Digital Islamic Studies and Humanities

www.disah.inoor.ir

How to secure personal data in digital humanities

Mahdieh Latifzadeh[1]✉

1. Assistant professor of the research group of jurisprudence and Islamic Law, Ferdowsi University of Mashhad, Mashhad, Iran. Email: M.latifzadeh@mail.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 12 April 2025
Received in revised form: 22 June 2025
Accepted: 11 July 2025
Available online: 23 August 2025

Keywords:
Principles relating to processing of personal data, Personal data processing, Sensitive personal data, Data protection management system, Pseudonymization.

ABSTRACT

Benefiting from personal data as one of the basic resources in the field of digital humanities; It is a multifaceted matter and a combination of advantages and challenges. Although data-based research provides valuable insight into how people interact with human and Islamic knowledge and helps to develop learning resources and tools, the use of personal data in the field of digital humanities has many challenges. One of the most important challenges is how to effectively protect information privacy and maintain the security of personal data. This is especially true for specific personal data that require special protection due to the nature of the data itself or the data subjects. In this regard, this research, focusing on the necessity of such protection, by relying on the descriptive-analytical method and benefiting from the comparative method, has concluded that in this field personal data must be protected in both technical and legal dimensions. In fact, the flow of requirements related to personal data, including the principles governing processing as a legal solution, as well as the use of data anonymization and pseudonymization methods and the use of the data protection management system as technical methods are necessary. It seems that paying attention to these dimensions and the legislator's effort to realize such protections can provide maximum benefit and minimum harm to the data subjects in the face of digital humanities.

Cite this article: Latifzadeh, M. (2025). How to secure personal data in digital humanities. *Digital Islamic Studies and Humanities*, 1 (1), 155-178. https://doi.org/10.22034/disah.2024.716148

 Publisher: Research Center for Digital Islamic Studies and Humanities (RCDISAH).
DOI: https://doi.org/10.22034/disah.2024.716148

علوم اسلامی و انسانی دیجیتال

www.disah.inoor.ir

چگونگی حفظ امنیت داده‌های شخصی در حوزه علوم انسانی دیجیتال

مهدیه لطیف‌زاده[1]

۱. استادیار گروه پژوهشی فقه و حقوق اسلامی، دانشگاه فردوسی مشهد، مشهد، ایران: M.latifzadeh@mail.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۱/۲۳
تاریخ بازنگری: ۱۴۰۴/۰۴/۰۱
تاریخ پذیرش: ۱۴۰۴/۰۴/۲۰
تاریخ انتشار: ۱۴۰۴/۰۶/۰۱

کلیدواژه‌ها:
اصول حاکم بر پردازش، پردازش داده‌های شخصی، داده‌های شخصی حساس، سیستم مدیریت حفاظت از داده، مستعار سازی.

چکیده

بهره‌مندی از داده‌های شخصی به‌عنوان یکی از منابع اساسی برای علوم انسانی دیجیتال، امری چندوجهی و مرکب از مزایا و چالش‌ها است. از یک‌سو، پردازش این داده‌ها فوایدی دارد، از جمله این که تحقیقات و پژوهش‌های مبتنی بر داده‌ها بینش‌های ارزشمندی را در مورد نحوه تعامل افراد با دانش انسانی و اسلامی ارائه می‌دهد که به توسعه منابع و ابزارهای یادگیری کمک می‌کند. از سوی دیگر، تعامل داده‌های شخصی با علوم انسانی دیجیتال چالش‌های متعددی را نیز به دنبال دارد. از جمله مهم‌ترین آن‌ها، چگونگی حمایت مؤثر از حریم خصوصی اطلاعاتی و حفظ امنیت داده‌های شخصی است. این امر خصوصاً در مورد داده‌های شخصی خاص که به دلیل ماهیت خود داده‌ها یا اشخاص موضوع داده نیاز به حمایت ویژه دارند، حائز اهمیت است. با توجه به ضرورت چنین حمایتی، باید از داده‌های شخصی در دو بعد فنی و قانونی حمایت صورت گیرد. در جنبه قانونی، جریان الزامات حقوقی مربوط به داده‌های شخصی راهگشا است، لیکن به دلیل فقدان این امر در نظام حقوقی ایران، در حال حاضر بهره‌مندی از بعد فنی باید بیشتر مورد توجه قرار گیرد. بدین جهت، پژوهش حاضر ضمن تلاش برای مساعدت به قانون‌گذار در جهت توجه به الزامات حقوقی مربوط به داده‌های شخصی در برخورد با علوم انسانی دیجیتال، روش‌های فنی متعددی را نیز در جهت تحقق حفظ امنیت داده‌ها ارائه نموده است. به نظر می‌رسد توجه به ابعاد مختلف این پژوهش و جریان آن در مقام عمل، می‌تواند برای اشخاص موضوع داده، بهره‌مندی حداکثری و آسیب حداقلی را در برخورد با علوم انسانی دیجیتال فراهم نماید.

استناد: لطیف‌زاده، مهدیه (۱۴۰۴). چگونگی حفظ امنیت داده‌های شخصی در حوزه علوم انسانی دیجیتال. علوم انسانی و اسلامی دیجیتال، ۱ (۱)، ۱۵۵-۱۷۸. https://doi.org/10.22034/disah.2024.716148

ناشر: پژوهشکده علوم اسلامی و انسانی دیجیتال (مرکز تحقیقات کامپیوتری علوم اسلامی نور).

مقدمه

علوم انسانی دیجیتال به‌عنوان بستری در حال رشد برای استفاده از ابزارها و روش‌های فناورانه در مطالعات علوم انسانی، یک حوزه بین‌رشته‌ای است که محققان متعددی را درگیر کرده است. در این راستا، محققان از طیف گسترده‌ای از ابزارها و فناوری‌های دیجیتالی برای مطالعه داده‌های علوم انسانی استفاده می‌کنند. این امر شامل متن‌کاوی است که به تجزیه‌وتحلیل مقادیر زیادی از داده‌های متنی مانند کتاب‌ها، مقالات و وب‌سایت‌ها می‌پردازد. متن‌کاوی می‌تواند برای شناسایی الگوها، شیوه‌ها و مضامین در داده‌ها مورد استفاده قرار گیرد. همچنین، آرشیوهای دیجیتالی، داده‌های علوم انسانی مانند کتاب‌های دیجیتالی، دست‌نوشته‌ها و تصاویر را ایجاد و نگهداری می‌کنند.

با وجود توسعه و تکامل چشم‌انداز دیجیتال در حوزه علوم انسانی، اهمیت وجود و استمرار امنیت برای داده‌ها روزافزون می‌شود، زیرا داده‌ها منبع اصلی فعالیت‌ها در حوزه علوم انسانی دیجیتال هستند. در این خصوص، چالش‌هایی در مورد امنیت داده‌ها، خصوصاً داده‌های شخصی، که به‌موجب نظام‌های حقوقی مختلف، الزامات حقوقی بسیاری در راستای حمایت از آن‌ها وجود دارد، ایجاد می‌شود (Cruz et al, 2022: 2). این امر به دلیل آن است که علوم انسانی دیجیتال اغلب حجم زیادی از داده‌های شخصی مانند اطلاعات کاربران، ابر داده‌ها و محتوای مرتبط را جمع‌آوری و ذخیره می‌کند. این داده‌های شخصی می‌توانند در برابر سرقت، سوءاستفاده یا دسترسی غیرمجاز آسیب‌پذیر باشند.

باید اطمینان حاصل شود که داده‌های شخصی مطابق با قواعد حریم خصوصی در طرح‌های علوم انسانی دیجیتال مورد استفاده قرار می‌گیرند. در این راستا، نه‌تنها باید محافظت از داده‌های شخصی در برابر دسترسی یا نقض غیرمجاز لحاظ شود، بلکه سایر مسائل مهم مربوط به حریم خصوصی اطلاعاتی، از جمله کسب رضایت معتبر، رعایت ملاحظات اخلاقی و تحقق مبانی حقوقی در پردازش داده‌های شخصی نیز مورد توجه قرار گیرد. بدین ترتیب، باید از روش‌های ایمن برای جلوگیری از سوءاستفاده یا بهره‌برداری نامناسب از داده‌های شخصی استفاده شود (Krtalic, Marcetic & Micunovic, 2016: 3).

با توجه به این مطالب، این پژوهش با روش توصیفی-تحلیلی و بهره‌مندی از مطالعات تطبیقی به دنبال دستیابی به امنیت داده‌های شخصی در علوم انسانی دیجیتال است. برای نیل به این هدف،

پژوهش حاضر با تعریف و تبیین انواع داده‌های شخصی مسیر خود را آغاز می‌کند؛ سپس چالش‌های امنیتی مربوط به داده‌های شخصی در حوزه علوم انسانی دیجیتال را مورد توجه قرار خواهد داد و در نهایت به مؤثرترین روش‌ها برای حفظ امنیت داده‌ها در این حوزه اشاره خواهد نمود. ناگفته نماند که با جست‌وجو در خصوص پیشینه موضوع حاضر، اثر قابل توجهی مشاهده نشده است؛ این امر خود دلیلی بر اهمیت پژوهش حاضر و موکدی بر ضرورت پرداختن به این موضوع با توجه به توسعه فناوری در حوزه علوم انسانی است.

الف. تعریف و تبیین انواع داده‌های شخصیِ مورد استفاده در علوم انسانی دیجیتال

داده‌های شخصی در مهم‌ترین سند حقوقی مربوط به آن، یعنی مقررات اروپایی حفاظت از داده‌ها،[1] به‌عنوان «هر نوع اطلاعاتی که مربوط به شخص حقیقی شناخته‌شده یا قابل‌شناسایی (شخص موضوع داده) است» تعریف می‌شود. یک فرد حقیقی قابل‌شناسایی کسی است که به‌طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به یک شناسه از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه آنلاین یا به یک یا چند ویژگی خاص، مانند هویت فیزیکی، فیزیولوژیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی، شناسایی شود (EUR-Lex, 2016: 33).

با توجه به این تعریف، ملاک دادهٔ شخصی بودن، شناسایی یک فرد بر اساس اطلاعات موجود است؛ بدین معنا که بتوان یک فرد را به‌طور مستقیم یا غیرمستقیم با ارجاع به یک شناسه، شناسایی کرد. یک فرد حقیقی می‌تواند با ارجاع به شناسه‌هایی نظیر ویژگی‌های زیستی مانند شکل ظاهری، قد، وزن، اثر انگشت، DNA و الگوهای شبکیه‌ای یا توسط شناسه‌های بیوگرافی کسب‌شده، مانند آدرس، تحصیلات، گواهی‌نامه رانندگی، گذرنامه، حساب بانکی، شماره‌های شناسایی منحصربه‌فرد مانند شماره تأمین اجتماعی و شماره‌حساب مالیاتی دائمی، قابل‌شناسایی باشد.

1. General Data Protection Regulation(GDPR).
Regulation (Eu) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/Ec (General Data Protection Regulation).

بدین ترتیب، اگر شناسه‌ها منجر به شناسایی شخص حقیقی شوند یا قابلیت شناسایی را فراهم کنند، دادهٔ شخصی محسوب می‌شوند. بنابراین، در مواردی ترکیبی از شناسه‌ها و اطلاعات، دادهٔ شخصی را تشکیل می‌دهند و در برخی موارد نیز یک شناسه یا یک اطلاعات با فراهم آوردن امکان شناسایی شخص حقیقی، دادهٔ شخصی محسوب می‌شود که می‌تواند انواع مختلف داده‌های شخصی تلقی شود (Singh, 2016: 124).

یک نوع مهم از داده‌های شخصی که الزامات حقوقی ویژه‌ای برای آن وجود دارد، داده‌های شخصی خاص است. بر اساس مقررات اروپایی حفاظت از داده‌ها، برای پردازش داده‌های شخصی عمومی، رعایت اصول خاصی لازم است[1] که مربوط به داده‌هایی با وضعیت عمومی هستند و حالت ویژه‌ای ندارند. در مقابل، برای پردازش سایر داده‌های شخصی که به‌واسطه ماهیت خود، خاص

۱. مقررات اروپایی حفاظت از داده‌ها برای پردازش داده‌های شخصی، اصول خاصی را در ماده ۵ با عنوان «اصول مربوط به پردازش داده‌های شخصی» مقرر کرده است. این اصول پایه و اساس این مقررات را تشکیل می‌دهند و با وجود این که الزامات پیچیده‌ای ندارند، عدم رعایت آن‌ها، اشخاص پردازش‌کننده داده (کنترل‌کننده‌ها و پردازنده‌ها) را در معرض ضمانت اجراهای متعددی قرار می‌دهد. ماده ۵ اصول حاکم بر پردازش داده‌های شخصی را به شرح ذیل مقرر می‌نماید. داده‌های شخصی باید:
به‌طور مشروع، منصفانه و به شیوه‌ای شفاف در رابطه با شخص موضوع داده پردازش شوند (اصل مشروعیت، انصاف و شفافیت).
برای اهداف مشخص، صریح و مشروع جمع‌آوری شده و به شیوه‌ای که با آن اهداف ناسازگار است، پردازش نشوند. پردازش بیشتر – نسبت به هدف پردازش – در جهت بایگانی برای منافع عمومی، اهداف تحقیقات علمی یا تاریخی یا اهداف آماری، مطابق با ماده ۸۹، با اهداف اولیه ناسازگار تلقی نمی‌شود (اصل محدودیت هدف).
کافی، مرتبط و محدود به آنچه در ارتباط با اهداف پردازش داده لازم است، پردازش شوند (اصل به حداقل رساندن داده).
صحیح و در صورت لزوم به‌روز باشند، هر گام معقول و منطقی باید برداشته شود تا اطمینان حاصل شود که داده‌های شخصی نادرست با توجه به اهداف پردازش بدون تأخیر حذف یا تصحیح می‌شوند (اصل صحت).
به شکلی نگهداری شوند که موجبات شناسایی اشخاص موضوع داده بیش از آنچه برای هدف پردازش لازم است، ایجاد نشود. داده‌های شخصی را می‌توان برای مدت طولانی‌تری ذخیره کرد، البته صرفاً تا زمانی که داده‌ها برای مقاصد بایگانی به نفع عموم، اهداف تحقیقات علمی یا تاریخی یا اهداف آماری مطابق با ماده ۸۹ پردازش شوند. این امر مشروط به اجرای اقدامات فنی و سازمانی مدنظر این مقررات به‌منظور حفظ حقوق و آزادی‌های شخص موضوع داده است (اصل محدودیت ذخیره‌سازی).
به شیوه‌ای پردازش شوند که امنیت مناسب داده‌های شخصی تضمین شود. این امر شامل محافظت در برابر پردازش غیرمجاز یا غیرقانونی و حفاظت در برابر ضرر ناگهانی، تخریب یا آسیب با توسل به روش‌ها و اقدامات فنی و سازمانی مناسب است (اصل تمامیت و محرمانگی) (EUR-Lex, 2016: 35).

تلقی می‌شوند (دسته‌های خاص داده‌های شخصی[1])، علاوه بر اصول یادشده، باید الزامات ویژه‌ای رعایت شوند. این داده‌ها شامل داده‌های شخصی حساس،[2] داده‌های شخصی مربوط به محکومیت‌ها و جرائم کیفری، و داده‌های شخصی مربوط به کودکان است.

ضرورت حمایت ویژه از داده‌های شخصی خاص، به ماهیت خود آن داده‌ها بازمی‌گردد. برای مثال، داده‌های شخصی حساس و داده‌های مرتبط با امور کیفری با توجه به ماهیتشان بر حقوق و آزادی‌های اساسی افراد تأثیرگذارند و پردازش بدون ضابطه آن‌ها می‌تواند خطرات جدی برای حقوق و آزادی‌های اساسی ایجاد کند. همچنین، لزوم حمایت ویژه از کودکان به دلیل شرایط سنی آن‌هاست که درک کمتری از پردازش و مسائل مربوط به داده‌های شخصی خود دارند (برای کسب اطلاعات بیشتر در خصوص مبانی حقوقی پردازش داده‌های شخصی خاص، ر.ک: لطیف زاده و دیگران، ۱۴۰۲).

با توجه به آنچه بیان شد، در حوزه علوم انسانی دیجیتال داده‌های شخصی مختلفی به شیوه‌های متفاوت مورد پردازش قرار می‌گیرند. پردازش نیز بر اساس متن مقررات اروپایی حفاظت از داده‌ها، «به معنای عملیات یا مجموعه‌ای از عملیات است که بر روی داده‌های شخصی یا مجموعه داده‌های شخصی با ابزار خودکار یا به‌صورت دستی صورت می‌گیرد. چنین عملیاتی شامل جمع‌آوری، ضبط، سازمان‌دهی، طبقه‌بندی، ذخیره‌سازی، اشتراک‌گذاری، تغییر، بازیابی، استفاده، تجزیه‌وتحلیل، انتشار، افشا به‌وسیله مخابره کردن یا ایجاد دسترسی به شیوه‌های دیگر، ترکیب، محدود نمودن، حذف و پاک کردن یا تخریب است (EUR-Lex, 2016: 33).

با توجه به دامنه گسترده داده‌های شخصی مورد استفاده در حوزه علوم انسانی دیجیتال و شیوه‌های متفاوت پردازش، بسیار مهم است که محققان، نهادها و سازمان‌ها، و به‌طور کلی اشخاص پردازش‌کننده داده (اعم از کنترل‌کنندگان و پردازنده‌ها[3]) اهمیت حفاظت از داده‌های شخصی را درک

1. Special category data.
2. Sensitive personal data

به دلیل ماهیت ویژه داده‌های شخصی حساس، پردازش چنین داده‌هایی به‌موجب مقررات اروپایی ممنوع است. بر اساس ماده ۹ این مقررات: «پردازش داده‌های شخصی که مبین منشأ نژادی یا قومی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی، عضویت در اتحادیه‌های صنفی، پردازش داده‌های ژنتیکی، داده‌های زیست‌سنجی به‌منظور شناسایی منحصربه‌فرد یک شخص حقیقی، داده‌های مربوط به‌سلامت یا داده‌های مربوط به زندگی جنسی یا گرایش جنسی یک شخص حقیقی باشد، ممنوع است (EUR-Lex, 2016: 38).

3. Controller & Processor

کنند و اقدامات مناسب را برای کاهش خطرات موجود و تحقق امنیت لازم برای داده‌های شخصی انجام دهند(Hawkins, 2021: 253) . در این راستا، توجه به مهم‌ترین دغدغه‌ها در مورد پردازش داده‌های شخصی در حوزه علوم انسانی دیجیتال ضروری است؛ بدین جهت در بند بعدی به این مهم -برای حرکت به سوی روش‌هایی برای تحقق امنیت داده‌های شخصی- پرداخته خواهد شد.

ب. مهم‌ترین چالش در مورد امنیت داده‌های شخصی در علوم انسانی دیجیتال

یکی از مهم‌ترین چالش‌های موجود در مسیر تأمین امنیت مناسب برای داده‌های شخصی در حوزه علوم انسانی دیجیتال، عدم وجود بسترهای حقوقی کارآمد به‌طور کلی و قانون خاص به‌طور جزئی در این خصوص است. فقدان الزامات حقوقی صریح، حریم خصوصی اشخاص موضوع داده را به خطر می‌اندازد و برای اشخاص پردازش‌کننده داده نیز مشکلات متعددی را به دنبال دارد. البته این فقدان مربوط به تمامی نظام‌های حقوقی نیست و برخی از آن‌ها به‌خوبی در خصوص حمایت از داده‌های شخصی و جزئیات آن، از جمله استفاده از داده‌های شخصی در زمینه تحقیقات علمی، قانون‌گذاری نموده‌اند (به زودی در همین بند توضیح آن خواهد آمد). با این وجود، نظام حقوقی ایران خلاء مهمی در این خصوص دارد و هنوز قانونی برای ساماندهی به بحث مهم حمایت از داده‌های شخصی با همه ابعاد آن، از جمله تحقیقات علمی و حوزه علوم انسانی ندارد.

البته حقوق ایران با ارائه پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» در تیرماه سال ۱۳۹۷ (منتشرشده در سایت سازمان فناوری اطلاعات ایران[1]) و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» در شهریورماه سال ۱۴۰۰ (منتشر شده در پایگاه ملی اطلاع‌رسانی قوانین و مقررات کشور) در این خصوص گامی برداشته است؛ لیکن این اقدامات جزئی برای حمایت از این داده‌ها کافی نیست. بدین جهت قانون‌گذار باید هرچه سریع‌تر در خصوص این مهم قانون‌گذاری نماید. در این راستا می‌تواند از آثار علمی و اسناد حقوقی سایر نظام‌های حقوقی نیز استفاده نماید.

«کنترل‌کننده به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که به‌تنهایی یا به‌طور مشترک با دیگران، اهداف و ابزار پردازشِ داده‌های شخصی را تعیین می‌کند اگر یک شخص - اعم از حقیقی یا حقوقی- یا یک مرجع عمومی یا یک نهاد تصمیم بگیرد که چرا و چگونه داده‌های شخصی باید پردازش شوند، کنترل‌کننده داده است. پردازنده نیز به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که از جانب کنترل‌کننده پردازش داده‌های شخصی را انجام می‌دهد. پردازنده داده‌های شخصی را فقط به نمایندگی از کنترل‌کننده پردازش می‌کند(EUR-Lex, 2016: 33).

۱. لینک دسترسی به پیش‌نویس: B2n.ir/x06417.

یکی از این موارد مقررات اروپایی حفاظت از داده‌ها است که پیش‌تر بدان اشاره شد. این مقررات جنبه‌های مختلفی را در خصوص داده‌های شخصی مورد توجه قرار داده و برای حمایت، الزامات مختلفی را مقرر نموده است. یکی از مهم‌ترین جنبه‌های حمایت از داده‌های شخصی بر اساس این مقررات، وجود مبانی حقوقی برای پردازش است. به‌موجب مواد مربوطه، کنترل‌کننده‌ها باید مبنای حقوقی معتبر جهت پردازش داده‌های شخصی داشته باشند تا تصرف در داده‌های شخصی مجاز باشد. در صورت فقدان این مبانی، پردازش داده‌ها ممنوع و غیرقانونی است.

همچنین به‌موجب مواد مختلفی از این مقررات، اشخاص موضوع داده از حقوق متعددی برخوردار هستند. این حقوق در راستای تحقق حمایت جامع از داده‌های شخصی و کنترل بیشتر افراد نسبت به داده‌های شخصی‌شان است. در مقابل، اشخاص پردازش‌کنندهٔ داده (کنترل‌کننده و پردازنده) تعهدات مختلفی در راستای حمایت از داده‌های شخصی دارند. تعهدات مقرر به‌طور کامل برای کنترل‌کننده‌ها، به‌عنوان مسئول اصلی پردازش، وجود دارد. پردازنده‌ها نیز که به نمایندگی از کنترل‌کننده‌ها در خصوص پردازش عمل می‌نمایند، ملزم به رعایت برخی از تعهدات موجود در این مقررات هستند.

در نهایت، این مقررات با تصریح بر ضمانت اجراهای مختلف، از جمله ضمانت اجراهای مدنی و کیفری، به حمایت‌های همه‌جانبهٔ خود جامهٔ عمل پوشانیده است. تمامی جنبه‌های مختلف بیان‌شده، از جمله مبانی پردازش، حقوق و تکالیف و ضمانت اجراها بر تحقق امنیت داده‌ها در حوزه علوم انسانی دیجیتال تأثیرگذار است و توجه به آن‌ها ضروری است(See. EUR-Lex, 2016) .

تفصیل مبانی حقوقی پردازش داده‌های شخصی مفید است، چرا که به نظر می‌رسد نخستین گام برای حفظ امنیت داده‌های شخصی، رفع چالش‌های مربوط به پردازش آن‌ها است. در این خصوص، تعریف و تحقق الزامات مربوط به پردازش بسیار مهم است. همان‌طور که در بند نخست پژوهش آمده است، پردازش مفهومی گسترده دارد و شامل مصادیق متفاوتی است. بنابراین، حفظ امنیت داده‌ها در گرو پردازشی قانونمند و ساماندهی شده است. در این زمینه، رعایت اصل شفافیت در پردازش و پردازش بر اساس مبانی حقوقی ضروری است.

اصل شفافیت بدین معنی است که اشخاص موضوع داده باید به شیوه‌ای مناسب از هدف و دامنه پردازش مطلع شوند؛ بنابراین، آن‌ها باید بدانند که داده‌های شخصی‌شان جمع‌آوری، استفاده، مورد مذاکره و یا به‌صورت‌های دیگر پردازش می‌شوند، و تا چه حد از این داده‌ها استفاده می‌شود و یا استفاده خواهد شد. اصل شفافیت به‌طور خاص شامل بیان اطلاعاتی در مورد هویت کنترل‌کننده، هدف پردازش، و آگاه ساختن افراد از خطرات، قواعد حفاظتی و حقوق مربوط به فعالیت‌های پردازش و چگونگی اعمال این حقوق است (Kubben et al, 2019: 62).

مبانی حقوقی پردازش داده‌های شخصی بر اساس مقررات اروپایی که الگویی برای امنیت داده است، تصریح می‌کند که پردازش داده‌های شخصی صرفاً در صورتی مشروع است که حداقل یکی از موارد ذیل وجود داشته باشد:

- رضایت فرد نسبت به پردازش داده‌های شخصی خود برای یک یا چند هدف خاص؛
- پردازش برای اجرای قراردادی که شخص موضوع داده طرف قرارداد است یا به‌منظور برداشتن گام‌هایی به درخواست شخص موضوع داده قبل از انعقاد قرارداد ضروری است؛
- پردازش جهت انطباق با تعهد قانونی که کنترل‌کننده تابع آن است، ضروری است؛
- پردازش به‌منظور حفظ منافع حیاتی شخص موضوع داده یا شخص حقیقی دیگر ضروری است؛
- پردازش برای انجام وظیفه‌ای به نفع عموم یا برای اِعمال اختیارهای رسمی واگذارشده به کنترل‌کننده ضروری است؛
- پردازش جهت اهداف منافع مشروع دنبال شده توسط کنترل‌کننده یا شخص ثالث ضروری است، به‌جز مواردی که منافع، حقوق و آزادی‌های اساسی شخص موضوع داده بر منافع مشروع کنترل‌کننده یا شخص ثالث حاکم است، به‌خصوص در مواردی که شخص موضوع داده یک کودک است.

اگر هیچ‌یک از مبانی حقوقی مذکور برای پردازش داده توسط اشخاص پردازش‌کننده داده وجود نداشته باشد، پردازش غیرمجاز و ممنوع است (EUR-Lex, 2016: 36).

با توجه به آنچه بیان شد، برای حفظ امنیت داده‌های شخصی در حوزه علوم انسانی دیجیتال، توجه به اصول مربوط به پردازش باید محور قرار گیرد.

فارغ از الزامات کلی که بر موضوع تأثیرگذار است، مقررات اروپایی به‌طور خاص نیز به بحث پردازش داده‌های شخصی در تحقیقات علمی پرداخته است. بر اساس این مقررات، اگر پردازش داده‌ها برای اهداف تحقیقات علمی باشد، نهادهای تحقیقاتی می‌توانند داده‌های شخصی را برای هر هدف تحقیقاتی پردازش کنند. این پردازش بدون نیاز به رعایت برخی از الزامات قانونی، مانند عدم نیاز به رضایت صریح برای هر هدف پردازشی و عدم اجرای برخی از حقوق مربوط به اشخاص موضوع داده، انجام می‌شود.

با توجه به ضرورت وجود رضایت خاص و آگاهانه، شخص موضوع داده باید از تمام اهداف پردازش مطلع باشد و زمانی که پردازش دارای اهداف متعدد است، باید برای همه آن‌ها رضایت کسب شود. اما در برخی موارد، مانند تحقیقات علمی، کسب رضایت خاص و آگاهانه در تمامی موارد ممکن نیست، زیرا محققان ممکن است در زمان کسب رضایت و جمع‌آوری داده‌ها نتوانند تمامی اهداف پردازشی آتی را شناسایی کنند. بنابراین، رضایت خاص و آگاهانه در این موارد قابل حصول نیست.

گرچه برخی معتقدند که این امر باعث می‌شود اشخاص پردازش‌کننده داده بتوانند در هر زمان به دلیل اهداف تحقیقاتی مدنظرشان از رضایت گسترده‌ای بهره‌مند شوند، اما این رضایت گسترده با اقدامات حفاظتی که فقدان یک هدف مشخص را جبران می‌کند، متعادل می‌شود. این اقدامات می‌تواند شامل تهیه یک طرح تحقیقاتی جامع قبل از شروع پروژه یا افزایش شفافیت در توسعه طرح باشد که به اشخاص موضوع داده اجازه می‌دهد تا حق خود را برای پس گرفتن رضایت اعمال کنند (Marelli & Testa, 2018: 497).

معافیت از برخی الزامات قانونی با هدف پردازش داده‌ها برای تحقیقات علمی به این دلیل است که پژوهش‌ها برای توسعه دانش ضروری هستند. نتایج تحقیقات موجبات دانش باکیفیت را فراهم می‌کند و می‌تواند مبنایی برای تدوین و اجرای سیاست‌های مبتنی بر دانش باشد و همچنین موجب بهبود کیفیت زندگی اشخاص شود. با این وجود، به‌منظور حفظ امنیت داده‌های شخصی در حوزه تحقیقات علمی باید شرایط مناسب و تدابیر حفاظتی مقرر در قانون اتحادیه یا کشور عضو رعایت شود (Pormeister, 2017: 140). در عمل، چنین تدابیر حفاظتی به کشورهای عضو واگذار شده است و تعریف روشنی از ماهیت این‌گونه تدابیر و اقدامات حفاظتی در مقررات اروپایی ارائه نشده است و صرفاً به مصداقی مانند مستعار سازی اشاره شده است.

در سایر منابع، علاوه بر مستعار سازی، تدابیری مانند استفاده از سیستم‌های مدیریت امنیت اطلاعات و اقداماتی برای رمزنگاری در طول ذخیره‌سازی بیان شده است. بنابراین، گرچه نام مستعار می‌تواند یک عامل محدودکننده برای استفاده از داده‌های شخصی باشد، اما اگر روش‌های حفاظتی دیگری وجود داشته باشد که امنیت پردازش را تضمین کند، پردازش بدون مستعار سازی نیز مجاز است (Shabani & Borry, 2018: 153-154). همچنین، منشورهای رفتاری موجود در خصوص تحقیقات علمی می‌توانند اقدامات و تدابیر حفاظتی مناسبی در این زمینه تلقی شوند (Koevoets, 2017: 45).

توجه قانون‌گذار و سیاست‌گذاران به ایجاد بسترهای حقوقی و قانونی و الزامات حقوقی در مورد تعامل با داده‌های شخصی در حوزه تحقیقات، به‌ویژه در علوم انسانی فناورانه، موجب تقویت امنیت داده‌ها، ایجاد اعتماد، تحقیق حمایت حداکثری از حریم خصوصی اطلاعاتی افراد و همچنین حفظ حقوق اشخاص موضوع داده در زمینه علوم انسانی خواهد شد. در حال حاضر، فقدان الزامات و بسترهای پیش‌گفته، خود موجب چالش‌های بسیاری است که مهم‌ترین آن‌ها نقض داده‌های شخصی و پیامدهای مربوط به آن است.

یکی از چالش‌های مهم در مورد داده‌های شخصی، به‌ویژه با فقدان الزامات حقوقی، نقض این داده‌ها است. به‌موجب مقررات اروپایی داده‌های شخصی، «نقض داده شخصی، نقض امنیت است که منجر به تخریب اتفاقی یا غیرقانونی، از دست دادن، تغییر، افشای غیرمجاز یا دسترسی غیرمجاز به دادهٔ شخصیِ منتقل‌شده، ذخیره‌شده یا پردازش‌شده به شیوه‌های دیگر می‌شود (EUR-Lex, 2016: 34).

نقض داده شخصی می‌تواند به‌صورت یک حادثه فنی یا فیزیکی رخ دهد و به عنصر قصد (عمد) یا سهل‌انگاری (غیر عمد) نیاز ندارد؛ بنابراین نسبت به هرگونه وقوع نقض داده اعمال می‌شود. در واقع، مهم نیست که نقض داده‌ها چگونه و چرا اتفاق افتاده است؛ حتی نقض تصادفی را نیز شامل می‌شود. احتمال دسترسی نیز شامل تعریف است؛ در نتیجه، از دست دادن واسطهٔ داده یا دسترسی به پایگاه داده رمزگذاری شده نیز نقض دادهٔ شخصی محسوب می‌شود (Eija, 2018: 23).

نقض داده‌ها در حوزه‌های مختلف، به‌ویژه در تحقیقات و زمینه‌های علمی، پیامدهای نامناسبی برای اشخاص موضوع داده و اشخاص پردازش‌کننده داده به همراه دارد. پیامدهای نقض برای اشخاص موضوع داده شامل سرقت هویت، ضرر مالی و حتی آسیب‌های روحی و وقوع خسارات معنوی است. این امر احساس امنیت و جریان حریم خصوصی اطلاعاتی افراد را از بین می‌برد و در بازه زمانی طولانی می‌تواند اشخاص موضوع داده را درگیر کند.

از منظر اشخاص پردازش‌کننده داده نیز، عواقب آن می‌تواند به همان میزان نامناسب باشد و منجر به خسارات مالی قابل توجه، قرارگیری در معرض تعهدات قانونی مختلف و آسیب به اعتبار شود. پیامدهای نقض مهم‌تر از حادثه اولیه است و نتایج نامناسب مختلفی را به دنبال دارد. به‌عنوان نمونه، یکی از پیامدهای نقض داده‌های شخصی برای شخص موضوع داده، سرقت هویت است که در آن مهاجم می‌تواند از داده‌های شخصی مورد تعرض قرار گرفته برای ایجاد خدشه به اعتبار و جایگاه علمی فرد استفاده کند. این امر می‌تواند منجر به خسارات مالی قابل توجه و آسیب به شهرت فرد شود (See. Cruz et al, 2022: 5).

با توجه به آنچه بیان شد، به‌ویژه فقدان بسترهای حقوقی و قانونی، استفاده از روش‌هایی کارآمد برای حفظ امنیت داده‌ها بسیار مهم است که در ادامه به آن‌ها پرداخته خواهد شد.

ج. موثرترین روش‌های برای حفظ امنیت داده‌های شخصی در علوم انسانی دیجیتال

در این بخش به مهم‌ترین روش‌های کلیدی برای تحقق امنیت داده‌های شخصی در زمینه علوم انسانی دیجیتال اشاره خواهد شد. این روش‌ها شامل رمزگذاری، مستعارسازی و ناشناس‌سازی داده‌ها هستند. رمزگذاری برای محافظت از داده‌های شخصی در طول انتقال و ذخیره‌سازی بسیار مهم است، در حالی که پروتکل‌های احراز هویت به تأیید هویت افراد برای دسترسی به داده‌ها کمک می‌کنند.

علاوه بر این، ناشناس‌سازی داده‌ها می‌تواند برای حذف داده‌های شخصی و به حداقل رساندن خطر نقض حریم خصوصی اطلاعاتی استفاده شود. همچنین، انجام ممیزی‌های امنیتی منظم و به‌روزرسانی الگوریتم‌های رمزگذاری برای جلوگیری از تهدیدات سایبری ضروری است.

علاوه بر این، مهم است که دسترسی‌ها و مجوزها فقط به افرادی که به اهداف تحقیقاتی نیاز دارند، محدود شود و دسترسی‌ها و چگونگی ذخیره‌سازی به‌طور دقیق کنترل شوند.

در نهایت، وجود برنامه‌های آموزشی و آگاهی مستمر نسبت به روش‌های پیش‌گفته برای ارتقای اطلاعات محققان و افراد درگیر نسبت به اهمیت امنیت داده‌ها نیز باید مورد توجه قرار گیرد.

استفاده از این روش‌ها، مواجهه اخلاقی و حقوقی مناسب با داده‌های شخصی در زمینه علوم انسانی دیجیتال را ممکن می‌سازد. همچنین، با اتخاذ این اقدامات، حوزه علوم انسانی دیجیتال می‌تواند حریم خصوصی اطلاعاتی و حفاظت از داده‌های شخصی را تقویت کند و در نهایت اعتماد اشخاص موضوع داده را در مطالعات تحقیقاتی جلب نماید (See. Pratomo, Mokodenseho & Aziz, 2023: 2-3).

تفصیل هر یک از روش‌های مذکور در ادامه خواهد آمد.

۱. ناشناس ساختن، مستعار سازی و رمزگذاری داده‌های شخصی

ناشناس‌سازی[1] روشی است برای تغییر داده‌های شخصی با هدف حذف هرگونه ارتباط بین داده‌ها و افراد. داده‌های ناشناس به اطلاعاتی اطلاق می‌شود که به شخص شناسایی‌شده یا قابل‌شناسایی مرتبط نیستند یا داده‌های شخصی که به شیوه‌ای ناشناس ارائه‌شده‌اند به‌گونه‌ای که فرد دیگر قابل‌شناسایی نیست.

به‌عبارت‌دیگر، ناشناس‌سازی شامل حذف یا مبهم کردن داده‌های شخصی از مجموعه داده‌ها است تا ردیابی داده‌ها و افراد خاص برای مهاجمان دشوار شود. ناشناس‌سازی داده‌ها به‌طورکلی در دو دسته جای می‌گیرد:

۱. تصادفی کردن (رندوم‌سازی): شامل تغییر صحت داده‌ها به‌منظور حذف ارتباط قوی بین داده‌ها و افراد است. اگر داده‌ها به‌اندازه کافی نامشخص شوند، دیگر نمی‌توانند به یک شخص خاص اشاره کنند.

۲. عمومی‌سازی: شامل عمومیت‌بخشی یا حذف خصایص اشخاص موضوع داده با تغییر مقیاس یا ترتیب داده‌ها (مثلاً استفاده از منطقه به‌جای یک شهر، یا یک ماه به‌جای یک هفته) است.

اگر کنترل‌کننده یا پردازنده بتوانند اطلاعات ناشناس شده را با احتمال منطقی بازیابی کنند، به نظر می‌رسد داده‌ها به‌درستی ناشناس نشده‌اند. ترکیبی از روش‌های تصادفی‌سازی و عمومی‌سازی می‌تواند برای تضمین مؤثر حفاظت از حریم خصوصی مورد استفاده قرار گیرد.

ازآنجایی‌که عنصر خطر همیشه در مورد ناشناس‌سازی وجود دارد، باید در هنگام ارزیابی روش‌های فنی موجود، شدت و احتمال خطر شناسایی نیز لحاظ شود. در نتیجه، راه‌حل مناسب باید برحسب مورد تعیین شود. این امر شامل ارزیابی موقعیت پردازش داده است. تمامی ابزارهای احتمالاً منطقی موجود برای شناسایی (مجدد) نیز باید در نظر گرفته شوند.

مستعارسازی نیز ابزاری متعارف برای جلوگیری از امکان شناسایی یک شخص از طریق داده‌ها است. در واقع، مستعارسازی به معنای آن است که داده‌های شخصی دیگر به یک شخص موضوع داده خاص بدون استفاده از اطلاعات اضافی قابل انتساب نباشند. این امر می‌تواند با جایگزین کردن نام یا

1. Anonymisation.

سایر ویژگی‌ها با شاخص‌های خاص حاصل شود. اطلاعات اضافی که به‌طور احتمالی اجازه شناسایی می‌دهند، باید جداگانه نگهداری شوند و مستعارسازی باید با اقدامات فنی تضمین شود. این امر می‌تواند با رمزگذاری اطلاعات و به اشتراک‌گذاری رمز صرفاً برای تعداد کمی از افراد حاصل شود.

با اینکه امکان شناسایی مجدد داده‌های مستعار بیشتر از داده‌های ناشناس است، مستعارسازی فوایدی دارد، ازجمله اینکه ابزاری مناسب برای دستیابی به حفاظت از داده‌ها در مواجهه با فناوری است. همچنین، مستعارسازی کامل می‌تواند به‌طور مؤثر از داده‌ها محافظت نماید.

رمزگذاری نیز شامل تبدیل داده‌ها به یک کد است که تنها با کلید رمزگشایی صحیح قابل دسترسی است. این روش اطمینان حاصل می‌کند که حتی اگر افراد غیرمجاز به داده‌ها دسترسی پیدا کنند، نمی‌توانند آن را بخوانند یا از آن استفاده کنند (See, Voigt & von dem Bussche, 2017: 13-16).

ناگفته نماند که در استفاده از این شیوه‌ها، پشتیبان‌گیری منظم از داده‌ها نیز نقش مهمی در امنیت داده‌ها دارد. با پشتیبان‌گیری منظم، اشخاص پردازش‌کننده داده می‌توانند اطمینان حاصل کنند که در صورت نقض امنیتی یا خرابی سیستم، می‌توانند داده‌های خود را به حالت قبلی بدون هیچ‌گونه ضرر و زیان بازگردانند.

۲. پیاده سازی اصول حاکم بر پردازش

یکی از روش‌های حفظ امنیت داده‌ها، رعایت اصول حاکم بر پردازش است. این اصول در بسترهای حقوقی نظام‌های مختلف برای حمایت از داده‌های شخصی مورد توجه قرار گرفته‌اند. اصول مذکور شامل اصل محدودیت هدف، اصل حداقل‌سازی داده‌ها، اصل صحت داده‌ها، اصل محدودیت ذخیره‌سازی داده‌ها، و اصل تمامیت و محرمانگی داده‌ها هستند که هر یک به شرح زیر است:

یک. اصل محدودیت هدف[1]: بر اساس این اصل، هدف پردازش داده‌های شخصی باید روشن باشد. پردازش داده‌ها باید برای یک هدف یا اهداف خاص صورت گیرد و افرادی که داده‌های شخصی آن‌ها پردازش می‌شود، باید از این هدف یا اهداف مطلع باشند. جمع‌آوری و پردازش داده‌های شخصی بدون هدف مشخص ممکن نیست. در واقع، «داده‌های شخصی باید برای اهداف مشخص، صریح و مشروع جمع‌آوری‌شده و به شیوه‌ای که با آن اهداف ناسازگار است، پردازش نشوند.» تغییر در هدف پردازش داده پس از جمع‌آوری داده‌ها فقط در شرایط خاص مجاز است (EUR-Lex, 2016: 35).

1. Purpose Limitation.

دو. اصل حداقل‌سازی داده‌ها[1]: بر اساس این اصل، داده‌های شخصی تنها باید در جایی پردازش شوند که به‌طور منطقی هدف از پردازش به شیوه‌ای دیگر ممکن نباشد. بهتر است از داده‌های ناشناس استفاده شود، اما در جایی که داده‌های شخصی موردنیاز است، باید کافی، مرتبط و محدود به آنچه برای هدف ضروری است، باشند. کنترل‌کننده مسئول ارزیابی میزان دادهٔ شخصی موردنیاز برای اهداف پردازش است و باید اطمینان حاصل کند که داده‌های نامربوط جمع‌آوری نمی‌شوند (Kubben et al, 2019: 62).

سه. اصل صحت داده‌ها[2]: بر اساس این اصل، اشخاص پردازش‌کننده داده باید اطمینان حاصل کنند که داده‌های نگهداری شده صحیح و به‌روز هستند. داده‌های نادرست باید پاک یا اصلاح شوند (Bhaimia, 2018: 25).

چهار. اصل محدودیت ذخیره‌سازی داده‌ها[3]: مطابق با این اصل، داده‌ها باید برای کوتاه‌ترین زمان ممکن ذخیره شوند. این دوره باید مطابق با نیاز کنترل‌کننده برای پردازش داده‌ها جهت حصول هدف از پردازش، به‌طورکلی یک دوره زمانی ثابت باشد. کنترل‌کننده باید محدودیت‌های زمانی جهت پاک کردن یا بررسی داده‌های ذخیره‌شده را تعیین کند. برای اجرای موفق این اصل، کنترل‌کننده‌ها باید سیاست‌های حفظ و نگهداری را اعمال کنند. این سیاست‌ها شامل مجموعه‌ای از دستورالعمل‌ها برای تعیین نحوه سازمان‌دهی داده‌ها، مدت زمان نگهداری داده‌ها برای پردازش و محدودیت‌های زمانی برای حذف داده‌های غیرضروری است. استفاده از سیستم‌های ذخیره‌سازی امن داده و کنترل دسترسی‌ها نیز می‌تواند امنیت داده‌های شخصی را در علوم انسانی دیجیتال افزایش دهد. به‌عنوان مثال، اجرای احراز هویت چند عاملی مانند ترکیب رمزهای عبور و تأیید زیست‌سنجی و کنترل دسترسی مبتنی بر نقش می‌تواند دسترسی به داده‌های شخصی را فقط به افراد مجاز محدود کرده و خطر نقض داده‌ها را کاهش دهد. با انجام این اقدامات، اشخاص پردازش‌کننده داده می‌توانند اطمینان حاصل کنند که داده‌ها به‌صورت ایمن ذخیره می‌شوند و فقط توسط افراد مجاز قابل دسترسی هستند (Voigt & von dem Bussche, 2017: 92).

1. Data Minimisation.
2. Accuracy.
3. storage limitation.

پنج. اصل تمامیت و محرمانگی داده‌ها[1]: بر اساس این اصل، دادهٔ شخصی باید به شیوه‌ای پردازش شود که امنیت مناسب داده‌های شخصی، از جمله حفاظت در برابر پردازش غیرمجاز یا غیرقانونی و در برابر ضرر، تخریب یا آسیب تصادفی، با استفاده از اقدامات فنی و سازمانی مناسب تضمین شود. اصل محرمانگی به‌معنای اطمینان از این است که داده‌ها برای اشخاص و نهادهای غیرمجاز افشا نمی‌شوند یا در دسترس قرار نمی‌گیرند. مطابق با اصل تمامیت، باید اطمینان حاصل شود که داده‌ها در حالت اصلی خود باقی می‌مانند و توسط هیچ نهاد یا شخص غیرمجازی دست‌کاری نمی‌شوند (Bitar & Bjorn, 2017).

۳. استفاده از سیستم مدیریت حفاظت از داده

کنترل‌کننده‌های حوزه علوم انسانی دیجیتال باید سیاست‌های حفاظت از داده‌ای مناسب و متناسب با فعالیت‌های پردازشی خود را اجرا کنند. این امر می‌تواند از طریق اجرای سیستم مدیریت حفاظت از داده[2] که مبتنی بر ارزیابی ریسک است، حاصل شود. سیستم مدیریت حفاظت از داده، یک سیستم انطباق داخلی است که اجرای الزامات مربوط به حفاظت از داده و ایمنی درون‌گروهی را کنترل می‌کند.

سیستم مدیریت حفاظت از داده معمولاً شامل امنیت فناوری اطلاعات است که هدایت فنی فعالیت‌های پردازش داده را معرفی و نظارت می‌کند. از نظر ساختار، سیستم مدیریت حفاظت از داده اساساً متفاوت از سایر سیستم‌های مدیریتی مانند سیستم‌های مدیریت کیفیت یا امنیت اطلاعات نیست؛ بنابراین، سیستم مدیریت حفاظت از داده می‌تواند مبتنی بر ساختارهای متعارف باشد. با وجود سیستم مدیریت حفاظت از داده مرکزی، هزینه‌ها کاهش می‌یابد و نیاز به اقدامات بیشتری نیست.

اشخاص پردازش‌کننده داده می‌توانند از قابلیت‌های این سیستم برای توسعه مفاهیم حفاظت، اجرای آموزش‌های حفاظت از داده برای کارکنان و یا تولید گزارش‌ها و اسناد استفاده کنند. هرچه دامنه اشخاص پردازش‌کننده داده وسیع‌تر و پیچیدگی آن بیشتر باشد، سیستم مدیریت حفاظت از داده مفیدتر و مناسب‌تر خواهد بود (Voigt & von dem Bussche, 2017).

1. Integrity and Confidentiality.
2. Data Protection Management System.

۴. بهره مندی از ابزارهای حمایتی «حریم خصوصی با طراحی» و «حریم خصوصی به‌طور پیش‌فرض»

در زمانی که پژوهشگران و توسعه‌دهندگان علوم انسانی دیجیتال داده‌های شخصی را با تجزیه و تحلیل گسترده داده‌ها و الگوریتم‌ها توسعه می‌دهند، می‌توانند از روش‌های «حریم خصوصی با طراحی» و «حریم خصوصی به‌طور پیش‌فرض»[1] استفاده کنند. حریم خصوصی با طراحی در شرایطی معنا دارد که پردازش داده‌ها اساساً با نرم‌افزار و سخت‌افزار انجام شود. در این راستا، استفاده از فناوری با وجود حفاظت‌های پیشگیرانه باید به‌عنوان مبنایی برای پردازش، جهت به حداقل رساندن تهاجم به داده‌ها باشد. هنگام استفاده از فناوری‌های جدید، اشخاص پردازش‌کننده داده باید اصل حداقل‌سازی داده‌ها را مورد توجه قرار دهند.

نمونه‌هایی از این امر شامل استفاده از سیستم‌های فناوری اطلاعات برای به حداقل رساندن داده‌ها و همچنین مستعارسازی کامل و به‌موقع داده‌های شخصی است. به‌عنوان مثال، پرسش‌نامه‌ها و سایر فرم‌های جمع‌آوری داده‌ها را می‌توان به‌گونه‌ای طراحی کرد که دامنهٔ داده‌های جمع‌آوری‌شده به میزان لازم برای تحقق هدف پردازش محدود شود.

همچنین، به‌موجب حریم خصوصی به‌طور پیش‌فرض صرفاً باید داده‌های شخصی که برای هدف خاص پردازش ضروری هستند، جمع‌آوری شوند. این امر به مقدار داده‌های شخصی جمع‌آوری‌شده، میزان پردازش آن‌ها، دورهٔ ذخیره‌سازی آن‌ها و قابلیت دسترسی آن‌ها بستگی دارد. بدین منظور، کنترل‌کننده باید اقدامات فنی مناسب را انجام دهد. هنگامی‌که کنترل‌کننده از پردازنده استفاده می‌کند، پردازنده باید به کنترل‌کننده امکان دستیابی به حریم خصوصی به‌طور پیش‌فرض را فراهم کند.

از لحاظ فنی، حریم خصوصی به‌طور پیش‌فرض را می‌توان در هر لحظه از طول پردازش اعمال نمود. این امر منجر به کاربردی‌شدن این ابزار و استفادهٔ بیشتر از آن در عمل می‌شود. به‌عنوان مثال، تغییر تنظیمات فنی نرم‌افزارها، برنامه‌ها، دستگاه‌ها یا حساب‌های کاربری که سابقاً ایجاد شده‌اند، به حالت تنظیمات پیش‌فرض خصوصی است.

با وجود این امر، همواره لازم است قبل از ارائهٔ خدمات یا محصولات جدید در بازار نیز، تلاش شود تا رویکرد حریم خصوصی به‌طور پیش‌فرض رعایت شود (See. Rousseaux & Saurel, 2015: 88-89).

1. Privacy by Design and Privacy by Default.

۵. اهمیت ممیزی های امنیتی منظم و توجه به آموزش و افزایش آگاهی اطراف درگیر

در زمینه امنیت داده‌های شخصی در حوزه علوم انسانی دیجیتال، ممیزی‌های امنیتی منظم و ارزیابی مداوم آسیب‌پذیری‌ها از اهمیت بالایی برخوردارند. این ارزیابی‌ها نقشی حیاتی در شناسایی هرگونه ضعف بالقوه در سیستم، چه در زیرساخت‌ها، نرم‌افزار یا عوامل انسانی، دارند. با انجام این ارزیابی‌ها، اشخاص پردازش‌کننده داده می‌توانند به‌سرعت هرگونه آسیب را برطرف و اصلاح کنند و اطمینان حاصل کنند که داده‌های شخصی امن باقی می‌مانند.

علاوه بر این، در کنار اقدامات فنی، آموزش در مورد بهترین شیوه‌های امنیت داده‌ها برای توسعه دانش مربوط به حفاظت از داده‌ها ضروری است. با آموزش منظم افرادی که در پردازش داده‌ها نقش دارند، می‌توان اطمینان حاصل کرد که همه افراد درگیر در طرح‌های علوم انسانی دیجیتال اهمیت حفاظت از داده‌های شخصی را درک می‌کنند. این آموزش‌ها می‌تواند به اشخاص پردازش‌کننده داده کمک کند تا خطرات بالقوه و عواقب نقض داده‌ها را بهتر بشناسند و بدین ترتیب افراد درگیر در پردازش را برای واکنش سریع نسبت به هرگونه نقض امنیتی توانمند سازند.

علاوه بر این، این دانش می‌تواند اشخاص پردازش‌کننده داده را قادر سازد تا نقاط ضعف بالقوه در زیرساخت‌های خود را شناسایی کرده و اقدامات لازم را برای تقویت آن‌ها انجام دهند. در نهایت، این امر برای درک چشم‌انداز کامل در حوزه علوم انسانی دیجیتال بسیار مؤثر است (See. Öğütçü et al, 2021: 86-87).

نتیجه‌گیری

حفظ امنیت داده‌های شخصی در تمامی جنبه‌های علوم انسانی دیجیتال ضروری است؛ چرا که داده‌های شخصی یکی از منابع اصلی برای توسعه علوم انسانی فناورانه هستند. با این وجود، داده‌های شخصی در حوزه علوم انسانی دیجیتال در معرض خطرات مختلفی قرار دارند. به‌عنوان مثال، بسیاری از داده‌های شخصی دیجیتالی علوم انسانی اغلب توسط چندین شخص پردازش‌کننده داده، اعم از حقیقی و حقوقی، پردازش می‌شوند که حمایت از آن‌ها را دشوار می‌سازد. علاوه بر این، اغلب داده‌های جمع‌آوری‌شده توسط محققان علوم انسانی دیجیتال، داده‌های شخصی حساس هستند که خود به حمایت‌های ویژه‌ای نسبت به داده‌های شخصی عمومی نیاز دارند.

با وجود اهمیت و ضرورت این مسئله، عوامل متعددی وجود دارند که حفاظت از داده‌ها را در حوزه علوم انسانی دیجیتال چالش‌برانگیزتر می‌کنند. مهم‌ترین این عوامل، عدم وجود بسترهای حقوقی و قانونی ایرانی برای حمایت از داده‌های شخصی و فقدان الزامات حقوقی در خصوص حفاظت از حقوق اشخاص موضوع داده است. فقدان این الزامات، چه در حوزه علوم انسانی دیجیتال و چه در سایر زمینه‌ها، مواجهه داده‌های شخصی با موضوعات متعدد را مخاطره‌آمیز نموده و اسباب تضییع حقوق اشخاص موضوع داده را فراهم کرده است.

با توجه به این شرایط، پژوهش حاضر ضمن توصیه به قانون‌گذار برای تدوین سند حقوقی مربوط به داده‌های شخصی و جریان آن در حوزه علوم انسانی دیجیتال با بهره‌مندی از اسناد حقوقی الگو، روش‌های مختلفی را برای محافظت از داده‌های شخصی در حوزه علوم انسانی دیجیتال ارائه کرده است. این روش‌ها شامل مستعارسازی، ناشناس‌سازی داده‌ها و رمزگذاری هستند. همچنین، توجه به اصول حاکم بر پردازش داده‌ها نیز از جمله روش‌های پیشنهادی است.

از سوی دیگر، بهره‌مندی از سیستم مدیریت حفاظت از داده و روش‌هایی نظیر حریم خصوصی با طراحی و حریم خصوصی به‌طور پیش‌فرض نیز توصیه می‌شود. در نهایت، جریان ممیزی‌های امنیتی منظم و توجه به آموزش و افزایش آگاهی افراد درگیر می‌تواند نقشی مؤثر در حمایت از داده‌های شخصی در تعامل با علوم انسانی فناورانه داشته باشد.

امید است همان‌گونه که فناوری در تمامی جنبه‌ها، از جمله علوم انسانی، در حال توسعه و تکامل است، الزامات حقوقی مرتبط نیز مورد توجه قانون‌گذار قرار گیرد تا بتوان از ابزارهای فناورانه به‌صورت مطلوب و با کمترین میزان آسیب به افراد بهره برد.

فهرست منابع

لطیف زاده، مهدیه؛ قبولی درافشان، سید محمد مهدی؛ محسنی، سعید و عابدی، محمد (۱۴۰۲)، چگونگی پردازش داده شخصی خاص در حقوق اتحادیه اروپا و بررسی آن در نظام حقوقی ایران. پژوهشنامه پردازش و مدیریت اطلاعات، شماره ۳۹، ص۱۵۷-۱۹۹.

Bhaimia, S. (2018). The General Data Protection Regulation: the Next Generation of EU Data Protection. Legal Information Management, 18(1), 21–28. https://doi.org/10.1017/s1472669618000051.

Bitar, H. and J, & Bjorn. (2017). GDPR: Securing Personal Data in Compliance with new EU-Regulations A7009N GDPR: Securing Personal Data in Compliance with new EU-Regulations. Luleå University of Technology. Business.

Cruz, A. do S. C, Alvarez, E. B, & Vital, L. P. (2022). Web application for data collection in marketing strategies: an approach from the perspective of Digital Humanities. ICST Transactions on Scalable Information Systems, 9(5), 1–10. https://doi.org/10.4108/eetsis.v9i5.2611.

Eija, S. (2018). Applying general data protection regulation in small organizations: simplified framework and templates for managing privacy. School of Business and Culture.

EUR-Lex. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). Official Journal of the European Union, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Hawkins, S. (Ed.). (2021). Access and Control in Digital Humanities. Routledge. https://doi.org/10.4324/9780429259616.

Koevoets, D. (2017). The Influence of Article 89 GDPR on the Use of Big Data Analytics for the Purpose of Scientific Research [Tilburg University]. http://arno.uvt.nl/show.cgi?fid=142885

Krtalic, M, Marcetic, H, & Micunovic, M. (2016). Personal digital information archiving among students of social sciences and humanities. Information Research: An International Electronic Journal, 21(2), 1-19.

Kubben, P, Dumontier, M, & Dekker, A. (Eds.). (2019). Fundamentals of Clinical Data Science. Springer International Publishing. https://doi.org/10.1007/978-3-319-99713-1.

Marelli, L, & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation: How will new decentralized governance impact research? Science, 496–498 .

https://doi.org/10.1126/science.aar5419.

Öğütçü, G, Testik, Ö. M, & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computers & Security, 56, 83-93.

Pormeister, K. (2017). Genetic data and the research exemption: Is the GDPR going too far? International Data Privacy Law, 7(2), 137–146. https://doi.org/10.1093/idpl/ipx006

Pratomo, A. B, Mokodenseho, S, & Aziz, A. M. (2023). Data Encryption and Anonymization Techniques for Enhanced Information System Security and Privacy. West Science Information System and Technology, 1(01), 1-9.

Rousseaux, F, & Saurel, P. (2015). How Should Digital Humanities Pioneers Manage Their Data Privacy Challenges? (pp. 75–91). https://doi.org/10.1007/978-3-319-28868-0_5.

Shabani, M, & Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. European Journal of Human Genetics, 26(2), 149–156. https://doi.org/10.1038/s41431-017-0045-7.

Singh, A. (2016). Protecting Personal Data as a Property Right. ILI Law Review, Winter Issue, 123–139.

Voigt, P, & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

References

Bhaimia, S. (2018). The General Data Protection Regulation: the Next Generation of EU Data Protection. *Legal Information Management*, *18*(1), 21–28. https://doi.org/10.1017/s1472669618000051

Bitar, H. and J., & Bjorn. (2017). *GDPR : Securing Personal Data in Compliance with new EU-Regulations A7009N GDPR : Securing Personal Data in Compliance with new EU- Regulations Luleå University of Technology*. Business.

Cruz, A. do S. C., Alvarez, E. B., & Vital, L. P. (2022). Web application for data collection in marketing strategies: an approach from the perspective of Digital Humanities. *ICST Transactions on Scalable Information Systems*, *9*(5), 1–10. https://doi.org/10.4108/eetsis.v9i5.2611

Eija, S. (2018). *applying general data protection regulation in small organizations simplified framework and templates for managing a privacy*. School of Business and Culture.

EUR-Lex. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). *Official Journal of the European Union*, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Hawkins, S. (Ed.). (2021). *Access and Control in Digital Humanities*. Routledge. https://doi.org/10.4324/9780429259616

Koevoets, D. (2017). *The Influence of Article 89 GDPR on the Use of Big Data Analytics for the Purpose of Scientific Research* [Tilburg University]. http://arno.uvt.nl/show.cgi?fid=142885

Krtalic, M., Marcetic, H., & Micunovic, M. (2016). Personal digital information archiving among students of social sciences and

humanities. *Information Research: An International Electronic Journal*, *21*(2), 1-19

Kubben, P., Dumontier, M., & Dekker, A. (Eds.). (2019). *Fundamentals of Clinical Data Science*. Springer International Publishing. https://doi.org/10.1007/978-3-319-99713-1

Latifzadeh, Mahdieh., Ghabooli Darafshan, Seyyed Mohammad Mahdi., Mohseni, Saeed., & Abadi, Mohammad. (2023). How personal data processing is conducted in the European Union law and its examination in the Iranian legal system. *Journal of Information Processing and Management, 39*(1), 157-199.

Marelli, L., & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation How will new decentralized governance impact research? *Science*, 496–498. https://doi.org/10.1126/science.aar5419

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

Pormeister, K. (2017). Genetic data and the research exemption: Is the GDPR going too far? *International Data Privacy Law*, *7*(2), 137–146. https://doi.org/10.1093/idpl/ipx006

Pratomo, A. B., Mokodenseho, S., & Aziz, A. M. (2023). Data Encryption and Anonymization Techniques for Enhanced Information System Security and Privacy. *West Science Information System and Technology*, *1*(01), 1-9.

Rousseaux, F., & Saurel, P. (2015). *How Should Digital Humanities Pioneers Manage Their Data Privacy Challenges?* (pp. 75–91). https://doi.org/10.1007/978-3-319-28868-0_5

Shabani, M., & Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection

Regulation. *European Journal of Human Genetics*, *26*(2), 149–156. https://doi.org/10.1038/s41431-017-0045-7

Singh, A. (2016). Protecting Personal Data as a Property Right. *ILI Law Review*, *Winter Issue*, 123–139.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7.