University of Tabriz

Contemporary Comparative Legal Studies

Online ISSN: 2821-0514
Volume: 17 **Issue:** 42
Spring 2026

Article Type: Research Article **Pages:** 23-50

The Impact of Artificial Intelligence on Customers' Personal Data in Banking Law of Iran and the United Kingdom

Mahmoud Bagheri[1]| Alireza Ghasemi Firouzabadi[2]

1. Associate Professor, Department of Private Law, University of Tehran, Iran mahbagheri@ut.ac.ir
2. Master's Student in Financial Law, University of Tehran, Iran (Corresponding Author) ar.gh.firozabadi@ut.ac.ir

Abstract

The use of artificial intelligence by banks has brought about profound transformations in the field of banking data processing. In traditional banking, data processing is generally carried out based on established principles, and necessary safeguards are implemented to protect the rights of data subjects. The prevailing literature in this area has predominantly focused on analyzing the concepts and instances of personal data, as well as the governing principles applicable thereto .This article, adopting a descriptive-analytical method and relying on library-based sources, addresses the question of what impact the emergence of artificial intelligence has on the principles governing the processing of personal banking data and on customers' rights, and whether Iranian law provides comprehensive and clear regulations in this regard .The findings of the study indicate that artificial intelligence poses challenges and obstacles, on the one hand, to principles such as informed consent, transparency of processing, data accuracy and currency, and data confidentiality, and, on the other hand, to customers' rights such as the right to data portability, the right to restriction of processing, the right to erasure (the "right to be forgotten"), and the right to object to automated decision-making .The results further suggest that the enactment of comprehensive data protection laws and regulations, taking into account the specific characteristics of artificial intelligence, along with the designation of clearly defined types of artificial intelligence for use by each institution within a specific regulatory framework, can to a large extent prevent violations of the principles governing data processing and the rights of customers.

Keywords: *Artificial Intelligence (AI); Personal Data; Data Protection; Data Processing Principles; Bank Customers' Rights*.

Received: 2025/11/13 **Received in revised form:** 2026/03/30 **Accepted:** 2026/04/13 **Published:** 2026/06/10

DOI: 10.22034/Law.2026.70218.3559

Publisher: University of Tabriz law@tabrizu.ac.ir

شاپا الکترونیکی: ۰۵۱۴-۲۸۲۱
مطالعات حقوق تطبیقی معاصر
دوره: ۱۷، شماره: ۴۲
بهار ۱۴۰۵
نوع مقاله: پژوهشی
صفحات: ۲۳-۵۰

تأثیر هوش مصنوعی بر داده‌های شخصی مشتریان در حقوق بانکی ایران و انگلستان

محمود باقری[۱] | علی‌رضا قاسمی فیروزآبادی[۲]

۱. دانشیار گروه حقوق خصوصی، دانشگاه تهران، ایران mahbagheri@ut.ac.ir
۲. دانشجوی کارشناسی ارشد حقوق مالی، دانشگاه تهران، ایران (نویسنده مسئول) ar.gh.firozabadi@ut.ac.ir

چکیده

استفادهٔ بانک‌ها از هوش مصنوعی تحولات شگرفی را در حوزهٔ پردازش داده‌های بانکی به‌وجود آورده است. در بانکداری سنتی پردازش داده‌ها معمولاً بر مبنای اصول مشخصی صورت می‌گیرد و جهت تضمین حقوق اشخاص موضوع داده نیز حمایت‌های لازم به‌عمل می‌آید. غالب ادبیات موجود در زمینهٔ داده‌ها موقوف بر تحلیل مفاهیم و مصادیق داده‌های شخصی و اصول حاکم بر آن است. نگارندگان مقالهٔ حاضر با روش توصیفی- تحلیلی و با استفاده از منابع کتابخانه‌ای به این پرسش می‌پردازند که پیدایش هوش مصنوعی چه تأثیری بر اصول حاکم بر پردازش داده‌های شخصی بانکی و حقوق مشتریان می‌گذارد و آیا حقوق ایران مقررات جامع و روشنی در این زمینه دارد؟ یافته‌های پژوهش نشان می‌دهد که هوش مصنوعی اصولی مانند اصل رضایت آگاهانه، شفافیت پردازش، دقیق و به‌روز بودن و محرمانگی داده‌ها را از یک سو، و حقوق مشتریان بانک، مانند حق انتقال‌پذیری، حق محدودسازی پردازش، حق فراموشی داده‌ها و حق اعتراض به تصمیمات خودکار را از سوی دیگر با چالش‌ها و موانعی مواجه می‌سازد. نتایج پژوهش حاکی از آن است که تدوین قوانین و مقررات جامع حفاظت از داده‌ها با درنظر گرفتن ویژگی‌های هوش مصنوعی و تعیین نوع مشخص هوش مصنوعی برای استفادهٔ هر نهاد با چارچوب خاص، می‌تواند تا حد زیادی از نقض اصول حاکم بر پردازش داده‌ها و حقوق مشتریان جلوگیری نماید.

واژگان کلیدی: *اصول پردازش داده‌ها، حفاظت از داده‌ها، حقوق مشتریان بانک، داده‌های شخصی، هوش مصنوعی.*

تاریخ دریافت: ۱۴۰۴/۰۸/۲۲ **تاریخ بازنگری:** ۱۴۰۵/۰۱/۱۰ **تاریخ پذیرش:** ۱۴۰۵/۰۱/۲۴ **تاریخ انتشار:** ۱۴۰۵/۰۳/۲۰

DOI: 10.22034/Law.2026.70218.3559

ناشر: دانشگاه تبریز law@tabrizu.ac.ir

مقدمه

بخش بانکی یکی از پیش‌گامان بهره‌گیری از فناوری هوش مصنوعی برای کاهش هزینه‌های عملیاتی و تسریع در ارائهٔ خدمات بانکی است[۱]. در گذشته، تفکر انجام برخی کارها از سوی پدیده‌ای غیر از انسان به‌ندرت وجود داشت، اما امروزه می‌توان هوش مصنوعی را یکی از ارکان بانکداری به‌شمار آورد که در برخی موارد به جای انسان یا در کنار آن، با بهبود بخشیدن به فعالیت‌های بانکی، کاهش ریسک‌های موجود، شناسایی الگوهای مشکوک به تقلب، تصمیم‌گیری آنی، شناسایی علائم اولیه جهت اعلان هشدار هنگام بحران مالی و ... نقش مهمی را ایفا می‌کند.

برخی از بانک‌ها مانند لویدز[۲] و بارکلیز[۳] انگلستان، بانک ارتباطات[۴] چین، اسبربانک[۵] روسیه و بانک ملی ایران از این فناوری در ارائهٔ برخی از خدمات بانکی استفاده می‌کنند. با این حال، هوش مصنوعی با دسترسی به حجم گسترده‌ای از داده‌های شخصی و حساس مشتریان می‌تواند با تحلیل رفتارها، پردازش و ذخیره‌سازی داده‌ها، پروفایل‌هایی را از آنان ایجاد و بر مبنای آن تصمیماتی را اتخاذ کند؛ تصمیماتی که در صورت فقدان نظارت و چارچوب‌های حقوقی مناسب ممکن است به نقض اصول حاکم بر پردازش داده‌ها از سوی بانک‌ها و نقض حقوق مشتریان منجر شود.

با اینکه انگلستان در سال‌های اخیر با تدوین مقررات عمومی حفاظت از داده‌ها[۶] و قانون حفاظت از داده‌ها مصوب ۲۰۱۸[۷]، تلاش داشته است چارچوب و اصول حاکم بر پردازش داده‌های شخصی را ایجاد کرده، از اشخاص موضوع داده حمایت‌های لازم را به‌عمل آورد، اما در حقوق ایران قوانین مرتبط پراکنده بوده، قواعد اختصاصی ناظر بر پردازش داده‌های شخصی از طریق سامانه‌های هوش مصنوعی در بانکداری به‌طور جامع تدوین نشده است.

1. Vijaya S. Tumma, *"Exploring Factors that Influence Artificial Intelligence Adoption in Banks and Credit Unions"* (PhD diss, University of South Florida, 2024), p. 10.
2. Lloyds Bank
3. Barclays
4. State-Owned Bank of Communications
5. Sberbank
6. United Kingdom General Data Protection Regulation (UK GDPR)
7. Data Protection Act 2018 (UK)

از این رو، مطالعهٔ تطبیقی دو نظام حقوقی می‌تواند به شناسایی خلأهای موجود و ارائهٔ راهکارهای مناسب برای رعایت اصول پردازش داده‌ها و حفاظت از حقوق مشتریان بانکی با توجه به تأثیر هوش مصنوعی کمک کند. بر این اساس، در ادامهٔ این نوشتار ذیل سه عنوانِ مفهوم‌شناسی، تأثیر هوش مصنوعی بر اصول پردازش داده‌های شخصیِ بانکی و تأثیر هوش مصنوعی بر حقوق مشتریان بانک، ابعاد این مهم بررسی شده است و در نهایت به این پرسش پاسخ داده خواهد شد که در کنار مزایای استفادهٔ بانک از هوش مصنوعی، آیا اصول پردازش داده‌ها از جانب بانک‌ها رعایت می‌شود و این فناوری بر حقوق مشتریان بانک‌ها چه تأثیری می‌گذارد.

۱. مفهوم‌شناسی

پیش از بررسی تأثیر هوش مصنوعی بر رعایت اصول پردازش داده‌های شخصی و حقوق مشتریان بانک و نیز چالش‌های آن در حقوق دو کشور، لازم است مفاهیم هوش مصنوعی، انواع آن، داده‌های شخصی و داده‌های شخصیِ حساس، تعریف و تفکیک گردد.

۱.۱. هوش مصنوعی و انواع آن

هوش مصنوعی برای افراد مختلف، معانی متفاوت دارد. از نظر برخی، هوش مصنوعی به معنی شکل زندگی مصنوعی است که می‌تواند انسان‌ها را هوشمند کند و برای برخی یک تکنولوژی پردازش داده‌ها است. اما در تعریف دقیق‌تر، هوش مصنوعی مجموعه‌ای است از فناوری‌هایی که به ماشین‌ها توانایی می‌دهد در سطوح بالاتری از هوشمندی عمل کنند و به قابلیت‌های انسانی، احساس، درک و رفتار برسند[۸].

با این همه، در حال حاضر تعریف واحدی از هوش مصنوعی که همگان بر آن اتفاق نظر داشته باشند، وجود ندارد و هر کشور با توجه به اقتضائات خود این فناوری را تعریف می‌کند[۹]. در ایران قانون‌گذار در مادهٔ ۱ سند ملی هوش مصنوعی مصوب ۱۴۰۳[۱۰]، این فناوری را تعریف کرده است.

---

۸. مهرنوش ابوذری، *حقوق و هوش مصنوعی* (تهران: نشر میزان، چ ۳، ۱۴۰۲)، ص ۱۱-۱۳.

9. Bank for International Settlements, "*Regulating AI in the Financial Sector: Recent Developments and Main Challenges*", FSI Insights No. 63 (December 2024), p. 2.

۱۰. هوش مصنوعی: به توانایی ماشین برای انجام عملکردهای خودکار و نظام‌مند ازجمله یادگیری، درک، استنتاج، حل مسئله، پیش‌بینی، تصمیم‌گیری و اقدام از طریق به کارگیری دانش و اطلاعات و پردازش داده گفته می‌شود که منشأ اثرگذاری های گسترده بر انسان و روابط انسانی در محیط فیزیکی یا مجازی و همچنین بازتاب‌های زیست‌محیطی است. هوش مصنوعی ماهیتی داده‌ای، شبکه‌ای، الگوریتمی، خوشه‌ای، لایه‌ای و یکپارچه، مبتنی بر منطق کلاسیک و سایر منطق‌های نوین دارد.

کاربرد هوش مصنوعی تقریباً تمامی بخش‌های بانک را دربر می‌گیرد. هوش مصنوعی در بانکداری در طیف گسترده‌ای از فعالیت‌ها ازجمله اعتبارسنجی، اعطای تسهیلات، کشف تقلب، مدیریت ریسک، احراز هویت و ارائهٔ خدمات به مشتریان به‌کار گرفته می‌شود[11] و همچنین ویژگی‌هایی مانند خستگی‌ناپذیری، فعالیت‌های شبانه‌روزیِ خارج از زمان اداری و قابلیت انجام محاسبات پیچیده را دارد و با پیش‌بینی ریسک‌ها و قوهٔ قاهره می‌تواند فرایندهای بانکی را بهتر و سریع‌تر از قبل انجام دهد.

از منظر میزان استقلال در تصمیم‌گیری، هوش مصنوعی را می‌توان به سه دستهٔ هوش مصنوعی مستقل[12]، هوش مصنوعی غیرمستقل[13] و هوش مصنوعی مشورت‌دهنده[14] تقسیم کرد.

برای مثال، در فرایند اعتبارسنجی و اعطای تسهیلات، چنانچه سامانهٔ هوش مصنوعی پس از تحلیل داده‌ها، بدون دخالت انسان تصمیم نهایی را اتخاذ و درخواست وام را رد یا تأیید کند، هوش مصنوعی مستقل محسوب می‌شود.

در مقابل، اگر هوش مصنوعی صرفاً ارزیابی اولیه را انجام دهد و تصمیم نهایی از سوی کارمند بانک اتخاذ شود، هوش مصنوعی غیرمستقل خواهد بود. همچنین، اگر هوش مصنوعی، تنها پیشنهادهایی ارائه دهد و هیچ نقشی در تصمیم‌گیری نهایی نداشته باشد، هوش مصنوعی مشورت‌دهنده تلقی می‌شود.

به نظر نگارندگان، هوش مصنوعی بانکی را می‌توان به‌عنوان سامانه‌ای درنظر گرفت که قابلیت تحلیل و تفسیر حجم گسترده‌ای از داده‌های بانکی را با کارایی بالا فراهم می‌سازد و در فرایندهای مختلف، ازجمله اعطای تسهیلات، می‌تواند در انجام وظایفی مانند استخراج داده‌ها از اسناد و مدارک ارائه‌شده از سوی متقاضیان و همچنین راستی‌آزمایی درآمد و سوابق مالی مشتریان نقش مهمی ایفا نماید.

11. Fares, O. H.; Butt, I.; & Lee, S. H. M. (2022), "*Utilization of Artificial Intelligence in the Banking Sector: A Systematic Literature Review"*, AI & Society, Springer, p. 1–2.
12. Independent Artificial Intelligence
13. Dependent Artificial Intelligence
14. Unsupervised Artificial Intelligence

۲.۱. داده‌های شخصی و حساس بانکی

اغلب یا شاید تمامی قوانین مربوط به حفاظت از داده‌ها با ارائهٔ تعریفی از دادهٔ شخصی آغاز می‌شوند تا به این ترتیب، حدود قانون معین شود و تنها پس از ارائهٔ این تعریف است که قوانین به بیان حقوق و تکالیف شخص موضوع داده و کنترل‌کننده می‌پردازند. با این همه، «دادهٔ شخصی» ترکیبی است سخت مبهم و نباید آن را مفهومی ثابت و روشن پنداشت[۱۵].

میان دادهٔ شخصی و دادهٔ شخصیِ حساس تفاوت وجود دارد. مطابق بند «ر» مادهٔ ۲ قانون تجارت الکترونیک مصوب ۱۳۸۲ و نیز دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوهٔ جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی مصوب ۱۴۰۲، داده‌های مرتبط با هویت و اطلاعات افراد در زمرهٔ داده‌های شخصی قرار می‌گیرد. در مقابل، دادهٔ شخصیِ حساس به اطلاعاتی اطلاق می‌شود که ماهیتاً خصوصی‌تر بوده، اشخاص معمولاً تمایلی به افشای آن‌ها ندارند[۱۶].

در انگلستان، طبق بند ۲ مادهٔ ۳ قانون حفاظت از داده‌ها مصوب ۲۰۱۸، دادهٔ شخصی به معنای هرگونه اطلاعات مربوط به یک فرد زنده شناسایی شده یا قابل شناسایی است[۱۷]. همچنین در بند ۱ مادهٔ ۹ مقررات عمومی حفاظت از داده‌های انگلستان، دسته‌های ویژهٔ داده‌های شخصی، مشخص شده‌اند[۱۸].

در حقوق ایران نیز در مادهٔ ۵۸ قانون تجارت الکترونیک و بند «ث» مادهٔ ۱ قانون مدیریت داده‌ها مصوب ۱۴۰۱، مفاهیم داده و پردازش آن مورد اشاره قرار گرفته است، هرچند تمایزی میان داده‌های شخصی با داده‌های شخصی در دستهٔ ویژه یا به‌عبارتی حساس ارائه نشده است.

---

۱۵. عباس میرشکاری و همکاران، «مفهوم و مصادیق داده‌ی شخصی»، *حقوق فناوری‌های نوین*، ش ۱۲(۱۴۰۴)، ص ۳۹۶.

16. Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., and Nouwt, S. (2009), *Reinventing Data Protection?*, Springer, Dordrecht. p. 4.

17. Data Protection Act 2018, s. 3(2): "Personal Data" Means any Information Relating to an Identified or Identifiable Living Individual.

18. UK GDPR, s. 9(1): Processing of Personal Data Revealing Racial or Ethnic Origin, Political Opinions, Religious or Philosophical Beliefs, or Trade Union Membership, and the Processing of Genetic Data, Biometric Data for the Purpose of Uniquely Identifying a Natural Person, Data Concerning Health or Data Concerning a Natural Person's Sex Life or Sexual Orientation Shall be Prohibited.

به نظر نگارندگان، داده‌های بانکی عمدتاً از داده‌های شخصی تشکیل شده‌اند و در برخی موارد نیز ممکن است شامل داده‌های شخصی حساس (ویژه) شوند.

داده‌هایی مانند شماره حساب، شماره کارت، کد اعتبارسنجی[۱۹]، نام دارندهٔ حساب، موجودی حساب، شماره تلفن همراه و ثابت، شمارهٔ شبا، رمز دوم، رمز پویا، آدرس محل سکونت، تراکنش‌های مالی (مانند سوابق خرید، پرداخت، نقل و انتقال برخط وجوه و مقصد آن)، داده‌های رفتاری بانکی (مانند زمان ورود و خروج از پلتفرم بانکی، نوع دستگاه استفاده‌شده برای ورود)، داده‌های اعتباری (مانند سوابق حساب، چک‌های برگشتی، اقساط بلند و کوتاه‌مدت و بدهی‌ها و اطلاعات واریزکنندگان یا گیرندگان وجوه) از مصادیق داده‌های شخصی محسوب می‌شوند.

علاوه بر موارد پیش‌گفته، داده‌های بیومتریک[۲۰]، ازجمله اثر انگشت دست یا صدا[۲۱] و یا اسکن چشم هرگاه به‌منظور شناسایی منحصربه‌فرد شخص پردازش شوند، از مصادیق داده‌های شخصیِ ویژه محسوب می‌شوند.

۲. تأثیر هوش مصنوعی بر اصول پردازش داده‌های شخصیِ بانکی

گسترش استفاده از هوش مصنوعی در بانکداری، پردازش داده‌های شخصی مشتریان را از یک فرایند سادهٔ سنتی به پردازشی گسترده، مستمر و الگوریتم‌محور تبدیل کرده است. از این رو، مسئلهٔ اصلی صرفِ استفاده از این فناوری نیست، بلکه میزان انطباق آن با اصول بنیادین پردازش داده‌های شخصی است. هوش مصنوعی بانکی در کنار مزایایی که دارد، ممکن است رعایت اصولی همچون رضایت آگاهانه، شفافیت پردازش، دقیق و به‌روز بودن و محرمانگی داده‌ها را با چالش‌هایی مواجه سازد. بر این اساس، در ادامه به بررسی تأثیر هوش مصنوعی بر هریک از این اصول در دو نظام حقوقی پرداخته می‌شود.

19. CVV2
20. Dana Turner, et al. v. Nuance Communications, Inc., United States District Court, Northern District of California, 28 May 2024.
۲۱. برخی هوش‌های مصنوعی می‌توانند هویت مشتریان را از طریق صدای آنان تایید کنند. بعد از این امر، هوش مصنوعی ممکن است، صدای مشتریان را ضبط کند و به اصطلاح فنی با ایجاد اثر انگشت صوتی، هویت مشتریان را برای تماس‌های بعدی شناسایی نماید.

۱.۲. رضایت آگاهانه جهت استفاده از داده‌ها

رضایت آگاهانه فرایندی است که مشتری با درک و فهمی روشن از واقعیت‌ها[۲۲]، امکان تصمیم‌گیری دربارهٔ مسائلی را به‌دست می‌آورد[۲۳]. این امر تضمین می‌کند که اشخاص پیش از اتخاذ تصمیم، گمراه، فریب‌خورده یا دچار اطلاعات نادرست نشوند.

طبق بند ۱ مادهٔ ۶ و بندهای چهارگانه مادهٔ ۷ مقررات عمومی حفاظت از داده‌های انگلستان، رضایت باید به صورت صریح، روشن، مشخص و جزئی اعلان شود و برای هر هدف یا فعالیت مرتبط و جدید، رضایت جداگانه أخذ گردد. بنابراین رضایت کلی یا مبهم کافی نیست[۲۴].

در ایران، مادهٔ ۵۹ قانون تجارت الکترونیک، مادهٔ ۱۵ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۸، مادهٔ ۱۷ قانون جرائم رایانه‌ای مصوب ۱۳۸۸، مواد ۳۱ و ۳۸ منشور حقوق شهروندی مصوب ۱۳۹۵ و مواد ۴ و ۵ طرح حفاظت از داده‌ها و اطلاعات شخصی[۲۵]، به وجود رضایت اشاره کرده‌اند. بنابراین در قوانین دو کشور سکوت نشانهٔ رضایت تلقی نمی‌شود، زیرا سکوت چیزی جز نوعی حالت سکون و عدم تحرک نیست، به همین جهت نمی‌تواند مبین اراده و وسیلهٔ ابراز باشد و از سکوت نمی‌توان به اراده و مقصود شخص ساکت پی برد[۲۶]. همچنین جمع‌آوری و یا ارائهٔ اطلاعات شخصی کاربران به دیگران بدون کسب رضایت آنان، در بسیاری از نظام‌های حقوقی جرم‌انگاری شده است[۲۷].

رأی دادگاه تجدیدنظر انگلستان در پروندهٔ *آر.تی.ام علیه بون تِر لیمیتد*[۲۸] مؤید نظر فوق است که اعتبار رضایت باید بر اساس معیارهای عینی و با توجه به آزادانه، مشخص، آگاهانه و بدون ابهام بودن آن ارزیابی شود و بررسی وضعیت ذهنی موضوع داده برای احراز رضایت کافی نیست.

---

۲۲. با استناد به مادهٔ ۱۹۹ قانون مدنی در اشتباه، عمل حقوقی آگاهانه شکل نمی‌گیرد و عمل انجام‌شده باطل است.

23. S. Radia, *Informed Consent*, Supported by CFA UK's Market Integrity and Professionalism Committee, CFA UK, London, 2014, p. 2.

24. https://ico.org.uk/for-organisation/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/consent/

۲۵. این طرح در جلسهٔ علنی مورخ ۱۴۰۰/۰۶/۲۴ مجلس شورای اسلامی اعلام وصول گردیده است.

۲۶ . مهدی شهیدی، *حقوق مدنی ۳ تعهدات*، (تهران: نشر مجد، چ ۲۴، ۱۳۹۹)، ص ۵۵.

۲۷. سعید حبیبا و مهدیس لطفی، «مطالعهٔ تطبیقی ممنوعیت طراحی فریب‌کارانه در فضای دیجیتال در حقوق مصرف‌کننده و حقوق رقابت در ایران، اتحادیهٔ اروپا و ایالات متحدهٔ امریکا»، *حقوق تطبیقی معاصر*، ش ۴۰ (۱۴۰۴)، ص ۴۰.

28. RTM v Bonne Terre Ltd and Hestview Ltd [2026]

در بانکداری سنتی مشتریان جهت استفاده از خدمات بانکی، علی‌الاصول با درج امضای خود به صورت کتبی یا دیجیتال رضایت خود را ابراز می‌کنند. برای مثال، مشتریان در انتقال وجه به صورت ساتنا با تکمیل نمودن فرم کاغذی و امضای آن، رضایت خود مبنی بر انتقال وجه را به‌صراحت تأیید می‌کنند.

حتی در انتقال وجه از طریق عابر بانک نیز مشتریان با وارد نمودن رمز کارت، به نوعی امضای خود را درج و اعلان رضایت می‌نمایند. در این موارد رضایت برای پردازش داده‌ها از سوی بانک، صرفا در چارچوب نقل و انتقال وجه داده شده است[۲۹].

با این حال، بسیاری از سامانه‌های هوش مصنوعی به‌گونه‌ای طراحی شده‌اند که در طول زمان، از داده‌های موجود برای توسعهٔ قابلیت‌های جدید، بهبود مدل‌ها یا استخراج الگوهای تازه استفاده می‌کنند. بنابراین امکان تعیین تمام اهداف پردازش در زمان أخذ رضایت کاهش می‌یابد.

چنین وضعیتی به نقض اصل آگاهانه بودن رضایت منجر می‌شود، زیرا در زمان اعلام رضایت، مشتری از تمامی پردازش‌های آینده و اهداف احتمالی آن آگاهی کامل و کافی ندارد و رضایت جهت انجام این قبیل اقدامات از سوی او داده نشده است. همچنین اگر بانک رضایت وی را به صورت کلی برای پردازش تمام داده‌ها با اهداف متفاوت أخذ نماید، این رضایت بلااثر خواهد بود، زیرا بایستی میان اهداف پردازش قائل به تفکیک شد و رضایت کلی و ناآگاهانه طبق بند ۲ مادهٔ ۷ مقررات عمومی حفاظت از داده‌های انگلستان و مادهٔ ۱۹۹ قانون مدنی، باطل تلقی می‌گردد.

در نهایت بانک با محدودیت عملی جهت أخذ رضایت برای پردازش داده‌ها مواجه می‌شود. بر این اساس، پیشنهاد می‌شود بانک‌ها برای هریک از اهداف مستقل پردازش هوش مصنوعی، رضایت جداگانه و مشخصی را از مشتریان أخذ کنند و از ابتدا برای هوش مصنوعی محدودیت‌هایی را اِعمال و قیودی را مشخص نمایند تا داده‌های مشتریان صرفاً برای هدف موردنظر مشتری پردازش گردد. این امر تا حد زیادی سبب جلوگیری از بروز اختلافات و طرح دعاوی در آینده می‌شود.

۲۹. محسن صادقی، *تقریرات درس بانکداری مجازی و ابعاد حقوقی آن*، دانشگاه تهران، ۱۴۰۴.

۲.۲. شفافیت پردازش داده‌ها

شفافیت پردازش به این معناست که اشخاص آگاه باشند که داده‌های شخصی آن‌ها چرا و چگونه پردازش می‌شود؛ چه داده‌هایی پردازش می‌شوند، این داده‌ها با چه اشخاص یا نهادهایی به اشتراک گذاشته شده و تا چه مدت نگهداری خواهند شد. از این منظر، شفافیت به‌عنوان یک هدف مستقل، نه صرفاً یک وسیله، اهمیت اساسی دارد[۳۰].

در بند ۱ مادۀ ۵ و بند ۱ مادۀ ۱۲ مقررات عمومی حفاظت از داده‌های انگلستان، اطلاع‌رسانی مرتبط با پردازش داده‌ها باید شفاف انجام شود. بانک باید اطلاعاتی مانند هویت و مشخصات خود، اهداف پردازش، مبنای قانونی پردازش و... و آثار آن را به زبانی ساده و قابل فهم در اختیار مشتریان قرار دهد. بنابراین، ارائۀ اطلاعات به زبان فنی یا تخصصی، خلاف اصل شفافیت تلقی می‌شود[۳۱].

در قوانین ایران، در بند «الف» مادۀ ۵۹ قانون تجارت الکترونیک به‌طور ضمنی به این اصل اشاره شده است و طبق آن، داده‌پیام باید به‌طور واضح شرح داده شود، اما همچنان معیار دقیقی در خصوص آن وجود ندارد.

در بانکداری سنتی معمولاً مبنای پردازش داده‌ها شفاف است؛ برای مثال، بانک‌ها طبق مادۀ ۱۶۹ مکرر قانون مالیات‌های مستقیم اصلاحی ۱۳۹۴، باید گردش حساب مشتریان را جهت تعیین مالیات اشخاص، در اختیار سازمان امور مالیاتی قرار دهند. این امر مطابق با قانون بوده، مشتریان نیز در این باره آگاه فرض می‌شوند.

با این حال، مدل‌های مبتنی بر یادگیری عمیق هوش مصنوعی موسوم به جعبۀ سیاه[۳۲]، عملکردی غیرشفاف دارند و حتی برای طراحانشان نیز غیرقابل تفسیر و توضیح باقی می‌مانند[۳۳].

30. Naudts, L., Dewitte, P., and Ausloos, J. (2022*), "Meaningful Transparency through Data Rights: A Multidimensional Analysis"*, in Kosta, E., Leenes, R., and Kamara, I. (eds.), Research Handbook on EU Data Protection. Edward Elgar Publishing. p. 8.
31. Carey, P. (2018), *Data Protection: A Practical Guide to UK and EU Law*. 5th Edition. Oxford University Press. p. 44.
32. Black Box
33. P. Hacker, J. Cordes and J. Rochon, "*Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond,"* European Journal of Risk Regulation, 2024, p. 108.

این امر باعث می‌شود مشتریان بانک از منطق پردازش، معیارهای تصمیم‌گیری، نوع داده‌های مورد استفاده، اشخاص ثالث دریافت‌کنندهٔ داده‌ها و نحوهٔ استفادهٔ ثانویه از اطلاعات خود آگاهی کافی نداشته باشند، زیرا تنها ورودی و خروجی داده‌ها مشخص است.

رأی دادگاه تجدیدنظر انگلستان در پروندهٔ *بریجز علیه رئیس پلیس ولز جنوبی*[۳۴] نشان می‌دهد که شفافیت و قانونی بودن پردازش داده‌های شخصی، مستلزم وجود چارچوبی روشن، قابل پیش‌بینی و محدودکنندهٔ اختیارات نهاد پردازش‌کننده است؛ به نحوی که مشخص باشد چه فناوری در چه مکان‌هایی به‌کار می‌رود و اشخاص موضوع داده بتوانند به‌طور مؤثر از نحوهٔ پردازش داده‌های زیستی خود آگاه شوند.

بنابراین، مشتریان بانک باید بدانند که هرگونه تعامل با فناوری‌های نوین، حتی اگر به‌نظر بی‌ضرر باشد، می‌تواند داده‌هایی تولید کند که در آینده علیه آن‌ها استفاده شود. از این رو، بانک‌ها باید اطلاعات مربوط به اهداف پردازش، نوع داده‌های پردازش‌شده، میزان اتکای تصمیمات به سامانه‌های هوش مصنوعی، پیامدهای احتمالی تصمیمات خودکار و مدت نگهداری داده‌ها را به زبانی ساده، روشن و قابل فهم در اختیار مشتریان قرار دهند.

همچنین بانک‌ها باید حدود و ضوابط پردازش از سوی سامانه‌های هوش مصنوعی را به‌گونه‌ای تعیین کنند که داده‌ها صرفاً در موارد مقرر قانونی در اختیار اشخاص یا نهادهای ثالث قرار گیرد. بنابراین مناسب است بانک‌ها از هوش مصنوعی قابل توضیح[۳۵] استفاده نمایند[۳۶] تا اصل شفافیت در محیط بانکداری مبتنی بر هوش مصنوعی به‌طور مؤثر محقق شود.

۳.۲. دقیق و به‌روز بودن داده‌ها

این اصل به اهمیت دقت و صحت اطلاعات اشاره دارد و تضمین می‌کند داده‌های پردازش‌شده و مورداستفاده برای هدف مشخص و دقیق، صحیح و به‌روز است[۳۷]. دقیق بودن

34. Bridges v Chief Constable of South Wales Police EWCA Civ 1058.

۳۵. با درنظر گرفتن مخاطب، هوش مصنوعی قابل توضیح سیستمی است که جزئیات یا دلایلی ارائه می‌دهد تا نحوهٔ عملکرد آن روشن یا به‌سادگی قابل درک شود.

36. P. Weber, K. V. Carl and O. Hinz, *"Applications of Explainable Artificial Intelligence in Finance-A Systematic Review of Finance, Information Systems, and Computer Science Literature," Management Review Quarterly*, No. 2, (2024), p. 868.

۳۷. کامبیز فاطمی، «رویکردهای نظری حاکم بر تعیین قلمرو حریم خصوصی و تاثیر آن بر اصول حاکم بر حریم خصوصی فضای دیجیتال»، *پژوهش‌های حقوقی*، قابل انتشار در دورهٔ ۲۳ شماره ۶۰.

اطلاعات به معنای ذخیرهٔ کامل، بدون خطا و عدم وجود دادهٔ نادرست است و به‌روز بودن به معنای ثبت فوری اطلاعات جدید در جایی است که تغییراتی در داده‌ها رخ می‌دهد.

طبق بند ۴ مادهٔ ۵ مقررات عمومی حفاظت از داده‌های انگلستان، داده‌های شخصی باید دقیق بوده، در صورت لزوم، به‌روز نگه داشته شوند. همچنین طبق مادهٔ ۱۶ مقررات پیش‌گفته، شخص موضوع داده حق دارد از بانک بخواهد که بدون تأخیر غیرضروری، داده‌های شخصی نادرست مربوط به وی را اصلاح کند و با توجه به اهداف پردازش، مشتری حق دارد داده‌های شخصی ناقص خود را تکمیل نماید.

در حقوق ایران، مطابق بند «ج» مادهٔ ۵۹ قانون تجارت الکترونیکی، داده‌پیام‌های شخصی باید صحیح و روزآمد باشند. همچنین بند «د» این ماده با اعطای حق اصلاح یا حذف داده‌پیام‌های ناقص و نادرست به اشخاص، تضمینی برای اجرای این اصل فراهم می‌کند.

در انگلستان طبق ماده ۱۲ مقررات عمومی حفاظت از داده‌ها، مهلت یکماه برای به‌روزرسانی و اصلاح داده‌ها پیش‌بینی شده است، امّا در حقوق ایران مدت زمانی برای این امر در نظر گرفته نشده و قانون‌گذار صرفاً به انجام به‌روزرسانی توجّه داشته است. بنابراین به نظر نگارندگان اصل بر فوری بودن است و بر همین اساس اگر در یک روز مشخص چندین مرتبه داده‌های شخص تغییر نماید، بانک‌ها موظف به انجام به‌روزرسانی هستند. همچنین با اینکه در قانون حق اصلاح و یا حذف داده‌های نادرست برای اشخاص پیش‌بینی شده است، وجود این حق نافی وظایف بانک نخواهد بود و بانک باید رأساً و بدون درخواست مشتری نیز داده‌ها را به‌روزرسانی و اصلاح نماید.

با این حال استثنایی بر اصل یاشده حاکم است. برای مثال، نگهداری سوابق یک شخص در سازمان‌هایی مانند ادارات مالیاتی، دادگستری و... امری است که می‌تواند به‌منزلهٔ استثنایی بر حکم کلی این نتیجه تلقی گردد. دلیل این موضوع نیز روشن است، سازمان‌هایی مانند دادگستری برای رسیدگی به پرونده‌های خود نیازمند دسترسی به سوابق اشخاص‌اند تا با اطلاع از اطلاعات پیشین آن‌ها، امکان حل و فصل امور قضایی برای آن‌ها میسر باشد[۳۸].

۳۸. ابوطالب کوشا و همکاران، «اصول حاکم بر پردازش داده‌پیام‌های شخصی در شبکه‌های تبادل اطلاعات»، *تعالی حقوق*، ش۲ (۱۴۰۳)، ص ۲۸۸.

با این همه، هوش مصنوعی اساساً بر داده متکی است و حیات و کارآمدی آن به دسترسی به داده وابسته است[۳۹]. داده‌های بانکی علی‌الاصول وضعیت اقتصادی شخص را معین نموده، معمولاً به صورت مداوم در حال تغییر هستند. هوش مصنوعی بانکی با ذخیره و تحلیل این داده‌های گوناگون در کنار داده‌های جدید ممکن است در تصمیم‌گیری به دلیل دسترسی هم‌زمان به اطلاعات منسوخ، دچار خطا و یا سوگیری شود و به همین دلیل اشخاص را از منافعی مانند دریافت تسهیلات محروم سازد. بنابراین، مناسب است بانک‌ها فوراً اطلاعات را اصلاح و به‌روز نمایند، زیرا عدم انجام این کار باعث تداوم تصمیم‌گیری بر مبنای داده‌های نادرست می‌شود که این امر مبتنی بر خطای[۴۰] هوش مصنوعی نخواهد بود.

رأی دادگاه تجدیدنظر انگلستان در پروندهٔ *سمیتون علیه اکویفکس*[۴۱] نیز اهمیت دقت و به‌روز بودن داده‌های شخصی را نشان می‌دهد. در این پرونده، شرکت اعتبارسنجی اکویفکس در پروندهٔ *اعتباری آقای سمیتون* همچنان وی را ورشکسته معرفی می‌کرد، درحالی که حکم ورشکستگی او پیش‌تر ازسوی دادگاه نقض شده بود.

آقای سمیتون مدعی شد که این اطلاعات نادرست موجب ردّ درخواست‌های اعتباری و ورود خسارت به وی شده است. هرچند دادگاه اعلام کرد که اکویفکس اقدامات معقول لازم برای حفظ دقت اطلاعات را انجام داده و مسئولیتی متوجه آن نیست، اما پرونده نشان داد که وجود داده‌های نادرست یا به‌روزرسانی‌نشده می‌تواند بر تصمیمات اعتباری و مالی اشخاص تأثیر مستقیم بگذارد.

در صورت عدم رعایت اصل دقت، مادهٔ ۷۱ قانون تجارت الکترونیک ضمانت اجرای جزایی پیش‌بینی نموده است و طبق مادهٔ ۷۹ مقررات عمومی حفاظت از داده‌ها و ماده ۸۲ قانون حفاظت از داده‌های انگلستان، مشتری می‌تواند علیه کنترلگر یا پردازشگر طرح دعوی نماید.

39. L. H. Prevignano, "The Impact of AI on the Law: Rethinking the Public-Private Dichotomy in the Age of Algorithms," *Retskraft – Copenhagen Journal of Legal Studies*, No. 1, (2021), p. 67.

۴۰. لفظ خطا برای هوش مصنوعی به‌کار می‌رود، زیرا ممکن است هوش مصنوعی مرتکب خطای فنی (error) شود. اما برای انسان لفظ اشتباه به‌کار می‌رود، زیرا اشتباه ناشی از تصمیمات انسانی است.

41. Smeaton v Equifax plc [2013] EWCA Civ 108

٤.٢. محرمانگی داده‌ها

محرمانه در لغت به معنای مخفیانه، پنهانی و پوشیده است[۴۲]. داده‌های محرمانه نیز داده‌هایی هستند که به صورت پنهانی و دور از دسترس عمومی نگهداری می‌شوند و انتشار یا افشای آن‌ها ممنوع است.

بانک‌ها فهرست‌ها و سوابقی را نگهداری می‌کنند که اطلاعات مربوط به حساب‌ها و سایر امور مالی مشتریان را دربر دارد. این اطلاعات اصولاً محرمانه بوده، در شرایط عادی نباید افشا شوند[۴۳]. طبق بند ۶ مادۀ ۵ مقررات عمومی حفاظت از داده‌های انگلستان[۴۴]، بانک‌ها باید داده‌ها را را به نحوی پردازش کنند که امنیتِ مناسبِ داده‌های شخصی تضمین شود، ازجمله حمایت در برابر پردازشِ غیرمجاز یا غیرقانونی و نیز ازدست رفتن، نابودی یا آسیبِ اتفاقی، با استفاده از تدابیر فنی یا سازمانیِ مقتضی، که این همان اصل محرمانگی است.

در قوانین ایران تعریفی از محرمانگی داده‌ها ارائه نشده، اما در مواد ۵۸، ۵۹، ۶۱ و ۷۱ قانون تجارت الکترونیک این اصل به‌طور ضمنی پیش‌بینی شده و در مواد ۴، ۵ و ۶ قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱، بر تکلیف دستگاه‌ها مبنی بر حفظ امنیت و محرمانگی داده‌ها تأکید شده است.

با این حال، بانک برای استفاده از هوش مصنوعی باید داده‌هایی را در اختیار آن بگذارد و همین امر به نقض اصل محرمانگی داده‌ها منجر می‌شود؛ زیرا هوش مصنوعی به حجم گسترده‌ای از داده‌های مشتریان، ازجمله اطلاعات هویتی، سوابق تراکنش‌ها، وضعیت مالی، الگوهای رفتاری و اعتباری دسترسی دارد و قادر به بازتولید اطلاعات است.

به نظر نگارندگان، شایسته است بانک‌ها برای هوش مصنوعی چارچوبی معین نمایند تا عملکرد هوش مصنوعی منطبق با آن باشد و به این ترتیب، از دسترسی به تمام داده‌های

۴۲. حسن عمید، *فرهنگ فارسی*، (تهران: انتشارات اشجع، چ ۲، ۱۳۸۹)، ص ۱۶۴۲.

43. A. A. Lytvynenko, *"Data Privacy and Banking Secrecy: Topical Issues in Commonwealth, Continental Europe and International Jurisprudence," Athens Journal of Law*, No. 3, (2019), p. 304.

44. Article 5, Personal Data Shall be: (f) Processed in a Manner that Ensures Appropriate Security of the Personal Data, Including Protection Against Unauthorised or Unlawful Processing and Against Accidental Loss, Destruction or Damage, Using Appropriate Technical or Organisational Measures ('Integrity and Confidentiality').

محرمانه جلوگیری شود؛ با این همه، حتی در فرض عملکرد صحیح و و عدم خروج از چارچوب، بازهم این اصل می‌تواند نقض شود، زیرا ممکن است هوش مصنوعی دچار اختلال شده یا هک شود و از این طریق داده‌های اشخاص افشا گردد. با توجه به مادۀ ۱۸ قانون تجارت الکترونیک، در فرض اخیر بانک مسئول افشای داده‌ها خواهد بود، زیرا هوش مصنوعی ابزار تحت کنترل بانک محسوب می‌شود[۴۵].

رای دادگاه تجدیدنظر انگلستان در *دعوی تورنیه علیه بانک ملی ایالتی و اتحادیه انگلستان*[۴۶] که جزء مبانی حقوق کامن‌لا به‌شمار می‌رود همسو با نظر پیش‌گفته است. این رای بیان می‌کند تعهد محرمانگی بانکدار نسبت به مشتری به عنوان یک شرط ضمنی در قرارداد بانکی شناخته می‌شود. در نتیجه، با توجه به قواعد عام مسئولیت و تکلیف بانک به حفظ محرمانگی داده‌های مشتری، به‌نظر می‌رسد به‌کارگیری هوش مصنوعی از دامنۀ این تعهد خارج نیست و بانک همچنان مسئول تضمین محرمانگی و عدم افشای داده‌های شخصی خواهد بود. در نتیجه، تعهد محرمانگی بانک ماهیتی مستمر دارد و استفاده از فناوری‌های نوین، ازجمله هوش مصنوعی، موجب زوال یا کاهش این تعهد نمی‌شود.

۳. تأثیر هوش مصنوعی بر حقوق مشتریان بانک

داده‌ها از ارزشمندترین دارایی‌های عصر دیجیتال هستند که چه به صورت تجمیع‌شده و چه به شکل مجزا، معنادار، قیمتی و راهبردی‌اند[۴۷]. مشتریان بانک‌ها نسبت به داده‌های خود دارای حقوقی هستند. هوش مصنوعی با وجود مزایای فراوان، می‌تواند بر اِعمال هریک از این حقوق تأثیر بگذارد و در برخی موارد مانند حق انتقال‌پذیری داده‌ها، حق محدودسازی پردازش داده‌ها، حق فراموشی داده‌ها و حق اعتراض به تصمیمات خودکار، اِعمال این حقوق را در عمل دشوار نماید. بر این اساس، در ادامه به بررسی تأثیر هوش مصنوعی بر حقوق مشتریان در دو نظام حقوقی می‌پردازیم.

---

۴۵. با وحدت ملاک از مادۀ ۷ قانون مسئولیت مدنی نیز می‌توان دریافت که عنصر نظارت و کنترل مهم‌تر از عنصر تصمیم‌گیری است.

46. Tournier v National Provincial and Union Bank of England [1924] 1 KB 462 (CA).

۴۷. عباس میرشکاری و همکاران، «تراست داده، سازوکاری برای مدیریت منافع ذی‌نفعان داده؛ رهنمودهایی برای نظام داده در حقوق ایران»، *حقوق تطبیقی معاصر*، ش ۳۴ (۱۴۰۳)، ص ۲۸۰.

۱.۳. حق انتقال‌پذیری داده‌ها

حق انتقال داده‌ها به اشخاص این امکان را می‌دهد که داده‌های شخصی خود را برای اهداف شخصی خود در سرویس‌های مختلف به‌دست آورند و دوباره از آن‌ها استفاده کنند. این حق به آن‌ها اجازه می‌دهد تا داده‌های شخصی خود را به‌راحتی از یک محیط فناوری اطلاعات به محیط دیگر به روشی ایمن و مطمئن، بدون تأثیر بر قابلیت استفادهٔ آن، کپی یا منتقل کنند. برخی این حق را در واقع بیشتر یک حق مصرف‌کننده می‌دانند[۴۸].

طبق مادهٔ ۲۰ مقررات عمومی حفاظت از داده‌های انگلستان و با رعایت شرایط مندرج در آن، مشتری بانک مالک کنترل بر داده‌های بانکی خود است و علی‌الاصول می‌تواند آن‌ها را برای استفاده نزد ارائه‌دهندهٔ دیگر خدمات مالی منتقل کند.

در ایران قانون مستقلی در این زمینه وجود ندارد و در قوانین پراکندهٔ موجود نیز تنها به حفاظت از داده‌های شخصی اشاره شده[۴۹] و چنین حقی در قوانین به‌صراحت پیش‌بینی نشده است. با توجه به اهمیت ویژهٔ این حق به‌عنوان یکی از حقوق شهروندی و جنبه‌ای از حقوق بشر، پیشنهاد می‌شود قانون‌گذار در ایران چارچوب مستقلی در این زمینه پیش‌بینی نماید.

در بانکداری سنتی، داده‌های مشتری عمدتاً به صورت داده‌های خام و قابل انتقال در اختیار بانک قرار می‌گیرد و اِعمال حق انتقال‌پذیری معمولاً با دشواری خاصی مواجه نیست. با این حال، سامانه‌های هوش مصنوعی از طیف گسترده‌ای از داده‌های شخصی استفاده می‌کنند که می‌توان آن‌ها را به طور کلی به داده‌های صریح و ضمنی تقسیم کرد.

داده‌های صریح شامل اطلاعاتی مانند نام، نشانی ایمیل و اطلاعات پرداخت است که مستقیماً از سوی کاربران ارائه می‌شود. داده‌های ضمنی به اطلاعاتی مانند عادت‌های مرور، سابقهٔ خرید و تعاملات با بسترهای آنلاین اشاره دارد که از رفتار مشتریان استنباط می‌شود. افزون بر این، سامانه‌های هوش مصنوعی اغلب داده‌های شخصی حساس، ازجمله سوابق

48. Li, W. (2022), *"Between Incrementalism and Revolution: How the GDPR Right to Data Portability Is Revamped by the EU and the UK Post Brexit,"* in Kosta, E., Leenes, R., and Kamara, I. (eds.), Research Handbook on EU Data Protection Law. Edward Elgar Publishing. p. 2.

۴۹. مهدیه لطیف‌زاده و سید محمدمهدی قبولی درافشان، «چگونگی انتقال بین‌المللی داده‌های شخصی»، *پژوهشنامه حقوق تطبیقی*، ش ۱ (۱۴۰۱)، ص ۲۲۱.

سلامت، اطلاعات زیست‌سنجی و داده‌های مکانی را نیز پردازش می‌کنند.[۵۰]

بنابراین، هوش مصنوعی بانکی داده‌های اولیهٔ مشتریان را پردازش کرده، از آن‌ها داده‌های جدید و مشتق، مانند پروفایل‌های رفتاری، امتیازهای اعتباری، ارزیابی ریسک و سایر داده‌های استنباطی را تولید می‌کند. مطابق مادهٔ ۲۰ مقررات عمومی حفاظت از داده‌های انگلستان و راهنمای رسمی ادارهٔ کمیسر اطلاعات انگلستان[۵۱]، حق انتقال‌پذیری صرفاً شامل داده‌های شخصی ارائه‌شده از سوی موضوع داده و داده‌های حاصل از مشاهدهٔ فعالیت‌های وی است و داده‌هایی را که کنترل‌کننده بر مبنای آن‌ها ایجاد یا استنتاج کرده است، دربر نمی‌گیرد[۵۲].

از این رو، خروجی‌های هوش مصنوعی، ازجمله پروفایل‌های کاربری، پیش‌بینی‌ها، طبقه‌بندی‌ها و امتیازهای اعتباری، اصولاً مشمول حق انتقال‌پذیری نیستند. این امر موجب می‌شود بخش قابل‌توجهی از ارزش اقتصادی داده‌های تولیدشده در سامانه‌های هوش مصنوعی بانکی خارج از قلمرو این حق قرار گیرند و در نتیجه، اثربخشی عملی حق انتقال‌پذیری داده در بانکداری مبتنی بر هوش مصنوعی کاهش یابد.

بنابراین، پیشنهاد می‌شود در قوانین یا دستورالعمل‌های بانکی، مصادیقی برای دامنهٔ این حق تعیین گردد تا حدود و قلمرو حق انتقال‌پذیری در خصوص داده‌های پردازش‌شده و داده‌های استنباطی ناشی از سامانه‌های هوش مصنوعی به‌طور شفاف مشخص شود و از بروز اختلاف میان مشتریان و بانک‌ها دربارهٔ قابلیت انتقال این دسته از داده‌ها جلوگیری گردد.

۲.۳. حق محدودسازی پردازش داده‌ها

محدودیت در پردازش داده‌ها، همان‌گونه که از عنوان آن پیداست به معنای ایجاد محدودیت در پردازش اطلاعات است تا داده‌های موجود در چارچوب اهداف تعیین‌شده پردازش شوند.

مادهٔ ۱۸ مقررات عمومی حفاظت از داده‌های انگلستان، در شرایط معین، به اشخاص حق

50. B. B. Atata, *"Artificial Intelligence and the Right to be Forgotten," International Journal of Research Publication and Reviews*, 2024, p. 4303.
51. The Information Commissioner's Office (ICO)
52. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/?

محدودسازی پردازش داده‌های شخصی را اعطا می‌کند. این حق به فرد امکان می‌دهد نحوهٔ استفادهٔ بانک از داده‌های شخصی او را محدود کند.

این حق، جایگزینی برای درخواست حذف داده‌های شخصی محسوب می‌شود. همچنین اشخاص زمانی از این حق برخوردارند که دلیل مشخصی برای درخواست این محدودیت داشته باشند؛ برای مثال، ممکن است نسبت به صحت اطلاعاتی که بانک دربارهٔ آنان نگهداری می‌کند یا نحوهٔ پردازش داده‌های شخصی اعتراض داشته باشند. در اغلب موارد، بانک موظف نیست این محدودیت را به‌طور دائمی اعمال کند، بلکه کافی است محدودیت برای مدت معینی برقرار شود.

به نظر نگارندگان، میان حق محدودسازی پردازش داده‌ها با حق اصلاح داده‌ها و حق اعتراض پردازش داده‌ها تمایز وجود دارد. بنابراین، اگر شخص درخواست اصلاح داده‌های نادرست خود را مطرح کند یا نسبت به پردازش داده‌ها اعتراض نماید، می‌تواند هم‌زمان درخواست کند تا زمان رسیدگی به درخواست، پردازش داده‌های وی نیز محدود شود.

در ایران حق مستقلی تحت عنوان حق محدودسازی پردازش داده‌های شخصی ولو در قوانین پراکندهٔ موجود به‌صراحت پیش‌بینی نشده است. با اینکه مادهٔ ۵۹ قانون تجارت الکترونیک مواردی همسو با فلسفهٔ ماده ۱۸ مقررات عمومی حفاظت از داده‌های انگلستان را پیش‌بینی کرده است، اما هیچ‌گونه سازوکار قانونی برای درخواست توقف موقت یا محدودسازی پردازش داده‌های شخصی ارائه نمی‌دهد و فقط به موارد محو یا اصلاح داده‌پیام‌های نادرست اشاره می‌کند.

بنابراین، شخص نمی‌تواند صرفاً به دلیل اعتراض به صحت داده‌ها یا مشروعیت پردازش، از بانک بخواهد تا زمان رسیدگی، پردازش داده‌های وی را متوقف یا محدود کند.

داده، سنگ بنای سامانه‌های هوش مصنوعی و یادگیری ماشین است. کارآمدی یک مدل هوش مصنوعی تا حد زیادی به کیفیت، کمیت و تنوع داده‌ای که بر اساس آن آموزش دیده است، بستگی دارد. در یادگیری ماشین، حجم زیادی از داده برای آموزش مدل‌ها جهت شناسایی الگوها، تصمیم‌گیری و بهبود عملکرد در گذر زمان لازم است. این داده‌ها اغلب شامل اطلاعات شخصی مانند رفتارهای کاربر، ترجیحات و... هستند[۵۳] که این فناوری پیچیده، مداوم در حال تجزیه و تحلیل آن‌ها بوده، خدمات بانکی نیز وابسته به این امر است.

53. Domingos, P. (2015), *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. Basic Books, New York. p. 11–16.

همچنین، هوش مصنوعی با جمع همهٔ داده‌ها در کنار هم در لحظه تصمیم‌گیری می‌کند و برخلاف بانکداری سنتی، داده‌ها به صورت جداگانه و پوشه‌ای نیستند که بتوان با درخواست محدودیت آن را سریعاً محدود یا متوقف نمود.

بنابراین در هوش مصنوعی علی‌الاصول داده‌ها از هم قابل تفکیک نیستند. در چنین شرایطی، اِعمال این حق مستلزم تفکیک دقیق انواع پردازش و تعیین این است که کدام بخش از استفاده از داده باید متوقف یا محدود گردد.

به همین دلیل، در عمل معمولاً امکان حذف یا توقف کامل استفاده از داده در همهٔ فرایندها وجود ندارد، اما می‌توان برخی کارکردها مانند پروفایل‌سازی را محدود کرد، درحالی که پردازش‌های ضروری مانند امنیت یا الزامات قانونی ممکن است ادامه یابد. از این رو، پیشنهاد می‌شود سامانه‌های هوش مصنوعی بانکی به‌گونه‌ای طراحی شوند که داده‌های مشتریان از ابتدا جدا یا علامت‌گذاری گردند تا با درخواست محدودسازی، این داده‌ها مجدداً مورد پردازش قرار نگیرند.

۳.۳. حق فراموشی داده‌ها

حق فراموش شدن[۵۴]، حقی مبتنی بر استقلال فردی و در ارتباط با حقِ داشتن نسبت به حذف اطلاعات شخصی در یک مقیاس زمانی است؛ مبنای دیگر این حق، غلبهٔ منافع شخصی بر منافع عمومی است[۵۵].

مادهٔ ۱۷ مقررات عمومی حفاظت از داده‌های انگلستان، حق حذف کامل داده‌ها را برای اشخاص ازجمله مشتریان بانک‌ها با رعایت شرایطی، پیش‌بینی نموده است. بر اساس این حق، در مواردی که ادامهٔ نگهداری یا پردازش داده فاقد مبنای قانونی باشد، شخص می‌تواند از بانک درخواست حذف داده‌های شخصی خود را بنماید.

در ایران نیز مانند سایر کشورها، اشخاص مالک داده‌هایی هستند که منتشر می‌کنند یا در اختیار نهادهایی مانند بانک می‌گذارند. با اینکه بند «ه» مادهٔ ۵۹ قانون تجارت الکترونیک به‌طور

54. Right to Erasure (“Right to be Forgotten”)

۵۵. سید محمدهادی قبولی درافشان و همکاران، «حق فراموش شدن در ترازو: نیاز ناشی از فضای مجازی یا تهدیدی برای آزادی بیان!؟»، *پژوهش حقوق عمومی*، ش ۵۸ (۱۳۹۷)، ص ۱۱۵.

ضمنی به حذف پروندهٔ رایانه‌ای اشاره نموده است، اما حقِ فراموش‌شدن در معنای امروزی مفهومی گسترده‌تر است و فقط به حذف یک پرونده در سامانه معطوف نمی‌شود.

متأسفانه تاکنون مراجع تقنینی به حق فراموش‌شدن توجه نکرده‌اند و حتی ادبیات حقوقی نیز با این مفهوم بیگانه است[۵۶]؛ فلذا عدم پذیرش و وضع قانون برای این حق می‌تواند سبب ورود ضررهای مادی و معنوی به اشخاص شود.

برخلاف سامانه‌های سنتی بانکی برای پردازش داده‌ها، سامانه‌های هوش مصنوعی اغلب غیرمتمرکز هستند و داده‌ها در چندین پلتفرم، مکان و حوزهٔ قضایی پردازش می‌شوند. این عدم تمرکز، شناسایی و حذف داده‌های مشخص بانکی را دشوار می‌سازد، به‌ویژه زمانی که داده برای آموزش مدل‌های یادگیری ماشین استفاده شده باشد. هنگامی که داده‌های شخصی مشتریان بانک وارد یک سامانهٔ هوش مصنوعی می‌شوند، بخشی از فرایند تصمیم‌گیری مدل می‌گردند و حذف آن‌ها بدون آسیب رساندن به عملکرد مدل، دشوار و حتی گاهی ناممکن است[۵۷].

در سامانه‌های هوش مصنوعی، داده‌ها غالباً در چندین نسخه تکثیر شده، در سامانه‌های مختلف، ازجمله سرورهای پشتیبان و فضای ذخیره‌سازی ابری، نگهداری می‌شوند. این امر اطمینان از حذف کامل داده‌ها را دشوار می‌سازد[۵۸]؛ بنابراین، تکثیر داده‌ها مانع اجرای کامل این حق می‌گردد.

به نظر نگارندگان، با توجه به روند سریع توسعهٔ فناوری‌های هوش مصنوعی بانکی، مناسب‌تر است که تعامل میان حق فراموشی و هوش مصنوعی در ابعاد حقوقی بازنگری شود و چارچوب حقوقی حاکم بر آن نیز به‌گونه‌ای ترسیم گردد که ضمن تضمین حمایت مؤثر از حق فراموشی داده‌ها که از حریم خصوصی اشخاص است، مانعی غیرضروری برای نوآوری و توسعهٔ فناوری ایجاد نکند.

---

۵۶. سیدقاسم زمانی و شیما عطار، «حقوق بشر و حق بر فراموش شدن در عصر فناوری‌های نوین اطلاعاتی»، *حقوقی بین‌المللی*، ش ۵۵ (۱۳۹۵)، ص ۱۰۲.

57. M. Ananny and K. Crawford, "*Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability,"* New Media & Society, 2018, p. 975–984.

58. M. Veale, R. Binns and L. Edwards, *"Algorithms that Remember: Model Inversion Attacks and Data Protection Law,"* Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, No. 2133, (2018), p. 9–10.

٤.٣. حق اعتراض به تصمیمات خودکار

اجازه به اشخاص جهت اعتراض به تصمیمات خودکار هوش مصنوعی که بـر وضـعیت آنـان تأثیر می‌گذارد، ابزاری سودمند برای حفاظت از حقوق و منافع آن‌ها است.

مادۀ ۲۲ مقررات عمومی حفاظت از داده‌های انگلستان در سه بخش، تعریف پردازش خودکار داده‌ها، شرایط و محدودیت‌های آن، و تضامین در این نوع تصمیم‌گیری را مشخص کرده اسـت. بنابراین بانک‌ها در فرض امکان تصمیم‌گیری خودکار طبق قسمت سوم مادۀ ۲۲، اولاً طبق مادۀ ۱۲ مقررات عمومی حفاظت از داده‌های انگلستان، لازم است این نوع تصمیم‌گیری را کتبی و در اسرع وقت به مشتریان اطلاع دهند و ثانیاً برای مشتریان حق اعتراض و توضیح[۵۹] درنظر بگیرند.

علاوه بر آن، این ماده بر امکان بررسی تصمیم از سوی عامل انسانی و امکان اعتراض مجدد و تجدیدنظرخواهی را برای مشتریان بانک تأکید نموده است.

در قوانین ایران ازجمله قانون تجارت الکترونیک و سایر قوانین معدود حـاکم بـر داده‌هـا، بـه موضوع تصمیم‌گیری خودکار از طریق هوش مصنوعی اشاره نشـده اسـت. ایـن مـوارد حقـوقی، خاص و جدید هستند که به برخورداری از آن‌ها، تعیین دامنه و چگونگی جریان آن‌ها باید به‌طـور ویژه اشاره شود[۶۰].

تنها در یک مورد خاص و در قانون مالیات‌های مستقیم، نشانی از این نـوع تصـمیم‌گیـری از سوی عامل غیرانسانی را می‌توان مشاهده کرد، بدون آنکه قانون‌گذار صراحتاً به اعمال این نـوع تصمیم‌گیری اشاره کرده باشـد؛ آن هـم بنـدهای ۲ و ۳ دسـتورالعمل تبصـرۀ مـادۀ ۱۰۰ قـانون مالیات‌های مستقیم برای مالیات‌های مقطوع سال ۱۴۰۱ که برای مؤدیان حق اعتراض به مالیات پیش‌بینی شده است[۶۱].

---

۵۹. طبق قسمت «الف» مادۀ ۱۲ مقررات عمومی حفاظت از داده‌های انگلستان، مهلت رسیدگی کنترل‌کننده به درخواست مشتری یک مـاه است.

۶۰. مهدیه لطیف‌زاده و همکاران، «حمایت از داده‌ی شخصی در حقوق اتحادیه اروپا و امکان سنجی آن در حقوق ایـران»، *مطالعـات حقـوق عمومی*، ش ۲ (۱۴۰۲)، ص ۹۹۹.

۶۱. زهرا عامری و همکاران، «حق اعتراض به تصمیم‌گیری‌های خودکار مبتنی بر هوش مصنوعی: جلوه‌ای از الزامات حقـوق بشـری عصـر فناوری»، *پژوهش‌های نوین حقوق اداری*، ش ۲۵ (۱۴۰۴)، ص ۵۵.

با این حال، تصمیمات مبتنی بر هوش مصنوعی معمولاً بر پایهٔ تحلیل حجم گسترده‌ای از داده‌ها و الگوریتم‌های پیچیده اتخاذ می‌شوند؛ از این رو، مشتری ممکن است از مبانی واقعی تصمیم و عوامل مؤثر در آن آگاهی کافی نداشته باشد. این امر می‌تواند امکان اعتراض مؤثر را کاهش دهد؛ زیرا شخص بدون اطلاع از دلایل تصمیم، قادر به ارائهٔ توضیحات یا دفاع مناسب از حقوق خود نخواهد بود.

از سوی دیگر، درصورتی که بازبینی اعتراض صرفاً به تأیید نتیجهٔ سامانه از سوی بانک محدود شود، حق اعتراض کارکرد حمایتی خود را ازدست خواهد داد. بنابراین، هرچه استفاده از هوش مصنوعی در تصمیمات بانکی افزایش یابد، ضرورت پیش‌بینی سازوکارهای مؤثر برای اعتراض، بازبینی انسانی واقعی و شفافیت در فرایند تصمیم‌گیری نیز بیشتر خواهد شد.

بنابراین قابلیت بازبینی در تصمیم‌گیری خودکار بر آشکار ساختن تمامی فرایند تصمیم‌گیری متمرکز است و چارچوبی حقوق‌محور، جامع، نظام‌مند و عملی برای پاسخگو ساختن معنادار سامانه‌های الگوریتمی ارائه می‌دهد[۶۲]. پیشنهاد می‌شود بانک‌ها از طریق سازوکارهای هدفمند ثبت سوابق و رویدادها، اطلاعاتی متناسب با زمینه فراهم آورند که امکان بازبینی و ارزیابیِ تصمیمات منفرد و نیز کل فرایند تصمیم‌گیری خودکار وجود داشته باشد.

نتیجه

مقالهٔ حاضر با هدف تحلیل حقوقی تأثیر هوش مصنوعی بر اصول حاکم بر پردازش داده‌های شخصی و حقوق اشخاص موضوع داده (مشتریان بانک‌ها) نگاشته شد. با اینکه استفاده از هوش مصنوعی در زمینهٔ بانکداری باعث افزایش سرعت، شفافیت و کارایی بیشتر نظام بانکی می‌شود، اما هم‌زمان چالش‌هایی را نیز ایجاد می‌کند. بررسی تطبیقی دو نظام حقوقی ایران و انگلستان نشان می‌دهد که نظام حقوقی انگلستان با اتکا بر قوانین و مقررات جامع حفاظت از داده‌ها، از یک سو اصول حاکم بر پردازش داده‌ها و شرایط آن، ازجمله اصل رضایت آگاهانه، شفافیت پردازش، دقیق و به‌روز بودن و محرمانگی داده‌ها را مشخص کرده و از سوی دیگر حقوق

62. Jennifer Cobbe, Michelle Seng Ah Lee and Jatinder Singh, *"Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems,"* Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21), Virtual Event, Canada, March 3–10, 2021, p. 602.

اشخاص موضوع داده، مانند حق انتقال‌پذیری، حق محدودسازی پردازش، حق فراموشی داده‌ها و حق اعتراض به تصمیمات خودکار را برای رعایت پردازش داده‌ها از سوی نهادهای مختلف ازجمله بانک‌ها پیش‌بینی نموده است. در مقابل، هرچند در حقوق ایران برخی اصول کلی مانند حفظ حریم خصوصی، محرمانگی اطلاعات، لزوم رعایت امنیت داده‌ها و حمایت از اطلاعات اشخاص در قوانین مختلف مورد توجه قرار گرفته‌اند، اما این مقررات پراکنده بوده، جامع و کافی نیستند.

با این همه، هوش مصنوعی با پردازش حجم گسترده و الگوریتمی داده‌ها، می‌تواند اصول حاکم بر پردازش داده‌های بانکی را نقض و اجرای حقوق مشتریان را دشوار و با موانعی مواجه سازد. از این رو، حمایت مؤثر از داده‌های شخصی بانکی در عصر هوش مصنوعی، مستلزم آن است که قواعد حقوقی علاوه بر حفظ کارآمدی فناوری، تضمین‌کنندهٔ حقوق بنیادین اشخاص نیز باشند.

با توجه به یافته‌های پژوهش، پیشنهاد می‌شود قانون‌گذار با بهره‌گیری و درنظر گرفتن تجارب کشورهای پیشرو در این زمینه، ازجمله انگلستان، در ابتدا نسبت به تدوین قوانین و مقررات منسجم و یکپارچهٔ حفاظت از داده‌های اشخاص اقدام نماید و ضمن تصریح حقوق اشخاص موضوع داده، سازوکارهای نظارتی مؤثر و الزامات شفافیت و پاسخگویی در پردازش‌های مبتنی بر هوش مصنوعی را پیش‌بینی نماید و سپس برای استفادهٔ هر نهاد از این فناوری، چارچوب هوش مصنوعی را با ویژگی‌های خاص برای هر نهاد، مانند بانک، در راستای تطبیق با اصول حاکم بر داده‌ها و حقوق مشتریان همان نهاد پیش‌بینی کند.

منابع و مآخذ

الف) منابع فارسی

کتاب‌ها

۱. ابوذری، مهرنوش (۱۴۰۲). ***حقوق و هوش مصنوعی***. تهران: میزان.

۲. شهیدی، مهدی (۱۳۹۹). ***حقوق مدنی ۳ تعهدات***. تهران: مجد.

۳. عمید، حسن، (۱۳۸۹). ***فرهنگ فارسی عمید***. تهران: اشجع.

مقالات

۴. عامری، زهرا؛ مقدسی، محمدباقر و حبیب‌نژاد، سید احمد (۱۴۰۴). حق اعتراض به تصمیم‌گیری‌های خودکار مبتنی بر هوش مصنوعی: جلوه‌ای از الزامات حقوق بشری عصر فناوری. ***پژوهش‌های نوین حقوق اداری،*** ۷ (۲۵)، ۳۷-۵۹.
Doi: 10.22034/MRAL.2024.2013708.1531

۵. فاطمی، کامبیز (۱۴۰۲). رویکردهای نظری حاکم بر تعیین قلمرو حق حریم خصوصی و تأثیر آن بر اصول حاکم بر حق حریم خصوصی در فضای دیجیتال. ***پژوهش‌های حقوقی***، پذیرفته‌شده و قابل انتشار، ۲۳ (۶۰). Doi: 10.48300/JLR.2024.431431.2526

۶. قبولی درافشان، سید محمدهادی؛ بختیاروند، مصطفی و آقامحمدی، اکرم (۱۳۹۷). حق فراموش شدن در ترازو: نیاز ناشی از فضای مجازی یا تهدیدی برای آزادی بیان؟!. ***پژوهش حقوق عمومی،*** ۱۹ (۵۸)، ۱۱۳-۱۳۵. Doi: 10.22054/QJPL.2018.15394.1361

۷. حبیبا، سعید و لطفی، مهدیس (۱۴۰۴). مطالعهٔ تطبیقی ممنوعیت طراحی فریب‌کارانه در فضای دیجیتال در حقوق مصرف‌کننده و حقوق رقابت در ایران. اتحادیهٔ اروپا و ایالات متحدهٔ امریکا. ***مطالعات حقوق تطبیقی معاصر،*** ۱۶ (۴۰)، ۳۳-۶۸.
Doi: 10.22034/LAW.2026.65180.3443

۸. زمانی، سیدقاسم و عطار، شیما (۱۳۹۵). حقوق بشر و حق بر فراموش‌شدن در عصر فناوری‌های نوین اطلاعاتی. ***حقوقی بین‌المللی،*** ۳۳ (۵۵)، ۸۱-۱۰۸.
Doi: 10.22066/CILAMAG.2016.23525

۹. لطیف‌زاده، مهدیه و قبولی درافشان، سید محمدمهدی (۱۴۰۱). چگونگی انتقال بین‌المللی داده‌های شخصی (مطالعهٔ تطبیقی در حقوق اتحادیهٔ اروپا و نظام حقوقی ایران). ***پژوهشنامهٔ حقوق تطبیقی***، ۶ (۱)، ۲۰۷-۲۳۰. Doi: 10.22080/LPS.2022.23212.1309

۱۰. لطیف‌زاده، مهدیه؛ قبولی درافشان، سید محمدمهدی؛ محسنی، سعید و عابدی، محمد (۱۴۰۲). حمایت از دادهٔ شخصی در حقوق اتحادیهٔ اروپا و امکان‌سنجی آن در نظام حقوقی ایران. ***مطالعات حقوق عمومی دانشگاه تهران***، ۵۳ (۲)، ۹۸۱-۱۰۰۵.
Doi: 10.22059/jplsq.2021.324694.2786

۱۱. 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)، ۲۷۹-۳۲۰. Doi: 10.22034/LAW.2024.56448.3268

۱۲. میرشکاری، عباس؛ عباس‌نیا، حامد و صفری، دریا (۱۴۰۴). مفهوم و مصادیق داده‌ی شخصی. ***حقوق فناوری‌های نوین***، ۶ (۱۲)، ۳۹۱-۴۱۰. Doi: 10.22133/mtlj.2025.452918.1321

۱۳. کوشا، ابوطالب؛ فرحزادی، علی‌اکبر و ناصر، مهدی (۱۴۰۳). اصول حقوقی حاکم بر پردازش داده‌پیام‌های شخصی در شبکه‌های تبادل اطلاعات. ***تعالی حقوق***، ۱۰ (۲)، ۲۵۵-۲۹۷.
Doi: 10.22034/thdad.2023.2009137.2533

تقریرات

۱۴. صادقی، محسن، «بانکداری مجازی و مسائل حقوقی آن»، گروه حقوق خصوصی و اسلامی، دانشگاه تهران، تهران، ایران، ۱۴۰۴.

قوانین و مقررات

۱۵. قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۸

۱۶. قانون مدنی مصوب ۱۳۰۷

۱۷. قانون مسئولیت مدنی مصوب ۱۳۳۹

۱۸. قانون تجارت الکترونیک مصوب ۱۳۸۲

۱۹. قانون جرایم رایانه‌ای مصوب ۱۳۸۸

۲۰. قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱

۲۱. منشور حقوق شهروندی مصوب ۱۳۹۵

۲۲. سند ملی هوش مصنوعی جمهوری اسلامی ایران مصوب ۱۴۰۳

۲۳. دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوهٔ جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی مصوب ۱۴۰۲

ب) منابع انگلیسی

Books

24. Carey, Peter (2018). ***Data Protection: A Practical Guide to UK and EU Law***. Oxford: Oxford University Press.

25. Domingos, Pedro (2015). ***The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World***. New York: Basic Books.

26. Gutwirth, Serge, Poullet, Yves, De Hert, Paul, De Terwangne, Cecile and Nouwt, Sjaak (2009). ***Reinventing Data Protection?*** Dordrecht: Springer.

27. Li, Wenlong (2022). ***Between Incrementalism and Revolution: How the GDPR Right to Data Portability Is Revamped by the EU and the UK Post Brexit. In Kosta, E., Leenes, R., and Kamara, I. (Eds.),*** Research Handbook on EU Data Protection Law. Cheltenham: Edward Elgar Publishing.

28. Naudts, Laurens, Dewitte, Pierre and Ausloos, Jef (2022). ***Meaningful Transparency through Data Rights: A Multidimensional Analysis. In Kosta, E., Leenes, R., and Kamara, I. (Eds.),*** Research Handbook on EU Data Protection Law. Cheltenham: Edward Elgar Publishing.

Articles

29. Ananny, Mike and Crawford, Kate (2018). Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability. ***New Media & Society,*** 20 (3), 973-989.

30. Atata, Bashirat Bukola (2024). Artificial Intelligence and the Right to be Forgotten. ***International Journal of Research Publication and Reviews,*** 5 (8), 4300-4310.

31. Cobbe, Jennifer, Lee, Michelle Seng Ah and Singh, Jatinder (2021). Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems. ***Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21),*** 598–609.

32. Fares, Omar H, Butt, Irfan and Lee, Seung Hwan Mark (2023). Utilization of Artificial Intelligence in the Banking Sector: A Systematic Literature Review. ***Journal of Financial Services Marketing,*** 28(4), 835–852.

33. Hacker, Philipp, Cordes, Johann and Rochon, Janina (2024). Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond. ***European Journal of Risk Regulation,*** 15(1), 49-86.

34. Lytvynenko, Anatoliy A. (2019). Data Privacy and Banking Secrecy: Topical Issues in Commonwealth, Continental Europe and International Jurisprudence. ***Athens Journal of Law,*** 5(3), 303–322.

35. Prevignano, Laure Helene (2021). The Impact of AI on the Law: Rethinking the Public-Private Dichotomy in the Age of Algorithms. ***Retskraft – Copenhagen Journal of Legal Studies,*** 5(1), 59–76.

36. Veale, Michael, Binns, Reuben and Edwards, Lilian (2018). Algorithms that Remember: Model Inversion Attacks and Data Protection Law. ***Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences,*** 376(20180083), 1-15.

37. Weber, Patrick, Carl, K. Valerie and Hinz, Oliver (2024). Applications of Explainable Artificial Intelligence in Finance—A Systematic Review of Finance, Information Systems, and Computer Science Literature. ***Management Review Quarterly,*** 74, 867–907.

Thesis

38. Tumma, Vijaya S (2024). ***Exploring Factors that Influence Artificial Intelligence Adoption in Banks and Credit Unions.*** Tampa: University of South Florida.

Documents

39. Bank for International Settlements. (2024). Regulating AI in the Financial Sector: Recent Developments and Main Challenges. FSI Insights on Policy Implementation, No. 63. Basel: Bank for International Settlements.
40. Radia, S. (2014). Informed Consent. London: CFA UK.

Foreign Case Law

41. Bridges v Chief Constable of South Wales Police EWCA Civ 1058.
42. Dana Turner, et al. v. Nuance Communications, Inc., United States District Court, Northern District of California, 28 May 2024.
43. RTM v Bonne Terre Ltd and Hestview Ltd [2026]
44. Smeaton v Equifax plc [2013] EWCA Civ 108
45. Tournier v National Provincial and Union Bank of England [1924] 1 KB 462 (CA).

Rules and Regulations

46. Data Protection Act 2018 (UK)
47. United Kingdom General Data Protection Regulation (UK GDPR).

Websites

48. https://ico.org.uk/for-organisations/uk-gdpr-guidance-andresources/-individual-rights/individual-rights/right-to-data-portability/?