می‌دهند که فقدان داده، رابطه سببیت را در حقوق ایران به شدت متزلزل می‌سازد و زیان دیده را در اثبات دعوی با مانع جدی مواجه می‌کند. با این حال، ظرفیت‌هایی چون مقررات قانون مسئولیت مدنی، قواعد اتلاف و تسبیب در قانون مدنی، قانون جرایم رایانه‌ای و قانون مدیریت داده‌ها امکان تحلیل حقوقی و جبران خسارت را فراهم می‌آورند.

۷۱. عباس میرشکاری و همکاران، «تراست داده، سازوکاری برای مدیریت منافع ذی‌نفعان داده؛ رهنمودهایی برای نظام داده در حقوق ایران»، *مطالعات حقوق تطبیقی معاصر*، ش ۱۵ (۱۴۰۳)، ص ۳۱۴.

تجربه اتحادیه اروپا نشان می‌دهد که بهترین راه‌حل، پذیرش فرض رابطه سببیت و واژگونی بار اثبات است. چنین رویکردی می‌تواند با تفسیر موسع از اصول فقهی (قاعده لاضرر و تسبیب) و اصول کلی جبران کامل ضرر، در نظام حقوقی ایران نیز تقویت شود.

نتیجه

تحلیل تطبیقی نشان داده که «ازدست رفتن داده» در نظام‌های حقوقی موردبررسی، به‌عنوان خسارت مستقل به معنای کلاسیک تثبیت نشده، اما آثار زیان‌بار آن در چارچوب‌های موجود قابل جبران است. در اتحادیه اروپا، بر اساس دستورالعمل مسئولیت ناشی از محصول، فقدان داده در صورت کاهش ایمنی می‌تواند در قالب نقص محصول تحلیل شود و در چارچوب مقررۀ عمومی حفاظت از داده‌ها نیز جبران خسارت منوط به اثبات ضرر مادی یا غیرمادی است. همچنین دستورالعمل مسئولیت هوش مصنوعی سازوکارهایی برای تسهیل اثبات رابطه سببیت پیش‌بینی کرده است.

در حقوق ایران، اگرچه مواد ۱ و ۲ قانون مسئولیت مدنی و قواعد اتلاف و تسبیب □ ظرفیت جبران این نوع زیان را دارند، اما فقدان تصریح تقنینی درباره جایگاه داده در مسئولیت مدنی، موجب ابهام و انتقال ریسک اثبات به زیان‌دیده می‌شود؛ از این رو، شفاف‌سازی تقنینی ضروری است.

در این راستا، الحاق ماده‌ای به قانون مسئولیت مدنی در خصوص مسئولیت ناشی از فقدان داده در سامانه‌های خودران می‌تواند راهکاری عملی و کوتاه‌مدت باشد. در عین حال، تدوین قانون مستقل در زمینه مسئولیت و ایمنی سامانه‌های خودران، راهکاری جامع‌تر و بلندمدت برای تنظیم منسجم ابعاد فنی، بیمه‌ای و مسئولیتی این فناوری خواهد بود.

پیشنهاد تقنینی

با توجه به خلأ موجود، پیشنهاد می‌شود ماده‌ای مشخص به قانون مسئولیت مدنی الحاق گردد:

ماده پیشنهادی: «هرگاه در اثر نقص فنی، طراحی، تولید، نگهداری یا بهره‌برداری از

سامانه‌های هوشمند یا خودروهای خودران، داده‌ها یا اطلاعات متعلق به اشخاص از بین برود، ثبت نگردد یا به گونه‌ای ناقص ذخیره شود و این امر موجب ورود ضرر مادی، معنوی یا تضییع متعارف امکان اثبات حق گردد، شخص یا اشخاصی که نقص به آنان منتسب است، بر اساس نظام مسئولیت بدون تقصیر، مسئول جبران خسارت خواهند بود؛ مگر آنکه ثابت نمایند فقدان داده ناشی از علت خارجی غیرقابل انتساب بوده است».

تبصره: «در مواردی که فقدان داده اثبات رابطه سببیت را به طور متعارف دشوار سازد، دادگاه می‌تواند در صورت احراز نقض تکالیف فنی یا ایمنی مربوط به ثبت و نگهداری داده، رابطه سببیت را مفروض تلقی کند؛ مگر آنکه خلاف آن ثابت شود».

این راهکار با اتکا بر مبانی فقهی اتلاف و لاضرر و با الهام از سازوکارهای تسهیل اثبات در حقوق اتحادیه اروپا، می‌تواند بدون ایجاد گسست در ساختار موجود، خلأ فعلی را به صورت هدفمند برطرف سازد.

در رویکردی جامع‌تر، می‌توان به تدوین قانون مستقلی در زمینه «مسئولیت و ایمنی سامانه‌های خودران» اندیشید. چنین قانونی می‌تواند افزون بر تعیین مبنای مسئولیت مدنی، موضوعاتی مانند استانداردهای ثبت و نگهداری داده‌های حیاتی، مدت زمان حفظ داده‌ها، الزامات بیمه‌ای، مسئولیت تضامنی بازیگران زنجیره فناوریانه و ضمانت اجرای مرتبط را به طور منسجم تنظیم کند. این رویکرد امکان هماهنگی بیشتر میان الزامات فنی، بیمه‌ای و مسئولیتی را فراهم خواهد ساخت.

منابع و مأخذ

الف) فارسی

کتاب

۱. حکمت‌نیا، محمود (۱۳۸۶). *مسئولیت مدنی در فقه امامیه: مبانی و ساختار*. تهران: پژوهشگاه علوم و فرهنگ اسلامی.

مقالات

۲. ابهری، حمید؛ مافی، همایون و پارسا، ناهید (۱۴۰۰). مطالعه تطبیقی ضابطه‌های تشخیص عیب خودرو در حقوق ایران، انگلیس و آمریکا. *مطالعات حقوق تطبیقی*، ۱۲(۲)، ۳۹۷-۴۱۵.
Doi:10.22059/jcl.2021.317984.634142
۳. پارسا، ناهید (۱۴۰۳). بررسی مسئولیت مدنی ناشی از نقص نرم‌افزار در خودروهای خودران با نگاهی به حقوق آمریکا. *فقه و حقوق اسلامی*، ۱۵(۳۴)، ۱۱۵-۱۴۷.
Doi:10.22034/law.2024.55488.3245
۴. جرفی، اسماء؛ صاحب، طیبه و شهبازی‌نیا، مرتضی (۱۴۰۳). مسئولیت مدنی مالک کشتی‌های خودران ناشی از تصادم کشتی. *پژوهش‌های حقوق تطبیقی*، ۲۸(۲)، ۳۱-۱.
Doi:10.22034/clr.2024.72019
۵. احمدوند، بهناز و جهانشاهی، آرتین (۱۴۰۲). بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی اتحادیه اروپا و ایران. *پژوهش‌های حقوق تطبیقی*، ۲۷(۱)، ۱۰۵-۱۳۲.
<http://clr.modares.ac.ir/article-66499-20-fa.html>
۶. کیشانی، مصطفی و اسدی، حسین (۱۳۹۹). ارزیابی اثر خطای انسانی بر اتکاپذیری سامانه‌های ذخیره‌سازی داده. *علوم رایانش و فناوری اطلاعات*، ۱۸(۱)، ۴۲-۵۵.
۷. میرشکاری، عباس؛ پیشنماز، سید امین و رکنی، امیرعباس (۱۴۰۳). تراست داده، سازوکاری برای مدیریت منافع ذی‌نفعان داده؛ رهنمودهایی برای نظام داده در حقوق ایران. *مطالعات حقوق تطبیقی معاصر*، ۱۵(۳۴)، ۳۲۰-۳۷۹.
Doi:10.22034/law.2024.56448.3268
۸. ذاکری‌نیا، حانیه (۱۴۰۲). ماهیت و مبنای مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران

و کشورهای اتحادیه اروپا. *حقوق خصوصی*، ۲۰(۱)، ۱۳۵-۱۵۲.

Doi:10.22059/jolt.2023.356703.1007186

۹. ولی‌زاده، حسین (۱۳۹۸). اثر قاعده لاضرر در مسئولیت مدنی و نقش قاعده اقدام در اثر رافعیّت آن. *قانون یار*، ۳(۱۰)، ۳۳۱-۳۴۸.
SID.https://sid.ir/paper/521350/fa

قوانین و مقررات

۱۰. قانون مدنی ایران، مصوب مجلس شورای ملی، روزنامه رسمی شماره ۹۰۳ مورخ ۱۸ اردیبهشت ۱۳۱۴.

۱۱. قانون مسئولیت مدنی مصوب ۱۳۳۹، روزنامه رسمی جمهوری اسلامی ایران، شماره ۴۰۸۲.

۱۲. قانون جرایم رایانه‌ای مصوب ۱۳۸۸، روزنامه رسمی جمهوری اسلامی ایران، شماره ۱۸۷۴۲.

۱۳. قانون تجارت الکترونیکی مصوب ۱۳۸۲، روزنامه رسمی جمهوری اسلامی ایران، شماره ۱۷۱۶۶.
۱۴. قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۸، روزنامه رسمی جمهوری اسلامی ایران، شماره ۱۸۷۷۳.

۱۵. قانون مدیریت داده و اطلاعات ملی مصوب ۱۴۰۱، روزنامه رسمی جمهوری اسلامی ایران، شماره ۲۲۸۰۷.

منابع الکترونیک

۱۶. آوخ، محمد (۱۴۰۱، ۲۵ آبان). درک مفهوم دیتا؛ دیتا دقیقاً چیست؟ اعتمادآنلاین. بازیابی شده از <https://www.etemadonline.com/> بخش-اجتماعی-۵۵۵۱۴۳/۲۳-درک-مفهوم-دیتا-دیتا-دیتا-دقیقا-چیست.

ب) منابع انگلیسی

Books

17. Anderson, J. M.; Kalra, N.; Stanley, K. D.; Sorensen, P., & Oluwatobi, A. O. (2014). *Autonomous Vehicle Technology: A Guide for Policymakers*. Santa Monica, CA: RAND Corporation.
18. Stair, R., & Reynolds, G. (2017). *Principles of Information Systems* (13th ed.). Cengage Learning.

Articles

19. Badue, C.; Guidolini, R.; Carneiro, R. V.; Azevedo, P.; Cardoso, V. B.; Forechi, A., & De Souza, A. F. (2021). Self-driving Cars: a Survey. *Expert Systems with Applications*, 165, 113816. Doi:10.1016/J.ESWA.2020.113816
20. Calo, R. (2016). Robotics and the Lessons of Cyberlaw. *California Law Review*, 103 (3), 513–563.
21. Bhemavarapu, S. V. R. (2025). *Cybersecurity for Autonomous Vehicles*. <https://arxiv.org/abs/2504.20180>
22. Fernández, Llorca, D.; Hamon, R.; Junklewitz, H.; Grosse, K.; Kunze, L.; Seiniger, P.; Swaim, R.; Reed, N.; Alahi, A.; Gómez, E.; Sánchez, I., & Kriston, Á. (2024). Testing Autonomous Vehicles and AI: Perspectives and Challenges from Cybersecurity, Transparency, Robustness and Fairness. *arXiv Preprint*, arXiv: 2403.14641. Doi10.48550/arXiv.2403.14641
23. Nolte, M.; Nolte, S., & Menzel, T. (2025). A Review of Conceptualizations of Safety and Risk in Current Automated Driving Regulation. *arXiv*: 2502.06594.
24. Pinciroli, R.; Yang, L.; Alter, J., & Smirni, E. (2020). The Life and Death of SSDs and HDDs: Similarities, Differences, and Prediction Models. *Conference Paper*. <https://www.researchgate.net/publication/-356678575>
25. Xu, Y.; Wei, J.; Mi, T., & Chen, Z. (2024). Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics. *World Electric Vehicle Journal*, 16 (1).

Laws and Regulations

26. European Commission. (2023). *Regulation (EU) 2023/... on General Product Safety*. Brussels: Official Journal of the European Union.
27. European Commission. (2024). *Directive 85/374/EEC on Liability for Defective Products* (Consolidated Version with 2024 Amendments). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31985L0374>

28. European Commission. (2024a). **Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)**. Brussels: COM(2022) 496 final.
29. European Parliament and Council. (2016). **Regulation (EU) 2016/679 (General Data Protection Regulation)**. OJ L119/1.
30. European Parliament and Council. (2022). **Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)**, COM/2022/496 final.
31. European Parliament and Council. (2024). **Artificial Intelligence Act. Regulation (EU) 2024/1381**. OJ L/2024/1381.
32. ISO/IEC. (2015). **ISO/IEC 2382:2015: Information Technology-Vocabulary**. International Organization for Standardization/International Electrotechnical Commission. <https://www.iso.org/standard/63598.html>
33. National Institute of Standards and Technology. (2004). **Standards for Security Categorization of Federal Information and Information Systems (FIPS Publication No. 199)**. U.S. Department of Commerce. Doi:10.6028/NIST.FIPS.199

Online Sources

34. Hornetsecurity. (n.d.). What is Data Loss? Retrieved July 23, 2025, from <https://www.hornetsecurity.com/en/knowledge-base/data-loss/>
35. National Institute of Standards and Technology. (n.d.). **Computer Security Resource Center glossary**. Retrieved July 24, 2025, from <https://csrc.nist.gov/glossary>

Court Cases

36. Court of Justice of the European Union (CJEU). (2014). **Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González**, Case C-131/12, ECLI:EU:C:2014:317. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A620-12CJ0131>