اهمیت و چالش‌های حقوقی مستعارسازی داده‌ها؛ با نگاهی به اصول پردازش داده‌های شخصی

امیرمحمد قربان‌نیا*
زهرا شاکری**

تاریخ دریافت: ۱۴۰۳/۰۹/۰۳ تاریخ پذیرش: ۱۴۰۴/۰۲/۰۲

چکیده

در تمام کشورها و در قوانین حمایت از داده‌های شخصی، به‌دلیل گسترش حجم پردازش داده‌ها توسط شرکت‌های مختلف، اصول خاصی مثل اصل مشروعیت، صحت و امنیت، محدودیت هدف و کمینه‌سازی، پیش‌بینی شده است تا نقض حریم داده‌های شخصی به حداقل برسد. علاوه‌بر این در اسناد مذکور، به برخی روش‌های فنی نیز برای پردازش امن داده‌های شخصی، ازجمله مستعارسازی داده‌ها، اشاره شده است. باوجود این، به‌دلیل عدم پرداخت کافی به جزئیات این روش‌ها و ابزارها در قوانین کشورهای پیشرو یا سکوت قانون در کشورهایی مثل ایران، درمورد نحوه اجرای صحیح، آثار و کارکردها، ابعاد اقتصادی و نحوه نقش‌آفرینی فرایندهایی مانند مستعارسازی در جهت رعایت اصول پردازش داده‌های شخصی، ابهامات بسیاری وجود دارد. پژوهش حاضر با روش توصیفی-تحلیلی، با استفاده از منابع کتابخانه‌ای مکتوب و دیجیتال، ضمن بررسی روش‌های فنی و الزامات خاص انجام مستعارسازی به‌شکلی کارآمد، در تلاش برای پاسخ‌گویی به این سؤال اصلی خواهد بود که فرایند مذکور، چگونه و تا چه حد، با اجرای دقیق اصول قانونی پردازش داده‌ها مرتبط است؟ یافته‌های این نوشتار نشان‌دهنده این موضوع‌اند که مستعارسازی به‌رغم کاستن از پیوند مستقیم داده‌ها با زندگی شخصی و هویت افراد، به‌تنهایی برای رعایت اصول قانونی پردازش کافی نیست؛ به‌ویژه اگر با عدم رعایت موارد فنی، به‌نحوی قابل کدگشایی، انجام پذیرد؛ البته از ترکیب مستعارسازی با روش‌های دیگری مثل رمزگذاری داده‌ها، می‌توان از رعایت اصول پردازش، تا حد زیادی مطمئن شد.

کلید واژگان:

اصول پردازش داده‌ها، حریم خصوصی، داده‌های شخصی، مستعارسازی داده‌ها.

---

* کارشناس ارشد، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
** دانشیار، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران (نویسنده مسئول)
zshakeri@ut.ac.ir

مقدمه

داده‌های شخصی امروز به یکی از ارزشمندترین منابع اطلاعاتی بدل شده‌اند که در بسیاری از زمینه‌ها، ازجمله صنعت، بازار و امور مالی، آموزش، بهداشت عمومی و حتی تبلیغات، نقش‌های کلیدی ایفا می‌کنند. به‌دنبال این کارکردهای اکثراً تجاری و با افزایش حجم داده‌های شخصی جمع‌آوری و پردازش شده توسط شرکت‌ها، خطرات و تهدیدات امنیتی و نگرانی‌های مربوط به حریم خصوصی نیز به‌طور چشمگیری افزایش یافته و مسئله حفظ حریم داده‌های شخصی، به یکی از چالش‌های اساسی برای سازمان‌ها، دولت‌ها و کاربران تبدیل شده است.[۱] به‌طور خاص، یکی از ابزارهای مؤثر برای کاهش ریسک‌های ناشی از پردازش داده‌های شخصی، مستعارسازی[۲] داده‌هاست. این روش با کاستن از پیوند میان داده‌ها و هویت افراد موضوع داده، به عنوان یکی از تکنیک‌های حفاظت از اطلاعات، توانسته است توجه زیادی را در فرایندهای تحلیل داده‌ای، به خود جلب کند.[۳]

مستعارسازی به‌طور کلی به فرایندی اطلاق می‌شود که طی آن، داده‌های شخصی که از طریق آنها می‌توان به‌طور مستقیم افراد موضوع داده را شناسایی کرد، به‌گونه‌ای تغییر می‌کنند که اطلاعات هویتی از آنها جدا می‌شود و فقط با کمک یک نام مستعار مشخص و به‌شکل غیرمستقیم، به شناسایی اشخاص مرتبط می‌انجامد.[۴] توسعه و اجرای مستعارسازی به‌عنوان یک راهکار امنیتی، به شرکت‌ها و سازمان‌ها این امکان را می‌دهد که بدون افشای هویت افراد، به تحلیل یا انتشار داده‌ها بپردازند و ضمن کسب سود و مزیت تجاری، اصول اساسی پردازش داده‌های شخصی را نیز رعایت کنند. این اصول، ازجمله اصل مشروعیت، شفافیت، کمینه‌سازی، امنیت و محدودیت هدف، در بسیاری از قوانین و مقررات بین‌المللی، نظیر قانون حمایت از داده‌های شخصی اتحادیه اروپا و قوانین حمایت از حریم خصوصی اطلاعات شخصی در ایالات

---

۱. اسماعیلی، محسن و مهدی نریمان‌پور، «مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)»، *حقوق اسلامی*، د. ۲۱، ش. ۸۲، ۱۴۰۳، ص ۱۲۷.

2. Pseudonymization

3. ISO/IEC, "Privacy Enhancing Data De-Identification Terminology and Classification of Techniques", Available at: (https://www.iso.org/obp/ui/#iso:std:iso-iec:20889:ed-1:v1:en) Visited 2025/01/25.

4. El Emam, K and Jonker, E and Arbuckle, L and Malin, B. "A systematic review of re-identification attacks on health data", *PLoS One*, Vol. 6, No. 12, 2015, pp 1-2.

متحده به‌طور واضح بیان شده و از مستعارسازی نیز به‌عنوان یکی از ابزارهای کلیدی برای تطابق با این مقررات، نام برده شده است.

اگرچه مستعارسازی راهکاری حیاتی برای حفظ گمنامی افراد و حفظ حریم خصوصی ایشان است، با چالش‌های فنی و حقوقی زیادی در مرحله اجرا همراه است که میزان تأثیرگذاری آن را بر رعایت صحیح و کامل اصول قانونی پردازش داده‌ها، دچار تردید می‌کند. از بزرگ‌ترینِ این چالش‌ها، رعایت استانداردهای فنی و قانونی در راستای کاهش احتمال بازشناسایی یا رمزگشایی از الگوریتم داده‌های مستعارسازی شده است. درصورتی‌که داده‌ها به‌درستی مستعارسازی نشوند، ممکن است امکان بازشناسایی افراد با استفاده از تکنیک‌های پیشرفته مانند تحلیل داده‌های مکمل یا الگوریتم‌های هوش مصنوعی وجود داشته باشد.[1] همچنین، مدیریت صحیح ابزارهای مستعارسازی نیاز به تخصص فنی و استفاده از روش‌های خاص ترکیبی دارد که می‌تواند هزینه‌بر باشد. ازسوی دیگر، مستعارسازی نباید بر دقت و قابلیت استفاده از داده‌ها تأثیر منفی بگذارد، به‌ویژه زمانی که داده‌ها برای تحلیل‌های پیچیده یا پژوهش‌های علمی مورد نیازند. بنابراین و باوجود چالش‌های حقوقی و فنی متعدد در اجرای درست مستعارسازی، هدف این مقاله با روش توصیفی- تحلیلی، بررسی استانداردهای فنی به‌منظورحفاظت از داده‌های شخصی در کنار حفظ کارکرد اقتصادی داده‌ها و همین‌طور ارزیابی نقش و اهمیت مستعارسازی در رعایت اصول قانونی پردازش داده‌های شخصی است. در این راستا، سؤالات اصلی پژوهش شامل این موارد است که چگونه مستعارسازی می‌تواند از اصول پردازش داده‌ها مانند مشروعیت، شفافیت، و کمینه‌سازی حمایت کند و آیا این ابزار به‌تنهایی برای اطمینان از تطابق با الزامات قانونی کافی است؟ آیا استانداردها یا رعایت جزئیات خاصی می‌تواند به افزایش نقش مستعارسازی در رعایت اصول مذکور کمک کند؟ و اینکه چه روش‌های دیگری به‌عنوان طرق مکمل قابل‌طرح‌اند؟ نوشتار حاضر در دو بخش (بخش اول در خصوص مفاهیم اصلی پژوهش، روش‌ها و قوانین مرتبط و بخش دوم درمورد کیفیت و نحوه مستعارسازی و تأثیر آن بر رعایت اصول پردازش داده‌ها) نگارش شده است و به بررسی پرسش‌های مذکور خواهد پرداخت.

1. Sweeney, L, "k-Anonymity: A Model for Protecting Privacy, International Journal on Uncertainty", *Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 5, 2002, p 557.

۱. مستعارسازی و مفاهیم مرتبط

به‌طور معمول پیش‌شرط جمع‌آوری و پردازش داده‌های شخصی، رعایت حریم خصوصی افراد موضوع داده است و لذا برای حفاظت از این داده‌ها، در منابع مختلف علمی و قانونی، روش‌های متفاوتی ذکر شده است.[۱] علاوه‌بر این موارد، شرکت‌ها نیز برخی رویه‌های فنی و عملی را به‌طور معمول در پردازش داده‌های در اختیار، به‌کار می‌گیرند. حال برای شناخت این روش‌ها و ازجمله مستعارسازی داده‌ها، آشنایی با چند مفهوم پایه‌ای در این خصوص ضروری است.

ابتدا باید به این نکته توجه کرد که روش‌های حفاظتی، اغلب نسبت به داده‌های شخصی صورت پذیرفته‌اند و درمورد این داده‌ها اهمیت خود را نشان می‌دهند. ضمن اینکه این اقدامات برعهده کنترلگر داده‌هاست؛ هرچند بخشی از آنها نیز ضمن فرایند پردازش داده‌ها و از جانب پردازشگر، به خواست و تحت‌نظر کنترلگر صورت می‌پذیرند. بنابراین پیش از بررسی خود روش‌های حفاظتی، با چهار مفهوم داده‌های شخصی، کنترلگر، پردازش و پردازشگر مواجهیم. در تعریف این مفاهیم، قانون حمایت از داده‌های شخصی اتحادیه اروپا،[۲] مصوب سال ۲۰۱۶، در میان سایر اسناد و قوانین بین‌المللی، منطقه‌ای و ملی در سایر کشورها، از جایگاه خاصی برخوردار بوده و به‌نوعی به اصلی‌ترین منبع الهام جهانی در حیطه حمایت از داده‌های شخصی بدل شده است. لذا تعاریف موجود در منابع حقوقی مختلف، تا حد زیادی مشابه تعاریف سند مذکورند[۳] و جز در موارد خاص، اغلب رجوع به این سند برای آشنایی دقیق با مفاهیم حوزه حمایت از داده‌های شخصی، کفایت می‌کند. در ماده (۴) این مقرره، داده‌های شخصی، به‌عنوان داده‌هایی تعریف شده‌اند که به شخص حقیقی شناسایی شده یا قابل‌شناسایی مربوط‌اند. به شخصی که داده‌ها را در اختیار دارد و اهداف و ابزار پردازش داده‌ها را تعیین می‌کند و مورد خطاب قوانین این حوزه و مسئول حفاظت از داده‌های شخصی است، کنترلگر گفته می‌شود. در مقابل، پردازشگر شخصی است که داده‌ها را برای کنترلگر و طبق دستورالعمل‌های ایشان پردازش می‌کند.[۴] خود عملیات

1. Al-Zubaidie, M. and Zhang, Z. and Zhang, J, "PAX: Using Pseudonymization and Anonymization to Protect Patients' Identities and Data in the Healthcare System", *International Journal of Environmental Research and Public Health*, Vol. 16, No. 9, 2019, p 1.
2. E.U. General Data Protection Regulation (GDPR) 2016.
۳. لطیف‌زاده، مهدیه، سید محمدمهدی قبولی درافشان، سعید محسنی و محمد عابدی، «تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا»، *پژوهشنامه پردازش و مدیریت اطلاعات*، د. ۳۷، ش. ۲، ۱۴۰۰، ص ۴۶۸.
4. Starchon, Peter and Pikulik, Tomas, "GDPR principles in Data Protection Encourage Pseudonymization through Most Popular and Full-Personalized Devices - Mobile Phones", *Procedia Computer Science*, No. 151, 2019, p 304.

پردازش نیز شامل هر عملی است که روی داده‌های شخصی انجام می‌شود؛ مانند جمع‌آوری، ثبت، سازمان‌دهی، ذخیره‌سازی، انطباق یا تغییر، بازیابی، استفاده، افشا از طریق انتقال، انتشار و ترکیب داده‌ها. متأسفانه در ایران مقرره جامعی برای حمایت از داده‌های شخصی وجود ندارد. بااین‌حال در تعدادی از طرح‌های ارائه شده در این خصوص، می‌توان تعریف داده‌های شخصی را جست‌وجو کرد (البته قانون انتشار و دسترسی آزاد به اطلاعات سال ۱۳۸۸ نیز مصادیق اطلاعات شخصی را ذکر کرده و قانون تجارت الکترونیکی هم، داده پیام‌های شخصی را تعریف کرده است، ولی طرح‌های آتی‌الذکر، از نظر موضوعی به‌شکل مستقیم‌تری به بحث مدنظر این پژوهش پرداخته‌اند). در طرح حفاظت از داده‌های شخصی سال ۱۴۰۳،[۱] هر نوع داده‌ای که به هر نحو باعث شناسایی شخص موضوع داده شود، داده شخصی معرفی شده است. درمورد تعریف کنترلگر، پردازشگر و خودپردازش نیز، در طرح مذکور و همین‌طور طرح حمایت و حفاظت از داده و اطلاعات شخصی،[۲] عباراتی مشابه و با الگوبرداری از مقرره اتحادیه اروپا، درج شده است.[۳]

پس‌از آشنایی با این مفاهیم مقدماتی، شناخت خودمستعاری و همین‌طور تفکیک آن از برخی روش‌های حفاظتی مشابه مثل ناشناس‌سازی داده‌ها، برای شناخت ابعاد و آثار آن ضروری است. لذا در بخش اول این پژوهش، به بررسی ماهیت این اصطلاحات و انعکاس آن در قوانین این حوزه پرداخته می‌شود.

۱.۱. تعریف مستعارسازی داده‌ها

در بازارهای دیجیتال امروز و برای پیشبرد فعالیت‌های اقتصادی، هنگامی که داده‌ها جمع‌آوری می‌شوند، اغلب به اشخاص ثالث، برای تجزیه‌وتحلیل، برون‌سپاری می‌شوند.[۴] در چنین حالتی و به‌دنبال دسترسی شخص ثالث به داده‌ها، به‌کارگیری روش‌هایی برای پردازش امن داده‌های شخصی اهمیت پیدا می‌کند. در گذشته روش‌های حفاظت از داده‌ها محدود به

۱. طرح حفاظت از داده‌های شخصی در جلسه علنی مورخ ۱۴۰۳/۰۷/۱۵ مجلس شورای اسلامی اعلام وصول گردید. (قابل مشاهده در: https://rc.majlis.ir/fa/legal_draft/show/1816729)

۲. طرح حمایت و حفاظت از داده و اطلاعات شخصی در جلسه علنی مورخ ۱۴۰۰/۰۶/۲۶ مجلس شورای اسلامی اعلام وصول شد. قابل مشاهده در:
https://media.dotic.ir/uploads/org/2021/10/09/163377045160152200.pdf

۳. فرحزادی، علی‌اکبر، حسین صادقی، و مهدی ناصر، «وظایف کنترل‌کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات»، *قضاوت*، د. ۲۲، ش. ۱۱۲، ۱۴۰۱، ص ۷۳.

4. Lehmann, Anja, "ScrambleDB: Oblivious (Chameleon) Pseudonymization-as-a-Service", *Privacy Enhancing Technologies*, No.3, 2019, p 289.

رمزگذاری، تشخیص نفوذ یا کنترل دسترسی مبتنی‌بر نقش افراد بودند؛ اما جدا از احتمال دور زدن این موارد توسط مهاجمان یا افشای اطلاعات با انگیزه‌های مختلف توسط کارکنان، به‌دلیل کنترل کامل مدیران بر این فرایندها و تصمیم‌گیری ایشان درمورد افراد مجاز به دسترسی به داده‌ها، احتمال خطا، سوءاستفاده یا سوءمدیریت نیز همواره وجود داشت. اما امروزه مکانیزم‌های کنترل دسترسی، جای خود را به‌روش‌های ترکیبی شامل مستعارسازی و رمزگذاری چندلایه داده‌اند. در واقع برای حل مشکلات روش‌های قدیمی، شرکت‌ها به مستعارسازی روی آورده‌اند.[۱] با عنایت به تعریف پردازش، که ذکر شد، مستعارسازی را نیز باید نوعی پردازش دانست؛ با این تفاوت که برخلاف سایر فعالیت‌های پردازشی، نه‌تنها از نظر قانونی با مانعی مواجه نیست، بلکه جزئی از وظایف کنترل‌کنندگان داده‌ها محسوب می‌شود.[۲]

اختصاص‌دادن نام مستعار روشی خاص از هویت‌زدایی است که برمبنای حق افراد بر بی‌نامی و محرمانگی اطلاعات و زندگی خصوصی انجام می‌پذیرد.[۳] مستعارسازی تکنیکی است که در آن داده‌های شناسایی با یک نام مستعار جایگزین می‌شود.[۴] در حقیقت اختصاص یک شناسه موقت به هر شخص موضوع داده باعث محرمانه و ناشناس ماندن هویت واقعی ایشان می‌شود.[۵] با مستعارسازی، داده‌ها به سه دسته تقسیم می‌شوند: ۱. داده‌های مستعارسازی شده، ۲. داده‌های شخصی منبع که در دستان کنترلگر به‌شکل محرمانه نگهداری می‌شوند و ۳. کلیدی که نحوه ارتباط بین نام‌های مستعار و اشخاص موضوع داده را توضیح می‌دهد تا شناسایی مجدد آنها ممکن شود.

1. Heurix, Johannes and Karlinger, Michael and Neubauer, Thomas, "Pseudonymization with Metadata Encryption for Privacy-Preserving Searchable Documents", *45th Hawaii International Conference on System Sciences, Maui, HI, USA*, 2012, p 3011.

۲. صادقی، حسین و مهدی ناصر، «جستاری در ماهیت‌شناسی داده‌های خصوصی در سازوکار عملکرد ابزارهای فناوری اینترنت اشیا»، *فصلنامه رشد فناوری*، د. ۱۹، ش ۲، ۱۴۰۲، ص ۳۹.

3. Gazizov, Andrey and Gazizov, Evgeny and Gazizova, Svetlana, "Theoretical aspects of the protection of Personal Data of Employees of the Enterprise by the Method of Pseudonymization", E3S Web Conf, 2020, p 2.

4. Neubauer, Thomas and Heurix, Johannes, "A Methodology for the Pseudonymization of Medical Data", *International Journal of Medical Informatics*, Vol. 80, No. 3, 2011, p 190.

۵. پوریوسف، زهرا، مهری رجایی و نیک‌محمد بلوچزهی، «حفظ حریم خصوصی خودروها در شبکه‌های ارتباطات خودرویی»، همایش ملی پژوهش‌های نوین در علوم و فناوری، ۱۳۹۷، تهران، ایران، ص ۶.

۱.۲. تفاوت مستعارسازی و ناشناس‌سازی داده‌ها

ناشناس‌سازی به‌معنی جدا کردن و حذف کامل نشانه‌های هویتی از داده‌های شخصی است. برای مثال طبق یک پرونده شخصی، علی با قد ۱۸۲ سانتی‌متر و وزن ۸۰ کیلوگرم و سن ۲۳ سال در یکی از محله‌های غرب تهران ساکن است و از خدمات شرکتی خاص استفاده می‌کند. حال قرار است برای تجزیه‌وتحلیل‌های آماری (مثلاً برای ارزیابی میانگین قد شهروندان تهران)، این داده‌های شخصی از شرکت کنترلگر به یک شرکت پردازشگر ثالث منتقل شود. یکی از روش‌های حفاظت از هویت کاربر ضمن این نقل و انتقالات و پردازش‌ها، ناشناس‌سازی داده‌هاست؛ به این معنا که با این روش، از پرونده فوق نام و آدرس علی به‌طور کلی حذف می‌شود. در این صورت همچنان می‌توان از داده‌ها برای هدف پردازش (که تشخیص میانگین قد است)، بدون شناختن اشخاص موضوع داده‌ها، استفاده کرد. احتمالاً ناشناس‌سازی نسبت به مستعارسازی، به‌دلیل کاهش یا به‌ظاهر قطع احتمال بازشناسایی افراد، با مزیت‌های بیشتری برای کاربران همراه است؛ اما با توضیحاتی که ارائه می‌شود، مشخص خواهد شد که چنین نیست و احتمال سوءاستفاده از داده‌ها پس‌از ناشناس‌سازی به‌کل منتفی نشده و همچنین از نظر اقتصادی نیز چنین روشی به‌دلیل کاهش کاربردهای تجاری، آماری و علمی داده‌ها، با موانعی همراه است.

به‌دلیل غیرقابل‌برگشت بودن ناشناس‌سازی، کاربرد داده‌های ناشناس‌شده، به همین استفاده‌های ثانویه محدود می‌شود (یعنی پس‌از ناشناس‌سازی، کارکردهایی که داده‌های شخصی به‌دلیل اشاره به اشخاص داشتند، برای همیشه از دسترس خارج و کارکردهای ثانویه غیرمبتنی بر ویژگی‌های هویتی، جایگزین می‌شوند). اما مستعارسازی در شرایط مشخص و کنترل‌شده قابل برگشت‌اند و همچنان می‌توان از داده‌های منبع نیز استفاده کرد. ضمن اینکه ناشناس‌سازی با حذف نشانه‌های هویتی، باعث کاهش دقت داده‌ها می‌شود؛ لکن مستعارسازی با جایگزینی نشانه‌ها، دقت داده‌ها را دست‌نخورده نگاه می‌دارد.[1] در واقع قطع ارتباط اشخاص با داده‌هایشان توسط ناشناس‌سازی، فقط تا زمانی مفید است که پتانسیل خروجی از داده‌ها، همچنان مطلوبیت خود را حفظ کند که در فرض ناشناس‌سازی، اغلب درعمل چنین نیست. این امر به‌دلیل ارزش یا

1. Heurix, Johannes and Karlinger, Michael and Schrefl, Michael & Neubauer, Thomas, "A Hybrid Approach Integrating Encryption and Pseudonymization for Protecting Electronic Health Records", *Proceedings of the 8th IASTED International Conference on Biomedical Engineering, Innsbruck, Austria*, 2011, p 3.

دانشی است که می‌توان از تجزیه‌وتحلیل مجموعه داده‌ها و با یافتن الگوها که اساساً بخش‌های مختلف داده را به‌هم پیوند می‌دهند، به‌دست آورد. ناشناس‌سازی با جدا کردن چنین پیوندهایی، به کاهش کاربرد پردازشی داده‌ها و همچنین حداقل‌سازی نتایج مفید حاصل از تحلیل آنها می‌انجامد.[1] در حقیقت با جداسازی هویت اشخاص، توانایی تجزیه‌وتحلیل و آمارسازی‌های دقیق از طریق داده‌ها (برای مثال، در همان پرونده مربوط به علی، با ناشناس‌سازی، دیگر نمی‌توان بین آمارهای مربوط به قد زنان و مردان، تفکیک کرد و لذا دقت پژوهش کاهش می‌یابد) کم می‌شود و اصطلاحاً با اتلاف داده‌ها[2] مواجهیم که با محدود کردن کارکردهای تجاری داده‌ها، با ابعاد اقتصادی نیز همراه است. بنابراین از نظر ارزشمندی محتوایی، داده‌های شخصی، داده‌های مستعار و داده‌های ناشناس، به‌ترتیب در رتبه‌های اول تا سوم قرار دارند. لذا از منظر تأمین اهداف پردازش، مستعارسازی داده‌ها به نسبت ناشناس‌سازی آنها در اولویت است؛ درحالی‌که از منظر حمایت از داده‌های شخصی، ناشناس‌سازی به‌دلیل عدم امکان بازشناسایی اشخاص موضوع داده، روش مطمئن‌تری است. البته درمجموع و با لحاظ نگرانی‌های مربوط به حریم خصوصی و لزوم استفاده تجاری مشروع از داده‌ها به‌شکل همزمان، به‌کارگیری ترکیبی از مستعارسازی و روش دیگری به نام رمزگذاری داده‌ها، که در بخش‌های آتی توضیح داده خواهد شد، برای تعادل‌بخشی به این دو وجه درخصوص داده‌های شخصی، روشی ایدئال است.[3]

فارغ از کارکرد اقتصادی داده‌ها و از منظر قانونی، اطلاعات ناشناس خارج از محدوده قوانین حمایت از داده‌های شخصی‌اند؛ چراکه اگر داده‌هایی ناشناس شوند، پس‌از افشا، دیگر به شناسایی هویت افراد موضوع داده‌ها منجر نخواهند شد و درواقع ارتباط آنها به‌طور کامل با اشخاص حقیقی قطع می‌شود. از آنجایی که موضوع قوانین حمایتی، داده‌های شخصی‌اند، پس‌از ناشناس‌سازی و به‌دلیل عدم اطلاق وصف شخصی بر داده‌ها، دیگر حمایت‌های قوانین این حوزه، درمورد چنین داده‌هایی ادامه نخواهد داشت. اما در مستعارسازی، همچنان از طریق کلید مربوطه برای تشخیص نحوه ارتباط نام‌های مستعار با اشخاص حقیقی موضوع داده‌ها یا از طریق

1. Bourdillon, Stalla and Alison, Sophie, "Anonymous Data v. Personal Data, A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data", *Wisconsin International Law Journal*, 2017, p 2.
2. Data loss
3. Shin, Soo Yong and kim, Hun Sung, "Data Pseudonymization in a Range That Does Not Affect Data Quality: Correlation with the Degree of Participation of Clinicians", *Journal of Korean Medical Science*, Vol. 36, No. 44, 2021, p 3.

فرمول‌های حفاظت‌شده برای معکوس کردن الگوریتم‌های خودکار اختصاص نام مستعار، همچنان داده‌ها توسط کنترلگر یا هر شخصی که به این کلیدها دسترسی دارد، قابل ارتباط با اشخاص است و در حقیقت ایشان همچنان قابل شناسایی‌اند. لذا داده‌های مستعارسازی‌شده را باید داده‌های شخصی و مشمول حمایت‌های قوانین مربوطه دانست. کمیسیون حفاظت از داده‌های ایرلند نیز به‌عنوان عضوی از اتحادیه اروپا، در سال ۲۰۱۹ راهنمایی را درمورد ناشناس‌سازی و مستعارسازی داده‌ها منتشر کرده است[1] که تأیید می‌کند داده‌های ناشناس برگشت‌ناپذیر (اگر همزمان با ناشناس‌سازی، داده‌های منبع حذف نشوند، همواره امکان شناسایی افراد وجود دارد؛ مگر پردازشگری که داده‌های ناشناس را در اختیار دارد، به‌هیچ‌نحو به داده‌های اصلی دسترسی نداشته باشد)، داده‌های شخصی نیستند و رعایت اصول حمایت از داده‌ها درخصوص این داده‌ها الزامی نیست؛ لکن داده‌های مستعار داده‌های شخصی باقی می‌مانند و لذا مورد حمایت قرار می‌گیرند. برای مثال، درمورد داده‌های ناشناس، نگهداری بدون قید مدت، استفادهٔ برخلاف مفاد اسناد خط‌مشی حریم خصوصی و برخلاف اهداف اولیه اعلام‌شده برای پردازش داده‌های شخصی و با اهدافی کاملاً متفاوت و حتی فروش و انتقال بی‌ضابطه این داده‌ها ممکن است؛ اما درمورد داده‌های مستعارسازی‌شده، چنین امکاناتی وجود ندارد. بنابر این تفاوت‌ها میان ناشناس‌سازی و مستعارسازی در میزان کاهش دقت داده‌ها و در سطح حمایت‌های قانونی و احتمال سوءاستفاده‌ها، به کنترل‌کنندگان داده توصیه می‌شود که اولاً، مستعارسازی را در اولویت قرار دهند و ثانیاً ناشناس‌سازی را به‌عنوان یک عمل آنی تلقی نکنند؛ بلکه با ارزیابی منظم ریسک و انجام نظارت، ضمن همگامی با تکامل فناوری‌ها، تا حد امکان با گیرندگان داده ارتباط برقرار کند تا ایشان نیز از قوانین حمایت از داده غافل نشوند و احتمال بازشناسایی افراد یا نقض حریم آنها با سوءاستفاده از داده‌های ناشناس یا مهندسی معکوس آنها به حداقل برسد.[2]

1. Data Protection Commission IE, "Guidance on Anonymisation and Pseudonymisation", Available at: (https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614% 20 Anonymisation%20and%20Pseudonymisation.pdf) Visited 2025/02/08.
2. Heurix, Johannes and Neubauer, Thomas, "Privacy-Preserving Storage and Access of Medical Data through Pseudonymization and Encryption", *Lecture Notes in Computer Science*, 6863, Berlin, Heidelberg, 2011, p 3.

۱.۳. مستعارسازی در قوانین و مقررات

همان‌طور که گفته شد، در قوانین و مقررات ایران به ابعاد و جزئیات مستعارسازی داده‌ها پرداخته نشده است. به‌طور خاص در اسناد مرتبط مثل قانون تجارت الکترونیکی، قانون انتشار و دسترسی آزاد به اطلاعات و همین‌طور طرح‌های مختلف ارجاع‌شده به مجلس در امر حمایت و حفاظت از داده‌ها (مثل طرح حفاظت از داده‌های شخصی سال ۱۴۰۳) صحبتی از مستعارسازی یافت نمی‌شود. بااین‌حال در برخی کشورها، منابع قانونی بسیاری روش‌های فنی حفاظت از داده‌ها را توضیح می‌دهند.

در حقوق آمریکا، در سطح فدرال، مقرره عمومی برای حمایت از داده‌های شخصی وجود ندارد؛ بلکه مقررات بخشی (یعنی قوانین جداگانه در حیطه بهداشت، کودکان، داده‌های مالی و کیفری) در هر زمینهٔ موضوعی متفاوت، بر حمایت از داده‌ها حکومت می‌کنند. دراین‌خصوص برای نمونه، در قانون قابلیت انتقال و مسئولیت‌پذیری بیمه‌های درمانی سال ۲۰۰۲،[1] مفاهیم مرتبط با ناشناس‌سازی یا حذف شناسه‌های شناسایی[2] ذکر شده، اما اصطلاح مستعارسازی به‌طور صریح در متن اصلی قانون آورده نشده است. در قوانین ایالتی نیز مانند قانون حمایت از داده‌های مصرف کنندگان ایالت کالیفرنیا[3] و ویرجینیا[4] به‌صورت مستقیم به مستعارسازی داده‌ها اشاره نشده، بلکه تأکید این مقررات بر ناشناس‌سازی است.

برخلاف حقوق آمریکا، در اتحادیه اروپا و در متون متعددی، به امر مستعارسازی توجه شده است. قانون حمایت از داده‌های شخصی اتحادیه اروپا، در بند «۵» ماده (۴)، به پردازش داده‌های شخصی به‌گونه‌ای‌که دیگر نتوان داده‌های شخصی را بدون استفاده از اطلاعات اضافی به یک موضوع داده خاص نسبت داد، مشروطبر اینکه این اطلاعات اضافی به‌طور جداگانه نگهداری شود و مشمول اقدامات فنی و سازمانی باشد تا اطمینان حاصل شود که داده‌های شخصی به یک شخص حقیقی شناسایی‌شده یا قابل‌شناسایی نسبت داده نمی‌شود، مستعارسازی گفته شده است. در ماده (۲۵) نیز با در نظر گرفتن وضعیت فنی، هزینه اجرا و ماهیت داده‌ها، دامنه، زمینه و اهداف پردازش و همچنین خطرات احتمالی و شدت آنها برای حقوق و آزادی‌های اشخاص

1. Health insurance portability and accountability act of 1996 (HIPAA).
2. de-identification
3. California Consumer Privacy Act 2018 (CCPA).
4. Virginia Consumer Data 2023 (VCDPA).

حقیقی ناشی از پردازش، کنترلگر باید چه در زمان تعیین ابزار پردازش و چه در زمان پردازش، اقدامات فنی مثل مستعارسازی را اجرا کند. ماده (۳۲) هم درخصوص تأمین امنیت پردازش، استفاده از نام مستعار و رمزگذاری داده‌های شخصی را پیشنهاد داده است. ماده (۸۹) درمورد پردازش در راستای منافع عمومی، اهداف تحقیقات علمی یا تاریخی یا اهداف آماری، اقدامات فنی و سازمانی را به‌ویژه برای اطمینان از رعایت اصل به حداقل رساندن داده‌ها (که توضیح داده خواهد شد) ضروری و این اقدامات را شامل مستعارسازی نیز می‌داند. در کنار مواد این قانون، تعدادی رسیتال (مقدمه یا یادآوری)[1] نیز وجود دارد که محتوای مواد اصلی را شرح و توضیح می‌دهد و تفاسیری در این زمینه ارائه می‌کنند. در رسیتال ۲۶، داده‌های شخصی که تحت نام مستعار قرار گرفته‌اند و با استفاده از اطلاعات اضافی می‌توانند به یک شخص حقیقی نسبت داده شوند، برخلاف داده‌های ناشناس، باید به‌عنوان اطلاعات یک شخص حقیقی قابل‌شناسایی در نظر گرفته شوند. طبق رسیتال ۲۸ نیز استفاده از نام مستعار برای داده‌های شخصی می‌تواند خطرهای مربوط به کاربران را کاهش دهد و به کنترلگرها و پردازشگرها کمک کند تا به تعهدات خود درزمینه حفاظت از داده‌ها عمل کنند. رسیتال ۱۵۶ هم محتوایی مانند ماده (۸۹) دارد.

۲. مستعارسازی و پردازش قانونی داده‌ها

در تمام قوانین و مقررات حمایت از داده‌ها، اصولی برای پردازش قانونی داده‌های شخصی پیش‌بینی شده است. در اتحادیه اروپا، مشروعیت و عادلانه بودن، شفافیت، محدودیت هدف، حداقلی و ضروری بودن، دقت، محرمانگی و امنیت و همین‌طور لزوم پاسخ‌گویی پردازشگر، جزو اصول پردازش داده‌های شخصی محسوب می‌شوند. در حقوق آمریکا و در قانون حریم خصوصی ۱۹۷۴[2] (اصلاح‌شده در سال ۲۰۲۰) نیز اصول رویه‌های منصفانه[3] شامل محدودیت هدف، حداقلی بودن و رضایت، درمورد پردازش داده‌های شخصی توسط نهادهای فدرال پیش‌بینی شده است. سازمان همکاری و توسعه اقتصادی هم حداقلی بودن، محدودیت هدف، دقت و کیفیت، امنیت، شفافیت، مشارکت و پاسخ‌گویی را تحت عنوان اصول پردازش داده‌ها ذکر کرده است.[4]

1. Recital
2. Privacy act of 1974.
3. Fair information practice principles FIPPs.
۴. انصاری، باقر، **اصول پردازش داده‌های شخصی**، چ ۱، تهران: شرکت سهامی انتشار، ۱۴۰۲، صص ۱۰۰–۱۲۸.

در حقوق ایران، طرح حفاظت از داده‌های شخصی ۱۴۰۳ و ماده (۵۹) قانون تجارت الکترونیکی، درمجموع به امنیت، مشروعیت، محدودیت هدف، رضایت، پاسخ‌گویی، اطلاع‌رسانی و صحت و تمامیت، اشاره کرده‌اند.[۱] بااین‌حال جای خالی مقرره‌ای با شأن قانونی، که به‌طور جامع به بحث حمایت از داده‌های شخصی و اصول پردازش داده‌ها بپردازد، در این زمینه احساس می‌شود.[۲]

حال برای رعایت این اصول به‌شکل صحیح، اقدامات و روش‌های مختلفی متصور است که یکی از آنها مستعارسازی داده‌هاست. در این بخش به‌تفکیک بررسی خواهد شد که اختصاص نام مستعار به داده‌های شخصی، در رعایت کدام‌یک از اصول پردازش داده‌ها و تا چه حد مؤثر خواهد بود و در نهایت تغییر فنون و جزئیات مستعارسازی یا ترکیب آن با روش‌های دیگر، چه تأثیری بر گسترش دامنه رعایت اصول پردازش خواهد داشت.

۲.۱. اصول پردازش داده‌های شخصی و نقش مستعارسازی

از مجموعه قوانین، مقررات و اسناد مذکور، کامل‌ترین و کاربردی‌ترین فهرست اصول پردازش داده‌های شخصی را می‌توان در قانون حمایت از داده‌های شخصی اتحادیه اروپا جست‌وجو کرد. اولین اصل از این اصول، لزوم مشروعیت و قانونی بودن پردازش است. طریق اصلی اطمینان از رعایت این اصل، اثبات وجود و احراز مبانی قانونی خاص پردازش داده‌ها در ماده (۶) مقرره مذکور است (مثل وجود رضایت شخص موضوع داده، تعهد قانونی، تکلیف قراردادی، نفع مشروع و...).[۳] بااین‌حال، در موارد خاصی، می‌توان چنین برداشت کرد که قانونی بودن پردازش، مشروط به رعایت امنیت داده‌ها و حفظ گمنامی کاربران است؛ لذا در این موارد، با انجام مستعارسازی، اصل قانونی بودن و مشروعیت پردازش، رعایت می‌شود. برای مثال، طبق ماده (۸۹) قانون حمایت از داده‌های شخصی، پردازش ثانوی داده‌های شخصی برای بایگانی، اهداف علمی، تاریخی و آماری، در صورت امکان و تحقق اهداف پردازش، به‌شکل مستعارسازی

۱. زند، حسین، **حمایت از داده‌ها در حقوق موضوعه ایران**، چ ۲، تهران: شرکت سهامی انتشار، ۱۴۰۳، ص ۳۵.
۲. عرب سرخی، ابوذر و طلا تفضلی، «تحلیل موضوعات راهبردی در قلمرو مقررات حفاظت از داده‌های عمومی»، *دوفصلنامه علمی منادی امنیت فضای تولید و تبادل اطلاعات*، د. ، ش. ۲، ۱۴۰۳، ص ۱۹.
۳. حسینی، علی، «حقوق حفاظت از داده‌های شخصی در پردازش الگوریتمی، چالش‌ها و راهکارها»، *دولت و حقوق*، د. ۵، ش. ۱، ۱۴۰۳، صص ۱۰۹-۱۱۲.

شده انجام می‌شود. در چنین مواردی مستعارسازی، شرط قانونی بودن پردازش است. همچنین کاهش ریسک ناشی از به‌کارگیری نام مستعار ممکن است کنترلگرها را قادر کند تا برای پردازش قانونی داده‌ها، برمبنای منافع مشروع (مثلاً استدلال شود که چون داده‌ها مستعار شده و امنیت و محرمانگی آنها از این طریق حفظ می‌شود، چنین امری گواه این است که اهداف شرکت برای پردازش داده‌ها از وجاهت و مشروعیت برخوردار هستند، زیرا در غیر این صورت حفظ حریم اشخاص مورد توجه و احترام از جانب شرکت نمی‌بود) تحت ماده ۶ قانون حمایت از داده‌های شخصی اتحادیه اروپا، تکیه کنند. در این صورت، اصل قانونی و مشروع بودن پردازش نیز رعایت می‌شود. ضمن اینکه در برخی موارد و قوانین، به‌ویژه درمورد داده‌های حساس و به‌خصوص داده‌های پزشکی، مستعارسازی داده‌ها اجبار می‌شود و به این دلیل نیز پردازش داده‌ها به‌شکل مستعار، قانونی و مشروع خواهد بود. همین‌طور برای انتقال فرامرزی داده‌های شخصی که نوعی پردازش است، برخی الزامات اضافی برای قانونی بودن این انتقال، باید رعایت شود. طبق ماده (۴۴) مقرره فوق‌الذکر، انتقال داده‌ها به کشور ثالث، فقط درصورتی انجام می‌شود که با رعایت سایر مقررات این سند، ازجمله اصول پردازش و مستعارسازی داده‌ها، انجام پذیرد. ماده (۴۶) نیز در همین راستا، امکان انتقال فرامرزی داده‌ها را مشروط به رعایت اقدامات فنی مناسب می‌کند. البته در این خصوص صراحتاً مستعارسازی تکلیف نشده است، بلکه به‌عنوان یکی از روش‌های مناسب قابل انجام است.

اصل دومی که رعایت آن از مستعارسازی بسیار تأثیر می‌پذیرد، اصل محدودیت هدف پردازش است. طبق ماده (۶) قانون حمایت از داده‌های شخصی، سازگاری اهداف ثانویه و استفاده‌های بعدی از داده‌ها با اهداف اولیهٔ اعلام‌شده در زمان جمع‌آوری، ضروری است. مستعارسازی داده‌ها با کاهش ارتباط بین استفاده‌های بعدی و شناسه‌های هویتی، به تأمین سازگاری این استفاده‌ها با اهداف و استفاده‌های مورد رضایت اشخاص موضوع داده کمک می‌کند.[1] دلیل این امر جلوگیری از پردازش بیشتر داده‌ها توسط پردازشگر، در راستای اهدافی است که تحقق آنها مستلزم هرگونه تعامل مستقیم با اشخاص موضوع داده یا هویت آنهاست. در

1. European Data Protection Board, "Guidelines 01/2025 on Pseudonymisation", Available at: (https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en) Visited 2025/02/08, pp 3-15.

واقع عدم دسترسی پردازشگر به شناسه‌های هویتی و کار کردن با داده‌های مستعار، از احتمال و امکانات ایشان برای پردازش بیشتر داده‌ها و برای اهداف و استفاده‌های فراتر از آنچه اعلام شده است، با تأثیر منفی بر کیفیت و دقت و همچنین میزان و کاربردی بودن محتوای داده‌ها به‌دنبال بی‌هویت‌سازی می‌کاهد. بنابراین اصل محدودیت پردازش و اهداف آن نیز تا حد زیادی با مستعارسازی رعایت می‌شود.

اصل لزوم پاسخ‌گویی و مسئولیت‌پذیری نیز به‌شکل مستقیم از اختصاص نام‌های مستعار تأثیر می‌پذیرد. مطابق با اعلام هیئت حفاظت از داده‌های اروپا (یک نهاد مستقل اروپایی است که مسئول اجرای قانون حمایت از داده‌های شخصی و هماهنگ‌سازی سیاست‌های حمایت از داده‌ها در سراسر اتحادیه اروپاست) در سال ۲۰۲۵ و در سند رهنمود مستعارسازی، اصل پاسخ‌گویی و مسئولیت‌پذیری، متضمن وظیفه‌ای برای کنترلگر داده‌هاست تا روش‌های مناسب حفظ حریم داده‌ها را متناسب با ماهیت، دامنه، زمینه و اهداف پردازش و خطرات مربوط به آن، انتخاب و اجرا گند. بنابراین به‌کارگیری مستعارسازی و تعیین نحوهٔ انجام و جزئیات آن به‌شکل صحیح، به‌دلیل اینکه یک اقدام فنی و سازمانی مناسب به‌منظور کاهش ریسک سوءاستفاده از داده‌های شخصی و شناسایی افراد موضوع داده است، تا حد زیادی با اصل مسئولیت‌پذیری شرکت مرتبط است و باعث پاسخ‌گویی ایشان در قبال کاربران برای تأمین بخش زیادی از الزامات قانونی در این خصوص می‌شود. در حقیقت چون شرکت باید مسئولیت‌پذیر و پاسخ‌گو باشد (در قبال رعایت حریم خصوصی کاربران)، پس باید داده‌ها را در هنگام لزوم مستعار کند.[۱]

از دیگر اصول پردازش داده‌ها، اصل حداقلی و ضروری بودن پردازش است. طبق این اصل، انتقال داده‌ها به پردازشگر برای پردازش و خود عملیات پردازش داده‌ها، باید به‌صورت حداقلی و کمینه‌سازی شده و در حد نیاز و ضرورت باشد و از پردازش داده‌های بیشتر خودداری کرد.[۲] استفاده از نام مستعار در این زمینه روش بسیار مناسبی است؛ چراکه انتقال داده‌های شخصی و شناسه‌های هویتی با مستعار شدن داده‌ها به حداقل می‌رسد و پردازش داده‌ها نیز محدود و کمینه می‌شود. در حقیقت این اصل با اصل محدودیت اهداف پردازش نیز مرتبط است. در راستای

1. European Data Protection Board, *Ibid*, pp 3-15.

۲. مزینانیان، سعیده، «تنظیم‌گری حریم خصوصی در فضای مجازی (مطالعه تطبیقی در حقوق ایالات متحده آمریکا، اتحادیه اروپا و ایران)»، *پژوهش‌های حقوق اقتصادی و تجاری*، د. ۱، ش. ۲، ۱۴۰۳، صص ۲۰۷-۲۱۰.

ضرورت پردازش هم، فقط اگر اهداف مشروع پردازش داده‌ها، انتقال آنها را به‌شکل شناس اقتضا کند و همچنین اگر روش دیگری برای نیل به این اهداف وجود نداشته باشد، انتقال داده‌های شخصی ممکن است؛ در غیر این صورت باید داده‌ها به‌دلیل نبود ضرورتی برای انتقال و پردازش به‌شکل شناس، به داده‌های ناشناس یا مستعار تبدیل و سپس منتقل شوند. ضمن اینکه از جنبه‌های دیگر اصل کمینه‌سازی، به حداقل رساندن و محدود کردن مدت زمان نگهداری داده‌هاست. اولاً به‌دلیل حذف شناسه‌های هویتی از داده‌ها و کاهش کاربردهای آنها، به‌صورت خودکار مدت‌زمان ممکن برای نگهداری از داده‌ها توسط پردازشگر کاهش می‌یابد؛ چراکه اگر می‌توانست برای مثال با سه سال نگهداری از داده‌های شخصی، آنها را برای ده هدف متفاوت پردازش کند، حال به‌دلیل مستعارسازی این داده‌ها و کاهش اطلاعات حاصل از تجزیه‌وتحلیل آنها، اهداف ممکن برای پردازش به پنج هدف کاهش می‌یابد که همین پنج هدف نیز با یک سال پردازش محقق می‌شوند. لذا در عمل مدت زمان نگهداری داده‌ها به‌شکل لاجرم کم شده، اصل نگهداری و پردازش حداقلی رعایت می‌شود. ثانیاً و پس‌از پردازش یا انجام عملیات لازم و انقضای هدف جمع‌آوری داده‌ها نیز، از آنجایی که به‌دلیل محدودیت هدف، حداقلی بودن و محدودیت زمان پردازش و نگهداری از داده‌ها، باید داده‌های شخصی از سرورهای شرکت حذف شوند، نگهداری برخی از بخش‌های داده‌ها بیش از این مدت و پس‌از انقضای هدف با ناشناس‌سازی یا مستعارسازی آنها (به‌شرط عدم امکان شناسایی اشخاص توسط پردازشگر، مثلاً از طریق مستعارسازی تصادفی و اطمینان از حذف داده‌های شخصی منبع از سیستم‌های ایشان) ممکن می‌شود. علاوه‌بر این موارد و از نظر قانونی، طبق ماده (۲۵) قانون حمایت از داده‌های شخصی اتحادیه اروپا، با در نظر گرفتن وضعیت فنی، هزینهٔ اجرا و ماهیت داده‌ها، دامنه، زمینه و اهداف پردازش و همچنین خطرات احتمالی و شدت آنها برای حقوق و آزادی‌های اشخاص حقیقی ناشی از پردازش، کنترلگر باید چه در زمان تعیین ابزار پردازش و چه در زمان پردازش، اقدامات فنی را مثل مستعارسازی اجرا کند تا اصول حمایت از داده‌ها، مانند اصل حداقل‌سازی پردازش، به شیوه‌ای مؤثر رعایت شوند. همچنین مطابق با ماده (۸۹) مقرره مذکور، درصورت نیاز به پردازش داده‌ها در راستای منافع عمومی و با اهداف علمی، آماری و تاریخی، اطمینان از رعایت اصل به حداقل رساندن داده‌ها، با مستعارسازی آنها ممکن می‌شود. به‌ویژه اینکه در برخی

موارد، حفظ قابلیت شناسایی مجدد شخص موضوع داده برای تحقق به اهداف پردازش مهم است؛ بنابراین، نمی‌توان از ناشناس‌سازی استفاده‌کرد و مستعارسازی در این خصوص اولویت دارد.[۱]

در نهایت، با توجه به کاهش احتمال بازشناسایی اشخاص موضوع داده‌ها و کاهش ریسک‌ها و شدت عواقب دسترسی غیرمجاز به داده‌ها به‌دنبال مستعارسازی، اصل امنیت و محرمانگی پردازش نیز رعایت می‌شود. همچنین انتقال داده‌ها به‌شکل محدود و با نام‌های مستعار به پردازشگر توسط کنترلگر، با تعیین نقاط تمرکز و ویژگی‌های کلیدی در مجموعه داده‌ها و در محدودهٔ اهداف اعلامی، به رعایت اصل دقت در پردازش داده‌ها هم کمک شایانی می‌کند.

۲.۲. مستعارسازی صحیح و مؤثر داده‌های شخصی

مستعارسازی برای داده‌های درحال پردازش،[۲] ذخیره‌شده[۳] و ارسال‌شده[۴] اعمال می‌شود.[۵] به‌کارگیری این روش علاوه‌بر مزایایی که برای کاربران به‌همراه دارد، در راستای منافع شرکت نیز با جلب اعتماد کاربران و افزایش مزیت رقابتی، کاهش اختلافات و دعاوی و درنتیجه خسارات و جریمه‌های احتمالی، نقش‌آفرینی می‌کند. البته تمام این کارکردها در فرضی محقق می‌شوند که این روش از طرق صحیح و استاندارد صورت پذیرد. در پرونده‌ای مربوط به شرکت گوگل،[۶] دادگاه تجدیدنظر انگلستان به مسائل مهمی درزمینه حقوق حریم خصوصی و حمایت از داده‌ها پرداخت. شاکیان ادعا کردند که گوگل بدون رضایت آنها، فعالیت‌های اینترنتی ایشان را ردیابی کرده و اطلاعات تولیدشده توسط مرورگر را جمع‌آوری و با اشخاص ثالث به اشتراک گذاشته است. دادگاه حکم داد که براساس قانون حمایت از داده‌ها، شاکیان می‌توانند برای ناراحتی روانی ناشی از نقض حریم خصوصی خود، بدون نیاز به اثبات خسارت مالی، درخواست

1. Bolognini, Luca and Bistolfi, Camilla, "Pseudonymization and Impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation", *Computer Law & Security Review*, Vol. 33, No. 2, 2017, p 173.
2. Data-In-Use
3. Data-At-Rest
4. Data-In-Motion
5. Ribeiro, S. L. and Nakamura, E. T, "Privacy Protection with Pseudonymization and Anonymization in a Health IoT System: Results from OCARIoT", IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE), Athens, Greece, 2019, p 904.
6. Google Inc. v. Vidal-Hall [2015] EWCA (Civ) 311 (U.K.) (appendix to the judgement).

جبران خسارت کنند.[1] اگر گوگل حداقل داده‌ها را از طریقی صحیح مستعارسازی می‌کرد و بعد با ثالث به اشتراک می‌گذاشت (هرچند خود جمع‌آوری داده‌ها نیز غیرقانونی بوده و حکم نهایی و میزان جریمه و خسارات مقوم ثابت است)، شاید در عمل تا حد زیادی از خسارات واقعی وارده به افراد جلوگیری و تا حدی نیز اعتبار شرکت برای این تلاش حفظ می‌شد.

بنا به مطالب مذکور و با شناختن اهمیت مستعارسازی، باید به این نکته توجه داشت که همین فرایند نیز خود از روش‌ها، مراحل و جزئیات و ظرافت‌های خاصی برخوردار است که نحوه اجرای آنها، به‌طور مستقیم بر نتیجه مستعارسازی و آثار آن، برای مثال میزان تأثیر استفاده از نام مستعار در رعایت الزامات قانونی مربوط به اصول پردازش داده‌ها، مؤثر خواهد بود. لذا شناسایی روش‌های مختلف مستعارسازی، ارزیابی و مقایسه این روش‌ها و همین‌طور بررسی مهم‌ترین ریسک‌های موجود، برای تشخیص نقش و کاربرد آن در رعایت الزامات قانونی برای حفظ امنیت داده‌های شخصی ضروری خواهد بود.

۲.۲.۱. روش‌های تعیین نام مستعار و بازشناسایی اشخاص

ابتدا تعیین نام‌های مستعار به‌روش‌های مختلفی ممکن است؛ ازجمله خود اشخاص موضوع داده می‌توانند با انتخاب یک شناسه کاربری آزادانه انتخاب‌شده، نام مستعار خویش را تعیین کنند. همچنین می‌توان تعیین نام مستعار را به اشخاص یا ابزارهای ثالث مدیر سایت یا شبکه واگذار کرد. سومین مورد نیز امکان تعیین نام توسط خود کنترلگر داده‌ها به‌وسیله تعیین شماره شناسایی است. حال برای شناخت نقاط ارتباط بین داده‌های منبع و نام مستعار هم، دو روش در دسترس است: یکی تهیه لیست (که به‌عنوان جدول تخصیص نیز شناخته می‌شود) و دیگری روش محاسبه. در روش محاسبه، نام مستعار با به‌کارگیری الگوریتمی خاص و انجام معادلاتی بر خود داده‌های هویتی تعیین می‌شود.[2] یعنی با دسترسی به داده‌های منبع و دانستن الگوریتم، با دادن هر داده‌ای به دستگاه و اعمال آن معادله خاص، نام مستعار مربوطه به‌دست می‌آید. حال اگر نام مستعار با الگوریتم‌های پیچیده یا به‌شکل تصادفی انتخاب نشود، همواره امکان مهندسی معکوس الگوریتم‌ها و بازشناسایی افراد توسط اشخاص ثالث غیرمجاز وجود دارد. برای مثال، در سال

1. Judiciary.uk, "google-v-vidal-hall-judgment", Available at: (https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf) Visited 2025/08/11.
2. European Data Protection Board, *Ibid*, pp 15-25.

۲۰۰۶ در پرونده‌ای،[1] شرکت نت‌فلیکس صدها میلیون رکورد را به‌طور عمومی منتشر کرد که صدها هزار رتبه‌بندی توسط کاربران را درمورد فیلم‌های مختلف از سال ۱۹۹۹ تا ۲۰۰۵ نشان می‌داد. این شرکت همچنین یک جایزه یک‌میلیون دلاری را برای اولین تیمی که بتواند به‌طور قابل‌توجهی الگوریتم توصیه فیلم نت‌فلیکس را بهبود ببخشد، در نظر گرفت. اگرچه داده‌ها حاوی هیچ شناسه مستقیمی نبودند، در عرض چند هفته پس‌از انتشار داده‌ها، دو محقق توانستند با ارجاع متقابل داده‌های نت فلیکس با رتبه‌بندی سایت دیگری، زیرمجموعه‌ای از افراد خاص را دوباره شناسایی کنند. محققان فقط با استفاده از رتبه‌بندی شش فیلم مشترک، افراد را (اگر در هر دو مجموعه عضو بودند) دوباره شناسایی کردند. البته این روش فقط برای شناسایی مجدد کاربران نت‌فلیکس کارایی داشت که در آن سایت خاص نیز حساب داشتند.[2] در پرونده دیگری در سال ۲۰۱۴، اداره تاکسی و لیموزین شهر نیویورک مجموعه داده‌ای از تمام سفرهای در آن سال را براساس سیاست‌های مربوط به داده‌های باز و برای اهداف و مقاصد علمی و آماری منتشر کرد. نکته اینجاست که در آن سال این اداره پیش از انتشار داده‌ها، اقدام به مستعارسازی و ناشناس‌سازی آنها کرد. ایشان به‌طور خاص شماره تاکسی و شماره گواهینامه راننده را مستعار کردند. بااین‌حال، وبلاگ‌نویسان توانستند الگوریتم مورد استفاده برای تغییر شماره تاکسی را کشف و سپس آنها را معکوس کنند. بنابراین اگر نام مستعار به‌طور مداوم در یک یا چند مجموعه داده یا برای مدت طولانی استفاده شود، کارایی خود را از دست می‌دهد. لذا نام مستعار فقط درصورتی یک مکانیسم مؤثر پاک‌سازی اطلاعات هویتی است که نتوان آن را معکوس کرد. همچنین قدرتمندترین و رایج‌ترین ابزار برای شناسایی مجدد داده‌های پاک‌شده، ترکیب دو مجموعه داده است که شامل افراد یکسانی در هر دو مجموعه است. درمورد دیگری که نمونه‌ای برجسته از چالش‌های ناشناس یا مستعارسازی داده‌های پزشکی است، دکتر سوینی[3] با خرید فهرست رأی‌دهندگان شهر کمبریج و سپس پیوند آن با داده‌های بیمارستانی منتشرشده به‌شکل ناشناس در ایالت ماساچوست، توانست اطلاعات مربوط به افراد را دوباره شناسایی کند. این تجربه نشان داد که داده‌های به‌ظاهر مستعار، درصورت ترکیب با منابع خارجی می‌توانند به‌راحتی

1. Netflix Prize Data Privacy
2. Lubarsky, Boris, "Re-Identification of “Anonymized” Data", *GEO. L. TECH. REV*, No. 202, 2017, pp 206-211.
3. Latanya Sweeney

دوباره به افراد خاص مرتبط شوند و ازاین‌رو، اهمیت استفاده از تکنیک‌های پیشرفته یا ترکیبی در حفاظت از حریم خصوصی را برجسته کرد.

۲.۲.۲. روش‌های نوین مستعارسازی

یکی از این روش‌ها برای کاهش احتمال بازشناسایی افراد، روش "k-anonymity" است. در این روش، داده‌ها به‌گونه‌ای تغییر می‌کنند که ذیل هر ویژگی چند شخص قرار می‌گیرند. در مرحله اول با تعمیم، مقادیر دقیق ویژگی‌ها با مقادیر کلی‌تر یا بازه‌های گسترده‌تر جایگزین می‌شوند.[۱] به‌عنوان مثال، سن دقیق افراد به بازه‌های سنی مانند بیست تا سی سال تعمیم داده می‌شود. در مرحله بعد، برخی از مقادیر ویژگی‌ها به‌طور کامل حذف یا با کاراکترهای خاصی مانند ستاره یا مربع، جایگزین می‌شوند تا از شناسایی فرد جلوگیری شود. در این روش، حرف k به‌معنی تعداد افراد دارای ویژگی یکسان است، مثلاً اگر k=3 باشد، به این معنی است که هر فرد در مجموعهٔ داده حداقل در کنار دو نفر دیگر (در مجموع سه نفر) دارای ویژگی‌های مشابهی است. درنتیجه، حتی اگر کسی به داده‌ها دسترسی داشته باشد، نمی‌تواند یک فرد خاص را شناسایی کند؛ زیرا حداقل سه نفر دارای ویژگی‌های یکسانی هستند. اگر k خیلی کوچک باشد (مثلاً k=1)، داده‌ها تقریباً مستعار و ناشناس نیستند و ممکن است به‌راحتی هویت افراد مشخص شود. اگر k خیلی بزرگ باشد نیز ممکن است داده‌ها بیش از حد کلی شوند و ارزش تحلیلی خود را از دست بدهند.[۲]

روش دیگری به اسم "l-diversity" یکی از تکنیک‌های پیشرفته در حوزه حفاظت از حریم خصوصی داده‌هاست که به‌منظور رفع محدودیت‌های روش قبل توسعه‌یافته است. با اینکه روش اول هر شخص را با بیش از یک شخص دیگر که در ویژگی‌های کلیدی مشترک‌اند، در یک مجموعه قرار می‌دهد، اما همچنان آسیب‌پذیر است. در مقابل، روش دوم بر این اصل استوار است که در هر گروه از اشخاص ناشناس‌شده، حداقل "l" مقدار متمایز برای ویژگی‌های حساس وجود داشته باشد. این تنوع در مقادیر ویژگی‌های حساس، احتمال شناسایی یا استنباط اطلاعات حساس درباره یک فرد خاص را کاهش می‌دهد. تصور کنید شما یک گروه از افراد را در نظر گرفته‌اید که همه آنها در یک دسته قرار گرفته‌اند، مثلاً تمام مردان سی تا چهل‌ساله که در یک

1. Pinnamaneni, Nikhil and Dodda, Sumanth and Muvva, Sai Charan, "Survey paper on anonymization and pseudo-anonymization for E-healthcare", I*nternational Research Journal of Modernization in Engineering, Technology and Science*, Vol. 3, No. 7, 2021, p 770.
2. Sweeney, L, *Op.Cit*, p 558.

منطقه خاص زندگی می‌کنند. اگر همه این افراد دقیقاً یک بیماری یکسان داشته باشند (مثلاً دیابت)، این امر یعنی اگر کسی بفهمد یک فرد به این گروه تعلق دارد، می‌تواند با قطعیت بگوید که او دیابت دارد. در این صورت دیگر مستعارسازی چاره‌ساز نیست. بنابراین طبق روش دوم، در هر گروه باید چندین بیماری مختلف وجود داشته باشد، مثلاً برخی دیابت داشته باشند، برخی فشار خون، برخی میگرن و... تا حتی اگر کسی بفهمد یک فرد در این گروه قرار دارد، نتواند با اطمینان بگوید که بیماری او کدام است.[1]

در نهایت و در جدیدترین تلاش‌ها برای حل مشکلات روش‌های قبلی، روش «t-closeness» توسعه‌یافته است. این روش بر این اصل استوار است که توزیع مقادیر ویژگی‌های حساس در هر گروه مستعار شده، باید با توزیع کلی آن ویژگی‌ها در کل مجموعه داده‌ها نزدیک باشد؛ به‌طوری‌که تفاوت بین این دو توزیع از یک مقدار آستانه مشخص، که با t نشان داده می‌شود، فراتر نرود. برای مثال، اگر در کل مجموعه داده‌ها، ۹۰ درصد افراد سالم و ۱۰ درصد بیمار باشند، در هر گروه مستعارشده نیز باید توزیع وضعیت سلامتی نزدیک به این نسبت باشد. با حفظ توزیع واقعی داده‌ها در هر گروه، احتمال برداشت‌های نادرست یا گمراه‌کننده کاهش می‌یابد. در مجموع روش اخیر، با تمرکز بر حفظ توزیع ویژگی‌های حساس در هر گروه مستعارشده، سعی در ارائه تعادلی بین حفاظت از حریم خصوصی و حفظ دقت داده‌ها (برای مثال با هدف حفظ کارکردهای تجاری آنها) دارد.[2]

۲.۲.۳. روش پیشنهادی مستعارسازی

در آخر باید دانست که باوجود این روش‌ها، استفاده از مستعارسازی از هر نوعی که باشد، برای رعایت کامل اصول پردازش داده‌ها کافی نیست. از آنجایی که برای مثال طبق رسیتال ۲۸ قانون حمایت از داده‌های شخصی اتحادیه اروپا، منظور از معرفی صریح نام مستعار در این مقرره، جلوگیری از اقدامات دیگر برای حفاظت از داده‌ها نیست، لذا به‌کارگیری ترکیبی از روش‌های حفظ حریم داده‌ها می‌توانند در رعایت هرچه بیشتر اصول پردازش مؤثر باشند. برای مثال، برای

1. Machanavajjhala, A. and Gehrke, A. and Kifer D. and Venkitasubramaniam, M. "L-diversity: privacy beyond k-anonymity", *22nd International Conference on Data Engineering (ICDE'06)*, Atlanta, GA, USA, 2006, p 24.
2. Ninghui, Li and Tiancheng, Li and Venkatasubramanian, Suresh, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity", *IEEE 23rd International Conference on Data Engineering (ICDE)*, No. 2, 2007, pp 106-115.

رفع نارسایی‌های مستعارسازی، باید آن را با رمزگذاری ترکیب کرد؛ طی این روش، امکان اطلاع از محتوای داده‌های شخصی محدود به افرادی می‌شود که به کلید خاص برای رمزگشایی آنها دسترسی دارند.[۱] برای این منظور ابتدا داده‌ها مستعار می‌شوند (یعنی نشانه‌های هویتی از داده‌ها جدا می‌شود و سپس نام یا شماره یا شناسهٔ مستعاری به آنها اختصاص پیدا می‌کند) و بعد آن نقطه ارتباط بین نام مستعار و شخص حقیقی (که کلید شناسایی شخص موضوع داده‌هاست) رمزگذاری می‌شود. برای مثال، در صورت نیاز به انتقال اطلاعات کاربران شرکت کنترلگر داده‌ها به شرکت ثالث پردازشگر، برای تجزیه‌وتحلیل نیازهای مشتریان، پس‌از حذف نام و آدرس از پرونده محمد محمدی، پرونده این شخص، که مشتری شرکت است و ماهانه از خدمات شرکت در زمینه طراحی سایت استفاده می‌کند، با نام مستعار «الف» به شرکت پردازشگر تحویل داده شده و اطلاعاتی که می‌گویند «الف» همان محمد محمدی به آدرس فلان است، در کنار داده‌های منبع، هر دو به‌صورت رمزگذاری‌شده نزد کنترلگر نگهداری می‌شوند. در این صورت، شرکت‌ها با سه مجموعه داده روبه‌رو هستند، ۱. داده‌های منبع (محمد محمدی به آدرس فلان، مشتری شرکت است)، ۲. داده‌های مربوط به ارتباط نام‌های مستعار («الف» همان محمد محمدی است) و ۳. داده‌های مستعار («الف» مشتری شرکت است). هر زمان کنترلگر یا شخص خاصی از جانب پردازشگر مایل بود تا به‌دلیل خاصی و در محدوده قوانین و توافقات قراردادی، «الف» را بشناسد، فقط با استفاده از کلید خاصی و به‌صورت محدود، با رمزگشایی از نام مستعار ازطریق دسترسی به داده‌های ارتباطی، به اطلاعات شخصی دسترسی پیدا می‌کند. در چنین وضعیتی، هم انتقال داده‌ها به‌صورت مستعار و بدون افشای هویت افراد به ثالث و پردازش امن آن توسط ایشان تضمین می‌شود و هم به‌دلیل رمزگذاری، در فرض دسترسی غیرمجاز یا نفوذ به داده‌های منبع یا داده‌های ارتباطی و یا افشای آنها، از برقراری ارتباط میان این داده‌ها با داده‌های مستعار و کشف نقاط ارتباط و بازشناسایی افراد جلوگیری می‌شود. در همین فرض نیز رعایت برخی جزئیات اازجمله نگهداری داده‌ها به‌شکل پراکنده و در مکان‌های متفاوت، استفاده از رمزهای تصادفی و گوناگون با ویژگی تغییر خودکار در طول زمان، گزینش مناسب افراد مجاز به

۱. انصاری، باقر و شیما عطار، **حقوق کاربران فضای مجازی**، چ ۱، تهران: شرکت سهامی انتشار، ۱۴۰۲، ص ۵۶.

دسترسی به کلیدها و استفاده از نام‌های مستعار غیریکسان در استفاده‌های مختلف از داده‌ها، از ریسک‌های موجود در نگهداری امن داده‌ها می‌کاهد.[1]

نتیجه‌گیری

ایجاد برنامه‌ها و خدمات داده‌محور جدید، شخصی‌سازی‌شده و بهینه‌سازی‌شده، معمولاً نیازمند جمع‌آوری، تجزیه‌وتحلیل و افشای مقادیر فزاینده‌ای از داده‌هاست. چنین سیستم‌هایی از مجموعه داده‌هایی استفاده می‌کنند که شامل داده‌های شخصی است و بنابراین استفاده و افشای آنها خطری برای حریم خصوصی کاربر (موضوع داده‌ها) است. این داده‌ها ممکن است توسط ثالث پردازش، برای اشخاص مورد اعتماد افشا یا برای منافع اجتماعی در حوزه عمومی منتشر شود (مانند تحقیقات علمی و پزشکی). همچنین ممکن است در داخل سیستم‌ها برای بهبود ارائه یک سرویس به کار رود (به‌عنوان مثال برای مدیریت بهتر منابع، یا بهینه‌سازی یک سرویس برای کاربران). نکته مهم این است که در تمام این موارد، حفظ حریم افراد اهمیت دارد. بنابراین مستعارسازی به‌عنوان یکی از بهترین روش‌ها مطرح می‌شود.[2] همان‌طورکه گفته شد، مستعارسازی درست و اصولی داده‌ها با کاهش یا حتی نفی احتمال بازشناسایی اشخاص موضوع داده توسط ثالث غیرمجاز همراه خواهد بود. در چنین فرضی و به‌شرط عدم امکان شناسایی افراد، مستعارسازی می‌تواند روش مناسبی برای رعایت برخی از اصول پردازش قانونی داده‌ها باشد؛ ازجمله اصل امنیت و محرمانگی داده‌ها تا حد زیادی از طریق استفاده از نام‌های مستعار و قطع ارتباط هویت افراد با داده‌های تحویل‌داده‌شده به پردازشگر اجرا می‌شود. همچنین اصل کمینه‌سازی پردازش داده‌ها و محدودیت اهداف پردازش نیز با مستعارسازی داده‌ها و کاهش حجم اطلاعات و شناسه‌های انتقالی و درنتیجه، محدود کردن دایره استفاده‌ها و اهداف ثانویه در پردازش رعایت می‌شود. در نهایت انجام مستعارسازی، نشان‌دهنده سطح بالایی از مسئولیت‌پذیری شرکت کنترلگر یا پردازشگر خواهد بود.

بااین‌حال، اولاً با عنایت به نحوه بیان قوانین و مقررات حمایت از داده‌های شخصی، که کدام شرکت‌ها را در عین تصریح در خصوص مستعارسازی، نسبت به انجام سایر رویه‌ها و

1. Heurix, Johannes and Karlinger, Michael and Neubauer, Thomas, *Op.Cit*, pp 3011-3013.
2. Neumann, G.K. and Grace, P. and Burns, D. et al, "Pseudonymization risk analysis in distributed systems", *Journal of Internet Services and Applications*, Vol. 10, No. 1, 2019, p 1.

تکنیک‌های فنی نیز ملزم می‌دانند و ثانیاً به‌دلیل عدم تأثیر مستقیم مستعارسازی در رعایت برخی از اصول پردازش مثل اصل مشروعیت و دقت، استفاده از ترکیبی از روش‌های حفاظتی، درزمینه رعایت اصول پردازش داده‌های شخصی، ضمن حفظ تعادل میان این جنبه‌های فردی و ابعاد تجاری و اقتصادی داده‌ها (با کاهش اتلاف داده‌ها و افزایش قابلیت به‌کارگیری آنها برای تأمین منافع تجاری مشروع) ضروری است. در همین راستا به‌عنوان یک روش پیشنهادی، مستعارسازی داده‌ها در کنار رمزگذاری کلیدهای مربوط به برقراری ارتباط میان نام‌های مستعار و هویت حقیقی افراد، با کاهش احتمال بازشناسایی اشخاص موضوع داده و همچنین تأمین امکان استفاده‌های ثانویه از داده‌ها (برخلاف ناشناس‌سازی که به‌دلیل بازگشت‌ناپذیری، با اتلاف ارزش داده‌ها همراه است)، یک روش فنی ترکیبی مناسب برای تضمین امنیت داده‌های شخصی و رعایت اصول پردازش داده‌ها به شمار می‌رود.

منابع

کتاب

۱. انصاری، باقر، **اصول پردازش داده‌های شخصی**، چ ۱، تهران: شرکت سهامی انتشار، ۱۴۰۲.

۲. انصاری، باقر و عطار، شیما، **حقوق کاربران فضای مجازی**، چ ۱، تهران: شرکت سهامی انتشار، ۱۴۰۲.

۳. زند، حسین، **حمایت از داده‌ها در حقوق موضوعه ایران**، چ ۲، تهران: شرکت سهامی انتشار، ۱۴۰۳.

مقاله

٤. اسماعیلی، محسن و مهدی نریمان‌پور، «مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران)»، *حقوق اسلامی*، د. ۲۱، ش. ۸۲، ۱۴۰۳، صص ۱۲۳-۱۶۵،

https://doi.org/10.22034/ilaw.2023.708599.

۵. پور یوسف، زهرا، مهری رجایی و نیک‌محمد بلوچزهی، «حفظ حریم خصوصی خودروها در شبکه‌های ارتباطات خودرویی»، همایش ملی پژوهش‌های نوین در علوم و فناوری، ۱۳۹۷، تهران، ایران.

۶. حسینی، علی، «حقوق حفاظت از داده‌های شخصی در پردازش الگوریتمی، چالش‌ها و راهکارها»، دولت و حقوق، د. ۵، ش. ۱، ۱۴۰۳، صص ۹۹-۱۲۲.

۷. صادقی، حسین و مهدی ناصر، «جستاری در ماهیت‌شناسی داده‌های خصوصی در سازوکار عملکرد ابزارهای فناوری اینترنت اشیا»، *فصلنامه رشد فناوری*، د. ۱۹، ش. ۲، ۱۴۰۲، صص ۳۳-۴۱.

۸. عرب سرخی، ابوذر و طلا تفضلی، «تحلیل موضوعات راهبردی در قلمرو مقررات حفاظت از داده‌های عمومی»، *دوفصلنامه علمی منادی امنیت فضای تولید و تبادل اطلاعات*، د. ۱۳، ش. ۲، ۱۴۰۳، صص ۱۲-۲۳.

۹. فرحزادی، علی‌اکبر، حسین صادقی، و مهدی ناصر، «وظایف کنترل‌کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات»، *قضاوت*، د. ۲۲، ش. ۱۱۲، ۱۴۰۱، صص ۷۱-۹۹.

۱۰. لطیف زاده، مهدیه، سید محمدمهدی قبولی درافشان، سعید محسنی و محمد عابدی، «تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا»، *پژوهشنامه پردازش و مدیریت اطلاعات*، د. ۳۷، ش. ۲، ۱۴۰۰، صص ۴۳۹-۴۷۲.

https://doi.org/10.52547/jipm.37.2.439 .

۱۱. مزینانیان، سعیده، «تنظیم‌گری حریم خصوصی در فضای مجازی (مطالعه تطبیقی در حقوق ایالات متحده آمریکا، اتحادیه اروپا و ایران)»، *پژوهش‌های حقوق اقتصادی و تجاری*، د. ۱، ش. ۲، ۱۴۰۳، صص ۲۰۷-۲۳۹.

https://doi.org/10.48308/eclr.2023.232727.1030.

منابع برخط

۱۲. طرح حفاظت از داده‌های شخصی مورخ ۱۴۰۳/۰۷/۱۵ مجلس شورای اسلامی، قابل دسترسی در: (https://rc.majlis.ir/fa/legal_draft/show/181672)، تاریخ آخرین بازدید: ۱۴۰۴/۰۵/۲۰.

۱۳. طرح حمایت و حفاظت از داده و اطلاعات شخصی مورخ ۱۴۰۰/۰۶/۲۶ مجلس شورای اسلامی، قابل دسترسی در:
https://media.dotic.ir/uploads/org/2021/10/09/163377045160152200.pdf)
تاریخ آخرین بازدید: ۱۴۰۴/۰۵/۲۰.

References

Books

1. Ansari, Bagher, **Principles of Personal Data Processing**, 1st edition, Tehran: Sherkat Sahami Enteshar, 2023. (in Persian)
2. Ansari, Bagher and Attar, Shima, **Rights of Cyberspace Users**, 1st edition, Tehran: Sherkat Sahami Enteshar, 2023. (in Persian)
3. Zand, Hossein, **Data Protection in Iranian Positive Law**, 2nd edition, Tehran: Sherkat Sahami Enteshar, 2024. (in Persian)

Articles

4. Al-Zubaidie, M. and Zhang, Z. and Zhang, J, "PAX: Using Pseudonymization and Anonymization to Protect Patients' Identities and Data in the Healthcare System", *International Journal of Environmental Research and Public Health*, Vol. 16, No. 9, 2019, pp 1-36, https://doi.org/10.3390/ijerph16091490.
5. Arab Sorkhi, Abouzar and Tafazoli, Tala, "Analysis of Strategic Issues in the Realm of General Data Protection Regulations", *Monadi AFTA*, Vol. 13, No. 2, 2024, pp 12-23. (in Persian)
6. Bolognini, Luca and Bistolfi, Camilla, "Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulation", *Computer Law & Security Review*, Vol. 33, No. 2, 2017, pp 171-181, https://doi.org/10.1016/j.clsr.2016.11.002.
7. Bourdillon, Stalla and Alison, Sophie, "Anonymous Data v. Personal Data, A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data", *Wisconsin International Law Journal*, 2017, pp 1-38.
8. El Emam, K and Jonker, E and Arbuckle, L and Malin, B. "A Systematic Review of Re-Identification Attacks on Health Data", *PLoS One*, Vol. 6, No. 12, 2015, pp 1-12, https://doi.org/10.1371/journal.pone.0126772.
9. Esmaeili, Mohsen and Narimanpour, Mehdi, "Legal Foundations of Personal Data Exchange (A Comparative Study of the EU General Data Protection Regulation and Iranian Law) ", *Islamic Law*, Vol. 21, No. 82, 2024, pp 123-165, doi: 10.22034/ilaw.2023.708599. (in Persian).
10. Farahzadi, Ali Akbar and Sadeghi, Hossein and Naser, Mehdi, "Duties of Controllers and Processors in Preventing Security Breaches in

Information Exchange Networks", *Ghezavat*, Vol. 22, No. 112, 2022, pp 71-99. (in Persian)

11. Gazizov, Andrey and Gazizov, Evgeny and Gazizova, Svetlana, "Theoretical Aspects of the Protection of Personal Data of Employees of the Enterprise by the Method of Pseudonymization", *E3S Web Conf*, 2020, pp 1-8, https://doi.org/10.1051/e3sconf/202021011001.
12. Heurix, Johannes and Karlinger, Michael and Neubauer, Thomas, "Pseudonymization with Metadata Encryption for Privacy-Preserving Searchable Documents", *45th Hawaii International Conference on System Sciences*, Maui, HI, USA, 2012, pp 3011-3020. https://doi.org/10.1109/HICSS.2012.491.
13. Heurix, Johannes and Karlinger, Michael and Schrefl, Michael & Neubauer, Thomas, "A Hybrid Approach Integrating Encryption and Pseudonymization for Protecting Electronic Health Records", *Proceedings of the 8th IASTED International Conference on Biomedical Engineering*, Innsbruck, Austria, 2011, pp 1-8. https://doi.org/10.2316/P.2011.723-117.
14. Heurix, Johannes and Neubauer, Thomas, "Privacy-Preserving Storage and Access of Medical Data through Pseudonymization and Encryption", *Lecture Notes in Computer Science*, 6863, Berlin, Heidelberg, 2011, pp 1-12, https://doi.org/10.1007/978-3-642-22890-2_16.
15. Hosseini, Ali, "Data Protection Law in Algorithmic Processing: Challenges and Solutions", *Government and Law*, Vol. 5, No. 1, 2024, pp 99-122. (in Persian)
16. Latifzadeh, Mahdieh and Ghobouli Dorafshan, Seyed Mohammad Mehdi and Mohseni, Saeed and Abedi, Mohammad, "Analysis of the Legal Framework for Personal Data Protection in the European Union", *Information Processing and Management Research Journal*, Vol. 37, No. 2, 2021, pp 439-472, https://doi.org/10.52547/jipm.37.2.439, (in Persian).
17. Lehmann, Anja, "ScrambleDB: Oblivious (Chameleon) Pseudonymization-as-a-Service", *Privacy enhancing technologies*, No 3, 2019, pp 289–309, https://doi.org/10.2478/popets-2019-0048.
18. Lubarsky, Boris, "Re-Identification of “Anonymized” Data", *GEO. L. TECH. REV*, 202, 2017, pp 202-213.
19. Machanavajjhala, A. and Gehrke, A. and Kifer D. and Venkitasubramaniam, M. "L-Diversity: Privacy Beyond k-Anonymity",

22nd International Conference on Data Engineering (ICDE'06), Atlanta, GA, USA, 2006, pp 24-24, https://doi.org/10.1145/1217299.1217302.

20. Mazinanian, Saeedeh, "Regulating Privacy in Cyberspace (A Comparative Study in the Laws of the United States, European Union, and Iran) ", *Economic and Commercial Law Research*, Vol. 1, No. 2, 2023, pp 207-239, doi: 10.48308/eclr.2023.232727.1030, (in Persian)
21. Neubauer, Thomas and Heurix, Johannes, "A Methodology for the Pseudonymization of Medical Data", *International Journal of Medical Informatics*, Vol. 80, No. 3, 2011, pp 190-204. https://doi.org/10.1016/j.ijmedinf.2010.10.016.
22. Neumann, G.K. and Grace, P. and Burns, D. et al, "Pseudonymization Risk Analysis in Distributed Systems", *Journal of Internet Services and Applications*, Vol. 10, No. 1, 2019, pp 1-16. https://doi.org/10.1186/s13174-018-0098-z.
23. Ninghui, Li and Tiancheng, Li and Venkatasubramanian, Suresh, "T-Closeness: Privacy Beyond k-Anonymity and l-Diversity", *IEEE 23rd International Conference on Data Engineering (ICDE)*, No 2, 2007, pp 106-115.
24. Pinnamaneni, Nikhil and Dodda, Sumanth and Muvva, Sai Charan, "Survey Paper on Anonymization and Pseudo-Anonymization for E-healthcare", *International Research Journal of Modernization in Engineering, Technology and Science*, Vol. 3, No. 7, 2021, pp 769-775.
25. Pouryousef, Zahra and Rajaei, Mehri and Balochzehi, Nik Mohammad, "Preserving Vehicle Privacy in Vehicular Communication Networks", *National Conference on New Researches in Science and Technology*, 2018, Tehran, Iran. (in Persian)
26. Ribeiro, S. L. and Nakamura, E. T, "Privacy Protection with Pseudonymization and Anonymization in a Health IoT System: Results from OCARIoT", *IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE)*, Athens, Greece, 2019, pp 904-908, https://doi.org/10.1109/BIBE.2019.00169.
27. Sadeghi, Hossein and Naser, Mehdi, "An Inquiry into the Nature of Private Data in the Functioning Mechanism of Internet of Things Technologies", *Technology Growth*, Vol. 19, No. 2, 2023, pp 33-41. (in Persian)
28. Shin, Soo Yong and kim, Hun Sung, "Data Pseudonymization in a Range That Does Not Affect Data Quality: Correlation with the Degree of

Participation of Clinicians", *Journal of Korean Medical Science*, Vol. 36, No. 44, 2021, pp 1-11, https://doi.org/10.3346/jkms.2021.36. e299.

29. Starchon, Peter and Pikulik, Tomas, "GDPR Principles in Data Protection Encourage Pseudonymization through Most Popular and Full-Personalized Devices - Mobile Phones", *Procedia Computer Science*, No 151, 2019, pp 303-312, https://doi.org/10.1016/j.procs.2019.04.043.
30. Sweeney, L, "K-Anonymity: A Model for Protecting Privacy, International Journal on Uncertainty", *Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 5, 2002, pp 557-570. https://doi.org/10.1142/S0218488502001648.

Websites

31. Data Protection Commission IE, "Guidance on Anonymisation and Pseudonymisation", Available at: 20 Anonymisation%20and%20Pseudonymisation.pdf) Visited 2025/02/08.
32. Dotic "Personal Data and Information Protection Bill, dated 26/06/1400 (September 17, 2021), Available at:
33. https://media.dotic.ir/uploads/org/2021/10/09/163377045160152200.pdf, Visited: 2025/08/11, [In Persian].
34. ISO/IEC, "Privacy Enhancing Data De-Identification Terminology and Classification of Techniques", Available at: (https://www.iso.org/obp/ui/#iso:std:iso-iec:20889:ed-1:v1:en) Visited 2025/01/25.
35. Judiciary.uk, "google-v-vidal-hall-judgment", Available at: (https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf) Visited 2025/08/11.
36. Majlis.ir "Personal Data Protection Bill, dated 15/07/1403 (July 6, 2024)", Available at: (https://rc.majlis.ir/fa/legal_draft/show/181672), Visited visited: 2025/08/11, [In Persian]
37. Robin data, "What is Pseudonymised Data? " Available at: (https://www.robin-data.io/en/data-protection-and-data-security-academy/wiki/pseudonymised-data) Visited 2025/01/25.
38. European Data Protection Board, "Guidelines 01/2025 on Pseudonymisation", Available at: (https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en) Visited 2025/02/08.

The Importance and Legal Challenges of Data Pseudonymization: Considering the Principles of Personal Data Processing

Amirmohammad Ghorban Nia*
Zahra Shakeri**

Received: 2025.03.06 Accepted: 2025.08.27

Abstract

Across all countries and within the framework of personal data protection laws, due to the expansion of data volume processed by various companies, fundamental principles such as legality, accuracy, security, purpose limitation, and data minimization have been established to minimize violations of individuals' privacy. Furthermore, these legal frameworks often reference specific technical methods designed to ensure the secure processing of personal data, including pseudonymization. However, due to insufficient attention to the details of these techniques and tools within the laws of leading jurisdictions—and the absence of explicit legal provisions in countries such as Iran—significant ambiguities persist regarding their proper implementation, effects, economic aspects, and the role of pseudonymization in ensuring compliance with data processing principles. This study adopts a descriptive-analytical approach, relying on both printed and digital library sources, and employs a comparative perspective to scrutinize the technical methodologies and specific requirements for effective pseudonymization. The primary research question addressed is: To what extent does pseudonymization contribute to precise implementation of legal data processing principles? The findings indicates that, although pseudonymization effectively reduces the direct linkage between data and individual identities, it alone is insufficient to guarantee full compliance with legal processing principles—particularly if the process remains reversible. Nonetheless, when combined with additional techniques such as data encryption, pseudonymization can substantially enhance compliance with data processing principles.

Keywords:

Data Processing Principles, Privacy, Personal Data, Pseudonymization.

* L.L.M., Faculty of Law & Political Science, University of Tehran, Tehran, Iran.
** Associate Professor, Faculty of Law & Political Science, University of Tehran, Tehran, Iran Corresponding Author Email: zshakeri@ut.ac.ir