Comparative Law Biquarterly
Volume 6. Issue 1. Serial Number 9. Spring and Summer 2022. Pages 207 to 230.

Research Paper

How to Transfer Personal Data Internationally: A Comparative Study of European Union Law and Iranian Legal System

Mahdieh Latifzadeh*[1] , Seyyed Mohammad Mahdi Qabuli Dorafshan [2]

[1] Ph.D. in Private Law, Faculty of Law and Political Sciences, Ferdowsi University of Mashhad, Mashhad, Iran.
[2] Associate Professor of Private Law, Faculty of Law and Political Sciences, Ferdowsi University of Mashhad, Mashhad, Iran.

10.22080/LPS.2022.23212.1309

Received:
February 28, 2022
Accepted:
June 16, 2022
Available online:
July 19, 2022

Keywords:
International transfer, Citizenship rights, Personal data, Third country, General Data Protection Regulation (GDPR)

Main Subjects:
CIVIL LAW

Abstract

To fully protect personal data and data subjects, the European Union Data Protection Regulation (GDPR) addresses various aspects of such protection, one of which is the international transfer of personal data. From the point of view of the EU legislature, the rights of data subjects should not be undermined, even if their data is transferred to third countries or international organizations. Therefore, in several articles, it has set different requirements in this regard. In this research, a descriptive method has been used to analyze the tools required for the transfer of personal data in accordance with the EU law. These tools include Adequacy Decision, Standard Contractual Clauses, Binding Corporate Rules, Certification Mechanism, Codes of Conduct and specific situations of Article 49. Also, the existence of these requirements in the Iranian Legal System has been studied in a comparative way. The results show that in the Iranian law, due to the lack of specific legislation on personal data and, consequently, the articles authorizing the international transfer of personal data, only some of the requirements mentioned in the European regulation, especially the situations of Article 49, can be applied through the legal doctrine and principles of the Iranian law. Therefore, according to the Iranian law, the consent of the data subject, the contractual necessity, the existence of vital interests and the public interest, as well as the overriding legitimate interests of the controller can be considered as the reasons for the international transfer of personal data. However, the legislature's attention to the important issue of personal data protection in general and the international transfer of personal data in particular is essential.

*Corresponding Author: Mahdieh Latifzadeh
Address: Ph.D. in Private Law, Faculty of Law and Political Sciences, Ferdowsi University of Mashhad, Mashhad, Iran.
Email: M.latifzadeh@mail.um.ac.ir

Extended Abstract

1. Introduction

The development of information technology tools and the further processing of personal data has increased the need for legal protection of information privacy, and in particular, the protection of personal data. Such legal protections, as aspects of human rights and civil rights, exist in some legal systems in particular. In this regard, the European Union has introduced a model for the protection of personal data to the world by adopting the General Data Protection Regulation (GDPR). This regulation is the most comprehensive legal framework in this regard, addressing various aspects of the protection of personal data. One of the items in this regulation is the specification of the requirements related to the international transfer of personal data. These requirements must be clarified since, on the one hand, the flow of personal data to countries outside the European Union and international organizations is essential for the expansion of trade and international cooperation. On the other hand, it creates new challenges and concerns regarding the protection of personal data. Therefore, from the European legislature's point of view, when personal data are transferred from the EU to controllers, processors or other recipients in third countries or international organizations, the level of protection of natural persons guaranteed by this regulation in the EU should not be diminished. This may involve the transfer of personal data from a third country or international organization to controllers or processors in the same country or a third country or other international organizations. Accordingly, after explaining these requirements from the perspective of the European GDPR (Section 1), this study explains how these requirements flow in the Iranian Legal System (Section 2). This is to strengthen the protection of personal data in accordance with the Iranian law and assist the legislature in specifying accurate and comprehensive protections for personal data.

2. Methods

The present study uses a descriptive and analytical method to explain the various tools that can be mentioned as requirements for the international transfer of personal data in the European Union. Also, the flow of the aforementioned requirements in the Iranian Legal System is examined by a comparative method.

3. Conclusion

Effective protection of personal data is provided when the rights of the data subject are respected in various circumstances and their data rights are not violated, e.g., when personal data is transferred to other countries or international organizations before or during processing. The GDPR also addresses the protection of data subjects in the event of international transfer of personal data, and sets out various requirements in this regard. In other words, according to this regulation, the international transfer of personal data is allowed only with special tools. These include adequacy decisions that secure a third country. Standard contractual clauses are also a means by which international data transfer is unrestricted. In fact, the parties (data transferor in the EU and data recipient outside the EU) are required to enter a contract based on

standard contractual clauses to provide an appropriate level of data protection for the data transfer. Another tool is the flow of binding corporate rules that ensure an adequate level of data protection in the undertaking group or a group of companies engaged in joint economic activity. Adherence to codes of conduct or certificates can also be considered a license to transfer the personal data internationally. Apart from these, the existence of special situations provided in Article 49 of the GDPR is also a license for the international transfer of personal data. These include the consent of the data subject, the contractual necessity, the existence of vital and public interests, as well as the overriding legitimate interests of the controller. Among the requirements set out in the GDPR for the international transfer of data, only the specific situations of Article 49 of the GDPR through legal doctrine, the Iranian legal principles and other laws and regulations - not laid down for personal data - are acceptable as transfer requirements in the Iranian law. The reason for this limited support is the lack of an independent law to protect personal data and the ambiguities in the existing drafts. Therefore, it is necessary to expedite the adoption of a special law on the protection of personal data and to pay attention to the various dimensions of such protection, including how to transfer the personal data internationally. The various proposals of this research help improve and strengthen the existing drafts and protecting the personal data in the present case helps the legislator.

Funding
There is no funding support.

Authors' contribution
Authors contributed equally to the conceptualization and writing of the article. All of the authors approved the content of the manuscript and agreed on all aspects of the work.

Conflict of interest
Authors declared no conflict of interest.

Acknowledgments
We are grateful to all the scientific consultants of this paper.

علمی پژوهشی

چگونگی انتقال بین‌المللی داده‌های شخصی(مطالعه تطبیقی در حقوق اتحادیه اروپا و نظام حقوقی ایران)

مهدیه لطیف زاده[1*]، سید محمد مهدی قبولی درافشان[2]

[1] دکتری حقوق خصوصی، دانشکده حقوق علوم و سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران.
[2] دانشیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران.

10.22080/LPS.2022.23212.1309

تاریخ دریافت:
۹ اسفند ۱۴۰۰
تاریخ پذیرش:
۲۶ خرداد ۱۴۰۱
تاریخ انتشار:
۲۸ تیر ۱۴۰۱

چکیده

در راستای حمایت مؤثر از داده‌های شخصی و اشخاص موضوع داده، مقررات اروپایی حفاظت از داده (GDPR) جنبه‌های حمایتی مختلفی را موردتوجه قرار داده است. یکی از این حمایت‌ها، چگونگی انتقال بین‌المللی داده‌های شخصی است. از منظر قانون‌گذار اتحادیه اروپا حق بر داده‌ی اشخاص موضوع داده حتی در صورت انتقال داده‌ای افراد به کشورهای ثالث یا سازمان‌ها بین‌المللی نباید تضعیف شود. بدین‌جهت در چند ماده الزامات متفاوتی را در این خصوص مقرر نموده است. پژوهش حاضر با روش توصیفی و تحلیلی ابزارهای متنوعی که به‌عنوان الزامات مربوط به انتقال بین‌المللی داده‌های شخصی در اتحادیه اروپا قابل اشاره‌اند را تبیین نموده است. این ابزارها وجود سطح کافی حفاظت از داده (تصمیم کفایت)، شروط قراردادی استاندارد ، قواعد الزامی شرکتی ، مکانیسم گواهی‌نامه، منشورهای رفتاری و وجود موقعیت‌های ویژه ماده ۴۹ GDPR است. با شفاف‌سازی این ابزارها و چگونگی تحقق آن‌ها به‌موجب حقوق اتحادیه اروپا، جریان الزامات پیش‌گفته با روش تطبیقی در نظام حقوقی ایران موردبررسی قرار گرفت. بررسی‌های انجام‌شده حکایت از این دارد که در حقوق ایران به دلیل فقدان قانون خاص نسبت به داده‌های شخصی و بالتبع مواد مصرح در خصوص انتقال بین‌المللی داده‌های شخصی، صرفاً برخی الزامات برای انتقال - موقعیت‌های مقرر در ماده ۴۹ GDPR - از مسیر دکترین حقوقی و مبانی حقوق ایران قابل جریان است. بدین‌جهت به‌موجب حقوق ایران رضایت شخص موضوع داده، ضرورت قراردادی، وجود منافع حیاتی، جریان منافع عمومی و همچنین غلبه منافع مشروع کنترل‌کننده می‌تواند مجوزی برای انتقال بین‌المللی داده‌های شخصی تلقی شود. باوجوداین توجه قانون‌گذار به مسئله حیاتی حمایت از داده‌ی شخصی به‌طورکلی و انتقال بین‌المللی داده‌های شخصی به‌طور خاص ضروری است.

کلیدواژه ها:
انتقال بین‌المللی، حقوق شهروندی، داده‌ی شخصی، کشور ثالث، مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)

* **نویسنده مسئول:** مهدیه لطیف زاده
آدرس: دکتری حقوق خصوصی، دانشکده حقوق علوم و سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران.
ایمیل: m.latifzadeh@mail.um.ac.ir

مقدمه

توسعه‌ی ابزارهای فناوری اطلاعات و ارتباطات و پردازش [1] بیشتر داده‌های شخصی، ضرورت حمایت قانونی از حریم خصوصی اطلاعاتی و به‌طور خاص داده‌های شخصی افراد را روزافزون نموده است. چنین حمایت قانونی به‌عنوان جنبه‌ای از حقوق بشر و مصداقی از حقوق شهروندی[2] در برخی از نظام‌های حقوقی به‌طور ویژه موردتوجه قرارگرفته است. در این راستا اتحادیه اروپا با تصویب مقررات عمومی حفاظت از داده [3] - از این به بعد GDPR - الگویی را در خصوص حفاظت از داده‌ی شخصی[4] به جهان معرفی نموده است. این مقررات با پرداختن به جنبه‌های مختلف نسبت به حمایت از داده‌های شخصی، جامع‌ترین بستر قانونی در این خصوص است. ازجمله حمایت‌های این مقررات، تصریح بر الزامات مربوط به انتقال بین‌المللی داده‌های شخصی است. هدف از تصریح بر این الزامات این است که از یک سو جریان داده‌های شخصی به کشورهای خارج از اتحادیه اروپا و سازمان‌های بین‌المللی، برای گسترش تجارت و همکاری بین‌المللی ضروری است. از سویی دیگر، این امر چالش‌ها و نگرانی‌های جدیدی نسبت به حفاظت از داده‌های شخصی ایجاد کرده است. بدین‌جهت از منظر قانون‌گذار اروپایی هنگامی‌که داده‌های شخصی از اتحادیه اروپا به کنترل‌کنندگان داده [5]،

---

[1] Processing
پردازش به معنای عملیات یا مجموعه‌ای از عملیات است که بر روی داده‌ی شخصی یا مجموعه داده‌های شخصی، با وسایل خودکار و غیر آن، صورت گیرد، این موارد اعم از جمع‌آوری، ضبط، سازمان‌دهی، طبقه‌بندی، ذخیره‌سازی، اشتراک‌گذاری، تغییر، بازیابی، استفاده کردن، تجزیه‌وتحلیل کردن، انتشار، افشاء به‌وسیله مخابره کردن یا ایجاد دسترسی به شیوه‌های دیگر، ترکیب کردن، محدود نمودن، حذف و پاک کردن و یا تخریب است (EUR-Lex, 2016: 33).

[2] حق بر حریم خصوصی اطلاعاتی و حفاظت از داده‌های شخصی از حقوق شهروندی و از جنبه‌های حقوق بشر است. این حق در اسناد ملی و بین‌المللی مختلفی به‌عنوان جنبه‌ای از حقوق بشر مورد تصریح قرارگرفته است، به‌عنوان نمونه ماده ۱۲ اعلامیه جهانی حقوق بشر، حق بر حریم خصوصی (با همه اقسام آن ازجمله حق بر حریم خصوصی اطلاعاتی) را به‌عنوان یک حق اساسی به رسمیت شناخته است (United Nations, ۲۰۱۵: ۲۶). هم‌چنین در اتحادیه اروپا، حریم خصوصی و حمایت از داده دو حق حیاتی هستند (European Data Protection Supervisor, n.d.) که در مواد ۷ و ۸ منشور حقوق اساسی اتحادیه اروپا (EUR-Lex, ۲۰۱۲: ۳۹۷) و ماده ۸ کنوانسیون اروپایی حقوق بشر مورد تصریح قرار گرفته اند (Council of Europe, ۱۹۵۰: ۱۱).

[3] General Data Protection Regulation (GDPR)

[4] Personal Data
داده‌ی شخصی به موجب مقررات اروپایی حفاظت از داده، به معنای هر اطلاعاتی است که مربوط به شخص حقیقی شناخته‌شده یا قابل‌شناسایی (شخص موضوع داده) باشد. یک فرد حقیقی قابل‌شناسایی کسی است که به‌طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به یک شناسه ازجمله 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).
داده‌ی شخصی ماهیتی دو جنبه‌ای دارد که مرکب از بُعد مالی (مادی) و غیرمالی (معنوی) است. بدین جهت این داده ها فی نفسه ارزشمند هستند و در زمره ی اموال اند. ابعاد مالی داده‌ی شخصی حق انحصاری هرگونه بهره‌برداری از داده‌ی شخصی است. ابعاد معنوی داده‌ی شخصی نیز حقوقی است که وابسته به شخصیت شخص موضوع داده است. این حقوق در نظام حقوقی ایران مورد تصریح قرار نگرفته‌اند؛ لیکن در مواد ۱۲ الی ۲۲ GDPR به آن‌ها اشاره‌شده است. چنین حقوقی ازجمله دریافت اطلاعات در مورد پردازش داده‌های شخصی، دسترسی شخص موضوع داده به داده‌های شخصی مربوط به خود، حق تصحیح داده‌های شخصی نادرست یا ناقص و حذف داده‌های شخصی (فراموش‌شدن)، حق محدودیت پردازش داده‌های شخصی، حق انتقال داده، اعتراض به پردازش داده‌های شخصی برای اهداف بازاریابی و یا زمینه‌های مربوط به موقعیت‌های ویژه و عدم قرار گرفتن در معرض تصمیمات خودکار است. با توجه به ماهیت داده‌ی شخصی، حق بر داده‌ی شخصی نمی‌تواند حق مالکیت مرسوم و هم‌چنین حقوق مالکیت معنوی باشد، زیرا قواعد حق مالکیت مرسوم و مصادیق مختلف مالکیت معنوی هیچ‌یک کاملاً منطبق بر داده‌ی شخصی نیستند و بدین‌جهت داده‌ی شخصی نمی‌تواند با جریان حق مالکیت مرسوم یا حقوق مالکیت معنوی حمایت شود؛ بنابراین بستر حقوقی مناسب جهت حمایت از داده‌ی شخصی، حق مالکیت ویژه‌ای است که متفاوت از حق مالکیت مرسوم است. این حق ویژگی‌های خاص خود را دارد که توضیح آن در این مقال نمی‌گنجد.

[5] controller

پردازنده‌های داده [1] یا سایر دریافت‌کنندگان در کشورهای ثالث یا سازمان‌های بین‌المللی منتقل می‌شوند، نباید سطح حفاظت از اشخاص حقیقی که توسط این مقررات در اتحادیه تضمین‌شده است، تضعیف شود. این امر می‌تواند شامل انتقال داده‌های شخصی از یک کشور ثالث یا سازمان بین‌المللی به کنترل‌کننده‌ها یا پردازنده‌هایی در همان کشور یا کشور ثالث یا سازمان بین‌المللی دیگر باشد.

با توجه به مطالب پیش‌گفته، پژوهش حاضر با شناسایی و تبیین این الزامات از منظر مقررات اروپایی حفاظت از داده (بند ۱) نسبت به چگونگی جریان آن‌ها در نظام حقوقی ایران تمرکز دارد (بند ۲). این امر به هدف تقویت حمایت از داده‌های شخصی به‌موجب حقوق ایران و مساعدت به قانون‌گذار برای تصریح بر حمایت‌هایی دقیق و جامع نسبت به داده‌های شخصی است.

قبل از ورود به بحث اصلی گفتنی است باوجوداینکه در خصوص حقوق فناوری اطلاعات، حمایت از حریم خصوصی اطلاعاتی و حق بر داده‌های شخصی آثار متعددی وجود دارد؛ لیکن موضوع پژوهش حاضر در سایر آثار مشاهده نشده است. به‌عنوان‌مثال نوری و نخجوانی (۱۳۸۳) کتابی با عنوان «حقوق حمایت از داده» تألیف نموده‌اند. کتاب مزبور ابتدا به مباحث مربوط به حریم خصوصی پرداخته و در گام بعد به حمایت از داده‌ها اشاره‌کرده است؛ لیکن جهت بررسی حمایت از داده‌های شخصی در نظام حقوقی ایران، صرفاً به قانون تجارت الکترونیکی پرداخته و از نگاه این قانون بحث را پیش برده است. به‌علاوه با توجه به سال نشر این کتاب واضح است که به GDPR اشاره نشده است. هم‌چنین کروبی (۱۳۸۴) کتابی با عنوان «اتحادیه اروپا و بحث حمایت از داده‌های شخصی و حریم خصوصی در ارتباطات الکترونیکی» تألیف نموده است. این کتاب نیز مانند اثر سابق، حمایت از داده‌های شخصی در حقوق ایران را صرفاً در بستر قانون تجارت الکترونیکی بررسی کرده است. به‌علاوه در مقام بررسی تطبیقی نیز به دستورالعمل ۱۹۹۵ اتحادیه اروپا نسبت به حفاظت از داده‌ی شخصی پرداخته است که در حال حاضر با جریان GDPR، این دستورالعمل نسخ شده و قابل استناد نیست. به‌علاوه اصلانی (۱۳۸۴) کتابی با عنوان «حقوق فناوری اطلاعات» تألیف نموده است. در این کتاب نیز، تفاوت‌های مذکور در آثار قبلی وجود دارد، همچنین عمده مباحث آن به‌طور خاص مربوط به حریم خصوصی است (به‌طور خاص نسبت به داده‌های شخصی نیست) و از منظر تطبیقی نیز به GDPR اشاره نکرده است.

فارغ از کتب بیان‌شده، در میان مقالات نیز موضوع پژوهش حاضر مغفول مانده است. به‌عنوان نمونه افراسیاب و ناصر (۱۳۹۹) مقاله‌ای با عنوان «چارچوب‌های حقوقی حفظ امنیت پردازش داده‌های خصوصی مطالعه تطبیقی حقوق ایران و اتحادیه اروپا» تدوین نموده‌اند. هم‌چنین آقایی طوق و ناصر (۱۳۹۹) مقاله‌ای با عنوان «چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا مطالعه تطبیقی حقوق ایران و اتحادیه اروپا» نگارش نموده‌اند. به‌علاوه رئیسی و قاسم‌زاده لیاسی (۱۳۹۹)

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. (EUR-Lex, 2016: 33) بدین جهت 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(Colcelli, 2019: 1031).

[1] Processor

پردازنده به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که از جانب کنترل‌کننده پردازش داده‌های شخصی را انجام می‌دهد(EUR-Lex, 2016: 33) . پردازنده داده‌های شخصی را فقط به نمایندگی از کنترل‌کننده پردازش می‌کند. پردازنده باید ضمانت‌های کافی را برای اجرای اقدامات فنی و سازمانی مناسب ارائه کند تا اطمینان حاصل شود که پردازش توسط پردازنده مطابق با استانداردهای GDPR و تضمین حفاظت از حقوق افراد است (European Commission, 2018d).

مقاله‌ای با عنوان «چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر» تدوین نموده‌اند. در این پژوهش‌ها نیز از الزامات مربوط به انتقال بین‌المللی داده‌های شخصی سخنی به میان نیامده است و به‌طور خاص نگاه GDPR نسبت به این مسئله بررسی نشده است.

۱ الزامات مربوط به انتقال بین‌المللی داده شخصی به‌موجب مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)

هدف قانون‌گذار اروپایی برای تصریح بر الزامات مربوط به انتقال بین‌المللی داده‌های شخصی، حمایت حداکثری از داده‌های شخصی است؛ زیرا کنترل‌کنندگان و پردازنده‌های خارج از اتحادیه اروپا - با اثرپذیری از قوانین و مقررات مختلف - ممکن است از داده‌های شخصی و اشخاص موضوع داده به‌اندازه کافی حفاظت نکنند و یا حتی از شیوه‌های پردازشی استفاده نمایند که حقوق اساسی اشخاص موضوع داده را تضعیف می‌کند. به‌عنوان نمونه ممکن است الزامات مختلف ازجمله مستعاری سازی[1]، حفاظت از داده با طراحی و به‌طور پیش‌فرض [2] و... رعایت نشوند.

الزامات مربوط به انتقال بین‌المللی داده شخصی در مواد ۴۴ الی ۴۹ GDPR مقررشده‌اند. به‌موجب ماده ۴۴ GDPR هرگونه انتقال داده‌ی شخصی که در حال پردازش است یا پس از انتقال به کشوری ثالث یا سازمانی بین‌المللی برای پردازش در نظر گرفته می‌شود، باید با شرایط مقرر در ماده ۴۴ GDPR و مواد ذیل آن مطابقت داشته باشد. درواقع برای مشروعیت انتقال داده به کشورهای ثالث به‌موجب GDPR گذر از دو مرحله لازم است. در مرحله اول، انتقال باید مطابق با الزامات پردازش در داخل اتحادیه اروپا یعنی مبتنی بر رضایت شخص موضوع داده یا سایر مبانی حقوقی باشد. در مرحله دوم - علاوه بر موارد پیش‌گفته - انتقال باید با شرایط موجود در ماده ۴۴ GDPR و مواد بعد آن، به‌منظور اطمینان از سطح مناسب حفاظت از داده نیز مطابقت داشته باشد. در صورت فقدان این امر، امکان انتقال وجود ندارد هرچند که مبانی حقوقی برای پردازش به‌موجب مرحله اول رعایت شده باشد (Voigt & von dem Bussche, 2017: 117).

---

[1] Pseudonymisation
مستعار سازی به‌موجب ماده ۴ GDPR «به معنای پردازش داده‌های شخصی به روشی است که داده‌های شخصی دیگر نتوانند به یک شخص موضوع داده‌ی خاص بدون استفاده از اطلاعات اضافی نسبت داده شوند؛ به شرطی که چنین اطلاعات اضافی به‌طور جداگانه و همراه با اقدامات فنی و سازمانی نگهداری شود تا اطمینان حاصل شود که داده‌ها به یک شخص حقیقی شناسایی‌شده یا قابل‌شناسایی نسبت داده نمی‌شوند» (EUR-Lex, 2016: 33).

[2] Data Protection By Design And By Default
اشخاص پردازش کننده داده ملزم به اجرای اقدامات فنی و سازمانی مناسب جهت حفاظت از داده هستند. بدین منظور از همان مراحل اولیه، طراحی عملیات پردازش باید به‌گونه‌ای باشد که اصول حفاظت از حریم خصوصی و حفاظت از داده از همان ابتدا رعایت شود (حفاظت از داده با طراحی). حفاظت از داده با طراحی درواقع اقدامات پیشگیرانه است که خطرات حریم خصوصی را پیش‌بینی می‌کند و از آن‌ها جلوگیری می‌کند؛ بنابراین این نوع از حفاظت، راه‌حلی برای معضلات ارائه نمی‌دهد، بلکه هدف آن جلوگیری از وقوع معضلات است (Ferrara & Spoto, 2018: 3).
به‌علاوه به‌طور پیش‌فرض، اشخاص پردازش کننده داده باید اطمینان حاصل کنند که داده‌ی شخصی با بالاترین سطح حفاظت از داده پردازش می‌شوند. برای مثال تنها داده‌های لازم باید پردازش شوند، دوره ذخیره‌سازی داده‌ها کوتاه و دسترسی محدود باشد و پردازش داده به‌طور پیش‌فرض باید به‌گونه‌ای باشد که داده‌ی شخصی برای تعداد زیادی از افراد قابل‌دسترس نباشد (حفاظت از داده به‌طور پیش‌فرض). با توجه به تعاریف مذکور، مثال‌های حفاظت از داده با طراحی مستعار سازی و رمزگذاری است و برای حفاظت از داده به‌طور پیش‌فرض می‌توان موردی را گفت که تنظیمات یک پیام‌رسان اجتماعی به‌گونه‌ای است که پروفایل کاربران از ابتدا و به‌طور پیش‌فرض، برای تعداد نامحدودی از افراد قابل‌دسترس نباشد (European Commission, 2018c).

گفتنی است الزامات مربوط به انتقال، همچنین شامل انتقال داده‌ی شخصی از کشوری ثالث یا سازمانی بین‌المللی به‌طرف دیگر است، درواقع تدابیر حفاظتی برای انتقال داده‌ی شخصی به کشور ثالث به‌موجب GDPR ، شرایط مناسبی را برای نقل و انتقالات بعدی نیز فراهم می‌نماید تا سطح مناسب حفاظت از داده - مشابه با آنچه در GDPR در مورد چنین انتقال‌هایی وجود دارد- حفظ شود (EUR-Lex, 2016: 60). ابزارهای متنوعی که در راستای تحقق الزامات مربوط به انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی موردتوجه GDPR قرارگرفته‌اند، وجود سطح کافی حفاظت از داده (تصمیم کفایت) [1]، شروط قراردادی استاندارد [2]، قواعد الزامی شرکتی [3]، مکانیسم گواهی‌نامه [4] و منشور رفتاری [5] و درنهایت وجود موقعیت‌های ویژه [6] در ماده ۴۹ GDPR است. تبیین این موارد در بندهای جداگانه به شرح ذیل است.

۱،۱ وجود سطح کافی حفاظت از داده

به‌موجب ماده ۴۵ (۱) GDPR امکان انتقال داده‌های شخصی به کشور ثالث یا سازمان‌های بین‌المللی وجود دارد، درصورتی‌که کمیسیون اروپا **تصمیم گیرد** که کشور ثالثی، منطقه‌ای، یک یا چند بخش مشخص در یک کشور ثالث یا سازمان بین‌المللی موردنظر، سطح **کافی** حفاظت از داده را تضمین می‌نماید. چنین تصمیمی با اصطلاح «**تصمیم کفایت**[7]» در GDPR مقررشده است. به دیگر سخن تصمیم‌گیری برای کفایت یعنی اتحادیه اروپا بر وجود سطح کافی حفاظت از داده در یک کشور ثالث یا سازمان بین‌المللی، تصمیم گرفته است. باوجوداین تصمیم کشورهای ثالث یا سازمان‌های بین‌المللی موردنظر، امن تلقی می‌شوند و انتقال داده‌های شخصی به آن‌ها به کسب مجوز دیگر از سوی مراجع نظارتی نیاز ندارد. (See. Voigt & von dem Bussche, 2017: 117).

همچنین در راستای رویه‌ی قضایی دیوان دادگستری اتحادیه اروپا[8]، ماده ۴۵ (۲) GDPR معیارهای مربوط به «**تصمیم‌گیری برای کفایت**» ازجمله بررسی قانون حفاظت از داده‌ی کشور ثالث، رویه‌های اجرایی، نظارت و تعهدات بین‌المللی آن کشور ثالث را مقرر می‌کند. البته لازم نیست همه معیارها به‌طور یکسان وجود داشته باشند؛ چراکه تشخیص سطح مناسب حفاظت از داده با ارزیابی کلی در شرایطِ خاص، ایجاد می‌شود. در صورت مثبت بودن نتیجه این ارزیابی، کمیسیون اروپا می‌تواند «تصمیم‌گیری برای کفایت» را انجام دهد[9]. در این صورت کمیسیون باید مکانیسم بازبینی دوره‌ای و چگونگی اعمال آن را مشخص نماید، همچنین در صورت امکان مراجع نظارتی کشور ثالث را نیز تعیین کند (See. Bu-Pasha, 2017: 222).

کمیسیون اروپا تاکنون آندورا، آرژانتین، کانادا (سازمان‌های تجاری آن)، جزایر فارو، گورنسی، دوگلاس (جزیره من)، جرسی، نیوزیلند، سوئیس، ایالات‌متحده امریکا- نسبت به شرکت‌های دارای مجوز سپر حریم خصوصی [10] - و اروگوئه را دارای

---

[1] Adequacy decision
[2] Standard Contractual Clauses (SCC)
[3] Binding Corporate Rules (BCR)
[4] Certification mechanism
[5] Codes of Conduct (COC)
[6] specific situations
[7] Adequacy decision
[8] European Court of Justice (ECJ)

[9] با توجه به نص ماده ۴۵ (۸) GDPR، کمیسیون اروپا در وب سایت و روزنامه رسمی اتحادیه اروپا، فهرستی از کشورهای ثالث، منطقه ها و بخش های مشخصی که بر کفایت آن ها تصمیم گرفته است یا تصمیم گیری کفایت خود را لغو کرده است، منتشر می کند.

[10] بر اساس دستورالعمل حفاظت از داده در اتحادیه اروپا (بستر قانونی سابق)، داده های شخصی تنها در صورتی می توانند به سایر کشورها منتقل شوند که به اندازه کافی در آنجا محافظت شوند. اینکه آیا سایر کشورها در موقعیتی هستند که سطح کافی حفاظت از داده را تضمین کنند، باید توسط کمیسیون اروپا ارزیابی شود. این پیش‌زمینه‌ای بود تا در سال ۲۰۰۰، کمیسیون اتحادیه اروپا در تصمیم بندرگاه امن خود (Safe Harbor decision) اعلام کند که ایالات متحده کشوری است

سطح کافی حفاظت از داده می‌داند (European Commission, 2019). به‌عنوان‌مثال یک شرکت فرانسوی قصد دارد خدمات خود را به آمریکای جنوبی به‌ویژه آرژانتین، اروگوئه و برزیل ارائه دهد. اولین گام این است که بررسی کند آیا آن کشورهای ثالث دارای «تصمیم کفایت» هستند. در این مثال، آرژانتین و اروگوئه، دو کشور امن اعلام‌شده‌اند و تصمیم کفایت نسبت به آن‌ها وجود دارد؛ بنابراین شرکت فرانسوی می‌تواند داده‌های شخصی را بدون هیچ‌گونه الزام حفاظتی دیگر به آن دو کشور ثالث انتقال دهد ولی برای انتقال به برزیل که دارای تصمیم کفایت نیست، شرکت فرانسوی باید از سایر ابزارهای معرفی‌شده برای انتقال بین‌المللی داده‌ها در GDPR استفاده نماید (European Commission, 2018e).

۱،۲ شروط قراردادی استاندارد

در برخی موارد ممکن است حتی با فقدان تضمین سطح مناسب حفاظت از داده مطابق با استانداردهای GDPR در یک کشور ثالث یا سازمان بین‌المللی، اشخاص پردازش کننده داده (کنترل‌کننده‌ها و پردازنده‌ها) هنوز مایل به انتقال داده‌های شخصی به چنین کشور یا سازمانی باشند. به‌منظور جبران فقدان حفاظت از داده، طرف ارسال‌کننده داده و طرف دریافت‌کننده، می‌توانند مطابق با ماده ۴۶ (۲) بندهای ج و دGDPR ، از شروط قراردادی استاندارد اتحادیه اروپا (scc) [1] استفاده نمایند. درواقع منتقل‌کننده داده در اتحادیه اروپا و دریافت‌کننده داده در خارج از اتحادیه اروپا، می‌توانند قراردادی مبتنی بر شروط قراردادی استاندارد منعقد نمایند تا سطح مناسب حفاظت از داده برای انتقال داده فراهم شود. البته در مواردی که طرفین متعاهد از شروط قراردادی استاندارد استفاده می‌کنند، سطح کافی حفاظت از داده، صرفاً توسط دریافت‌کننده‌ی داده که طرف قرارداد است - و در کشور ثالث مستقر بوده- تضمین‌شده تلقی می‌شود و کل کشور ثالث، کشوری «امن» برای انتقال داده از اتحادیه اروپا محسوب نمی‌گردد. این امر در شرایطی است که این شروط به‌طور قراردادی، صرفاً یک شخص پردازش کننده داده‌ی غیر عضو اتحادیه اروپا را متعهد می‌سازد تا سطح حفاظت از داده را به میزان اتحادیه اروپا تضمین نماید (Voigt & von dem Bussche, 2017: 119).

شروط قراردادی استاندارد باید به‌طور کامل و بدون تغییر اتخاذ شوند ولی استفاده از آن‌ها، مانعی برای کنترل‌کننده یا پردازنده با دریافت‌کنندگان خارج از اتحادیه‌ی اروپا برای انعقاد قراردادی موسع نیست. بدین‌جهت متعاقدین می‌توانند سایر بندها یا ضمانت‌های اضافی را لحاظ کنند، مشروط بر این‌که این موارد، به‌طور مستقیم یا غیرمستقیم با شروط قراردادی استاندارد مغایرت نداشته باشند و حقوق اشخاص موضوع داده را نیز نقض نکند. (EUR-Lex, 2016: 20 & 21).

تاکنون کمیسیون اروپا سه مجموعه از این شروط را تصویب نموده است. دو مجموعه از آن‌ها برای انتقال داده از کنترل‌کنندگان در اتحادیه اروپا به کنترل‌کنندگان در غیر اتحادیه اروپا و یکی از آن‌ها برای انتقال داده از کنترل‌کنندگان در اتحادیه اروپا به پردازنده‌های در غیر اتحادیه اروپا است[2]. از

که سطح مناسبی در خصوص حفاظت از داده‌ها دارد. بدین جهت داده‌های شخصی مشتریان یا کاربران اینترنت و همچنین کارمندان را می‌توان از کشورهای عضو اتحادیه اروپا بدون هیچ‌گونه الزام دیگر به ایالات متحده آمریکا منتقل کرد. با این حال، دیوان دادگستری اروپا (ECJ) در حکم خود در ۶ اکتبر ۲۰۱۵ (مراجعه به C-۳۶۲/۱۴) بیان کرد که سطح مناسب حفاظت از داده در ایالات متحده وجود ندارد و داده های شخصی به اندازه کافی در ایالات متحده محافظت نمی شود. با توجه به این امر، ECJ ، تصمیم کمیسیون اتحادیه اروپا در خصوص بندرگاه امن را بی اعتبار اعلام کرد و از این رو مبنای حقوقی برای انتقال داده های شخصی به ایالات متحده را پس گرفت. کمیسیون اروپا و ایالات‌متحده برای ایجاد یک چارچوب جدید در سال ۲۰۱۶، معروف به «سپر حریم خصوصی اروپا - ایالات‌متحده» به توافق رسیدند (See. Sullivan, ۲۰۱۹; ۳۸۸-۳۸۹ & See. Bu-Pasha, ۲۰۱۷: ۲۲۴)

[1] Standard Contractual Clauses(scc)

[2] هر سه مجموعه شروط قراردادی استاندارد در وب سایت کمیسیون اروپا موجود است:

شروط قراردادی استاندارد کنترل‌کننده به کنترل‌کننده باید به‌صورت متناوب استفاده شود و ترکیبی از شروط هر دو مجموعه مجاز نیست. مجموعه اول مربوط به تصمیم 2001/497/EC است که به‌موجب آن هر دو طرف مسئولیت مشترک و چندجانبه برای تعهدات حفاظت از داده دارند. مجموعه دوم نیز در خصوص تصمیم 2004/915/EC است که عموماً به‌عنوان تجارتی دوستانه‌تر در نظر گرفته می‌شود؛ زیرا با همکاری انجمن‌های تجاری مختلف توسعه‌یافته است. به‌موجب این مجموعه، تعهدات حفاظت از داده به‌وضوح بین طرفین تخصیص می‌شوند و هر طرف مسئولیت تعهدات خود را بر عهده دارد. مجموعه سوم نیز شروط قراردادی استاندارد کنترل‌کننده به پردازنده مبتنی بر تصمیم 2010/87/EU است. به‌موجب این دسته از شروط قراردادی، فعالیت‌های برون‌سپاری به پردازنده فرعی درصورتی‌که بتواند سطح مناسب حفاظت از داده را فراهم کند، مجاز است (European Commission, 2018b).

در مقام عمل استفاده از این شروط مزایا و معایبی دارد که باید قبل از انتخابِ این مبنای حقوقی، در نظر گرفته شوند. مزیت‌ها عبارت‌اند از اینکه استفاده از آن‌ها سریع است و نسبت به مذاکره برای انعقاد یک قرارداد یا اتخاذ قواعد الزامی شرکتی - که توضیح آن در بند بعد خواهد آمد- به تلاش کمتری نیاز دارد؛ شروط قراردادی استاندارد حاوی قواعد حفاظت از داده مطابق با قانون است و ازآنجایی‌که آن‌ها باید به‌طور کامل و بدون تغییر پذیرفته شود، مذاکرات بین طرفین بر استانداردهای قانونی حفاظت از داده تأثیر منفی نمی‌گذارد؛ آن‌ها می‌توانند به‌عنوان مبنای قراردادی برای انتقال بین کنترل‌کننده‌های ارسال‌کننده و کنترل‌کننده‌ها یا پردازنده‌های دریافت‌کننده بدون توجه به رابطه شخصی‌شان عمل کنند، بنابراین هیچ محدودیتی ازجمله فعالیت‌های پردازشی درون‌گروهی وجود ندارد؛ هم‌چنین از آن‌ها می‌توان در شرایطی استفاده کرد که بیش از دو طرف درگیر هستند. در مقابل معایبی نیز وجود دارد، ازجمله اینکه در استفاده از این شروط فردیت و انعطاف‌پذیری برای توجه به نیازهای خاص هر شخص پردازش کننده داده مفقود است، البته این امر ویژگی ذاتی همه‌ی اقسام قراردادهای نمونه است؛ هم‌چنین استفاده از آن‌ها برای فعالیت‌های پردازشی درون‌گروهی ممکن است در مقایسه با قواعد الزامی شرکتی به تلاش بیشتر برای تحقق نیاز داشته باشد، زیرا باید بین همه اعضای گروه به‌طور جداگانه توافق شود (Voigt & von dem Bussche, 2017: 122).

۱،۳ قواعد الزامی شرکتی

ابزار دیگرِ قابل‌استفاده برای جبران فقدان حفاظت از داده، در کشور ثالثی که به‌موجب ماده ۴۵ GDPR «امن» نیست، قواعد الزامی شرکتی (BCR) [1] است. اشخاص پردازش کننده داده می‌توانند به‌موجب مواد ۴۶ (۲) (ب) و ۴۷ GDPR برای انتقال بین‌المللی داده‌های شخصی از قواعد الزامی شرکتی (BCR) استفاده نمایند. این قواعد حفاظت کافی برای انتقال بین‌المللی داده‌ها را ایجاد می‌کنند و برای اولین بار الزامات قانونی دقیق آن توسط GDPR موردتوجه قرارگرفته است. درواقع این ابزار، سیاست‌های حریم خصوصی جهانی اعضای گروه را برای انتقال بین‌المللی داده‌های شخصی به آن دسته از اعضای گروه که در کشورهای ثالث واقع‌شده‌اند و سطح مناسب حفاظت از داده را به‌موجب ماده ۴۵ GDPR ندارند، تبیین می‌نماید. این ابزار مطابق با منافع گروه تعهدات (سازمان تجاری) [2] یا شرکت‌های درگیر در فعالیت اقتصادی مشترک و در جهت دسترسی به داده‌های شخصی برای تمام شرکت‌های درگیر - صرف‌نظر از اینکه آن‌ها در داخل یا خارج از اتحادیه اروپا قرار دارند- است؛ بنابراین این قواعد

[1] Binding Corporate Rules (BCR)
[2] Group of Undertakings

http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm, accessed 3 Feb 2017

استانداردی برای حفاظت از داده درون‌گروهی است که سطح مناسبی از امنیت داده را مطابق با استانداردهای قانونی اتحادیه اروپا تضمین می‌کند. به دیگر سخن این قواعد مربوط به دو موقعیت است. اولاً شرکت‌های چندملیتیِ گروه تعهدات (سازمان تجاری) که متشکل از یک کنترل‌کننده‌ی گروه تعهدات (سازمان تجاری) و کنترل شونده‌ی گروه تعهدات (سازمان تجاری) [۱] است. ثانیاً برای گروهی از شرکت‌های درگیر در فعالیت اقتصادی مشترک است. لازم به ذکر است اعضای این گروه، برخلاف گروه تعهدات (سازمان تجاری) ازنظر قانونی مستقل هستند و به دلیل استقلال خود، گروه تعهدات (سازمان تجاری) محسوب نمی‌شوند. (See. European Commission, 2018a).

با توجه به مطالب پیش‌گفته، قواعد الزامی شرکتی نمی‌تواند به‌عنوان مبنایی برای انتقال بین‌المللی داده، به شرکت‌هایی که مربوط به گروه تعهدات (سازمان تجاری) یا شرکت‌های درگیر در یک فعالیت اقتصادی مشترک نیستند، مورداستفاده قرار گیرد. به‌علاوه، شرکت‌های گروه باید به خاطر داشته باشند که این قواعد صرفاً سطح مناسب حفاظت از داده در گروه را اثبات می‌کند؛ لیکن نمی‌تواند به‌عنوان مبنای حقوقی برای پردازش عمل کند. بدین‌جهت شرکت‌های گروه باید تضمین کنند که مبنای حقوقی برای پردازش – مقرر در ماده ۶ (۱) GDPR [۲] - دارند (See. Eija, 2018: 28).

باوجوداین که این قواعد به‌عنوان ابزاری برای انتقال بین‌المللی داده‌های شخصی قابل اتخاذ است؛ لیکن استفاده از آن‌ها در مقام عمل مستلزم مزایا و معایبی است که اشخاص پردازش کننده داده، باید قبل از اتخاذ، این موارد را موردتوجه قرار دهند. ازجمله معایب این است که پیاده‌سازی آن‌ها مستلزم بررسی دقیق جریان داده‌ها درون گروه است تا مشخص شود که کدام کشورهای ثالث در معرض دائم انتقال داده هستند و چه سطحی از حفاظت داده را فراهم می‌کنند؛ هم‌چنین استفاده از آن‌ها محدود به انتقال داده‌ها درون گروه است؛ به‌علاوه ضرورت تأیید آن‌ها توسط مرجع نظارتی ذی‌صلاح، به تلاش قابل‌توجهی توسط گروه نیاز دارد تا بتوانند این قواعد را پیاده‌سازی کنند. در مقابل مزیت‌ها عبارت‌اند از اینکه استفاده از آن‌ها استانداردهای حفاظت از داده را به شیوه‌ای اجرا می‌کند که متناسب با نیازهای خاص گروه باشد؛ آن‌ها در مقایسه با شروط قراردادی استاندارد، ابزاری مستقل و انعطاف‌پذیر برای انتقال بین‌المللی داده‌ها هستند؛ هم‌چنین فرآیند اجرای دقیق این قواعد، مستلزم شناسایی دقیق جریان داده‌ها است و می‌تواند برای انجام سایر تعهدات بر اساس GDPR مانند حقوق اشخاص موضوع داده، مفید باشد (Voigt & von dem Bussche, 2017: 129).

---

[۱] در ماده ۴ (۱۹) GDPR، گروه تعهدات (سازمان تجاری) شرکت کنترل کننده به همراه شرکت کنترل شونده ی تحت آن، تعریف شده است.

[۲] ماده ۶ (۱) GDPR مقرر می‌کند « پردازش مجاز است اگر حداقل یکی از موارد ذیل وجود داشته باشد :

أ. شخص موضوع داده به پردازش داده‌های شخصی خود برای یک یا چند هدف خاص رضایت داده باشد؛

ب. پردازش برای اجرای قرارداد ضروری است، شخص موضوع داده باید یکی از اطراف قرارداد باشد یا پردازش به‌منظور انجام مراحل به درخواست شخص موضوع داده قبل از انعقاد قرارداد رخ دهد؛

ج. پردازش برای انجام تعهد قانونی که کنترل‌کننده تابع آن است، ضروری است؛

د. پردازش برای حفظ منافع حیاتی شخص موضوع داده یا شخص حقیقی دیگری ضروری است؛

ه. پردازش برای انجام‌وظیفه‌ای در جهت منافع عمومی یا اعمال اختیارات رسمی واگذارشده به کنترل‌کننده، ضروری است؛

و. پردازش برای اهداف مشروع دنبال شده توسط کنترل‌کننده یا شخص ثالث، ضروری است، مگر در مواردی که این منافع تحت‌الشعاع منافع، حقوق یا آزادی‌های اساسی شخص موضوع داده قرار گیرند که مستلزم حفاظت از داده‌های شخصی است، به‌خصوص درصورتی‌که شخص موضوع داده کودک است.

بند « و » برای پردازش توسط مراجع عمومی در انجام وظایفشان اعمال نمی شود» (EUR-Lex, 2016, p. 36).

۱،۴ گواهی‌نامه‌ها و منشورهای رفتاری

ابزارهای دیگری که در خصوص انتقال بین‌المللی داده‌ها قابل اشاره هستند، ابزارهای «خود – مقرراتی»[1] اند که می‌توانند در جهت اثبات انطباق با GDPR کمک نمایند. چنین ابزارهایی منشورهای رفتاری [2] (مقرر در ماده ۴۰ و GDPR ۴۱) و مکانیسم گواهی‌نامه [3] (مقرر در ماده ۴۲ و GDPR ۴۳) هستند که به‌طورکلی می‌توانند سطح مناسبی از امنیت داده را تضمین نمایند و به‌عنوان مبنای حقوقی برای انتقال بین‌المللی داده‌ها نیز استفاده شوند (Segovia Domingo & Desmet Villar, 2018: 3).

منشور رفتاری از منظر GDPR از ابزارهای پاسخگویی داوطلبانه است که تعهدات بر اساس GDPR را برای یک بخش یا فناوری خاص مشخص می‌کند. این منشورها برای اشخاص پردازش کننده‌ی داده (کنترل‌کننده‌ها و پردازنده‌ها) شناسایی چالش‌های کلیدی درزمینه‌ی حفاظت از داده را در شرکت، سازمان و نهاد خود ممکن می‌سازند تا در جهت رفع آن‌ها اقدامات مناسب مورد توجه قرار گیرند. با وجود منشور رفتاری، کنترل‌کننده‌ها و پردازنده‌ها می‌توانند اطمینان حاصل نمایند که آن‌ها GDPRرا به‌طور مؤثری اعمال می‌کنند (ICO, 2018a). مکانیسم گواهی‌نامه نیز، روشِ صدور گواهی برای یک محصول، فرآیند یا سرویس خاص است. بر اساس GDPR [4]، گواهی‌نامه‌ها نیز ابزاری داوطلبانه برای کنترل‌کننده‌ها و پردازنده‌ها در راستای افزایش شفافیت و اثبات انطباق با GDPR هستند. این ابزار متضمن اصل پاسخگویی است و برای اشخاص موضوع داده، امکان ارزیابی سریعِ سطح حفاظت از داده‌ی کالاها و خدمات مربوطه را ممکن می‌سازد. به‌طورکلی گواهی‌نامه‌ها برای اثباتِ انطباق فعالیت‌های گواهی‌شده با GDPR ، مورداستفاده قرار می‌گیرند (Practical Law, n.d).

این دو ابراز می‌توانند برای انتقال بین‌المللی داده‌های شخصی نیز استفاده شوند. بدین ترتیب که اشخاص پردازش کننده داده که در کشوری ثالث واقع‌شده‌اند، می‌توانند به یک منشور رفتاری تائید شده با اعتبار عمومی به‌موجب ماده ۴۰ (۳) [5] پایبند باشند. از سویی دیگر کنترل‌کننده‌ها و پردازنده‌ها نیز تعهدات الزامی نسبت به شرکتی که داده از طریق قرارداد یا سایر ابزارهای حقوقیِ لازم‌الاجرا به آن منتقل‌شده است، دارند. هم‌چنین اشخاص پردازش کننده داده در کشور ثالث می‌توانند گواهی‌نامه‌ای به دست آورند که مبین سطح مناسبِ حفاظت از داده به‌موجب ماده ۴۲ (۲) GDPR [6] است. این

---

[1] Self-regulation
[2] Codes of Conduct (COC)
[3] Certification mechanism
[4] البته مقررات اروپایی حفاظت از داده، اصطلاح مربوط به مکانیسم گواهی‌نامه را تعریف نکرده است و این تعریف از منابع دیگر و با توجه به رویکرد حمایتی GDPR استنباط شده است.
[5] ماده ۴۰ (۳) GDPR «علاوه بر پایبندی کنترل کننده ها یا پردازنده های موضوع این مقررات به منشورهای رفتاری تایید شده به موجب بخش ۵ این ماده و داشتن اعتبار عمومی مطابق بخش ۹ این ماده، ممکن است منشورهای رفتاری توسط کنترل‌کننده‌ها یا پردازنده هایی رعایت شوند که تابع این مقررات مطابق با ماده ۳ نیستند. این امر برای تحقق حفاظت مناسب در چارچوب انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی به موجب شرایط مذکور در بند (ه) ماده ۴۶ (۲) است. این کنترل‌کننده‌ها یا پردازنده ها باید از طریق ابزارهای قراردادی و یا سایر ابزارهای حقوقی الزام‌آور، تعهدات لازم و قابل اجرایی را برای اعمال حفاظت های مناسب از جمله در خصوص حقوق اشخاص موضوع داده، انجام دهند» (EUR-Lex, 2016: 57).
[6] ماده ۴۲ (۲) GDPR « (۱) علاوه بر پایبندی کنترل کننده ها یا پردازنده های موضوع این مقررات به مکانیسم گواهی نامه ی تصویب شده حفاظت از داده، مهر و یا علائم تاییده شده به موجب بخش ۵ این ماده، ممکن است این موارد به منظور اثبات وجود حفاظت های مناسب ارائه شده توسط کنترل کننده ها یا پردازنده هایی که موضوع این مقررات به موجب ماده ۳ نیستند، در چارچوب انتقال داده های شخصی به کشورهای ثالث یا سازمان های بین المللی به موجب شرایط مندرج در بند (و) ماده (۴۶)۲ انجام شود. (۲) این کنترل‌کننده‌ها یا پردازنده ها باید از طریق ابزارهای قراردادی یا سایر ابزارهای حقوقی الزام‌آور، تعهدات لازم و قابل اجرایی را برای اعمال حفاظت های مناسب از جمله برای اِعمال حقوق شخص موضوع داده رعایت نمایند» (EUR-Lex, 2016: 59)..

گواهی‌نامه می‌تواند به‌عنوان مبنای حقوقی برای انتقال بین‌المللی داده نیز عمل کند، درصورتی‌که دریافت‌کننده داده نیز به رعایت تعهدات الزامی به‌عنوان‌مثال از طریق قرارداد، ملزم شود (See. Sullivan, 2019; 390).

۱،۵ وجود موقعیت‌های ویژه مقرر در ماده ۴۹ GDPR

تا بدین جا با استناد به مواد ۴۴ الی ۴۸ GDPR ابزارهای مختلفی که به‌عنوان مجوز برای انتقال بین‌المللی داده‌های شخصی وجود داشت، موردتوجه قرار گرفت. فارغ از این موارد، انتقال داده‌های شخصی به کشورهای ثالث یا سازمان‌های بین‌المللی ممنوع است مگر این‌که موقعیت‌های خاص در ماده ۴۹ GDPR وجود داشت باشند. بدین‌جهت در صورت فقدان ابزارهای پیش‌گفته برای انتقال بین‌المللی داده‌های شخصی، وجود هر یک از موقعیت‌های ویژه مقرر در ماده ۴۹ GDPR نیز می‌تواند مجوزی برای انتقال بین‌المللی داده‌ها باشد. به‌موجب نص این ماده «در صورت فقدان تصمیم‌گیری برای کفایت مطابق با ماده ۴۵ (۳) یا ضمانت‌های حفاظتی مناسب به‌موجب ماده ۴۶ شامل قواعد الزامی شرکتی؛ انتقال یا مجموعه انتقال‌های داده‌ی شخصی به کشور ثالث یا سازمان بین‌المللی صرفاً با حصول هر یک از شرایط ذیل قابل انجام است: الف- پس از مطلع شدن از خطرات احتمالی، شخص موضوع داده حتی با فقدان تصمیم‌گیری برای کفایت و سایر ضمانت‌های حفاظتی مناسب برای داده‌های موردنظر، به انتقال پیشنهادی رضایت صریح داده است؛ ب- انتقال برای اجرای قرارداد بین شخص موضوع داده و کنترل‌کننده یا برای انجام اقدامات پیش قراردادی به درخواست شخص موضوع داده ضروری است. ج- انتقال برای انعقاد یا اجرای قرارداد منعقده در جهت منافع شخص موضوع داده بین کنترل‌کننده و یک شخص حقیقی یا حقوقی دیگر ضروری است؛ د- انتقال به دلایل منافع مهم عمومی ضروری است؛ ه- انتقال برای ایجاد، اِعمال یا دفاع از مطالبات حقوقی ضروری است؛ و- انتقال به‌منظور حفاظت از منافع حیاتی شخص موضوع داده یا افراد دیگر درجایی که شخص موضوع داده از نظر جسمی یا قانونی قادر به رضایت نیست، ضروری است؛ ز- انتقال از طریق سیستم ثبتی انجام می‌شود که به‌موجب قانون اتحادیه یا کشورهای عضو، اطلاعاتی را در اختیار عموم قرار می‌دهد یا به‌طورکلی برای عموم یا هر شخصی که منافع قانونی دارد قابل‌دسترسی است؛ لیکن صرفاً درصورتی‌که شرایط مقرر در قانون اتحادیه یا کشورهای عضو برای دسترسی در مورد خاص محقق شود. در صورت فقدان تصمیم‌گیری برای کفایت، قانون اتحادیه یا کشور عضو می‌تواند به دلایل منافع مهم عمومی به‌صراحت، محدودیت‌هایی را برای انتقال دسته‌های خاص از داده‌های شخصی به کشور ثالث یا سازمان بین‌المللی مشخص کند. کشورهای عضو باید این مفاد قانونی را به کمیسیون اطلاع دهند» (EUR-Lex, 2016: 64). با توجه به کثرت موقعیت‌های مقرر در این ماده توضیح اهم این موارد به شرح ذیل است.

به‌موجب ماده ۴۹ (۱) (الف) GDPR امکان انتقال داده‌ی شخصی به یک کشور ثالث - فارغ از سطح حفاظت از داده‌ای که در آن کشور وجود دارد - درصورتی‌که شخص موضوع داده صراحتاً با انتقال موافقت کرده باشد وجود دارد. دلیل این امر احترام به حق حریم خصوصی افراد است که آن‌ها را قادر می‌سازد تا در مورد رفتار با داده‌های شخصی خود، آن‌گونه که مناسب می‌دانند تصمیم گیرند. البته علاوه بر شرایط رضایتِ معتبر بر اساس GDPR [۱]،

[۱] «ماده ۷ - شرایط رضایت: ۱- درجایی که پردازش بر اساس رضایت است، کنترل‌کننده باید بتواند ثابت کند که شخص موضوع داده با پردازش داده‌های شخصی خود موافقت کرده است. ۲- اگر رضایت شخص موضوع داده در ضمن اظهارنامه کتبیِ مرتبط با موضوعات دیگر کسب شود، درخواست رضایت باید به شیوه‌ای ارائه شود که به‌وضوح از سایر موارد، به شکلی قابل‌فهم و در دسترس، با استفاده از زبانی روشن و ساده قابل‌تشخیص باشد. هر بخشی از چنین اظهارنامه‌ی کتبی که

رضایت باید صراحتاً به انتقال یا انتقال‌های موردنظر مربوط باشد. هم‌چنین با توجه به نص ماده ۴۹ (۱) (الف) GDPR شخص موضوع داده باید از خطرات احتمالیِ انتقال - به دلیل فقدان سطح مناسب حفاظت از داده در کشور ثالث - مطلع شود. بدین‌جهت در زمان اعلام رضایت، اشخاص موضوع داده باید از اینکه سطح حفاظت از داده در کشور ثالث متناسب با سطح حفاظتی مقرر در GDPR نیست، مطلع شوند (See. EUR-Lex, 2016: 64).

هم‌چنین بر اساس ماده ۴۹ (۱)(ب) GDPR درصورتی‌که برای اجرای قرارداد بین شخص موضوع داده و ارسال‌کننده‌ی داده یا برای انجام امور پیش قراردادی به درخواست شخص موضوع داده، انتقال ضروری باشد، این امر مجاز است. ضرورت انتقال صرفاً درجایی است که ارتباط نزدیک و اساسی بین شخص موضوع داده و اهداف قراردادی وجود داشته باشد. بدین‌جهت اگر اهداف قرارداد، بدون انتقال داده به کشور ثالث قابل تحقق است، چنین انتقالی غیرضروری است و بر اساس ماده ۴۹ (۱) (ب) GDPR مجاز نیست (Voigt & von dem Bussche, 2017: 130). هم‌چنین به‌موجب ماده ۴۹ (۱) (ج) GDPR ضرورت انتقال برای انعقاد یا اجرای قراردادِ منعقدشده - به نفع شخص موضوع داده - بین کنترل‌کننده و شخص ثالث نیز مجوزی برای انتقال است (EUR-Lex, 2016: 64).

مجوز دیگر، ضرورت انتقال به جهت منافع مهم عمومی یا حفاظت از منافع حیاتی افراد است. به‌موجب ماده ۴۹(۱) (د) GDPR این جواز به دلیل وجود ملازمه بین انتقال داده‌ها و تحقق منافع مهم عمومی است. البته متعاقب ماده ۴۹ (۴) GDPR صرفاً منافع مهم عمومی شناسایی‌شده به‌موجب قانون اتحادیه اروپا یا قانون کشور عضوی که برای کنترل‌کننده لازم‌الاجرا است، در این زمینه معتبر هستند. برای مثال منافع مهم عمومی می‌توانند تبادل بین‌المللی داده‌ها بین مراجع رقابتی، ادارات مالیات یا گمرک، بین مراجع نظارت مالی، بین مراجع خدماتی ذی‌صلاح برای مسائل تأمین اجتماعی یا برای بهداشت عمومی باشند. هم‌چنین بر اساس ماده ۴۹ (۱) (و) GDPR انتقال مجاز است، درصورتی‌که برای حفاظت از منافع حیاتی شخص موضوع داده یا افراد دیگر ضروری بوده و شخص موضوع داده نیز ازلحاظ جسمی یا قانونی قادر به رضایت دادن نباشد (See. EUR-Lex, 2016: 64-65).

در نهایت نیز می‌توان به ماده ۴۹ (۱) GDPR اشاره نمود. به‌موجب این مفاد قانونی درصورتی‌که منافع مشروع کنترل‌کننده بر منافع شخص موضوع داده غالب باشد، انتقال بین‌المللی داده‌های شخصی مجاز است. با توجه به نص این ماده، این بند نمی‌تواند به‌عنوان مبنای حقوقی برای پردازنده‌ها به‌منظور انتقال داده‌های شخصی به پردازنده‌های فرعی در خارج از اتحادیه اروپا عمل کند. هم‌چنین صرفاً در صورتی قابل‌اعمال است که سایر مبانی حقوقی (مجوزها) برای انتقال بین‌المللی داده‌های شخصی وجود نداشته باشد و کنترل‌کننده‌ی ارسال‌کننده نیز شرایط مقرر در این ماده را رعایت نماید (See. EUR-Lex, 2016: 64).

ناقض این مقررات است، الزام‌آور نیست. ۳- شخص موضوع داده باید این حق را داشته باشد که در هر زمان رضایت خود را پس بگیرد. پس گرفتن رضایت، بر مجاز بودن پردازش مبتنی بر رضایت قبل از پس گرفتن، تأثیری نخواهد داشت. قبل از کسب رضایت، شخص موضوع داده باید از حق پس گرفتن مطلع شود. انصراف از رضایت باید به‌راحتی کسب رضایت باشد. ۴- هنگام ارزیابی این‌که آیا رضایت آزادانه است، باید حداکثر توجه را مبذول داشت که آیا اجرای یک قرارداد، ازجمله ارائه‌ی یک خدمت، مشروط به رضایت برای پردازش داده‌های شخصی است که برای اجرای آن قرارداد ضروری نیستند یا خیر» (EUR-Lex, 2016: 37).

۲ بررسی الزامات مربوط به انتقال بین‌المللی داده شخصی در نظام حقوقی ایران

باوجود اهمیت حفاظت از حق بر داده‌های شخصی و لزوم توجه ویژه هر نظام حقوقی به این حق به‌عنوان یکی از حقوق شهروندی و جنبه‌ای از حقوق بشر، هنوز برخی از کشورها مانند ایران قانونی مستقل در این خصوص ندارند. البته در قوانین و مقررات ایران می‌توان مواد مختلفی را یافت که به مناسبت به حمایت از داده‌های شخصی اشاره نموده‌اند. این مواد که به طور کلی در خصوص حمایت از داده‌های شخصی است و به به جزئیات چنین حمایتی و حفاظت‌های تفصیلی - مانند الزامات مربوط به انتقال بین المللی داده های شخصی- نپرداخته است، شامل اصل ۲۴ و ۲۵ قانون اساسی مصوب ۱۳۵۸، مواد ۵۸، ۵۹ و ۷۱ قانون تجارت الکترونیکی مصوب ۱۳۸۲، مواد ۱۴ و ۱۵ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷، مواد ۱، ۳، ۴، ۸، ۱۲ و ۱۷ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ ، ماده ۴۰ ، ۹۶، ۹۷، ۱۰۱ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ با اصلاحات ۱۳۹۴، مواد ۶۵۳ و ۶۵۶ و ۶۵۸ و ۶۶۰ قانون جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ است. البته در حقوق موضوعه ایران، حفاظت از داده‌ی شخصی و حریم خصوصی دو اصطلاح مترادف هستند و به‌جای هم به کار می‌روند (برخلاف حقوق اتحادیه اروپا) لذا در قوانین و مقرراتی که برای حمایت از داده‌های شخصی قابل استناد است، اصطلاح حریم خصوصی یا حریم خصوصی اطلاعاتی نیز در خصوص حمایت از داده‌های شخصی به‌کاررفته است.

استناد به مواد پیش‌گفته در برخی موارد مفید است؛ لیکن این اشارات جزئی در خصوص این مهم کافی نیست و خلأ وجود قانونی خاص نسبت به داده‌های شخصی در حقوق ایران هم چنان احساس می‌شود. بدین جهت در این خصوص تلاش هایی صورت گرفته است، یکی از این موارد پیش‌نویس لایحه‌ی «صیانت و حفاظت از داده‌های شخصی» است که در تیرماه سال ۱۳۹۷ در سایت سازمان فناوری اطلاعات ایران منتشر شده است [۱] و دیگری نیز طرح «حمایت و حفاظت از داده و اطلاعات شخصی» است که در شهریورماه ۱۴۰۰ در صحن علنی مجلس اعلام وصول‌شده است [۲]. گرچه توجه قانون‌گذار به حمایت از داده‌های شخصی در قالب این اسناد گامی مثبت است، خصوصاً این‌که در آن‌ها سعی شده است با توجه به الزامات مقررات اروپایی حفاظت از داده، حمایت‌های مختلفی نسبت به داده‌های شخصی موردتوجه قرار گیرد ولی - فارغ از وضعیت قانونی این اسناد - آن‌ها با اشکالات و ابهامات مختلفی مواجه هستند[۳]. بدین‌جهت استناد

[۱] لینک دسترسی به پیش‌نویس
https://www.ict.gov.ir/fa/newsagency/21691/%D9%84%D8%A7%DB%8C%D8%AD%D9%87-%D8%B5%DB%8C%D8%A7%D9%86%D8%AA-%D9%88-%D8%AD%D9%81%D8%A7%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87-%D9%87%D8%A7%DB%8C-%D8%B4%D8%AE%D8%B5%DB%8C-%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C-%D8%B4%D8%AF

[۲] لینک دسترسی به طرح
https://dotic.ir/news/10419

[۳] گفتنی است که سند «صیانت و حفاظت از داده‌های شخصی» صرفا پیش نویس است و تاکنون حتی نسخه نهایی برای این پیش‌نویس منتشرنشده است، البته به نظر می‌رسد با ارائه‌ی طرح «حمایت و حفاظت از داده و اطلاعات شخصی» که در بیست و چهارم شهریورماه ۱۴۰۰ در صحن علنی مجلس اعلام وصول‌شده است، پیش‌نویس مذکور در همین مرحله رهاشده باشد. خصوصاً اینکه طرح مذکور گزیده‌ای از پیش‌نویس سابق است. درواقع این طرح که با چند سال فاصله از ارائه‌ی پیش‌نویس، در خصوص حمایت از داده‌ی شخصی و اشخاص موضوع داده، مورد توجه قرار گرفته است؛ در محتوا نسبت به مواد استفاده‌شده از پیش‌نویس، تغییری نکرده است و با عدم شفافیت و فقدان افزایش حمایت از داده‌ی شخصی و اشخاص موضوع داده، با همان کیفیتِ مقرر در پیش‌نویس، به حمایت از داده‌های شخصی و اشخاص موضوع داده، پرداخته است.

به آن‌ها برای تبیین چگونگی حمایت از داده‌های شخصی به‌طورکلی و الزامات مربوط به انتقال بین‌المللی داده‌های شخصی به‌طور جزئی - موضوع پژوهش حاضر- از قوت کافی برخوردار نیست.

البته در اسناد مذکور، اشارات مرتبطی نسبت به انتقال بین‌المللی داده‌های شخصی وجود دارد که بیان آن‌ها مفید به نظر می‌رسد. توضیح این‌که مواد ۳۷ و ۳۸ پیش‌نویس (مواد ۴۳ و ۴۴ طرح) به پردازش فرامرزی داده‌های شخصی اشاره نموده‌اند. به‌موجب مواد پیش‌گفته «در موارد ذیل، پردازش داده‌های شخصی، فرامرزی انگاشته می‌شود: الف) هریک از کنترل‌گران یا پردازشگران تابعیت خارجی داشته باشند؛ ب) سامانه‌های پردازنده داده‌ها در بیرون از قلمرو حاکمیتی جمهوری اسلامی ایران قرار داشته باشد؛ پ) پردازنده‌های نرم‌افزاری در ایران ثبت‌نشده باشد (بند پ صرفاً در طرح بیان‌شده است) همچنین بیان‌شده است «در خصوص پردازش داده‌های شخصی اتباع ایرانی، رعایت شرایط ذیل الزامی است: الف) تنها در مراکز داده واقع در قلمرو حاکمیتی جمهوری اسلامی ایران یا مراکز داده خارجی مورد تأیید مراجع صلاحیت‌دار ذخیره شوند؛ ب) همه پردازنده‌های سخت‌افزاری و نرم‌افزاری از گواهی مراجع صلاحیت‌دار ذی‌ربط برخوردار باشند؛ پ) بر روی شبکه ارتباطی مطمئن جابه‌جا شوند؛ ت) صلاحیت کنترل‌گران و پردازشگران خارجی مورد تأیید مراجع ذی‌ربط قرارگرفته باشد؛ ث) پردازش‌های فرامرزی بر پایه ضوابط مقرر به ثبت برسد». به نظر می‌رسد این مواد به‌غایت خود در خصوص پردازش فرامرزی یا به‌عبارت‌دیگر پردازش بین‌المللی داده‌های شخصی، مبنی بر حمایت کامل از حریم خصوصی اطلاعاتی افراد و داده‌های شخصی نرسیده‌اند. این امر بدین دلیل است که در این مواد صرفاً پردازش فرامرزی تعریف‌شده است و الزامات مربوط به چنین پردازشی و ابزارهای لازم در جهت تحقق این الزامات موردتوجه قرار نگرفته است. به‌علاوه آنچه در این مواد نیز بیان گردیده است، دارای اشکال می‌باشد. به‌عنوان نمونه به‌موجب بند الف ماده ۳۷ پیش‌نویس (۴۳ طرح) اگر «اشخاص پردازش کننده داده تابعیت خارجی داشته باشند این پردازش فرامرزی است» درحالی‌که به نظر می‌رسد این بند مناسب نباشد؛ چراکه ممکن است فردی خارجی مقیم ایران باشد و پردازش در داخل مرزهای ایران رخ دهد، در این صورت بر خارجی بودن شخص پردازش کننده داده چه اثری مترتب است که لازم است، پردازش فرامرزی تلقی شود و چه حمایت ویژه‌ای در مورد این پردازش وجود دارد. همین امر در مورد بند پ نیز که صرفاً در طرح بیان‌شده است نیز وجود دارد.

همچنین می‌توان بر ماده ۳۸ پیش‌نویس (۴۴ طرح) بحث نمود که در آن صرفاً الزامات پردازش فرامرزی منوط به اتباع ایرانی شده است؛ درحالی‌که با توجه به ماده ۳ پیش‌نویس و طرح ایرانی که دامنه‌ی شمول را بیان می‌کند و تصریح بند ب این ماده «اتباع خارجی حقیقی یا حقوقی عمومی یا خصوصی که داده‌های شخصی آن‌ها از سوی کنترل‌گر یا پردازشگر ایرانی پردازش می‌شود» نیز در دامنه‌ی شمول این اسناد هستند. حال سؤال اینجاست که به چه دلیل در ماده ۳۸ پیش‌نویس (۴۴ طرح) در خصوص پردازش فرامرزی، صرفاً اتباع ایرانی موردحمایت ویژه قرارگرفته‌اند و الزاماتی برای چنین پردازشی در نظر گرفته‌شده است. به نظر می‌رسد اشکال اساسی در ماده ۳ پیش‌نویس و طرح است که متضمن دامنه‌ی شمول اسناد مذکور است. فارغ از نقدهای دیگری که بر ماده ۳ وارد است، به‌موجب بند ب از اشخاص موضوع داده دارای تابعیت خارجی حمایت‌شده است. با لحاظ بند ب ماده ۳ به همین صورت، در فرضی که پردازنده ایرانی در یک کشور دیگر، داده‌های شخصی یک شخص موضوع داده فرانسوی را پردازش می‌کند (که در خصوص فرد فرانسوی GDPR جاری است)، با چه مبنای حقوقی، قانون ایرانی باید قابل جریان باشد. پس به نظر می‌رسد ماده ۳ این اسناد باید مورد

بازبینی قرار گیرد تا بالتبع ماده ۳۸ پیش‌نویس (۴۴ طرح) با اشکال مبنایی کمتری مواجه باشد [۱].

فارغ از این اشکال، در بند الف ماده ۳۸ پیش‌نویس (۴۴ طرح) بیان‌شده است که پردازش فرامرزی باید «تنها در مراکز داده واقع در قلمرو حاکمیتی جمهوری اسلامی ایران یا مراکز داده خارجی مورد تأیید مراجع صلاحیت‌دار ذخیره شوند». درحالی‌که اگر داده‌های شخصی در مرکز داده واقع در ایران پردازش شوند، چنین پردازشی، فرامرزی نیست که ضرورت رعایت الزامات خاص وجود داشته باشد. هم‌چنین بندهای دیگر مذکور در این ماده نیز خالی از اشکال نیست. به‌عنوان نمونه ادامه بند الف که بیان می‌کند پردازش فرامرزی باید در «مراکز داده خارجی مورد تأیید مراجع صلاحیت‌دار ذخیره شوند» با بند ب که بیان می‌کند «همه پردازنده‌های سخت‌افزاری و نرم‌افزاری از گواهی مراجع صلاحیت‌دار ذی‌ربط برخوردار باشند» و بند ت که بیان می‌کند «صلاحیت کنترل‌گران و پردازشگران خارجی مورد تأیید مراجع ذی‌ربط قرارگرفته باشد» بسیار مشابه است و علت اینکه در بندهای مختلف بیان‌شده‌اند، مشخص نیست. درواقع تمامی این بندها مبین است که صلاحیت اشخاص پردازش کننده داده اعم از ابزارهای مورداستفاده، چگونگی پردازش توسط آن‌ها و... مورد تائید مراجع ذی‌صلاح ایران باشد - این امر می‌تواند مشابه با تصمیم‌گیری کفایت اتحادیه اروپا تلقی شود- بدین‌جهت دلیلی بر بیان در بندهای جداگانه نیست. به‌علاوه بند ث که بیان می‌کند «پردازش‌های فرامرزی بر پایه ضوابط مقرر به ثبت برسد» مشعر به کدام ضوابط است درحالی‌که باید بر الزامات تصریح شود. درنهایت بند پ که «جابه‌جایی بر روی شبکه ارتباطی مطمئن» را از الزامات پردازش فرامرزی می‌داند، درواقع تعهد اشخاص پردازش کننده داده در هر نوعی از پردازش است و ارتباط خاصی به پردازش فرامرزی ندارد و به‌عنوان حمایتی ویژه در این خصوص قابل‌بیان نیست.

فارغ از پیش‌نویس و طرح ایرانی و با توجه به فقدان قانون در خصوص حمایت از داده‌ی شخصی، هم‌چنین عدم اشاره قوانین و مقررات ایران نسبت به موضوع پژوهش حاضر، این امر باید در دکترین حقوقی و مبانی حقوق ایران جستجو شود. گرچه در این خصوص نیز در منابع مذکور، صراحتی وجود ندارد تا بتوان به‌طورقطع حمایت‌های خاصی را به حقوق ایران نسبت داد؛ لیکن به نظر می‌رسد با تمسک به این منابع می‌توان برخی از الزامات مربوطه به‌خصوص موقعیت‌های ماده ۴۹ GDPR را در حقوق ایران نیز جاری دانست.

توضیح این‌که با توجه به ماهیت داده‌های شخصی که دارای ابعاد مالی است، شخص موضوع داده مالک داده‌های شخصی است و توانایی هرگونه تصرفی را دارد [۲]. چنین تصرفی می‌تواند انتقال

---

[۱] به عنوان پیشنهاد می توان ماده ۳ پیش نویس و طرح بدین صورت اصلاح نمود:
دامنه‌ی مشمول این قانون عبارت‌اند از: الف) اشخاص موضوع داده‌ای که داده‌های شخصی‌شان در زمینه‌ی فعالیت‌های کنترل‌کننده یا پردازنده‌ی مستقر (دارای مقر) در ایران انجام می‌شود، اعم از آنکه داده‌های شخصی آن‌ها درون یا بیرون از ایران پردازش شوند (معیار مقر). ب) هم‌چنین این قانون برای پردازش داده‌ی شخصیِ اشخاص موضوع داده‌ای که در ایران هستند و پردازش داده‌هایشان توسط کنترل‌کننده یا پردازنده‌ای که در ایران مستقر نشده‌اند، انجام می‌شود، نیز اعمال می‌شود؛ درصورتی‌که فعالیت‌های پردازش، مربوط به ارائه کالا یا خدمات به اشخاص موضوع داده در ایران یا نظارت بر رفتار اشخاص موضوع داده در ایران باشد و مشروط به اینکه چنین ارائه کالا و خدمات یا نظارتی، هدفمند باشد (معیار هدف). ج) این قانون برای پردازش داده‌های شخصی، توسط کنترل‌کننده‌ای که در ایران مستقر نشده است، اما در محلی واقع‌شده است که قانون ایران، به‌موجب حقوق بین‌الملل عمومی اعمال می‌شود؛ نیز کاربرد دارد».

[۲] با توجه به این که عرف در تعیین مصادیق مال نقشی برجسته‌ای دارد و به دلیل پیشرفت فناوری اطلاعات و تغییر جامعه، به‌طور منطقی باید مصادیق مال روزبه‌روز گسترده‌تر شوند؛ به‌عنوان نمونه ازنظر برخی از فقها (فاضل لنکرانی، ۱۳۹۶: ۲/ ۳۲۹) امروزه کسی در مال بودن حق بهره‌برداری از آثار ادبی و هنری، اختراع و مصادیق مختلف مالکیت‌های معنوی شکی ندارد، چراکه «مال» در تعریف عقلا، امری اعتباری است و عینیت در آن دخالتی ندارد و شامل منافع اعیان نیز می‌شود، بنابراین

داده‌های شخصی باشد؛ بنابراین وجود رضایت صریح شخص موضوع داده می‌تواند مجوزی برای انتقال داده‌های شخصی باشد.

همچنین ضرورت قراردادی نیز می‌تواند به‌عنوان دلیلی برای مشروعیت انتقال داده‌های شخصی بر اساس نظام حقوق ایران محسوب شود. چنین امری با قاعده‌ی «اذن در شی، اذن در لوازم آن است» - الإذنُ فِی الشیء إذنٌ فِی لَوازِمه (توابعه)- قابل تطبیق است. به‌موجب این قاعده که مورد تصریح فقها قرارگرفته است (ر.ک محقق کرکی، ۱۴۱۴ ق، ۶/ ۱۰؛ صافی، ۱۳۸۱: ۱/ ۲۲۳؛ طباطبایی یزدی، ۱۴۲۱ ق، ۴/ ۳۵۸؛ حکیم، ۱۳۷۴: ۱۴/ ۲۹۶؛ نجفی، ۱۴۲۱ ق، ۱۳/ ۷۰) اگر کسی به دیگری نسبت به امری اذن دهد، گستره‌ی اذن، به آنچه مورد تصریح اذن دهنده قرارگرفته، محدود نمی‌شود؛ بلکه لوازم و توابع آن را نیز در برمی‌گیرد (هاشمی شاهرودی، ۱۳۸۲ ق: ۶/ ۵۹). چنین لوازم و توابعی شامل لوازم ذاتی و عقلی، عرفی و قانونی مورد اذن است (محقق داماد، ۱۳۸۴: ۲۳۶ و ۲۳۷). در بحث حاضر نیز زمانی که شخص موضوع داده، طرف قرارداد است و انعقاد قرارداد یا انجام تعهد قراردادی مستلزم انتقال داده‌های شخصیِ شخص موضوع داده است؛ به‌موجب این قاعده، رضایت شخص موضوع داده نسبت به قرارداد، رضایت به انتقال داده‌های شخصی است که جهت انعقاد قرارداد یا انجام تعهد قراردادی ضروری است. در حقیقت انتقال داده‌های شخصی شخص موضوع داده از لوازم عقلی و عرفی قرارداد است که به‌تبع قرارداد ضرورت می‌یابد. بدین‌جهت در نظام حقوقی ایران نیز ضرورت قراردادی به‌عنوان مجوزی برای انتقال بین‌المللی داده‌های شخصی بر اساس قاعده‌ی مذکور و بر اساس مبنای قراردادی موردپذیرش است.

علاوه بر این، وجود منافع حیاتی و منافع عمومی نیز به‌موجب نظام حقوق ایران می‌تواند مبنایی برای انتقال تلقی شود. دلیل این است که حفاظت از منافع حیاتی افراد به معنی حفاظت از جان شخص موضوع داده و افراد دیگر است. اهمیت حفظ جان در فقه، حقوق و قوانین موضوعه ایران مورد تصریح قرارگرفته است. به‌موجب فقه امامیه حفظ جانِ خود و افراد دیگر، واجب است و در معرض هلاکت قرار دادن آن و همچنین تعرض به جان انسانِ محترم، حرام است (هاشمی شاهرودی، ۱۳۸۲ ق: ۳/ ۳۱۶؛ مکارم شیرازی، ۱۳۸۵: ۱/ ۴۸۴) حتی برای حفظ جان ارتکاب به بعضی از محرمات جایز می‌شود (مدرسی، ۱۳۹۳: ۱۶۹). از قوانین موضوعه ایران نیز این امر قابل استنباط است. به‌عنوان نمونه به‌موجب ماده ۱۵۸ قانون مجازات اسلامی مصوب ۱۳۹۲ «ارتکاب رفتاری که طبق قانون جرم محسوب می‌شود، درصورتی‌که ارتکاب رفتار برای اجرای قانون اهم لازم باشد، قابل مجازات نیست» به‌موجب این ماده درصورتی‌که امری اهم وجود داشته باشد، لطمه به منافع افراد قابل مجازات نیست. در نظریات دکترین مصادیق این ماده علاوه بر سایر موارد، تخریب اموال و اشیاء برای نجات جان، سلب آزادی برای نجات جان و ورود با قهر و غلبه به ملک دیگری برای نجات جان بیان‌شده است (گلدوزیان، ۱۳۹۷:

برخی حقوق مانند حق بهره‌برداری از آثار ادبی و هنری مطابق سیرهٔ عقلا مشمول مصادیق مال است. داده‌ی شخصی نیز با توجه به نظر عرف ویژگی های اصلی مال را دارد؛ چراکه مفید بودن و ارزش اقتصادی در خصوص داده‌های شخصی وجود دارد و حتی داده‌های شخصی افراد عادی نیز ارزشمند هستند و چنین داده‌هایی ارزش اقتصادی به دنبال دارند (Singh, 2016: 138). به‌عنوان‌مثال بسیاری از کسب‌وکارهای نوآورانه موفق، مانند شبکه‌های اجتماعی، موتورهای جستجو، شرکت‌های تبلیغاتی با داده‌های شخصی پیشرفت می‌کنند و موفقیت آن‌ها غالباً با مقدار داده‌های موجود برای آن‌ها تعیین می‌شود (Purtova, 2015: 5) به دلیل همین ارزشمندی، بخش عمومی و خصوصی داده‌های شخصی را جمع‌آوری و پردازش می‌کنند. به‌علاوه داده‌های شخصی قابلیت اختصاص به شخص معین را نیز دارند؛ بنابراین عرف امروز در مال بودن داده‌های شخصی تردیدی ندارد. با مال بودن داده‌ی شخصی تمامی مبانی و حمایت‌هایی که به جهت محترم بودن اموال وجود دارند، در خصوص داده‌های شخصی نیز قابل پذیرش هستند. همچنین بسیاری از قواعد فقهی مانند قاعده‌ی محترم بودن مال غیر، قاعده ی تسلیط و... قابلیت جریان بر داده‌های شخصی را دارند.

۲۳۵-۲۳۷). منافع عمومی یا مصالح عامه نیز از منظر فقه امامیه، قوانین موضوعه ایران و دکترین حقوقی، بر منافع خاصه یا مصالح فردی مقدم‌اند. مبنای چنین تقدمی نیز رعایت صلاح عموم مردم و توجه به احوال کلی آنان است؛ چراکه منافع عمومی، مصالحی است که نفع آن ناظر به جمع زیادی از مردم است (ایازی، ۱۳۸۹: ۳۴۹ و ۳۶۰). بدین ترتیب حفظ منافع حیاتی و منافع عمومی بر حق افراد نسبت به داده‌هایشان اولویت‌دارند. چنین تقدمی مقتضای نظم عمومی و عدالت است (ر.ک. عمید زنجانی، ۱۳۹۱: ۱۷۹) و از موجبات انتقال بین‌المللی داده‌های شخصی است.

همچنین برای بررسی غلبه منافع مشروع کنترل‌کننده به‌عنوان مجوزی برای انتقال بین‌المللی داده‌های شخصی می‌توان به تعارض منافع فردی بین اشخاص خصوصی توجه نمود. در حقوق ایران نمونه‌های مختلفی برای چنین تعارضی بیان‌شده است. از میان این موارد، به نظر می‌رسد تعارض منافع شخص موضوع داده با منافع کنترل‌کننده، می‌تواند مصداقی از تعارض منافع ناشی از اعتماد به امانت‌داری باشد که مربوط به نمایندگی است و عمدتاً ذیل عنوان «بحران نمایندگی» قابل‌بررسی است (بادینی و سیاه بیدی کرمانشاهی، ۱۴۰۰: ۲۲۱). در جهت رفع این تعارض باید بررسی شود که آیا منفعت کنترل‌کننده از لوازم و توابع حق او در خصوص انتقال است. در صورت وجود این امر، چنین منفعتی مشروع است؛ لیکن مشروعیت منافع کفایت نمی‌کند، بلکه باید در تقابلِ منافع کنترل‌کننده با شخص موضوع داده، منافع کنترل‌کننده غالب نیز باشد. بدین‌جهت باید غلبه منافع نیز با جریان قاعده‌ی «تقدیم اهم بر مهم» روشن شود (ر.ک. مکارم شیرازی، ۱۳۸۵: ۱/ ۲۲۱). ازآنجایی‌که معیار تشخیص اهم حکم عقل است و به‌حکم عقل اهم بر مهم مقدم است (منتظری، ۱۳۶۷: ۸/ ۳۰۲) اگر عرف عقلا منافع کنترل‌کننده را اهم بدانند، چنین منافعی مقدم است و از موجبات انتقال بین‌المللی داده‌های شخصی است.

درنهایت نیز اشاره به این نکته مفید است که با توجه به عدم تصریح منابع مختلف حقوق ایران در خصوص الزامات مربوط به انتقال بین‌المللی داده‌های شخصی، به نظر می‌رسد بتوان در این خصوص از حقوق فناوری اطلاعات و مباحث مربوط به انتقال فناوری نیز بهره جست. چراکه فناوری در ماهیت خود به داده‌ی شخصی شباهت دارد. توضیح این‌که در آثار فناورانه گرچه وجود جنبه‌های مالی صاحب فناوری وجود دارد؛ لیکن به اعتبار پیوند مستحکم جنبه‌های معنوی این آثار به صاحب آن، اصولاً توجه و حمایت از جنبه‌های معنوی حقوق صاحبان آثار مذکور انکارناپذیر است (ماندگار، ۱۳۹۳: ۱۲۲و ۱۲۳) (این امر مشابه با ماهیت دو جنبه‌ای داده شخصی است که مرکب از بعد مالی و معنوی است). این ماهیت خاص در انتقال فناوری نیز اثرگذار است. در حقیقت انتقال اساساً متوجه انتقال قابلیت‌ها و توانایی‌های انتقال‌دهنده نیز می‌باشد (احسنی فروز، ۱۳۹۲: ۹۵). با توجه به شباهت در ماهیت و انتقال فناوری به ماهیت و انتقال داده‌های شخصی می‌توان از منابع مربوطه خصوصاً قوانین و مقررات مرتبط استفاده نمود.

۳ نتیجه‌گیری

حمایت مؤثر از داده‌های شخصی زمانی محقق می‌شود که حقوق اشخاص موضوع داده در شرایط مختلف رعایت شوند و حق بر داده آن‌ها مورد تعرض قرار نگیرد. این امر ازجمله در زمانی است که داده‌های شخصی قبل از پردازش یا در مسیر پردازش به کشورهای دیگر یا سازمان‌های بین‌المللی منتقل می‌شوند. مقررات اروپایی حفاظت از داده‌های شخصی، حمایت از اشخاص موضوع داده را در صورت انتقال بین‌المللی داده‌های شخصی نیز موردتوجه قرار داده است و در این خصوص الزامات مختلفی را مقرر کرده است. به دیگر سخن به‌موجب این مقررات، صرفاً با وجود ابزارهایی خاص، انتقال بین‌المللی داده‌های شخصی مجاز است. این موارد ازجمله وجود سطح کافی حفاظت از داده (تصمیم کفایت) است که موجب امن شدن کشور ثالث

می‌باشد. هم‌چنین شروط قراردادی استاندارد از ابزارهایی است که باوجودآن، انتقال بین‌المللی داده بلامانع است. در این موارد متعاقدین (منتقل‌کننده داده در اتحادیه اروپا و دریافت‌کننده داده در خارج از اتحادیه اروپا) ملزم به قراردادی مبتنی بر شروط قراردادی استاندارد هستند تا سطح مناسب حفاظت از داده برای انتقال داده فراهم شود. ابزار دیگر، جریان قواعد الزامی شرکتی است که متضمن سطح مناسب حفاظت از داده در شرکت‌های چندملیتیِ گروه تعهدات (سازمان تجاری) یا گروهی از شرکت‌های درگیر در فعالیت اقتصادی مشترک است. هم‌چنین پایبندی به منشورهای رفتاری یا گواهی‌نامه‌ها نیز می‌تواند از موجبات انتقال بین‌المللی داده‌های شخصی تلقی شود. فارغ از این موارد، وجود موقعیت‌های ویژه مقرر در ماده ۴۹ GDPR نیز می‌تواند مجوزی برای انتقال بین‌المللی داده‌های شخصی باشد. این موارد رضایت شخص موضوع داده، ضرورت قراردادی، وجود منافع حیاتی و منافع عمومی و هم‌چنین غلبه منافع مشروع کنترل‌کننده است. از میان الزامات مقرر در GDPR برای انتقال بین‌المللی داده‌ها، صرفاً موقعیت‌های ویژه ماده ۴۹ GDPR از مسیر دکترین حقوقی، مبانی حقوقی ایران و سایر قوانین و مقررات - که برای داده‌های شخصی وضع نشده‌اند- به‌عنوان الزامات انتقال در حقوق ایران پذیرفتنی است. دلیل این حمایت محدود، فقدان قانون مستقل برای حمایت از داده‌های شخصی و ابهام و اشکالات مختلف اسناد موجود - پیش‌نویس لایحه‌ی صیانت و حفاظت از داده‌های شخصی و طرح حمایت و حفاظت از داده و اطلاعات شخصی – است. بدین‌جهت تسریع در تصویب قانونی خاص نسبت به حمایت از داده‌های شخصی و توجه به ابعاد مختلف چنین حمایتی ازجمله چگونگی انتقال بین‌المللی داده‌های شخصی ضروری است. پیشنهادهای مختلف این پژوهش برای اصلاح و تقویت اسناد موجود و چگونگی حمایت از داده‌های شخصی در موضوع حاضر، می‌تواند قانون‌گذار را یاری نماید.

References

Afrasyab, Mahboob. and Naser, Mehdi. (2020). Legal frameworks for maintaining the security of private data processing (A comparative study of Iranian and EU law). Islamic Law, 17(66), pp. 209-232. (In Persian)

Aghaei Togh, Muslim and Nasser, Mehdi. (2016). Challenges of Private Data Protection in the Field of IoT: A Comparative Study of Iranian and EU Law, Journal of Administrative Law, 7 (23), pp. 33-55. (In Persian)

Ahsani Forouz, Mohammad. (2013). Technology Transfer Law. Tehran, Dadgostar Publishing. (In Persian)

Amid Zanjani, Abbas Ali .(2012). General Rules of Contracts in the Book of Al-Baya Val-Motaajer. Tehran, Khorsandi Publishing. (In Arabic)

Aslani, Hamidreza. (2005). Information Technology Law. Tehran, Mizan. (In Persian)

Ayazi, Mohammad Ali .(2010). Criteria of Rulings and Methods of Its Exploration. Qom, Qom Seminary Islamic Propaganda Office. (In Persian)

Badini, Hassan, and Saeed Siahbidi Kermanshahi. (2020). Analysis of the concept and examples of conflict of interest in private law. The Judiciarys Law Journal, 85 (116), pp. 209-231 .(In Persian)

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. Information and Communications Technology Law, 26(3), 213–228.

Colcelli, V. (2019). Joint Controller Agreement Under GDPR. Eu and Member States – Legal and Economic Issues, 3, 1030–1047.

Council of Europe. (1950). European Convention on Human Rights. In Vertical Judicial Dialogues in Asylum Cases. https://www.echr.coe.int/Documents/Convention_ENG.pdf

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. (2012). Charter Of Fundamental Rights Of The European Union (2012/C 326/02). Official Journal of the European Union, 391–407. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

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

European Commission. (2018a). Binding Corporate Rules (BCR). https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-

protection/binding-corporate-rules-bcr_en

European Commission. (2018b). Standard Contractual Clauses (SCC). https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

European Commission. (2018c). What does data protection 'by design' and 'by default' mean? | European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

European Commission. (2018d). What is a data controller or a data processor? | European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

European Commission. (2018e). What rules apply if my organisation transfers data outside the EU? | European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en

European Commission. (2019). Adequacy decisions | European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Data Protection Supervisor. (n.d.). Data Protection. Retrieved June 17, 2020, from https://edps.europa.eu/data-protection/data-protection_en

Fazel Lankarani, Mohammad Javad. (2017). Makaseb Muharama. Qom, Jurisprudential Center of the Imams (PBUH). (In Persian)

Ferrara, P., & Spoto, F. (2018). Static analysis for GDPR compliance. CEUR Workshop Proceedings, 2058, 1–10.

Goldozian, Iraj. (2018). General Criminal Law. Tehran, University of Tehran Press. (In Persian)

Hakim, Seyyed Mohsen. (1995). Al-Urwa Al-Wathqi, Qom, Dar al-Tafsir. (In Arabic)

Hashemi Shahroudi, Mahmoud.(2003). The culture of jurisprudence according to the religion of the Ahl al-Bayt Pbuh, Qom, Encyclopedia of Islamic jurisprudence on the religion of the Ahl al-Bayt (PBUH). (In Persian)

ICO. (2018). Codes of conduct. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/

Karroubi, Mohammad Taghi. (2005). The European Union and the discussion of the protection of personal data and privacy in electronic communications. Tehran, Baqa. (In Persian)

Makarem Shirazi, Nasser. (2006). Encyclopedia of Contemporary Jurisprudence. Qom, Imam Ali Ibn Abi Talib School (PBUH). (In Persian)

Mandegar, Mostafa. (2014). International Trade Agreements for Technology Transfer. Tehran, Shahr-e Danesh. (In Persian)

Modarressi, Mohammad Reza. Al-Bayaa. (2014). Qom, Dar al-Tafsir. (In Arabic)

Mohaqeq Damad, Seyed Mostafa. (2005). Rules of Jurisprudence (Civil Section Property Law and Responsibility). Tehran, Islamic Sciences Publishing Center. (In Persian)

Mohaqeq Karki, Ali Ibn Hussein. (1994). Jame Al-Maqassid Fi Sharh Al-Qawaed. Qom, Ahl al-Bayt Institute (PBUH). (In Arabic)

Montazeri, Hossein Ali (1988), the jurisprudential principles of the Islamic government (Derasat Fi Velayat Al- Faqih Va Fiqh Al-Dolat Al-Islami: Studies in the Juris Consult Leader and Jurisprudence of the Islamic Government), Qom, Keyhan Publishing. (In Persian)

Najafi, Mohammad Hassan. (2001). Jawahar al-Kalam. Qom, Institute of the Encyclopedia of Islamic Jurisprudence on the religion of the Ahl al-Bayt (PBUH). (In Arabic)

Nouri, Mohammad Ali and Nakhjavani, Reza. (2005). Data Protection Law. Tehran, ktabkhaneh ganj dansh. (In Persian)

Personal Data Protection and Safeguarding Draft Act in July 2018, Published on the website of the Ministry of Communications and Information Technology of Iran. (In Persian)

Practical Law. (n.d.). Certification mechanism. Retrieved March 11, 2020, from https://uk.practicallaw.thomsonreuters.com/w-014-8170?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

Purtova, N. (2015). The illusion of personal data as no one's property. Law, Innovation and Technology, 7(1), 1–29.

Raisi, Leila, and Liyasi Flore Ghassemzadeh. (2020). The challenges of the Iranian legal system in violating the personal data and privacy in cyber space. The Judiciarys Law Journal. 84 (110), pp. 119-142. (In Persian)

Safi, Lotfallah. (2002). Fiqh al-Hajj. Qom, Hazrat Masoumeh Publishing (PBUH). (In Arabic)

Segovia Domingo, A. I., & Desmet Villar, N. (2018). Self-regulation in data protection. BBVA Research, October 2018, 1–4.

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

Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to

United Nations. (2015). Universal Declaration of Human Rights (pp. 1–62). https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf

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

cross border data transfers and protection of personal data in the IoT era. Computer Law and Security Review, 35(4), 380–397.

Support and protection of personal data and information Draft Act in September 2021. (In Persian)

Tabatabai Yazdi, Mohammad Kazem. (2001). Al-Urwa Al-Wathqi, Qom, Islamic Publishing Institute. (In Arabic)