Journal of comparative public law
Homepage: http://cpl.qom.ac.Ir

Exceptions to the Prohibition on Processing Special Categories of Personal Data in Communication Networks and Appropriate Policy-Making: A Comparative Study of the Legal Systems of the European Union and Iran

Muslim Aghaei Tog,[1] Mahdi Naser,[2]

PhD in Public Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran; Email: Moslemtog@yahoo.com

PhD in Private Law, University of Judicial Sciences and Administrative Services, Tehran, Iran (Corresponding Author); Email: Mn.ujsasac0077@yahoo.com

Abstract

A network refers to interconnected computers that process information. The data processed in communication networks can be categorized into personal and non-personal information. Non-personal data consists of information that is publicly accessible and can be processed without formalities or restrictions. In contrast, personal data refers to information that, directly or indirectly, leads to the identification of individuals and whose processing requires certain conditions and prerequisites. Among personal data, a particular subset—referred to as 'special categories of personal data'—is subject to stricter limitations on processing. Nevertheless, lawmakers in various jurisdictions have provided exceptions to these prohibitions based on specific interests or considerations. The central question of this study is: What are the exceptions to the prohibition on processing special categories of personal data in communication networks? To answer this question, this research adopts a document-based and comparative method, examining the legal systems of Iran and the European Union. It classifies the exceptions into two categories: involuntary (statutory) and contractual exceptions. In its conclusion, the study also offers policy recommendations to address the existing legal gaps in Iran's legal system.

Keywords: Special Categories of Personal Data, Communication Networks, Exceptions, European Union law, IranianLaw.

Received: 11/05/2024; **Revised**: 24/07/2024; **Accepted**: 26/08/2024**; Published online**: 21/12/2024

How To Cite: Aghaei Tog, M, Naser, M (2024). Exceptions to the Prohibition on Processing Special Categories of Personal Data in Communication Networks and Appropriate Policy-Making: A Comparative Study of the Legal Systems of the European Union and Iran, *Journal of Comparative Public Law*, 1(4).1-24.

http://www. doi.org/ 10.22091/cpl.2024.10741.1023.

Published by: University of Qom **Article type**: Research

حقوق عمومی تطبیقی
Homepage: http://cpl.qom.ac.Ir

استثنائات ممنوعیت پردازش داده‌پیام‌های شخصی خاص در شبکه‌های ارتباطی و سیاست‌گذاری مناسب: مطالعه تطبیقی نظام حقوقی اتحادیه اروپا و ایران

مسلم آقایی طوق،[1] مهدی ناصر[2]

دکترای حقوق عمومی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران؛ رایانامه:
Moslemtog@yahoo.com

دکترای حقوق خصوصی دانشگاه علوم قضایی و خدمات اداری، تهران، ایران (نویسنده مسئول)[4]، رایانامه:
Mn.ujsasac0077@yahoo.com

چکیده

شبکه به کامپیوترهای متصل به هم اطلاق می‌گردد که نسبت به پردازش اطلاعات اقدام می‌کنند. اطلاعات تحت پردازش در شبکه‌های ارتباطی در دو دسته شخصی و غیرشخصی تقسیم‌بندی می‌شوند. اطلاعات غیرشخصی، اطلاعاتی هستند که در اختیار عموم جامعه بوده و پردازش آن‌ها فاقد هرگونه تشریفات یا محدودیت‌ها است. اما اطلاعات شخصی، اطلاعاتی هستند که پردازش آن‌ها به‌طور مستقیم یا غیرمستقیم منجر به شناسایی اشخاص شده و شروع فرایند پردازش آن‌ها نیاز به برخی شرایط و ملزومات دارد. در این میان دسته خاصی از اطلاعات شخصی نیز که به‌عنوان اطلاعات شخصی خاص شناخته می‌شوند، دربردارنده محدودیت‌های بیشتری در اجرای فرایند پردازش هستند. بااین‌حال، قانون‌گذاران کشورها بنابر مصالحی، استثنائاتی را بر این ممنوعیت‌ها پیش‌بینی کرده‌اند. سؤال اصلی پژوهش حاضر این است که استثنائات ممنوعیت پردازش داده‌پیام‌های شخصی خاص در شبکه‌های ارتباطی چیست؟ برای پاسخ به سؤال مذکور، پژوهش حاضر به روش اسنادی و مطالعه تطبیقی حقوق ایران و اتحادیه اروپا، استثنائات مذکور را در دو دسته استثنائات قهری و قراردادی تقسیم‌بندی نموده و در قسمت نتیجه‌گیری نیز نسبت به ارائه برخی توصیه‌های سیاست‌گذارانه در رفع خلأهای موجود در نظام حقوقی ایران اقدام کرده است.

واژگان کلیدی: داده‌پیام شخصی خاص، شبکه ارتباطی، استثنائات، حقوق اتحادیه اروپا، حقوق ایران.

تاریخ دریافت: ۱۴۰۳/۰۲/۲۲؛ **تاریخ اصلاح**: ۱۴۰۳/۰۵/۰۳؛ **تاریخ پذیرش**: ۱۴۰۳/۰۶/۰۵؛ **تاریخ انتشار آنلاین**: ۱۴۰۳/۱۰/۰۱

استناد: آقامحمدی، احسان؛ رحمت‌اللهی حسین؛ هاشمی سید فتح‌الله (۱۴۰۳). رهیافتی به «جماعت‌گرایی معاصر» و بازخوانی تمایزات آن با «کمال‌گرایی» در نگرش به زندگی فرد، حقوق عمومی تطبیقی، ۱(۴)، ۲۴-۱.
http://www. doi.org/ 10.22091/cpl.2024.10741.1023

ناشر: دانشگاه قم

نوع مقاله: پژوهشی

مقدمه

قرن بیست‌ویکم به‌عنوان قرن توسعه فناوری اطلاعات شناخته می‌شود. توسعه فناوری اطلاعات در عصر حاضر، در کنار تمامی مزایایی که در پیشرفت بشریت و بهبود روند امور چه در زندگی خصوصی افراد و چه در روابط اجتماعی و یا سیاسی اشخاص حقیقی و حقوقی داشته، دربردارنده چالش‌هایی نیز بوده است. این موضوع منجر به تصویب برخی قوانین و مقررات توسط کشورها در جهت نظام‌مند کردن نحوه بهره‌برداری از فناوری اطلاعات توسط اشخاص حقیقی یا حقوقی در بخش‌های مختلف صنعت و تجارت شده است.

آنچه در عصر حاضر، به‌عنوان مبنای توسعه فناوری اطلاعات شناخته می‌شود، داده‌پیام الکترونیکی است که در معنای خود دربردارنده تمامی انواع اطلاعات مورد تبادل و پردازش می‌گردد. پردازش داده‌پیام‌های الکترونیکی در بخش‌های مختلف تجارت، صنعت، پزشکی و... که به‌طور کلی در شمول مفهوم عام شبکه‌های ارتباطی قرار می‌گیرند، به‌عنوان راهکاری در جهت تبادل علم یا کسب نتایج حاصل از تحلیل اطلاعات تلقی می‌شود.

شبکه به معنای دو یا چند کامپیوتر است که به‌منظور به اشتراک گذاشتن منابع (مانند چاپگرها و سی‌دی‌ها)، تبادل فایل‌ها یا داده‌پیام‌های الکترونیکی به یکدیگر متصل شده‌اند. رایانه‌های موجود در یک شبکه ممکن است از طریق کابل، خطوط تلفن، امواج رادیویی، ماهواره‌ها یا پرتوهای نور مادون‌قرمز به هم متصل شوند (Winkelman, 2024). خصوصیت اساسی شبکه‌های کامپیوتری، تبادل داده‌پیام‌ها و منابع است. در این فرایند پروتکل‌هایی ارتباطی -مانند TCP/IP، برای تبادل داده بین دستگاه‌های شبکه استفاده می‌شوند (Yasar&Gillis, 2024). شبکه‌های تبادل اطلاعات در دو تقسیم‌بندی قابل تفکیک می‌باشند. تقسیم‌بندی نخست، این نوع شبکه‌ها را از حیث امکان دسترسی کامپیوترها به اینترانت و اینترنت و تقسیم‌بندی دوم از حیث ماهیت شبکه‌ها به متمرکز و نامتمرکز مورد بررسی قرار می‌دهد.

اینترانت به شبکه‌ای خصوصی از کامپیوترها اطلاق می‌شود که نسبت به تبادل اطلاعات با یکدیگر اقدام می‌کنند (Lutkevich,2024). بنابراین در شبکه‌های اینترانت، کامپیوترهای مخصوصی ازجمله با داشتن آدرس‌های IP منحصربه‌فرد امکان ورود به شبکه را داشته و همگان از حق ورود و تبادل اطلاعات به شبکه برخوردار نیستند. ازجمله این شبکه‌ها می‌توان به شبکه‌های داخلی سازمان‌ها و یا در پهنایی گسترده‌تر به شبکه‌های ملی اطلاعات اشاره نمود. در مقابل شبکه اینترنت به شبکه گسترده

جهانی[1] اطلاق می‌شود که در آن کلیه کامپیوترهای متصل به شبکه از امکان دسترسی و تبادل اطلاعات برخوردار هستند.

در یک تقسیم‌بندی دیگر، شبکه‌های تبادل اطلاعات به دو نوع متمرکز و نامتمرکز تقسیم‌بندی می‌شوند. شبکه‌های متمرکز، شبکه‌هایی هستند که در آن‌ها کامپیوترهای موجود به یک نقطه مرکزی که کنترل تبادل و ذخیره اطلاعات در شبکه را بر عهده دارد، متصل هستند. در شبکه‌های تبادل اطلاعات، کامپیوترها اصطلاحاً گره نامیده می‌شوند که به گره مرکزی متصل هستند. بنابراین وجود و فعالیت گره‌های شبکه، منوط به کارکرد درست گره مرکزی خواهد بود. ازاین‌رو، می‌توان نتیجه‌گیری نمود که در صورت هک یا از کار افتادن یا کارکرد نادرست گره مرکزی، در عملکرد کلیه گره‌های متصل به شبکه اخلال ایجاد می‌گردد (Bhalla,2024). در مقابل شبکه‌های نامتمرکز، شبکه‌هایی می‌باشند که فاقد گره مرکزی بوده و کامپیوترها در این نوع شبکه‌ها به صورت متقارن یا نامتقارن نسبت به تبادل اطلاعات با یکدیگر اقدام می‌کنند. بنابراین در این نوع شبکه‌ها، گره مرکزی یا کامپیوتر مرکزی جهت نظارت و کنترل بر تبادل اطلاعات وجود نداشته و این مهم بر عهده کامپیوترهای موجود در شبکه در فرایندی موسوم به اثبات کار صورت می‌پذیرد (Alexandria, 2024).

فرایند پردازش اطلاعات در شبکه‌های ارتباطی، گاه در خصوص برخی از دسته‌های اطلاعات به جهت خطراتی که می‌تواند داشته باشد، با محدودیت‌هایی توسط قانون‌گذاران مواجه شده است. این محدودیت‌ها درزمینهٔ داده‌پیام‌های شخصی خصوصاً انواع داده‌پیام شخصی خاص با تصویب مقررات عمومی حفاظت از اطلاعات[2] مصوب سال ۲۰۱۶ اتحادیه اروپا (لازم‌الاجرا شد در ماه می سال ۲۰۱۸) و همچنین قانون تجارت الکترونیکی مصوب سال ۱۳۸۲ و طرح حمایت و حفاظت از داده و اطلاعات شخصی واصل شده به مجلس شورای اسلامی در سال ۱۳۹۹ در حقوق ایران و اتحادیه اروپا جلوه نموده‌اند. بااین‌حال، محدودیت‌های کلی موجود در قوانین فوق‌الذکر، به جهت برخی سیاست‌ها و مقتضیات مبتنی بر نظم عمومی یا حفظ امنیت داخلی و خارجی و همچنین دستیابی به اهداف تحقیقاتی و آماری و علمی و...، با استثنائاتی مواجه شده‌اند که محل بحث پژوهش حاضر می‌باشند. سؤالی که پژوهش حاضر در پی یافتنِ پاسخِ آن است، این است که استثنائاتِ حاکم بر ممنوعیتِ پردازشِ داده‌های شخصیِ خاص در نظامِ حقوقیِ ایران و اتحادیهٔ اروپا کدامند؟

1. World Wide web
2. General Data Protection Regulation

برای پاسخ به این سؤال، پژوهش حاضر به روش اسنادی و مطالعه تطبیقی قواعد حقوقی حاکم بر نظام حقوقی ایران و اتحادیه اروپا، پس از تبیین داده‌پیام‌های شخصی خاص به‌عنوان متغیر اصلی پژوهش، به صورت تطبیقی به تشریح استثنائات موجود در نظام حقوقی اتحادیه اروپا و ایران پرداخته و در قسمت نتیجه‌گیری مبادرت به ارائه برخی توصیه‌های سیاست‌گذارانه در جهت رفع خلأهای تقنینی موجود در نظام حقوقی ایران نموده است.

در بدایت امر یادآور می‌گردد که درزمینهٔ پردازش اطلاعات در شبکه‌های ارتباطی مقالات متعددی به تألیف درآمده یا گردآوری شده‌اند و هر یک به یکی از جنبه‌های حقوقی و چالش‌های مرتبط با سازوکار پردازش اطلاعات ازجمله حقوق اشخاص موضوع داده (اشخاصی که اطلاعات آن‌ها مورد پردازش قرار می‌گیرند)، وظایف اشخاص فعال در فرایند پردازش اطلاعات، سازوکار تبادل فراملی اطلاعات، سازوکار جبران خسارات وارده به اشخاص و... پرداخته‌اند. اما حلقهٔ مفقودهٔ پژوهش‌های منتشرشده در نشریات علمی کشور، استثنائات مبتنی بر محدودیت‌ها و ممنوعیت‌های پردازش اطلاعات است که موضوع اصلی پژوهش حاضر را تشکیل می‌دهد. ازاین‌رو، این پژوهش در محور موضوعی خود پژوهشی بدیع محسوب می‌شود.

نکته آخر در این زمینه، این است که مقاله حاضر از این حیث مرتبط با حقوق عمومی است که محوریت اصلی آن سیاست‌گذاری تقنینی و اجرایی در جهت نظام‌مند نمودن فرایند پردازش اطلاعات به‌عنوان یک اقدام حاکمیتی تلقی می‌گردد. به‌عبارت‌دیگر، اگرچه در مطالب اصلی مقاله به موضوع استثنائات ممنوعیت از پردازش اطلاعات به‌عنوان موضوع بحث در حقوق ایران و اتحادیه اروپا پرداخته است، اما همان‌طور که در قسمت نتیجه‌گیری نیز به صورت مصرح تأکید شده، نقش اصلی در نظام‌مند نمودن فرایند پردازش در شبکه‌های ارتباطی بر عهده دولت و حاکمیت است که با سیاست‌گذاری‌های تقنینی همچون اصلاح مقررات قانون تجارت الکترونیکی و همچنین سیاست‌گذاری اجرایی در جهت آموزش آحاد جامعه و نظارت بر فرایند پردازش، همانند آنچه در بخش نتیجه‌گیری ذکر گردید نسبت به انجام وظایف حاکمیتی خود اقدام می‌کند.

۱. تعریف متغیرهای اصلی پژوهش

محوریت اصلی پژوهش حاضر به‌عنوان یک پژوهش بین‌رشته‌ای، استثنائات ممنوعیت پردازش اطلاعات شخصی خاص در شبکه‌های ارتباطی (شبکه‌های تبادل اطلاعات) است. بنابراین داده‌پیام‌های شخصی و انواع خاص آن‌ها به‌عنوان متغیر اصلی این پژوهش شناخته می‌شوند که تبیین قواعد کلی حاکم

بر پردازش این اطلاعات و استثنائات ممنوعیت پردازش آن‌ها نیازمند شناسایی مفهوم و ماهیت این نوع داده‌پیام‌ها است.

قانون‌گذار ایران در بند «ر» از ماده ۲ قانون تجارت الکترونیکی، داده‌پیام‌های الکترونیکی را به صورت غیرمصرح به دو دسته شخصی و غیرشخصی تقسیم نموده و در تعریف داده‌پیام‌های شخصی بیان داشته است که «داده‌پیام‌های شخصی، یعنی «داده‌پیام»های مربوط به یک شخص حقیقی موضوع «داده» مشخص و معین».

توجه به تعریف فوق‌الذکر، این موضوع را مشخص می‌کند که داده‌پیام شخصی، تنها در خصوص اشخاص حقیقی جریان داشته و امکان تعریف و تخصیص آن بر اشخاص حقوقی فراهم نیست. بااین‌حال، تعریف فوق‌الذکر اجمالی بوده و خصایص داده‌پیام‌های شخصی را مورد بحث قرار نداده است. درحالی‌که در نظام حقوقی اتحادیه اروپا، موازین دقیقی در تمیز این مفهوم با سایر مفاهیم قابل استخراج است. بند نخست از ماده ۴ مقررات عمومی حفاظت از اطلاعات اتحادیه اروپا مقرر می‌دارد:[1]

«اطلاعات شخصی، به هرگونه اطلاعاتی که به صورت مستقیم یا غیرمستقیم امکان شناسایی موضوع داده را فراهم آورد، اطلاق می‌گردد. این داده‌ها می‌توانند انواع داده‌های شناسایی مانند نام و شماره شناسنامه، یا داده‌های مکانی یا شناسه‌های آنلاین برای شناسایی وضعیت هویتی فرد ازجمله عوامل خاص جسمی، فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی آن شخص طبیعی باشند.» (Intersoft Consulting, 2024).

مطابق ماده فوق، داده‌های شخصی داده‌هایی هستند که در شناسایی مستقیم یا غیرمستقیم یک شخص حقیقی می‌توانند به کار گرفته شوند. ازاین‌رو، اطلاعات مربوط به اشخاص حقوقی در نظام حقوقی اتحادیه اروپا نیز جزو مجموعه داده‌های شخصی محسوب نشده و در ذیل مقررات حاکم بر این عنوان قرار نمی‌گیرند (van der Sloot, 2017). علاوه‌بر آنچه بیان شد، داده‌های شخصی و معیارهای شناسایی این داده‌ها در نظام حقوقی اتحادیه اروپا منحصر به داده‌های مربوط به خود شخص نمی‌گردد. بلکه این اطلاعات صرف‌نظر از ماهیت شکلی خود از نوع داده، فیلم، تصویر، عدد و حتی صوت که قابلیت دستیابی به آن‌ها از طریق ابزارها تحت اختیار موضوع داده ازجمله گوشی تلفن همراه یا خودرو

1. Article 4(1) GDPR ‘personal data’ means any information relating to an identiifed or identiifable natural person (‘data subject’); an identiifable natural person is one who can be identiifed, directly or indirectly, in particular by reference to an identiifer such as a name, an identiifcation number, location data, an online identiifer or to one or more factors speciifc to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

وجود داشته باشد نیز قابلیت قرارگیری در ذیل عنوان داده‌های شخصی را برخوردار می‌باشند (Finck&Pallas, 2020: 22). نکته قابل توجه درزمینهٔ داده‌پیام‌های شخصی و غیرشخصی این است که آنچه در باب حفظ حریم خصوصی اطلاعات در فرایند پردازش شبکه‌های ارتباطی مطرح می‌شود، حفظ حریم خصوصی داده‌پیام‌های شخصی خواهد بود و داده‌پیام‌های غیرشخصی که در اختیار کلیه اشخاص صرف‌نظر از موقعیت مکانی خود قرار دارند، از موضوع بحث خارج خواهند بود. همچنین آنچه در محوریت پژوهش حاضر نیز ملاک بحث و بررسی است، داده‌پیام‌های شخصی می‌باشند که در شبکه‌های ارتباطی تحت پردازش قرار گرفته یا می‌گیرند. بنابراین داده‌پیام شخصی، هیچ ارتباطی به یک شبکه تبادل اطلاعات نداشته و در این شبکه تحت پردازش قرار نگرفته یا نمی‌گیرد، اصولاً نمی‌تواند موضوع حمایت‌های قانونی حفظ حریم خصوصی اطلاعات در شبکه‌های ارتباطی قرار گیرد (آقایی طوق و ناصر، ۱۴۰۳: ۲۸).

مطابق مطالب پیش‌گفته که دارای تعریفِ مشخصی از داده‌پیام‌های شخصی است، قانون‌گذاران ایران و اتحادیهٔ اروپا در بند اول مادهٔ ۹ مقررات مصوب سال ۲۰۱۶ اتحادیهٔ اروپا و مادهٔ ۵۸ قانون تجارت الکترونیکی ایران، حکم کلی پردازشِ دستهٔ خاصی از داده‌پیام‌های شخصی را ممنوع اعلام نموده‌اند. این ممنوعیت عمدتاً به‌دلیل حساسیت و اهمیتِ این نوع اطلاعات است؛ زیرا پردازشِ آن‌ها می‌تواند در صورت سوءاستفاده، آثارِ جبران‌ناپذیری بر اشخاصِ موضوعِ داده داشته باشد. بند اول ماده ۹ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا مقرر می‌دارد: پردازش داده‌های شخصی که منشأ نژادی یا قومیتی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی یا عضویت در اتحادیه‌های کارگری را آشکار می‌سازد و پردازش داده‌های ژنتیکی، داده‌های بیومتریک به‌منظور شناسایی منحصربه‌فرد یک شخص حقیقی، داده‌های مربوط به سلامتی یا داده‌های مربوط به زندگی جنسی یا گرایش جنسی یک شخص طبیعی ممنوع است[1] (Intersoft Consulting, 2024).

ماده ۵۸ قانون تجارت الکترونیکی مصوب سال ۱۳۸۲ مقرر می‌دارد: «ذخیره، پردازش و یا توزیع داده‌پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (Intersoft Consulting, 2024)

و داده‌پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است.»

همان‌طور که در مطالب فوق‌الذکر مشاهده می‌گردد، قانون‌گذاران اتحادیه اروپا در مواد ۹ و ۵۸ قوانین فوق‌الذکر، برای دسته خاصی از اطلاعات شخصی شرایط خاصی در فرایند پردازش پیش‌بینی نموده که نشان از اهمیت این نوع اطلاعات دارد. آنچه مسلم است ممنوعیت کلی پردازش این نوع اطلاعات است. اطلاعات بیان شده که اصطلاحات اطلاعات شخصی خاص محسوب می‌شوند در دسته داده‌های قومیتی، نژادی، عقیدتی، مذهبی، زیستی، اخلاقی، جنسی و... قرار می‌گیرند.

نکته قابل توجه تمثیلی بودن مصادیق ذکر شده در مواد ۵۸ قانون تجارت الکترونیکی ایران و ۹ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا است. به‌عبارت‌دیگر، قانون‌گذار ایران با ذکر واژه «داده‌پیام‌های شخصیِ مبینِ...» سعی در بیان وصف داده‌پیام‌های شخصی خاص داشته و قصدی در ذکر مصادیق احصایی نداشته است. ازاین‌رو، هر نوع اطلاعاتی که به‌عنوان مثال دارای وصف قومیتی یا عقیدتی یا خصوصیات زیستی باشد، می‌تواند در زمره داده‌پیام‌های شخصی خاص قلمداد شود.

این موضوع با ذکر عبارت «داده‌پیام‌های شخصی که منشأ ... را آشکار می‌سازد» در نظام حقوقی اتحادیه اروپا نیز قابل برداشت است. بنابراین آنچه در محدوده داده‌پیام‌های شخصی در اتحادیه اروپا قرار می‌گیرند، داده‌های دارای منشأ نژادی، قومیتی، اعتقادی، عضویت در اتحادیه‌های کارگری، ژنتیکی، بیومتریک و داده‌های مربوط به سلامت می‌باشند. اما سؤال اینجاست که منظور از داده‌های ژنتیکی، بیومتریک و داده‌های مربوط به سلامت چه بوده و این اطلاعات چه تمایزی نسبت به یکدیگر دارد؟

پاسخ سؤال فوق در ماده ۴ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا موجود است. بندهای سیزدهم تا پانزدهم از این ماده در تعریف داده‌های ژنتیکی، بیومتریک و داده‌های مربوط به سلامت بیان می‌دارند:

داده‌های ژنتیکی: به داده‌های شخصی مربوط به ویژگی‌های ژنتیکی ارثی یا اکتسابی یک شخص طبیعی که اطلاعات منحصربه‌فردی درباره فیزیولوژی یا سلامت آن شخص طبیعی به دست می‌دهد و به‌ویژه از تجزیه‌وتحلیل نمونه‌های بیولوژیکی از افراد طبیعی ناشی می‌شود، اطلاق می‌گردد.[1]

1. ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question; (Intersoft Consulting, 2024)

داده‌های بیومتریک: به معنای داده‌های شخصی ناشی از پردازش فنی خاص مربوط به ویژگی‌های فیزیکی، فیزیولوژیکی یا رفتاری یک شخص طبیعی مانند تصاویر چهره است که امکان شناسایی منحصربه‌فرد آن شخص حقیقی را فراهم می‌کند.[۱]

داده‌های مربوط به سلامتی: به معنای داده‌های شخصی مربوط به سلامت جسمی یا روانی یک شخص حقیقی، ازجمله ارائه خدمات مراقبت‌های بهداشتی است که اطلاعاتی را درباره وضعیت سلامتی او نشان می‌دهد.[۲]

اگرچه در مقایسه تعاریف ارائه شده از سه واژه فوق می‌توان به نوعی به تشابه آن‌ها دست یافت، اما تفاوت‌های ریز میان تعاریف می‌تواند مبین تمایز آن‌ها باشد. به‌عنوان مثال، داده‌های ژنتیکی به داده‌های ارثی یا اکتسابی افراد اطلاق می‌گردد. درحالی‌که، داده‌های بیومتریک داده‌های ذاتی اشخاص است که حاصل ارث یا اکتساب از محیط خارجی نیست. داده‌های مربوط به سلامتی نیز جدا از داده‌های بیومتریکی، شامل خصایص و حالات انسان مانند سلامت یا مریضی بوده و به خصوصیات بیومتریک افراد مانند شکل عنبیه چشم یا چهره ارتباط ندارند.

در هر حال حکم کلی پردازش این اطلاعات ممنوعیت این موضوع است. بااین‌حال، قانون‌گذاران ایران و اتحادیه اروپا استثنائاتی را برای این مهم در نظر گرفته‌اند که در گفتار آتی مورد تحلیل و بررسی قرار می‌گیرند.

۲. استثنائات ممنوعیت پردازش داده‌پیام‌های شخصی خاص

استثنائات حکم کلی ممنوعیت پردازش داده‌پیام‌های شخصی خاص در بند دوم ماده ۹ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا و مواد ۵۸، ۵۹ قانون تجارت الکترونیکی و برخی مقررات پراکنده در قانون تأسیس وزارت اطلاعات مصوب سال ۱۳۶۲، قانون مدیریت داده‌ها و اطلاعات ملی مصوب سال ۱۴۰۱ و طرح حمایت و حفاظت از داده و اطلاعات شخصی واصل شده به مجلس در سال ۱۳۹۹ مورد تصریح قانون‌گذاران قرار گرفته‌اند که در گفتارهای دوگانه ذیل مورد تحلیل و بررسی قرار می‌گیرند. در بدایت امر نیز یادآور می‌گردد که آنچه در بند دوم ماده ۹ مقررات مصوب سال ۲۰۱۶ ذکر گردیده،

1. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; (Intersoft Consulting,2024)

2. data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status; (Intersoft Consulting,2024)

احصایی نبوده و در خصوص داده‌پیام‌های ژنتیکی، بیومتریک و داده‌های مربوط به سلامت برمبنای بند چهارم این ماده، هر یک از کشورهای عضو اتحادیه اروپا نیز می‌توانند شرایط و محدودیت‌های بیشتری را اعمال نمایند. بر این مبنا بند چهارم ماده ۹ مقرر می‌دارد: «کشورهای عضو ممکن است شرایط بیشتری ازجمله محدودیت‌ها را در مورد پردازش داده‌های ژنتیکی، داده‌های بیومتریک یا داده‌های مربوط به سلامت حفظ یا معرفی کنند.»[1] استثنائات ذکر شده در بند دوم ماده ۹ در دو دسته استثنائات قراردادی و استثنائات قهری به شرح ذیل قرار می‌گیرند.

۲-۱. استثنائات قراردادی

استثنائات قراردادی، به آن دسته از استثنائات قید می‌گردد که مسبوق بر انعقاد قرارداد میان شخص موضوع داده و اشخاص فعال در فرایند پردازش اطلاعات در شبکه‌های ارتباطی، امکان پردازش اطلاعات فراهم می‌شود. شق دوم از بند دوم از ماده ۹ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا درزمینهٔ ارائه استثنا بر قاعده ممنوعیت کلی مقرر در بند اول ماده ۹ درزمینهٔ تعهدات قراردادی بیان می‌دارد:[2]

«پردازش به‌منظور انجام تعهدات و اعمال حقوق خاص کنترل کننده یا موضوع داده درزمینهٔ استخدام و قانون تأمین اجتماعی و حمایت اجتماعی تا جایی که توسط قانون اتحادیه یا کشور عضو یا قانون اتحادیه مجاز باشد ضروری باشد. یک قرارداد جمعی بر اساس قانون کشورهای عضو که تضمین‌های مناسبی را برای حقوق اساسی و منافع موضوع داده ارائه می‌کند.»

همان‌طور که ملاحظه می‌شود، قانون‌گذار اتحادیه اروپا پس از ذکر برخی مصادیق در انجام تعهدات قراردادی در حوزه تأمین اجتماعی یا استخدام، با ذکر واژه حمایت اجتماعی، نسبت به توسعه وسعت شمول مصادیق پردازش در راستای انجام تعهدات قراردادی پرداخته و حتی قراردادهای جمعی را نیز در این شمول ذکر کرده است. بااین‌حال عنصر مهم در انجام این فرایند، ضرورت انجام آن بوده و به صورت مطلق نمی‌توان نسبت به انعقاد قرارداد و پردازش به هر شکل ممکن اقدام نمود.

در مطالعه بند بیان شده در این ماده، می‌توان دو شرط را برای پردازش اطلاعات موضوع داده استخراج نمود. این دو شرط طرف قرارداد بودن موضوع داده و ضرورت پردازش برای اجرای مفاد

1. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. (Intersoft Consulting,2024)

2. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (Intersoft Consulting,2024)

قرارداد می‌باشند. بنابراین اطلاعات اشخاص در قراردادهایی که این افراد جزو طرفین قرارداد نباشند، غیرقانونی و ممنوع است. در خصوص واژه ضرورت، می‌توان بیان داشت که پردازش در صورتی ضروری است که قرارداد بدون انجام آن تکمیل نگردد[1] (Voigt, Paul, & von dem Bussche, 2017:102). بااین‌حال، این بدان معنا نیست که تنها راه برای اجرای مفاد قرارداد، پردازش داده‌ها باشد، بلکه وجود یک گام هدفمند و متناسب با تعهدات کفایت می‌کند، بنابراین وجود راه‌های دیگر مانع از احراز ضرورت نخواهد بود (لطیف زاده و دیگران، ۱۴۰۱: ۳۴۶).

سؤالی که در اینجا مطرح می‌شود این است که وجود راه‌های دیگر تا کجا می‌تواند مانع احراز ضرورت نباشد؟ آیا در صورت وجود گزینه‌های هم‌عرض می‌توان به صرف استناد به تناسب و وجود گام هدفمند نسبت به پردازش اطلاعات اقدام نمود یا باید معیار خاصی در این زمینه وجود داشته باشد؟ در دیدگاه نگارنده صرف وجود گام هدفمند و تناسب با تعهدات در این خصوص کفایت نمی‌کند. چراکه در بیان دیدگاه فوق یکپارچگی میان اقدامات و تعهدات نیز شرطی است که مورد توجه قرار نگرفته است. به‌عبارت‌دیگر تناسب میان تعهدات و وجود گام هدفمند، در صورتی می‌تواند افاده معنای ضرورت نماید که یکپارچگی میان تعهدات نیز وجود داشته باشد. بنابراین در یک موضوع خاص، راهکارهای دیگر به‌عنوان راهکارهای طاقت‌فرسا یا مشقت پیش رو باشند و منطقاً پردازش اطلاعات به‌عنوان راهکاری معقول تلقی گردد (Barrett & Doggett, 2024).

علاوه‌بر آن در دیدگاه برخی در این فرایند لازم نیست حتماً یک قرارداد رسمی یا مکتوب میان طرفین منعقد شود، بلکه صرف توافق کفایت می‌کند (لطیف زاده و دیگران، ۱۴۰۱: ۳۴۵). در نقد این دیدگاه نیز می‌توان بیان داشت که اولاً، توافقات گاه به‌منزله قراردادهای شفاهی و گاه توافقات پیش از قرارداد هستند. بر فرض اینکه منظور نویسندگان فوق‌الذکر، قراردادهای شفاهی باشد، سؤال اینجاست که آیا حساسیتی که قانون‌گذار اتحادیه اروپا در تعیین مورد به مورد شرایط پردازش داشته، می‌توان در قراردادهای شفاهی که هر طرف می‌تواند در مقام اثبات منکر تعهدات خود گردد، امر پردازش را مورد پذیرش قرار داد؟ با توجه به اینکه مسئولیت‌های متعددی در خصوص اشخاص فعال در فرایند پردازش اطلاعات در اتحادیه اروپا در مقررات مواد ۸۰ به بعد مقررات مصوب سال ۲۰۱۶ پیش‌بینی شده است، به نظر می‌رسد قانون‌گذار حکیم اتحادیه اروپا، اصولاً هر نوع قراردادی را به‌منزله قراردادی که موضوع

---

۱. نقل شده در لطیف زاده و دیگران، ۱۴۰۱، ۳۴۵.

پردازش اطلاعات نیز جزو فرایند اجرای تعهدات باشد، در نظر نگرفته و به نظر نگارنده منظور همان قراردادهای کتبی بوده است.

نکته دیگر آن است که در فرایند پردازش، امعان‌نظر از مفهوم ضرورت ایجاب می‌نماید که «اجرای قرارداد» تنها در محدوده تعهدات قراردادی تفسیر شده و امور فراتر جزو این عنوان تلقی نگردد. به‌عنوان مثال در اجرای مفاد یک قرارداد خرید کالا از یک سایت اینترنتی، مسئولین شبکه حق جمع‌آوری اطلاعات در خصوص علایق کاربر سایت در انتخاب نوع کالا و ارائه پیشنهادهای مشابه را ندارند (لطیف زاده و دیگران، ۱۴۰۱: ۳۴۶)، چراکه این موضوع ارتباطی به اجرای مفاد قرارداد ندارد. ضمن اینکه آنچه بیان شد عموماً در محدوده پیش از انعقاد قرارداد قرار می‌گیرد که اصولاً هیچ کاربری درخواست ارائه کالاهای مشابه با علایق خود را از مسئولین شبکه مطرح نمی‌نماید. در کنار تعهدات قراردادی، شق اول از بند دوم ماده ۹ مقررات مصوب سال ۲۰۱۶، امکان پردازش اطلاعات در صورت دریافت رضایت صریح از شخص موضوع داده را پیش‌بینی کرده است. این بند مقرر می‌دارد:

موضوع داده رضایت صریح به پردازش آن داده‌های شخصی برای یک یا چند هدف مشخص داده است، به استثنای مواردی که قانون اتحادیه یا کشور عضو مقرر می‌دارد که ممنوعیت ذکر شده در بند ۱ ممکن است توسط موضوع داده لغو نشود.[1]

با توجه به حساسیت فرایند پردازش اطلاعات، اصلح دریافت مجوز پردازش از طریق رضایت در قالب یک توافقنامه میان موضوع داده و پردازنده است تا از اختلافات بعدی پیشگیری گردد. ازاین‌رو، موضوع پردازش مسبوق بر رضایت نیز در قالب استثنائات قراردادی پیش‌بینی شده است. در نظام حقوقی ایران نیز ماده ۵۸ از قانون تجارت الکترونیکی ایران مصوب سال ۱۳۸۲، اعلام رضایت در پردازش داده‌های شخصی را منوط به ارائه رضایت «صریح» توسط موضوع داده نموده است. این ماده مقرر می‌دارد: ذخیره و پردازش و یا توزیع «داده‌پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است.

همان‌طور که ملاحظه می‌گردد، ماده مرقوم، در صورت عدم وجود رضایت صریح موضوع داده، پردازش اطلاعات را غیرقانونی تلقی کرده است. اما، سؤال اینجاست که ملاک اعلام رضایت صریح

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;. (Intersoft Consulting,2024)

چه است؟ آیا صرف بیان صریح واژه رضایت می‌تواند مثبت وجود رضایت صریح و قانونی موضوع داده باشد یا باید شرایطی نیز در این امر به‌عنوان شرایط مقدماتی وجود داشته باشد تا بتوان رضایت صریح موضوع داده را احراز نمود؟ برای پاسخ به سؤالات فوق باید ابتدا مفهوم «رضایت صریح» را تبیین کرد. در دیدگاه برخی که نگارنده نیز قائل بر آن است، اعلام رضایت باید دربردارنده سه شرط باشد:

- فرد باید بداند به چه چیزی رضایت داده است؛
- قصد رضایت دادن را داشته باشد؛
- علم خویش به مفاد رضایت به همراه قصد رضایت خود را به مخاطب ابراز نماید (لاریجانی، ۱۳۸۷: ۱۶۲).

بنابراین اولین شرط در اعلام رضایت صریح، علم به مفاد چیزی که بدان رضایت داده شده است. اگرچه قانون‌گذار ایران در باب اعلام شرایط و چگونگی انجام پردازش به موضوع داده حکمی در قانون تجارت الکترونیکی قید ننموده، اما می‌توان با تدبر در فلسفه استفاده از این واژه در ماده ۵۸ و همچنین اخذ وحدت ملاک از سایر متون، ضرورت این موضوع را ایجاب نمود. به‌عنوان مثال ماده ۳۳ طرح حمایت و حفاظت از داده و اطلاعات شخصی بر ضرورت ذکر کلیه جزئیات فرایند پردازش ازجمله هدف پردازش، نحوه پردازش، شرایط فنی پردازش، سطح ایمنی موجود، حقوق موضوع داده و فرایند نظارت بر امر پردازش به موضوع داده تأکید نموده است.

این موضوع در دستورالعمل‌های شماره ۴۲ و ۴۳ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا نیز مورد تصریح قانون‌گذار این اتحادیه قرارگرفته است (ICO, 2024). بنابراین صرف اعلام رضایت چه به صورت کتبی و چه به صورت شفاهی، برای احراز صریح بودن آن در فرایند پردازش اطلاعات کفایت نمی‌نماید. به عبارتی اعلام رضایت، شرط لازم بوده، اما شرط کافی تلقی نمی‌گردد و باید علاوه‌بر اعلام، دو شرط دیگر که همان اطلاع از مفاد چیزی که بدان باید رضایت داده شود و همچنین وجود قصد بر اعلام وجود داشته باشد. نکته قابل توجه این است که در احراز وجود یا عدم وجود شروط نخست و دوم (علم و قصد) به نظر نگارنده، اصل بر وجود نداشتن شرط نخست بوده و قاضی در مقام قضاوت باید نسبت به احراز علم رضایت دهنده بر مفاد چیزی که بدان رضایت داده اقدام نماید. ازاین‌رو، در صورتی که دلیلی بر اطلاع موضوع داده از چیزی که بدان رضایت داده کشف نگردد، نمی‌توان رضایت صریح وی را احراز نمود. اما در فرض احراز یا عدم احراز وجود قصد، ابراز آنکه مثبت شرط سوم است، می‌تواند مبین وجود قصد بر ابراز نیز بوده و شرایطی مانند اکراه یا اجبار یا اشتباه باید

از سوی مدعی نداشتن وجود رضایت اثبات شده و به عبارتی باید به ظاهر امر در ابراز رضایت توجه داشت.

در نظام حقوقی ایران طرح حمایت و حفاظت از داده‌ها و اطلاعات شخصی در مواد ۴ و ۵ خود، واجد شروط دیگری غیر از اعلام رضایت صریح است. ماده ۴ این طرح بیان می‌دارد: پردازش اطلاعات شخصی اشخاص مربوط به وضعیت‌ها یا موقعیت‌های غیرعمومی منوط به اعلام رضایت آن‌ها بوده و اعلام رضایت اشخاص موضوع داده باید با رعایت شرایط ذیل همراه باشد:

- پیش از پردازش باشد؛
- بیانگر آگاهی شخص موضوع داده باشد؛
- استنادپذیر باشد.

تصریح صورت گرفته در بند نخست شرایط مقرر در ماده ۴ بر بیان رضایت پیش از پردازش، در انعقاد قراردادهای پردازشی نمود بیشتری دارد. بر این مبنا، اشخاص فعال در فرایند پردازش اطلاعات می‌توانند با اخذ امضا از موضوع داده، نسبت به اخذ رضایت وی اقدام نمایند. اما چالش موجود عموماً در شبکه‌هایی که متشکل از سایت‌های فروش و عرضه محصولات یا شبکه‌های اجتماعی می‌باشند، جلوه می‌کند که در این سایت‌ها عموماً معرفی کالای متناسب با علایق یک مراجعه کننده برای خرید، پیش از پذیرش شرایط تعیین شده از سوی سایت صورت می‌پذیرد که خلاف مقررات مصرح در این طرح است. برای حل این مشکل، گردانندگان سایت‌ها می‌توانند با ایجاد آیکنی که هنگام ورود کاربر به سایت بر روی شبکه باز شده و پیش از تأیید اطلاعات امکان ملاحظه محتویات سایت را به کاربر ندهد، نسبت به حل مشکل اقدام کنند. اما در شبکه‌های اجتماعی مانند اینستاگرام و فیس‌بوک و توییتر و... که ورود کاربر به شبکه منطبق با جمع‌آوری اطلاعات وی بوده و تنها دسترسی به مخاطبین تلفن همراه یا برخی اطلاعات دیگر وی منوط به اخذ رضایت است، نقض این شرط جلوه بیشتری دارد.

علاوه‌بر آن ماده ۵ طرح، پردازش داده‌ها و اطلاعات شخصی مربوط به وضعیت‌ها یا موقعیت‌های عمومی را بدون رضایت شخص در صورتی بلامانع تلقی کرده که «یا خود وی داده‌ها را در معرض پردازش قرار داده یا پردازش داده‌ها را منع یا محدود نکرده باشد». سؤالی که می‌تواند مطرح گردد این است که فردی که مبادرت به انتشار اطلاعات شخصی خود در شبکه‌های اجتماعی که میلیون‌ها بیننده دارد، نموده و به عبارتی آن‌ها را عمومی کرده باشد، چطور می‌تواند پردازش این داده‌ها را منع یا محدود نماید؟ در صورتی که انتشار اطلاعات در شبکه خاص با کاربران خاصی صورت گرفته باشد، این مشکل

جلوه کمتری دارد، اما در شبکه‌های اجتماعی نمی‌توان به سادگی نسبت به این مهم اقدام کرد. حال سؤال دیگری که مطرح می‌گردد این است که موضوع داده باید به چه طریقی نسبت به ایجاد منع یا محدودیت در پردازش اقدام کرده و در صورتی که شخصی از این موضوع مطلع نشده و مبادرت به پردازش نماید، سازوکار و کمیت و کیفیت شناسایی مسئولیت برای وی به چه نحوی خواهد بود.

نکته دیگری که باب مقررات این طرح می‌توان بدان توجه نمود این است که ماده ۱۰ این مقررات، مصادیق استثنا از اخذ رضایت موضوع داده را با عنایت به قواعدی مانند «انجام اقدام اهم نسبت به مهم» مورد تصریح قرار داده است. مصادیقی که در این ماده پردازش بدون اخذ رضایت موضوع داده ذکر شده شامل موارد ذیل است:

- برای صیانت از حیثیت، جان یا مال شخص موضوع داده ضروری باشد؛
- برای صیانت از حیثیت یا جان دیگری یا پیشگیری از زیان مالی شدید به او ضروری باشد؛
- برای پیشگیری یا پاسخ به تهدیدهای نظم، ایمنی و امنیت عمومی ضروری باشد؛
- برای کشف جرائم یا تخلفات یا شناسایی متهمان یا اجرای احکام قضایی و انتظامی ضروری باشد.

نکته‌ای که در بررسی مصادیق بیان شده در بندهای چهارگانه ماده ۱۰ می‌توان به آن توجه نمود این است که بند دوم از این ماده، شرط پردازش بدون رضایت را در وقوع زیان مالی به دیگران، «زیان مالی شدید» قلمداد کرده است. حال سؤال اینجاست که منظور از زیان مالی شدید چه است؟ آیا در این زمینه معیار شخصی باید ملاک قرار گیرد یا معیار نوعی؟ به‌عبارت‌دیگر، در تعیین زیان مالی شدید باید میزان خسارت مالی وارد شده به شخص را متناسب با درآمد و دارایی وی در نظر گرفت یا معیار در نظر گرفته شده باید بر اساس وضعیت مالی یک شخص عادی در جامعه استوار باشد؟

مبنای طرح این سؤالات این است که ارائه دهندگان طرح مذکور در هنگام تدوین این طرح توجهی به مفاهیم واژگان به کار برده شده نداشته و با به‌کارگیری مفاهیمی بسیط که امکان هرگونه تفسیر متناقض را فراهم می‌آورد، مبادرت به ارائه طرحی نموده‌اند که تصویب آن در مجلس قانون‌گذاری ایران می‌تواند چالش‌های اجرایی فراوانی را ایجاد نماید. اما در پاسخ به سؤالات فوق، به نظر نگارنده، اصلح تعیین معیار شخصی در این بند خواهد بود. دلیل ارائه این نظر نیز آن است که اولاً، پردازش بدون رضایت اطلاعات شخصی دیگران که برمبنای آن طرحی مشتمل بر ۵۶ ماده در دستور کار بررسی مجلس شورای

اسلامی قرار گرفته، امری استثنایی بوده و در تفسیر استثنائات این قاعده نیز باید در حد ممکن مبادرت به ارائه تفسیر مضیق نمود و به عبارتی مصادیق شمول بندهای ماده ۱۰ را تا حد ممکن محدود کرد؛ ثانیاً، بند دوم ماده ۱۰، در بیان این استثنا، به واژه «پیشگیری» تصریح کرده است که نشان از پردازش اطلاعات بدون رضایت شخص موضوع داده در حالتی دارد که هیچ ضرر و زیانی به دیگری وارد نشده است که بتوان میزان شدید بودن یا نبودن آن را احراز نمود. بر این مبنا چه دلیلی دارد با ارائه معیارهای نوعی و گسترش شمول مصادیق این ماده، به صرف پیشگیری از وقوع زیان، نسبت به پردازش بدون رضایت اطلاعات دیگران اقدام کرد.

نکته آخر این است که ماده ۱۱ از طرح پیش‌گفته، انجام پردازش اطلاعات بدون اخذ رضایت را منوط به وجود سه شرط «حفظ گمنامی اطلاعات، عدم وجود زیان مادی یا معنوی برای موضوع داده و عدم امکان اخذ رضایت» نموده است. چالشی که در ارتباط با این ماده نیز می‌تواند مطرح شود این است که در تقابل میان پیشگیری از وقوع زیان مالی شدید به دیگران و وقوع زیان مادی بسیار خفیف به موضوع داده یا زیان معنوی به وی، کدام حالت را باید نسبت به دیگری اولویت داد؟ برای پاسخ به سؤال فوق، موضوع را باید از دو منظر بررسی کرد.

دیدگاه نخست، بر این استدلال استوار است که هدف از تدوین مقررات حمایت از داده‌های شخصی، حفظ و پیشگیری از نقض امنیت این اطلاعات است. بنابراین در تقابل مقررات مواد این طرح، اولویت را باید نسبت به پذیرش موادی قرار داد که در جهت صیانت از امنیت داده‌پیام‌ها تصویب شده‌اند. ازاین‌رو، در مقررات ماده ۱۱ را باید در هر حال نسبت به مقررات ماده ۱۰ اولویت‌بندی نمود.

دیدگاه دوم که به نظر نگارنده نیز صحیح‌تر است، این است که مستفاد از اصل ۴۰ قانون اساسی یا موادی مانند ماده ۱۳۲ یا ۹۷۵ قانون مدنی می‌توان بیان داشت که اعمال حقوق اشخاص تا جایی جاری است که با نظم عمومی یک کشور در تعارض نباشد. بنابراین، در فرضی که ممکن است اعمال حق موضوع داده منجر به زیان شدید مالی به دیگران شود، طبیعتاً باید نسبت به حقوق موجود تعادل برقرار نمود. علاوه‌بر آن بندهای سوم و چهارم ماده ۱۰ نیز مصادیق مهمی مانند حفظ امنیت کشور یا انجام تحقیقات قضایی را نیز ذکر نموده‌اند که اگر قائل بر حکومت مقررات ماده ۱۱ بر ماده ۱۰ باشیم، در این زمینه نیز نمی‌توان نسبت به پردازش اطلاعات اشخاص برای حفظ امنیت ملی یک کشور به صرف وقوع زیان به آن‌ها اقدام کرد. درحالی‌که موادی مانند ماده ۱۱ قانون مسئولیت مدنی ایران، دولت را حتی از

جبران خسارت در امور حاکمیتی که بر حسب ضرورت برای تأمین منافع اجتماعی انجام گیرد نیز معاف دانسته است.

۲-۲. استثنائات قهری

استثنائات قهری، به استثنائاتی تلقی می‌گردد که انجام تعهدات قراردادی یا اخذ رضایت از موضوع داده و در یک کلام موضوع توافق میان اشخاص موضوع داده و اشخاص فعال در فرایند پردازش اطلاعات، منتفی بوده و پردازش بر اساس منافع عمومی یا حیاتی اشخاص صورت می‌پذیرد. این موضوع در شقوق سوم تا ششم از بند دوم ماده ۹ مقررات مصوب سال ۲۰۱۶ مورد تصریح قانون‌گذار قرار گرفته و در بررسی مقررات پراکنده در نظام حقوقی ایران نیز می‌توان نسبت به تصحیح آن اقدام نمود.

نکته قابل توجه این است که بنابر نظر عده‌ای حفظ منافع حیاتی اشخاص تنها در خصوص حفظ جان و منافع حیاتی و زندگی آن‌ها مانند پردازش اطلاعات وی در هنگام عمل جراحی در بیمارستان برای دستیابی به سوابق عمل جراحی یا گروه خونی و... کاربرد داشته و نمی‌توان به مسائل دیگر آن را تسری داد. علاوه‌بر آن در خصوص دیگران نیز باید به‌طریق‌اولی تنها در خصوص منافع حیاتی و زندگی، مانند پردازش داده‌های شخصی والدین جهت حفاظت از منافع زندگی و حیاتی فرزند تفسیر نمود. اگرچه این بند نیز در مقررات مصوب در کشور ایران مورد تصریح قرار نگرفته؛ اما مقررات پراکنده مانند بند سوم از ماده ۴ منشور حقوق بیماران ایران در خصوص حریم خصوصی بیماران دارای مقرراتی در این زمینه است (لطیف زاده و دیگران، ۱۴۰۱: ۳۵۱). ماده ۴ این منشور مقرر می‌دارد:

ارائه خدمات سلامت باید مبتنی بر احترام به حریم خصوصی بیمار (حق خلوت) و رعایت اصل رازداری باشد، فقط بیمار و گروه درمانی و افراد مجاز از طرف بیمار و افرادی که به حکم قانون مجاز تلقی می‌شوند، می‌توانند به اطلاعات دسترسی داشته باشند. اگرچه این مقرره می‌تواند به‌منزله توجیه کننده اقدامات مراکز درمانی در دسترسی به اطلاعات شخصی بیماران بدون اخذ رضایت تلقی شود و منطقاً نیز در مواردی که صحبت از جان اشخاص مطرح می‌شود باید تمامی موانع قانونی کنار گذاشته شوند، اما سؤال اینجاست که آیا در تقابل این مقرره با مقررات ماده ۵۸ قانون تجارت الکترونیکی و این موضوع که قانون‌گذار در آن ماده از عبارت «بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است» و توجه به این موضوع که قانون‌گذار صراحتاً از واژه به هر عنوان اشاره نموده، نمی‌توان عدم وجود استثنا در پردازش اطلاعات شخصی را از این ماده استناد و استثنای بیان شده در ماده ۴ منشور را فاقد وجاهت

قانونی تلقی نمود؟ به نظر نگارنده جواب این سؤال مثبت بوده و سیاست‌گذاران تقنینی باید نسبت به اصلاح این مقرره و رفع خلأهای قانونی آن اقدام نمایند.[۱]

در خصوص منافع عمومی نیز می‌توان بیان داشت که واژه منفعت عمومی امری بسیط بوده و تفسیر موسع از آن می‌تواند آثار بندهای دیگر ازجمله بند نخست مبنی بر ضرورت اخذ رضایت را از بین ببرد. به نظر برخی، منفعت عمومی به امری اطلاق می‌گردد که در آن عموم مردم سهیم بوده و به عبارتی به «آنچه برای کل جامعه بهترین باشد» اطلاق می‌گردد (Garner, 2024). این واژه می‌تواند حقوق آزادی اشخاص، حقوق مصرف کنندگان، حقوق سلامت و حتی اعمال اختیارات مقامات رسمی در جهت حفظ حقوق عموم جامعه و موارد مشابه را در برگیرد. اختیارات رسمی به اختیاراتی گفته می‌شود که مقامات رسمی دولتی برای انجام وظایف قانونی اعطا می‌شود (Authority, 2024). بنابراین می‌توان نتیجه‌گیری نمود که این اختیارات بیشتر جنبه حاکمیتی داشته و از مفهوم تصدی‌گری فاصله دارند. در این حالت نیز مقام دارای اختیار، از اخذ رضایت موضوع داده یا هر الزام قانونی دیگر معاف است.

اگرچه مشابه این مقرره در قانون تجارت الکترونیکی ایران پیش‌بینی نشده، بااین‌حال، مفهوم آن از سایر مقررات قانونی ازجمله ماده ۱۱ قانون مسئولیت مدنی مصوب سال ۱۳۳۹ و ماده ۸ قانون مدیریت خدمات کشوری مصوب سال ۱۳۸۶ قابل استنباط است. التفات به مقررات ماده ۱۱ قانون مسئولیت مدنی که مقرر می‌دارد «... در مورد اعمال حاکمیت دولت، هرگاه اقداماتی که بر حسب ضرورت برای تأمین منافع اجتماعی طبق قانون به عمل می‌آید و موجب ضرر دیگری شود، دولت مجبور به پرداخت خسارت نخواهد بود» می‌تواند منتج به این نتیجه شود که دولت در مقام اعمال حاکمیت می‌تواند نسبت به اموری اقدام نماید که انجام آن از سوی اشخاص عادی امکان‌پذیر نیست و موجب مسئولیت است. مصادیق اعمال حاکمیت در ماده ۸ قانون مدیریت خدمات کشوری ذکر شده که با امور عام‌المنفعه، هم‌پوشانی دارند. بنابراین در صورتی که دولت یا هر مقام صلاحیت‌داری در مقام اعمال حاکمیت مبادرت به انجام فرایند پردازش اطلاعات نمایند، این موضوع استثنایی بر مقررات ماده ۵۸ قانون تجارت الکترونیکی تلقی و فاقد ضمانت اجرای مقرر در ماده ۷۱ همان قانون خواهد بود.[۲]

---

۱ . نکته جالب توجه در پردازش اطلاعات پزشکی این است که ماده ۶۰ قانون تجارت الکترونیکی، فرایند ذخیره، پردازش و توزیع داده‌پیام‌های مربوط به سوابق پزشکی و بهداشتی را تابع آیین نامه ماده ۷۹ این قانون قرار داده، درحالی‌که آیین نامه ماده ۷۹، فاقد هر گونه مقرره در این زمینه می‌باشد.

۲. ماده ۷۱- هر کس در بستر مبادلات الکترونیکی شرایط مقرر در مواد (۵۸) و (۵۹) این قانون را نقض نماید، مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود.

نکات بیان شده، فارغ از پردازش اطلاعات از ناحیه مراجع امنیتی در کشور ایران و حتی سطح بین‌الملل است. چراکه رسیدگی و کشف جرائم امنیتی و مقابله با مرتکبین آن‌ها همواره در دستور کار ویژه قانون‌گذاران کشورها و حتی مجامع بین‌المللی بوده و این اهمیت به قدری است، که در بسیاری از قوانین و مقررات مصوب در سطح ملی و بین‌المللی، قواعد مبتنی بر رسیدگی و احراز جرائم امنیتی به‌عنوان قواعدی، اخص از اصول کلی موجود در قوانین و مقررات شمرده شده‌اند. به‌عنوان مثال می‌توان به ماده ۴ کنوانسیون توکیو مصوب سال ۱۹۶۳ که طبق قانون الحاق دولت شاهنشاهی ایران به کنوانسیون توکیو راجع به جرائم و برخی از اعمال ارتکابی دیگر در هواپیما مصوب سال ۱۳۵۵ در کشور ایران نیز لازم‌الاجرا است، اشاره نمود که مقرر می‌دارد: «دولت متعاهدی که دولت ثبت کننده هواپیما نباشد، نمی‌تواند به‌منظور اعمال صلاحیت جزایی خود در مورد جرم ارتکابی در داخل هواپیما در امر پرواز آن مداخله نماید، مگر در موارد مشروحه ذیل: ... ج. جرم امنیت دولت را به مخاطره اندازد». همچنین ماده ۳ عهدنامه ژنو مصوب سال ۱۹۵۸ نیز پس از بیان این اصل که رسیدگی به جرم ارتکابی در کشتی‌های غیرجنگی (مسافربری، تجاری) در صلاحیت کشور صاحب پرچم است، یکی از استثنائات این اصل در بند سوم خود را ارتکاب جرائم ناقص امنیت بندر برشمرده است.

ارائه مصادیق فوق نشان دهنده، اهمیت جرائم امنیتی و کشف و مقابله ویژه با آن‌ها در نظام حقوقی کشورها دارد که لازم است کلیه نهادهای دولتی و غیردولتی کشورها در تحقق این مهم، اهتمام لازم را داشته باشند. در کشور ایران نیز قانون‌گذار از شناخت این مهم مغفول نبوده و در تبصره سوم ماده ۱ قانون تأسیس وزارت اطلاعات مصوب سال ۱۳۶۲ تصریح گردیده: «هر یک از وزارتخانه‌ها و مؤسسات و شرکت‌های دولتی و نهادها و نیروهای نظامی و انتظامی که در کسب اطلاعات تخصصی خود به مسائل امنیتی برخورد نمایند، همچنین هرگونه اطلاعاتی که مورد تقاضای وزارت اطلاعات باشد، موظف‌اند در اختیار وزارت اطلاعات قرار دهند». همان‌طور که در متن این تبصره مصرح است، امکان پردازش کلیه اطلاعات شخصی اشخاص از ناحیه وزارت اطلاعات است.

نکته قابل توجه آن است که قانون تأسیس وزارت اطلاعات یک قانون غیرکیفری بوده و امکان ارائه تفسیر موسع از مقررات آن وجود دارد. این دیدگاه از آن جهت تقویت می‌گردد که واژگان استفاده شده در مقررات تبصره ۳ ماده ۱ این قانون صراحتاً مشتمل بر ارائه «هرگونه اطلاعات» بوده و قصد قانون‌گذار در توسعه مفاهیم این قانون را نشان می‌دهد، بنابراین می‌توان با تفسیر موسع از مقررات این تبصره و قیاس اولویت نتیجه‌گیری نمود که وقتی در نظر قانون‌گذار تمامی نهادهای کشوری و لشکری دولتی موظف

به همکاری کامل و ارائه اطلاعات به وزارت اطلاعات هستند، نهادهای غیردولتی نیز به‌طریق‌اولی موظف به انجام این مهم خواهند بود. علی‌رغم وجود این استدلال‌ها، قانون‌گذار ایران حتی به این موضوع نیز اکتفا ننموده و مجدداً در ماده ۱۴ قانون یاد شده، صراحتاً کلیه نهادهای دولتی و غیردولتی را موظف به همکاری کامل با وزارت اطلاعات نموده است.

متن ماده ۱۴ مقرر می‌دارد: «کلیه نهادها و ارگان‌ها موظف‌اند همکاری‌های لازم را درزمینهٔ در اختیار قرار دادن نیروی انسانی، امکانات و تجربیات اطلاعاتی به‌منظور تسهیل در انجام مسئولیت‌های وزارت اطلاعات معمول دارند». آنچه در مقررات ماده ۱۴ و تبصره ۳ ماده ۱ قانون تأسیس وزارت اطلاعات هویدا می‌سازد، توجه ویژه قانون‌گذار ایران به کشف جرائم امنیتی در صلاحیت وزارت اطلاعات بوده و با توجه به اینکه این قانون یک قانون خاص مقدم نسبت به سایر قوانین محدود کننده پردازش، مانند آیین دادرسی کیفری یا تجارت الکترونیکی تلقی و قوانین اخیرالذکر نسبت به قانون تأسیس وزارت اطلاعات عام مؤخر به شمار می‌روند، با توجه به ارجحیت قوانین خاص مقدم بر قوانین عام مؤخر، امکان پردازش اطلاعات شخصی خاص اشخاص از ناحیه این وزارت خانه در هر حال در کشور ایران فراهم شده است.

نتیجه‌گیری

همان‌طور که بیان شد، پردازش داده‌پیام‌های شخصی خاص در نظام حقوقی ایران به حکم ماده ۵۸ قانون تجارت الکترونیکی دارای حکم ممنوعیت بوده و جز در صورت اخذ رضایت صریح موضوع داده امکان پردازش اطلاعات وجود ندارد. در این میان برخی استثنائات قهری و قراردادی نیز برای این حکم کلی در قوانین و مقررات مصوب یا در حال تصویب در کشور ایران قابل استخراج می‌باشند که در متن پژوهش به آن‌ها اشاره شد. اما مشکل اساسی موجود در این نظام، خلأ برخی سیاست‌گذاری‌های تقنینی و اجرایی است که می‌توان به شرح ذیل نسبت به رفع آن‌ها اقدام نمود:

۱. متأسفانه ماده ۲ قانون تجارت الکترونیکی ایران که دربردارنده مفهوم داده‌پیام و داده‌پیام شخصی است، دارای اجمال و ابهام بوده و این مفهوم را به درستی نمی‌توان از ماده ۲ برداشت نمود. اثر این ابهام نیز می‌تواند در تفسیر ماده ۵۸ قانون تجارت الکترونیکی که از عبارت ذخیره، پردازش و توزیع داده‌پیام شخصی پرده برداشته نیز تسری یابد. به‌عبارت‌دیگر، بند (ر) ماده ۲ قانون فوق‌الذکر از عبارت «داده‌پیام مربوط به شخص» پرده برداشته که می‌تواند در وهله اول این موضوع را به ذهن حواله دهد که در نظام حقوقی ایران داده‌پیام شخصی داده‌پیامی است که تنها به‌طور مستقیم منجر به شناسایی یک فرد

می‌گردد. درحالی‌که بسیاری از داده‌پیام‌ها به نوعی می‌باشند که پردازش آن‌ها به‌طور غیرمستقیم نیز می‌تواند منجر به شناسایی اشخاص گردد و این یک خلأ تقنینی در کشور ایران است. بر این مبنا متن پیشنهادی در خصوص اصلاح بند (ر) ماده ۲ قانون فوق‌الذکر به شرح ذیل است:

بند (ر) ماده ۲: داده‌پیام‌های شخصی به هرگونه اطلاعاتی که پردازش آن‌ها به صورت مستقیم و غیرمستقیم امکان شناسایی شخص موضوع داده را فراهم نموده اطلاق می‌گردد که می‌تواند از طریق معیارهای ذیل شناسایی شود:

الف. بر اساس ماهیت داده‌پیام: داده‌پیام‌هایی که ماهیتاً به اشخاص منتسب می‌باشند و شامل داده‌های بیومتریک، شخصیتی و زیستی آن‌ها هستند. همچنین داده‌هایی که در صورت ضمیمه به سایر اطلاعات قابلیت انتساب و شناسایی افراد را فراهم نمایند نیز داده‌پیام‌های شخصی خواهند بود.

ب. بر اساس اهداف حاصل از پردازش: داده‌پیام‌هایی که در راستای شناخت خصیصه یا خصوصیاتی از اشخاص حقیقی مورد پردازش قرار می‌گیرند.

تبصره: به هرگونه عملیاتی که در جهت اقداماتی مانند جمع‌آوری، نگهداری، آنالیز، ذخیره، حذف، اصلاح و تغییر اطلاعات انجام می‌گیرد، پردازش گفته می‌شود.

۲. تعیین سازوکار اعطای مجوز فعالیت به شرکت‌های پردازنده اطلاعات در راستای بهبود نظارت بر فعالیت آن‌ها: با توجه به اینکه ماده ۷۹ قانون تجارت الکترونیکی، وزارت صنعت، معدن و تجارت را مکلف به ایجاد زیرساخت‌های اجرای این قانون نموده است، این وزارت خانه باید مراکزی مانند مرکز توسعه تجارت الکترونیکی، سازمان تنظیم مقررات رادیویی یا نظام فنی رایانه‌ای یا اتحادیه کسب و کارهای اینترنتی را مکلف به اعطای مجوز فعالیت به شرکت‌های فعال در فرایند پردازش و نظارت بر عملکرد آن‌ها نماید. در این راستا مرجع نظارتی می‌تواند ضوابطی را در جهت اعطای مجوز به شرکت‌های مذکور و همچنین ارائه گزارش عملکرد پیش‌بینی نماید. ازجمله ضوابطی که می‌توان در جهت اعطای مجوز به این شرکت‌ها در نظر گرفت، برخورداری این شرکت‌ها از تمکن مالی برای جبران خسارات ناشی از عملکرد است که می‌تواند از طریق اعطای وثیقه و تضمین مالی در هنگام اخذ مجوز فعالیت صورت پذیرد. علاوه‌بر آن برخورداری از تخصص در حوزه فعالیت موضوع مهم دیگری است که می‌تواند از طریق بررسی مدارک ارائه شده در این زمینه احراز نمود.

۳. نکته دیگر در این زمینه ضرورت تعیین ضمانت اجراهای مدنی و جبران خسارات و اعطای سازوکار تعیین و وصول این نوع جریمه‌ها از طریق نهاد ناظر پیش‌بینی شده در پیشنهاد فوق است.

مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا در ماده ۸۳ خود، امکان اعمال جریمه‌ای معادل ۲۰۰۰۰ یورو یا چهار درصد از کل گردش مالی شرکت در سال گذشته را به متخلفین از دستورات مقامات نظارتی مصرح در مقررات این قانون پیش‌بینی کرده است. درحالی‌که قانون تجارت الکترونیکی در ماده ۷۱ خود، تنها نسبت به تعیین مجازات حبس کیفری برای تخلف از مقررات مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی اکتفا نموده و ضمانت اجرای دیگری در جهت تضمین امنیت پردازش اطلاعات ندارد. این در حالی است که می‌توان به پیش‌بینی جریمه‌های نقدی هم در محدوده اجرای دستورات مقامات نظارتی و هم تخلف از مقررات پیش‌بینی شده در پیشگیری از تشکیل پرونده‌های قضایی مؤثر است.

۴. صداوسیمای جمهوری اسلامی نیز می‌تواند با ایجاد برنامه‌های آموزشی، متناسب با سن هر قشر جامعه و دعوت از کارشناسان حقوقی نسبت به برگزاری برنامه‌های آموزشی به اقشار مختلف جامعه اقدام نماید. در برنامه‌های آموزشی باید سه محور مورد توجه قرار گیرد که شامل تبیین مفهوم داده‌پیام‌های شخصی و دسته خاص آن‌ها، حقوق اشخاص موضوع داده در فرایند پردازش و وظایف مدیران و اشخاص پشتیبان شبکه‌های تبادل اطلاعات در امر پردازش و همچنین اصول قانونی حاکم بر پردازش اطلاعات می‌باشند.

فهرست منابع

آقایی طوق، مسلم؛ ناصر، مهدی (۱۴۰۳). «محدودیت‌های اعمال قواعد حفاظت از پردازش اطلاعات در شبکه‌های ارتباطی: مطالعه‌ای تطبیقی در حقوق ایران و اتحادیه اروپا»، فصلنامه حقوق عمومی تطبیقی، دوره ۱، شماره ۲.

لاریجانی، مریم (۱۳۸۷). «نظریه لاک: رضایت یا قرارداد»، فصلنامه پژوهش‌های فلسفی-کلامی، دوره ۹، شماره ۴.

لطیف زاده، مهدیه؛ قبولی درافشان، سید محمدمهدی؛ محسنی، سعید (۱۴۰۱). «تبیین اسباب مشروعیت پردازش داده‌های شخصی از منظر حقوق اتحادیه اروپا و ایران»، فصلنامه مطالعات حقوقی.

References

Authority, (Last visited 28/02/2024), Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/authority.

Barrett Paula, Doggett Lorna, (Last visited 08/05/2024), Shining a light on the meaning of "necessity" under GDPR Our eight point summary of the EDPB's draft guidance, online Edition: https://www.eversheds-sutherland.com/documents/services/what-necessity-means-for-gdpr-our-eight-point-summary.pdf, 2019

Rekosh Edwin, (Last visited 22/04/2024), Who defines the public interest?, international Journal of Human rights, online edition https://sur.conectas.org/en/defines-public-interest/

ICO Information Commissioners Office, (Last Visited 10/03/2024), What is valid consent?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/#top

Winkelman Roy, (Last visited 17/03/2024), Director, What is a Network?, Florida Center for Instructional Technology College of Education, University of South Florida, https://fcit.usf.edu/network/chap1/chap1.htm,

Yasar Kinza, (Last visited 15/02/2024), Gillis Alexander , computer network, https://www.techtarget.com/searchnetworking/definition/network

Alexandria, (Last visited 15/03/2024), Decentralized Network, https://coinmarketcap.com/alexandria/glossary/decentralized-network

Bhalla Anshika, (Last visited 11/02/2024), Centralized vs. Decentralized Digital Networks: Understanding The Differences, https://www.blockchain-council.org/blockchain/centralized-vs-decentralized-digital-networks/

Lutkevich Ben,, (Last visited 12/03/2024), Definition Intranet, https://www.techtarget.com/whatis/definition/intranet

van der Sloot, Bart, (2017), 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System', 31 Computer Law and Security Review, Volume 13, Issue 8, pp 18-34

Voigt, Paul, & von dem Bussche, Axel, (2017), The EU General Data Protection Regulation (GDPR). Springer International Publishing

Finck Michèle,Pallas Frank, (2020), They who must not be identified—distinguishing personal from non-personal data under the GDPR»,International Data Privacy Law,Volume10,Issue1,February, pp11–36

Intersoft Consulting, (Last visited 22/4/2024), General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-40-gdpr/

In Persian

Aghaei Touq, Muslim, Naser, Mahdi, (1403), Limits of applying the rules of protection of information processing in communication networks: a comparative study in the laws of Iran and the European Union, Comparative Public Law Quarterly, Volume 1, Number 2, pp. 20 -41

Larijani, Maryam, (1999), Locke's Theory: Consent or Contract, Philosophical-Theological Research Quarterly, Volume 9, Number 4, 1387, pp. 178-147

Latif Zadeh, Mahdieh, Gubouli Darafshan, Seyed Mohammad Mahdi, Mohseni, Saeed, (2022), Explanation of the reasons for the legitimacy of personal data processing from the perspective of European Union and Iranian laws, Legal Studies Quarterly, pp. 335-364