Analysis of the Legal Framework for the Protection of Personal Data in the European Union

Mahdieh Latifzadeh
PhD Candidate in Private Law; Ferdowsi University of Mashhad; Mashhad, Iran Email: m.latifzadeh@mail.um.ac.ir

Sayyed Mohammad Mahdi Qabuli Dorafshan*
PhD in Private Law; Associate Professor; Ferdowsi University of Mashhad; Mashhad, Iran Email: ghaboli@um.ac.ir

Saeed Mohseni
PhD in Private Law; Associate Professor; Ferdowsi University of Mashhad; Mashhad, Iran Email: s-mohseni@um.ac.ir

Mohammed Abedi
PhD in Private Law; Assistant Professor; Ferdowsi University of Mashhad; Mashhad, Iran Email: dr.m.abedi@um.ac.ir

Iranian Journal of Information Processing and Management

Received: 20, Aug. 2020 **Accepted: 15, May 2021**

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 37 | No. 2 | pp. 439-472
Winter 2022

Abstract: Personal data is of great economic importance, which is called the currency of the future, but the environment in which people live and work with it constantly, collect and process personal data and use it in a variety of ways. Therefore, there is a need for laws that protect this valuable thing. The most important legal framework for the protection of personal data is the General Data Protection Regulation (GDPR). This regulation was approved in 2016 and came into force in 2018, and is currently the most comprehensive framework for the protection of personal data. However, in previous years the EU has enacted legislation on the protection of personal data (Personal Data Protection Directive 1995), but this regulation is the most complete legal framework for data protection due to its innovative features and protections. Due to the importance of this regulation in the protection of personal data, it is necessary to introduce this legal framework and express the basic concepts, scope of application and strengths of this regulation in order to better understand the protections contained in the GDPR. The present article, by searching this regulation and related sources, states this and takes steps to clarify this regulation to help formulate an appropriate legal framework regarding the protection of personal data in the Iranian legal system.

Keywords: GDPR, Personal Data, Processing, Controller, Processor

* Corresponding Author

تحلیل بستر قانونی حمایت از دادهٔ شخصی در اتحادیهٔ اروپا[1]

مهدیه لطیف‌زاده | دانشجوی دکتری حقوق خصوصی؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛ m.latifzadeh@mail.um.ac.ir

سید محمدمهدی قبولی درافشان | دکتری حقوق خصوصی؛ دانشیار؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛ پدیدآور رابط ghaboli@um.ac.ir

سعید محسنی | دکتری حقوق خصوصی؛ دانشیار؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛ s-mohseni@um.ac.ir

محمد عابدی | دکتری حقوق خصوصی؛ استادیار؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛ dr.m.abedi@um.ac.ir

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۳۹۹/۰۵/۳۰ | پذیرش: ۱۴۰۰/۰۲/۲۵ | مقاله برای اصلاح به مدت ۲۵ روز نزد پدیدآوران بوده است.

چکیده: داده‌های شخصی اهمیت اقتصادی فراوانی دارند، به‌طوری‌که آن‌ها را پول آینده نامیده‌اند. در عین حال، محیط‌هایی که اشخاص در آن‌ها زندگی می‌کنند و به‌طور مداوم با آن‌ها سروکار دارند، داده‌های اشخاص را جمع‌آوری و پردازش کرده و به شیوه‌های مختلف از داده‌ها استفاده می‌کنند. بنابراین، ضرورت وجود قوانینی که از این امر ارزشمند در مقابل استفاده‌های فراوان حفاظت کند، احساس می‌شود. مهم‌ترین بستر قانونی برای حمایت از دادهٔ شخصی، مقررات عمومی حفاظت از داده (GDPR) است. این مقررات در سال ۲۰۱۶ توسط پارلمان و شورای اروپا تصویب و از سال ۲۰۱۸ در تمامی کشورهای عضو اتحادیهٔ اروپا لازم‌الاجرا شده است و به‌دلیل ویژگی‌ها و حمایت‌های بدیع و دقیق خود، جامع‌ترین بستر قانونی در خصوص حمایت از داده است. به جهت اهمیت GDPR در خصوص حفاظت از داده‌های شخصی، معرفی این بستر قانونی، پرداختن به مفاهیم اساسی، دامنهٔ اعمال و بیان نقاط قوت این مقررات به‌منظور درک بهتر حمایت‌های مندرج در GDPR ضروری است. پژوهش حاضر با

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۷ | شمارهٔ ۲ | ص‌ص ۴۳۹-۴۷۲
زمستان ۱۴۰۰

۱. این پژوهش تحت حمایت مادی صندوق حمایت از پژوهشگران و فناوران کشور (INSF) برگرفته از طرح شماره ۹۸۰۲۸۶۸۹ انجام شده است.

تتبع در مقررات مذکور و منابع مرتبط، به این مهم می‌پردازد و در جهت شفاف‌سازی این مقررات برای کمک به تدوین بستر قانونی مناسب، در خصوص حمایت از دادهٔ شخصی در نظام حقوقی ایران گام برمی‌دارد.

کلیدواژه‌ها: GDPR، داده شخصی، پردازش، کنترل‌کننده، پردازنده

۱. مقدمه

استفاده از داده‌های افراد در عصر کنونی به‌عنوان بخش جدایی‌ناپذیر از زندگی انسان‌هاست. همچنین، گسترش روزافزون استفاده از ابزارهای دیجیتال و افزایش قابلیت‌های فناوری برای تجزیه و تحلیل داده‌ها، فرصت‌های اقتصادی عظیمی را به‌وجود می‌آورد، اما چالش‌های حریم خصوصی را نیز موجب می‌شود. داده‌های اشخاص زمینه‌ساز معاملات و عملیات در اقتصاد جهانی هستند. افراد در حال حاضر با فعالیت‌های مختلفی مانند معاملات بانکی آنلاین، ارسال عکس و اطلاعات در شبکه‌های اجتماعی و ...، عنصر کلیدی اقتصاد مبتنی بر داده‌ها هستند (OECD 2010). بنابراین، داده‌ها در حال تبدیل شدن به یکی از دارایی‌های اصلیِ بسیاری از بازارهای مدرن هستند تا جایی که می‌توان آن‌ها را «نفت جدید اینترنت و پول جدید دنیای دیجیتال» در نظر گرفت (Feijóo, Gómez-Barroso & Voigt 2014, 248).

با توجه به ارزشمندی داده‌ها، ضرورت وجود قوانینی که هدف آن‌ها ایجاد تعادل بین منافع حریم خصوصی افراد، حمایت از داده‌های شخصی اشخاص، و نیاز سازمان‌ها، شرکت‌ها و اشخاص برای استفادهٔ منصفانه و منطقی از داده‌های مربوط به افراد در عملیاتشان باشد، احساس می‌شود. وجود چنین قوانینی بدان معنا نیست که استفاده از داده‌های افراد ممکن نیست یا اینکه همیشه باید رضایت فرد برای استفاده وجود داشته باشد، بلکه ایجاد تعادل و تحمیل محدودیت‌ها در استفاده از داده‌های شخصی است (University of Oxford 2018, 2).

در این راستا در سال ۲۰۱۶، اتحادیهٔ اروپا مقررات عمومی حفاظت از داده[1] – از این به بعد GDPR – را به‌عنوان یکی از بزرگ‌ترین دستاوردهای خود در سال‌های اخیر به تصویب رساند. این مقررات جایگزین دستورالعمل حفاظت از دادهٔ ۱۹۹۵ شده و در حال

1. General Data Protection Regulation (GDPR)

حاضر، GDPR به‌عنوان قانون در سراسر اتحادیهٔ اروپا به رسمیت شناخته شده است (EDPS, n.d.).

GDPR به استاندارد طلایی[1] در حفاظت از دادهٔ شخصی معروف است، چرا که جامع‌ترین بستر قانونی برای حمایت از دادهٔ شخصی است. پژوهش حاضر به تشریح و بررسی این مقررات می‌پردازد. بنابراین، در این پژوهش به‌ترتیب، قانون‌گذاری GDPR، تبیین مفاهیم و واژگان کلیدی، دامنهٔ اعمال و نقاط قوت این مقررات بررسی خواهد شد.

۲. پیشینهٔ پژوهش

مقررات جدیدِ حفاظت از دادهٔ شخصی اتحادیهٔ اروپا (GDPR) با هدف یکسان‌سازی قانونی و حمایت حداکثری از صاحبان دادهٔ شخصی، اکنون در مباحث مربوط به حریم خصوصی و دادهٔ شخصی مهم‌ترین بستر قانونی قابل استناد است. این سند قانونی گرچه مصوب اتحادیهٔ اروپاست، لیکن به‌دلیل الزامات خاص خود بر بسیاری از اشخاص خارج از اتحادیهٔ اروپا نیز اثرگذار بوده و ضمانت اجراهای آن بر دامنهٔ وسیعی از اشخاص قابل اجراست.

با توجه به جدید بودن این مقررات و الزامات و مفاد دقیق و جریان آن بر بسیاری از اشخاص، در پژوهش‌های نظام‌های حقوقی مختلف به این مقررات و شفاف‌سازی مفاد آن اشاره شده است. در چنین پژوهش‌هایی به ابعاد مختلف GDPR اشاره شده و این مقررات از جنبه‌های متفاوتی مورد واکاوی قرار گرفته است. به‌عنوان نمونه «جان فیلیپ» در مقاله‌ای با عنوان «چگونه GDPR جهان را تغییر داد» به بیان تحولات و نکات برجستهٔ این مقررات نسبت به مفاد قانونیِ سابق و بررسی این امر که GDPR تمامی مسائل مربوط به دادهٔ شخصی را به‌طور مستقیم تنظیم می‌کند و تنها اختیارات استثنایی و محدودی به کشورهای عضو اتحادیهٔ اروپا ارائه می‌دهد، اشاره نموده است (Jan Philipp 2016). «کورپیساری» نیز در مقاله‌ای با عنوان «بررسی الزامات GDPR در فنلاند» به تطبیق قانون حفاظت از دادهٔ فنلاند با الزامات موجود در GDPR پرداخته است (Korpisaari 2019). همچنین، «رینی» پایان‌نامه‌ای با عنوان «الزامات GDPR»، نگارش نموده و الزامات این مقررات را به‌صورت کاربردی تشریح نموده است (Reini 2019). «مارلی و تستا» نیز در مقاله‌ای با عنوان «بررسی دقیق

1. gold-standard in protection of data

مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا و چگونگی تأثیر آن بر پژوهش‌ها» به بیان مبانی حقوقی پردازش دادهٔ شخصی، مفاد مربوط و ارتباط آن با پژوهش‌ها پرداخته‌اند (Marelli & Testa 2018).

با توجه به پژوهش‌های مذکور و موارد مشابه در مورد GDPR، روشن است که پرداختن به این مقررات در نظام‌های حقوقی مختلف، بحث جدیدی است و در بسترهای علمی به این مقررات و بررسی حمایت از دادهٔ شخصی از نگاه این مقررات پرداخته می‌شود. ضرورت بررسی GDPR در نظام حقوقی ایران نیز احساس می‌شود، چرا که پژوهش مستقلی به شفاف‌سازی و معرفی این مقررات به‌طور خاص نپرداخته است. پژوهش حاضر عهده‌دار این مهم است و در کنار بررسی مفاد GDPR، در موارد مرتبط با نظام حقوقی ایران تطبیق داده شده و به تحلیل پرداخته است تا مسیر تدوین سند قانونی ایرانی در خصوص حمایت مؤثر از داده‌های شخصی هموار گردد.

۳. روش پژوهش

با توجه به این امر که پژوهش حاضر به توسعهٔ مرزهای دانش در علم حقوق کمک می‌کند، این پژوهش بر اساس هدف، از نوع بنیادی بوده و به این علت که به‌دنبال معرفی و شفاف‌سازی GDPR و تحلیل مفاد آن است، بر اساس ماهیت، توصیفی-تحلیلی است. همچنین، باید گفت از آنجا که جامعهٔ مورد بررسی در این پژوهش به‌طور کلی، سند قانونی اتحادیهٔ اروپا در خصوص حفاظت از دادهٔ شخصی و حریم خصوصی و به‌طور جزئی توجه به این موضوع در سایر نظام‌های حقوقی -مانند ایران و آمریکا و غیره- است، پژوهش حاضر جنبهٔ تطبیقی نیز دارد.

روش پژوهش نیز به‌صورت پژوهش اسنادی[1] است. این روش با تحلیل اسنادی که حاوی اطلاعاتی در مورد موضوع مد نظر است و از طریق بررسی اسناد مختلف مانند اسناد رسمی به‌عنوان منبع اطلاعات انجام می‌شود، یکی از پایه‌های اصلی در تحقیقات علوم انسانی و اجتماعی است (Ahmed 2010, 2).

در این پژوهش، ادبیات مربوط به حفاظت از دادهٔ شخصی و حریم خصوصی با تمرکز بر سند قانونی اتحادیهٔ اروپا مورد توصیف و تحلیل قرارگرفته، و مفاد GDPR برای ایجاد

1. documentary research method

درک جامعی از حفاظت‌های موجود در این مقررات بررسی شده است، تا در نهایت، در مقام عمل منجر به شفاف‌سازی این مقررات و استفادهٔ مؤثر از آن شود. همچنین، در بندهای مختلف پژوهش برای روشن‌تر شدن ادبیات حفاظت از دادهٔ شخصی و حریم خصوصی مباحث مربوط در کنار تحلیل، به‌صورت تطبیقی بیان شده است.

٤. قانون‌گذاری مقررات عمومی حفاظت از داده (GDPR)

در ماه آوریل سال ۲۰۱۶، بستهٔ اصلاحات قوانین حفاظت از داده تصویب شد که شامل مقررات عمومی حفاظت از داده (GDPR) بود. GDPR، جامع‌ترین بستر قانونی در خصوص حمایت از دادهٔ شخصی است. این مقررات اصول مندرج در دستورالعمل حفاظت از دادهٔ ۱۹۹۵ اتحادیهٔ اروپا[1] را، جهت تضمین حق حمایت از دادهٔ اشخاص، به‌روزرسانی کرده است و بر تقویت حقوق افراد، تقویت بازار داخلی اتحادیهٔ اروپا، تسهیل انتقال بین‌المللی دادهٔ شخصی و تدوین استانداردهای جهانی حفاظت از داده تمرکز دارد. GDPR به اشخاص حقیقی امکان کنترل بیشتری بر داده‌های شخصی‌شان داده و دسترسی به داده‌ها را آسان‌تر کرده است. در حال حاضر، GDPR به‌عنوان قانون در سراسر اتحادیهٔ اروپا به رسمیت شناخته شده است (EDPS n.d.).

این مقررات به‌طور مستقیم در تمام کشورهای عضو اتحادیهٔ اروپا لازم‌الاجراست. این بدان معناست که این مقررات نیاز به هیچ‌گونه اقدامی در قانون ملی ندارد و مستقیماً توسط شهروندان، ادارات دولتی و سایر شرکت‌ها، نهادها و سازمان‌هایی که داده‌های شخصی را پردازش می‌کنند باید رعایت شود (European Commission n.d.-a). گرچه مطابق با GDPR، کشورهای عضو باید گام‌های لازم برای انطباق قوانین خود با این مقررات، مانند لغو یا تصحیح قوانین موجود و ایجاد «مراجع ملی حفاظت از داده»[2] را بردارند[3]، در عین حال، این مقررات به کشورهای عضو این امکان را می‌دهد که کاربرد GDPR

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
2. data protection authority

به مرجع مذکور به‌طور مختصر «مرجع نظارتی» (Supervisory Authority) نیز گفته می‌شود.

۳. به‌عنوان مثال، پیاده‌سازی مقررات GDPR در کشور فنلاند از اوایل فوریهٔ ۲۰۱۶ آغاز شده و در نهایت، قانون حفاظت از دادهٔ فنلاند در ژانویهٔ ۲۰۱۹ به اجرا درآمد، که هفت ماه پس از لازم‌الاجرا شدن GDPR بود (Korpisaari 2019, 237).

را در زمینه‌های خاص مشخص کنند؛ مانند اشتغال و تأمین اجتماعی، بهداشت عمومی، اهداف بایگانی در جهت منافع عمومی، اهداف تحقیقات علمی، تاریخی یا اهداف آماری و همچنین، برای داده‌های ژنتیکی، داده‌های زیست‌شناختی و داده‌های مربوط به سلامت که مقررات به کشورهای عضو اختیار می‌دهد تا شرایط بیشتری برای ایجاد محدودیت‌ها حفظ یا معرفی کنند (Viorescu 2017, 32 & 33).

همان‌طور که بیان شد، GDPR جایگزین دستورالعمل حفاظت از دادهٔ ۱۹۹۵ است[۱]. با توجه به اهمیت این مقررات در خصوص حمایت از داده لازم است در خصوص چگونگی قانون‌گذاری این مقررات بحث مختصری داشته باشیم. در این خصوص باید گفت، بستهٔ اصلاحات قوانین حفاظت از دادهٔ اتحادیهٔ اروپا که در ژانویهٔ ۲۰۱۲، آغاز شده بود، منجر به سه بخش کلیدی در قانون‌گذاری در مورد حمایت از داده شده است که به‌شرح زیر است:

الف) مقررات عمومی حفاظت از داده (GDPR) 2016/679 (EU)[۲] که در ۲۷ ماه آوریل ۲۰۱۶ تصویب شد و از ۲۵ ماه می ۲۰۱۸ لازم‌الاجرا شد. این مقررات در خصوص حفاظت از اشخاص حقیقی نسبت به پردازش دادهٔ شخصی آن‌ها و جریان آزاد چنین داده‌هایی است که موضوع پژوهش حاضر است؛

---

۱. اولین قانون حفاظت از داده در اتحادیهٔ اروپا در سال ۱۹۵۰ تصویب و در سال ۱۹۵۳ لازم‌الاجرا شد (Goethem 2018, 7). با افزایش استفاده از رایانه‌ها در اواسط دههٔ ۱۹۶۰ و ۱۹۷۰ مسئلهٔ حفظ حقوق حریم خصوصی و حفاظت از دادهٔ اشخاص مورد توجه قرار گرفت و در اوایل دههٔ ۱۹۷۰ به دنبال پیشرفت‌های سریع در زمینهٔ فناوری اطلاعات و افزایش مباحث در مورد مسائل مربوط به حریم خصوصی، دولت فدرال آلمان اولین قانون حفاظت از دادهٔ ملی را در جهان وضع نمود (Bitar & Bjorn 2017, 9). این اقدام در کانادا در سال ۱۹۷۷، در فرانسه، اتریش، دانمارک و نروژ در سال ۱۹۷۸، در لوکزامبورگ در سال ۱۹۷۹ انجام شد. بعدها تقریباً تمام کشورهای اروپایی به تدوین مقررات مرتبط با حمایت از دادهٔ شخصی پرداختند (Serzhanova 2012, 4).

۲. مقررات اتحادیه اروپا به شماره ۶۷۹/۲۰۱۶ مصوب پارلمان و شورای اروپا در تاریخ ۲۷ آوریل ۲۰۱۶ در مورد حمایت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی، انتقال آزاد چنین داده‌هایی و لغو دستورالعمل EC/۴۶/۹۵.

این مقررات در سال ۲۰۱۸، اصلاحات جزئی داشته که از لینک ذیل قابل دسترسی است:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679R(02)&from=EN

ب) دستورالعمل حفاظت از داده در حوزهٔ انتظامی و قضایی 2016/680 (EU)[1] که در ۲۷ ماه آوریل ۲۰۱۶ تصویب شده و از ۶ ماه می ۲۰۱۸ لازم‌الاجراست (European Data Protection Supervisor n.d.). این دستورالعمل در خصوص حفاظت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی مرتبط با جرایم جنایی یا اجرای مجازات جنایی و در مورد جریان آزاد چنین داده‌هایی است، زمانی که داده‌های شخصی توسط مراجع اجرای قوانین کیفری به هدف اجرای چنین قوانینی مورد استفاده قرار می‌گیرند. این دستورالعمل از حقوق اساسی شهروندان در مورد حفاظت از داده‌هایشان در مورد مذکور محافظت می‌کند؛ به‌ویژه تضمین خواهد کرد که داده‌های شخصی قربانیان، شاهدان و مظنونان به جرم به‌درستی محافظت شود و همکاری فرامرزی در مبارزه با جرم و تروریسم را تسهیل می‌نماید (European Commission 2016).

ج) مقررات پردازش دادهٔ شخصی توسط مؤسسات، نهادها، ادارات و آژانس‌های اتحادیهٔ (EU) 2018/1725[2] که در ۲۳ اکتبر ۲۰۱۸ تصویب شده است. این مقررات، قواعد حفاظت از داده در مؤسسات اتحادیهٔ اروپا و همچنین وظایف سرپرست حفاظت از دادهٔ اتحادیهٔ اروپا را تعیین می‌کند (European Data Protection Supervisor n.d.). این مقررات با GDPR همسوست و از ۱۱ دسامبر ۲۰۱۸، لازم‌الاجراست (European Commission 2016).

---

۱. دستورالعمل اتحادیه اروپا به شماره ۶۸۰/۲۰۱۶ مصوب پارلمان و شورای اروپا در تاریخ ۲۷ آوریل ۲۰۱۶ در مورد حفاظت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی توسط مقامات ذی‌صلاح به‌منظور پیشگیری، تحقیق، کشف یا تعقیب جرایم کیفری یا اجرای مجازات‌های جنایی، همچنین جریان آزاد این‌گونه داده‌ها و لغو تصمیمات شورا به شماره JHA/۹۷۷/۲۰۰۸.
این دستورالعمل در سال ۲۰۱۸، اصلاحات جزئی داشته است که از لینک ذیل قابل دسترسی است:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680R(01)&rid=3

۲. مقررات اتحادیه اروپا به شماره ۱۷۲۵/۲۰۱۸ مصوب پارلمان و شورای اروپا در تاریخ ۲۳ اکتبر ۲۰۱۸ در مورد حفاظت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی توسط نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه و در مورد حرکت آزاد چنین داده‌هایی و لغو مقررات کمیسیون به شماره ۲۰۰۱/۴۵ و تصمیم کمیسیون به شماره ۲۰۰۲/۱۲۴۷
این مقررات از لینک ذیل قابل دسترسی است:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN

۵. تعریف برخی از اصطلاحات مهم در مقررات عمومی حفاظت از داده (GDPR)

برای فهم صحیح GDPR، شناسایی اصطلاحات اساسی و واژگان کلیدی آن ضروری است.

۵-۱. دادهٔ شخصی

دادهٔ شخصی[1] در تعریف GDPR، به معنای هر اطلاعاتی است که مربوط به شخص حقیقی شناخته‌شده یا قابل شناسایی (شخص موضوع داده) است. یک فرد حقیقی قابل شناسایی کسی است که به‌طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به یک شناسه از جمله نام، شمارهٔ شناسایی، اطلاعات مکانی، شناسهٔ آنلاین یا ارجاع به یک یا چند ویژگی خاص مانند هویت فیزیکی، فیزیولوژیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی، شناسایی شود (EUR-Lex 2016, 33).

ملاک دادهٔ شخصی بودن، شناسایی یک فرد بر اساس اطلاعات موجود است؛ به این معنا که بتوان یک فرد را به‌طور مستقیم یا غیرمستقیم با ارجاع به یک شناسه، شناسایی کرد. یک فرد حقیقی با ارجاع به شناسه‌هایی نظیر ویژگی‌های زیستی مانند شکل ظاهری، قد، وزن، اثر انگشت، دی‌ان‌اِی و الگوهای شبکیه‌ای یا توسط شناسه‌های بیوگرافی کسب‌شده مانند آدرس، تحصیلات، گواهینامهٔ رانندگی، گذرنامه، حساب بانکی، شماره‌های شناسایی منحصربه‌فرد مانند شمارهٔ تأمین اجتماعی و شمارهٔ حساب مالیات دایمی، قابل شناسایی است. این شناسه‌ها، اطلاعات شخصی[2] فرد را شکل می‌دهند (Singh 2016, 123) و اگر منجر به شناسایی شخص حقیقی شوند یا قابلیت شناسایی را فراهم نمایند، دادهٔ شخصی محسوب می‌شوند. بنابراین، در مواردی ترکیبی از شناسه‌ها و اطلاعات، دادهٔ شخصی را تشکیل می‌دهد و در برخی موارد نیز یک شناسه یا یک اطلاعات با حصول شناسایی شخص حقیقی یا قابلیت شناسایی، دادهٔ شخصی محسوب می‌شود.

با توجه به تعریف مذکور می‌توان درک نمود که شناسایی و قابلیت شناسایی، عنصری مهم برای تعریف دادهٔ شخصی است (Taylor 2006, 74). به همین جهت داده‌های شخصی که شناسایی نشده‌اند، رمزگذاری[3] شده‌اند یا مستعار[4] هستند، ولی می‌توانند برای شناسایی مجدد یک فرد استفاده شوند، داده‌های شخصی هستند و در محدودهٔ GDPR

1. personal data
2. personal information
3. encryption
4. pseudonymisation

قرار می‌گیرند. در مقابل، داده‌های شخصی اگر به‌گونه‌ای ناشناس- ناشناس ساختن[1]- ارائه شوند که فرد قابل شناسایی نباشد یا دیگر قابل شناسایی نیست، داده‌های شخصی نیست. البته، برای اینکه داده‌ها به‌درستی ناشناس شوند، داده‌های ناشناس‌شده باید غیرقابل بازگشت باشند (European Commission 2019b). بنابراین، روشن است داده‌هایی که هیچ مرجع شخصی ندارند، (برای مثال، داده‌های‌ی که صرفاً ماشینی هستند و به‌طور کلی داده‌های شخصی در هیچ مرحله‌ای مورد پردازش واقع نمی‌شوند)، مشمول GDPR نیستند. لیکن اگر این داده‌ها بتوانند به یک شخص حقیقی مرتبط شوند و شناسایی فرد ممکن شود، دادهٔ شخصی تحت حفاظت GDPR است (Spindler & Schmechel 2016, 168).

تعریف GDPR از دادهٔ شخصی موسع (به‌عنوان نمونهٔ استفاده از کلمهٔ «هر اطلاعاتی» در ابتدای تعریف و همچنین شناسایی به‌طور «مستقیم یا غیرمستقیم»)، انعطاف‌پذیر و سازگار با بسترهای فناوری است (Allison 2009, 49). برای تعیین اینکه آیا یک شخص حقیقی قابل شناسایی است یا خیر، باید تمام ابزارهایی که احتمال استفاده از آن وجود دارد، (مانند ابزارهای قابل استفاده توسط کنترل‌کننده و یا توسط شخص دیگری برای شناسایی مستقیم یا غیرمستقیم فرد حقیقی)، در نظر گرفته شود (Purtova 2018, 44).

همچنین، برای تعیین اینکه آیا ابزارها به‌طور منطقی قابل استفاده هستند یا خیر، باید تمام عوامل نوعی مانند هزینه و مقدار زمان مورد نیاز برای شناسایی، با در نظر گرفتن فناوری موجود در زمان پردازش و پیشرفت‌های فناوری را در نظر گرفت (همان).

---

1. anonymisation

ناشناس ساختن – بی‌نام‌ونشان کردن- جدای از رمزگذاری و مستعارسازی به معنای روشی است برای اصلاح داده‌های شخصی با این هدف که هیچ ارتباطی بین داده‌های شخصی با یک فرد وجود نداشته باشد. داده‌های ناشناس اطلاعاتی هستند که به یک فرد شناسایی‌شده یا قابل شناسایی مرتبط نیستند یا داده‌های شخصی هستند که به شیوه‌ای ناشناس ارائه شده‌اند که فرد دیگر قابل شناسایی نیست. به‌عنوان مثال، یک مؤسسهٔ خصوصی آموزشی به مناسبت بیستمین سالگرد تأسیس خود می‌خواهد بداند که چند نفر از دانشجویان سابق در دانشگاه شرکت کرده‌اند و اگر چنین است چه چیزی را مطالعه کرده‌اند. برای این منظور، مؤسسهٔ آموزشی، داده‌های دانشجویان خود را از ۲۰ سال قبل جمع‌آوری کرده و از طریق ایمیل با آن‌ها تماس می‌گیرد تا در یک نظرسنجی آنلاین شرکت کنند. به‌منظور ناشناس ساختن داده‌ها، این نظرسنجی حاوی سؤالاتی در مورد نام، آدرس ایمیل، سال فارغ‌التحصیلی یا تاریخ تولد نیست، نشانی IP شرکت‌کنندگان نیز ثبت نمی‌شود، بلکه به‌منظور جلوگیری از شناسایی دانشجویان قبلی که فارغ‌التحصیل شده‌اند، افراد به حوزه‌های مطالعاتی آن‌ها مانند «علوم طبیعی»، «مطالعات حقوقی»، «مطالعات اجتماعی» و «مطالعات زبانی» گروه‌بندی می‌شوند (Voigt & von dem Bussche 2017, 13 & 14).

از مصادیق دادهٔ شخصی می‌توان به نام و نام خانوادگی، آدرس محل سکونت، آدرس پست الکترونیکی، شمارهٔ کارت شناسایی، داده‌های مکانی (برای مثال، داده‌های مکانی روی یک تلفن همراه)، آدرس اینترنتی (IP)، کوکی‌ها، شناسه‌های تلفن همراه، داده‌های موجود نزد بیمارستان یا پزشک که شناسایی منحصربه‌فرد یک شخص را ممکن می‌سازد، اشاره کرد. لیکن، شمارهٔ ثبت شرکت‌ها، و آدرس پست الکترونیکی مربوط به شرکت دادهٔ شخصی محسوب نمی‌شوند (European Commission 2019b)؛ چرا که در تعریف دادهٔ شخصی در مقررات GDPR —که در ابتدای این قسمت بیان شد– دادهٔ شخصی منحصر بر اشخاص حقیقی است. بنابراین، اشخاص حقوقی بدون توجه به شکل حقوقی خود، از حفاظت تحت GDPR بهره‌مند نمی‌شوند. علت عدم حمایت از اشخاص حقوقی این است که قانون‌گذار خواهانِ حمایت از افراد حقیقی با توجه به حقوق اساسی‌شان تحت ماده ۸ منشور حقوق اساسی اتحادیهٔ اروپا[1] و ماده ۱۶ از پیمان عملکرد اتحادیهٔ اروپا[2] (TFEU) بوده است[3]. با این حال، اگر داده‌های اشخاص حقوقی حاوی اطلاعاتی در مورد افراد مرتبط با شخص حقوقی باشد، می‌تواند داده‌های شخصی تحت GDPR تلقی شود؛ مثل اطلاعات مربوط به سهم یا عملکرد افراد یک شرکت (Voigt & von dem Bussche 2017, 21).

۵-۲. پردازش

پردازش[4] در GDPR، به معنای عملیات یا مجموعه‌ای از عملیات است که بر روی دادهٔ

---

1. Charter Of Fundamental Rights Of The European Union

ماده ۸ این منشور در خصوص حفاظت از دادهٔ شخصی بدین شرح است:
۱. هر کس حق حفاظت از داده‌های شخصی مربوط به خود را دارد. ۲. چنین داده‌هایی باید به‌طور منصفانه برای اهداف مشخص و بر اساس رضایت فرد و یا برخی مبانی قانونی دیگر که توسط قانون وضع شده‌اند، پردازش شوند. هر کس حق دسترسی به داده‌هایی را دارد که در رابطه با او جمع‌آوری شده است و حق تصحیح آن‌ها را دارد. ۳. مطابقت با این قواعد، امور [مربوط به داده‌های شخصی] باید تحت کنترل یک مرجع مستقل باشد (EUR-Lex 2012, 397).

2. Treaty on the Functioning of the European Union

ماده ۱۶ این پیمان مقرر می‌دارد: «هر کس حق حفاظت از داده‌های شخصی مربوط به خود را دارد» (EUR-Lex 2012b, 55).

۳. باید گفت اشخاص حقوقی نیز دادهٔ شخصی دارند؛ لیکن GDPR از آن حمایتی ندارد، اما می‌توان از سایر بسترهای حقوقی از قبیل مباحث مسئولیت مدنی و مالکیت‌های فکری برای اشخاص حقوقی نیز حمایت‌هایی را دنبال نمود.

4. processing

شخصی یا مجموعهٔ داده‌های شخصی، با وسایل خودکار و غیر آن صورت گیرد. چنین عملیاتی اعم از جمع‌آوری، ضبط، سازماندهی، طبقه‌بندی، ذخیره‌سازی، تطبیق، تغییر دادن، بازیابی، استفاده کردن، مورد مذاکره قرار دادن، افشا به‌وسیلهٔ مخابره کردن یا منتشر کردن یا دیگر طرق دسترسی، تنظیم یا ترکیب کردن، محدود کردن، حذف و پاک کردن و یا تخریب است (EUR-Lex 2016, 33). بنابراین، پردازش، مصادیق متعددی دارد. به‌طور نمونه، پردازش می‌تواند مدیریت داده‌های کارکنان و ادارهٔ حقوق و دستمزدها، دسترسی به یک پایگاه دادهٔ حاوی دادهٔ شخصی، ارسال پست الکترونیکی تبلیغاتی، تفکیک اسناد حاوی داده‌های شخصی به‌منظور شناسایی اشخاص حقیقی، ارسال یا قرار دادن عکس از یک شخص در یک وب‌گاه، ذخیرهٔ آدرس‌های IP یا ضبط ویدیوئی باشد (European Commission 2019a).

همچنین باید گفت GDPR مربوط به حمایت از دادهٔ شخصی فارغ از فناوری مورد استفاده برای پردازشِ داده‌هاست و برای هر دو پردازش خودکار و دستی اعمال می‌شود. همچنین، مهم نیست که داده‌ها چگونه و در کجا ذخیره می‌شوند. به‌عنوان مثال، داده‌های شخصی در یک سیستم فناوری اطلاعات از طریق نظارت ویدیوئی یا بر روی کاغذ، در همهٔ موارد، منوط به الزامات حفاظتی GDPR است (European Commission 2019b).

۵-۳. کنترل‌کننده

کنترل‌کننده[1]، 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). اگر شخصی –اعم از حقیقی یا حقوقی- یا یک مرجع عمومی یا نهاد وقتی که تصمیم بگیرد چرا و چگونه داده‌های شخصی باید پردازش شوند، کنترل‌کنندهٔ داده است.

GDPR شکل جدیدی از رابطهٔ قانونی، تحت عنوان «کنترل‌کنندگان مشترک –مقرر در ماده[2] ۲۶–» را پیش‌بینی می‌کند. این مفهوم زمانی حاصل می‌شود که چند شخص، مرجع عمومی یا نهاد دیگر در خصوص تعیین اهداف و ابزار پردازش مشارکت داشته

1. controller

۲. «در صورتی‌که دو یا چند کنترل‌کننده به‌طور مشترک اهداف و ابزار پردازش را تعیین می‌کنند، آن‌ها کنترل‌کنندگان مشترک هستند. آن باید به‌طور شفاف، مسئولیت‌های مربوط به خود را در قبال تعهدات مندرج در این مقررات مشخص کنند، ...» (EUR-Lex 2016, 48).

باشند. کنترل‌کنندگان مشترک باید جهت تنظیم مسئولیت‌های مربوط به خود برای انطباق با مقررات GDPR، قراردادی منعقد نمایند که در آن نقش‌های مربوطه، روابط کنترل‌کنندگان مشترک در مقابل اشخاص موضوع داده و همچنین، تخصیص مسئولیت‌ها بین کنترل‌کنندگان روشن و واضح باشد و جنبه‌های اصلی این قرارداد به افرادی که داده‌های آن‌ها پردازش می‌شود، ابلاغ شود (Colcelli 2019, 1031). به‌عنوان مثال، یک شرکت، خدمات نگهداری از کودک را از طریق یک برنامهٔ آنلاین ارائه می‌دهد. این شرکت در عین حال، با شرکت دیگری قرارداد دارد که به شرکت اول اجازه می‌دهد تا خدمات دیگری را نیز ارائه دهد. این خدمات شامل اجارهٔ بازی‌ها و نرم‌افزارهای آموزشی برای والدین است. هر دو شرکت در راه‌اندازی فنی وب‌گاه برای ارائهٔ آنلاین خدمات مشارکت داشته‌اند. در این صورت، دو شرکت تصمیم گرفته‌اند که از یک بستر خاص برای هر دو هدف استفاده کنند (خدمات نگهداری از کودک و اجارهٔ بازی‌ها و نرم‌افزارهای آموزشی) و غالباً این دو شرکت نام مشتریان را برای هم به اشتراک می‌گذارند. بنابراین، این دو شرکت کنترل‌کنندگان مشترک هستند، زیرا نه‌تنها توافق کرده‌اند که «خدمات ترکیبی» ارائه دهند، بلکه یک بستر مشترک را نیز طراحی کرده و استفاده می‌کنند (European Commission 2018a).

۵-٤. پردازنده

پردازنده[1]، 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 دهد تا اطمینان حاصل شود که پردازش توسط پردازنده مطابق با استانداردهای GDPR و تضمین حفاظت از حقوق افراد است. وظایف پردازنده نسبت به کنترل‌کننده باید در یک قرارداد یا طی یک اقدام قانونی دیگر مشخص شود[2] (European Commission 2018a).

برای درک بهتر مفهوم پردازنده می‌توان مثالی را ذکر کرد، بدین ترتیب که یک شرکت آرایشی تصمیم می‌گیرد نسخهٔ پشتیبان پایگاه دادهٔ مشتریان خود را بر روی

1. processor

۲. در ماده ۲۶ GDPR به این وظیفه اشاره شده است.

یک فضای ابری[1] ذخیره کند. برای رسیدن به این هدف، این شرکت با یک شرکت تأمین‌کنندهٔ فضای ابری که به‌خاطر استانداردهای حفاظت از داده مشهور است و همچنین دارای یک سیستم رمزنگاری داده است، قرارداد منعقد می‌کند. تأمین‌کنندهٔ فضای ابری، پردازنده است چون با ذخیره‌سازی داده‌های شخصی مشتریان در فضای ابری، داده‌های شخصی را از جانب شرکت آرایشی پردازش خواهد کرد (EC. European Commission, n.d.).

همچنین باید گفت که اگر پردازنده مجوز کتبی قبلی از کنترل‌کننده دریافت کرده باشد تا یک پردازندهٔ دیگر را جهت مشارکت منصوب نماید، پردازنده می‌تواند بخشی از کار خود را به پردازندهٔ دیگر –پردازندهٔ فرعی[2]– واگذار کند (European Commission 2018a). بنابراین، پردازنده نمی‌تواند پردازندهٔ دیگری را بدون مجوز کتبی قبلی خاص یا به‌طور مطلقِ کنترل‌کننده منصوب کند[3].

این امر که پردازنده بدون اجازهٔ کنترل‌کننده نمی‌تواند بخشی از کار خود را به دیگری واگذار کند، با نظام حقوقی ایران و مبانی حاکم بر عقد وکالت قابل تطبیق است؛ چرا که یکی از مطالب مطرح در عقد وکالت بحث توکیل به غیر است و مطابق ماده ۶۷۲ قانون مدنی «وکیل در امری نمی‌تواند برای آن امر به دیگری وکالت دهد، مگر اینکه صریحاً یا به دلالت قرائن وکیل در توکیل باشد». دلیل این مطلب آن است که اعطای نیابت به وکیل با توجه به شخصیت اوست و قائم به شخص است. بنابراین، نبودِ حق توکیل اصل است و در صورت وجود اجازهٔ صریح یا ضمنی، به‌عنوان یک استثنا، چنین حقی برای وکیل وجود دارد (کاتوزیان ۱۳۹۶، ۸۳ و ۸۴). منوط بودن حق توکیل به غیر، به اجازهٔ صریح یا ضمنیِ موکل، در منابع فقهی مورد تصریح قرار گرفته است (شهید ثانی ۱۴۱۰ ه.ق، ۳۷۴؛ علامه حلی ۱۴۲۰ ه.ق، ۳۰؛ سیستانی ۱۴۱۵ ه.ق، ۳۴۵ و ۳۴۶؛ حسینی عاملی بی‌تا، ۵۳۴؛ شیخ طوسی ۱۳۸۷ ه.ق، ۳۶۴؛ ابن ادریس حلی ۱۳۸۷، ۱۲۳).

این مطلب با سایر نظام‌های حقوقی نیز قابل تطبیق است، به‌عنوان نمونه، تحت اصل 'Delegatus non-potest delegare'. در حقوق انگلیس شخصی که اختیار یا قدرتی از

1. cloudy servers
2. sub-processor

۳. این الزام در ماده ۲۸ بخش ۲ GDPR مقرر شده است: «پردازنده نباید پردازندهٔ دیگری را، بدون مجوز قبلی کتبی خاص یا عام کنترل‌کننده درگیر کند. در مورد مجوز کتبی عام پردازنده باید کنترل‌کننده را از هرگونه تغییرات در نظر گرفته‌شده در رابطه با اضافه‌کردن یا جایگزینی پردازنده‌های دیگر مطلع کند و بدین‌وسیله به کنترل‌کننده فرصت اعتراض به چنین تغییراتی را بدهد» (EUR-Lex 2016, 49).

مرجعی بالاتر به آن واگذار شده، به‌نوبهٔ خود نمی‌تواند دوباره آن را به دیگری تفویض کند، مگر اینکه مرجع اصلی به صراحت یا به‌طور ضمنی آن را مجاز بداند. به‌عنوان مثال، وکیل دارای مجوز قانونی در وکالتنامه نمی‌تواند با رضایت خود، اعمال اختیارات را بدون رضایت موکل، به شخص دیگری (وکیل فرعی)[1]، تفویض کند (Sabti & Subbaiah 2017, 76). در حقوق فرانسه نیز قانون مدنی فرانسه در مباحث مرتبط با وکالت 'mandate' – در ماده ۱۹۸۹– بیان می‌کند که وکیل نمی‌تواند کاری فراتر ازآنچه در اختیار او قرار داده شده، انجام دهد (Legifrance, n.d.). از چنین مفادی به‌طور ضمنی می‌توان مطلب مورد بحث را استنباط نمود.

در مسئلهٔ مورد بررسی نیز کنترل‌کننده در واقع، پردازنده را نمایندهٔ خود می‌کند تا پردازش را از جانب کنترل‌کننده انجام دهد و شخصیت پردازنده نیز مهم است؛ چرا که مطابق با ماده ۲۸ بخش ۱ GDPR: «در جایی که قرار است پردازش از طرف کنترل‌کننده انجام شود، کنترل‌کننده باید تنها از پردازنده‌هایی استفاده کند که ضمانت‌های کافی برای اجرای اقدامات فنی و سازمانی مناسب را ارائه می‌دهند، به‌گونه‌ای که پردازش مطابق با الزامات این مقررات باشد و حفاظت از حقوق اشخاص موضوع داده تضمین شود» (EUR-Lex 2016, 49). در واقع، برای کنترل‌کننده انتخاب پردازندهٔ مناسب مهم است و بدین جهت انجام امر پردازش مرتبط با شخصیت پردازنده و قائم به شخص اوست. البته، نگاه GDPR سخت‌گیرانه‌تر است؛ چرا که در نظام حقوقی ایران اجازه در توکیل برای وکیل را می‌توان هم به‌صورت شفاهی و هم به‌صورت کتبی داد، لیکن بر اساس GDPR، اجازه در انتخاب پردازندهٔ دیگر جهت مشارکت، صرفاً با مجوز کتبی کنترل‌کننده امکان‌پذیر است. به‌عنوان مثال، یک شرکت ساخت‌وساز از یک پیمانکار فرعی برای کار ساخت‌وساز در موردی خاص استفاده می‌کند و جزئیات تماس مشتریان را که کار ساخت‌وساز دارند، به پیمانکار فرعی ارائه می‌کند. پیمانکار فرعی از داده‌ها برای ارسال مطالب بازاریابی به مشتریان استفاده می‌کند. پیمانکار فرعی در این مورد صرفاً یک «پردازنده» تحت GDPR نیست، زیرا پیمانکار فرعی نه‌تنها داده‌های شخصی را به نمایندگی از شرکت ساخت‌وساز پردازش می‌کند، بلکه آن را برای اهداف خود نیز پردازش می‌کند. بنابراین، پیمانکار فرعی به‌عنوان «کنترل‌کننده» محسوب می‌شود، زیرا

1. sub-delegation

پردازنـده بـدون دسـتورالعمل کنترل‌کننـده به‌گونـه‌ای عمـل کـرده اسـت کـه هـدف و ابـزار پـردازش را تعییـن کـرده اسـت، بنابرایـن، یـک کنترل‌کننـده اسـت و ماننـد یـک کنترل‌کننـده مسـئولیت خواهـد داشـت (ICO 2018b).

٦. بررسی قلمرو مقررات عمومی حفاظت از داده (GDPR)

در خصـوص ایـن مقـررات، می‌تـوان از دامنـهٔ ایجابـی و دامنـهٔ سـلبی سـخن گفـت. در واقـع، نخسـت بایـد مـوارد داخـل در GDPR بررسـی شـود و در گام بعـدی از مـواردی کـه از مقـررات خـارج اسـت، سـخن بـه میـان آورد.

٦-١. موارد اعمال GDPR (دامنهٔ ایجابی)

در ایـن قسـمت، دامنـهٔ اعمـال مقـررات از دو جنبـهٔ موضوعـی و جغرافیایـی روشـن خواهـد شـد.

بـه لحـاظ دامنـهٔ موضوعـی بایـد گفـت کـه مخاطبـان قانونـی ایـن مقـررات کنترل‌کننده‌هـا، پردازنده‌هـا و ذی‌نفعـان تحـت حمایـت GDPR هسـتند؛ بـا ایـن توضیـح کـه هـر شـخص حقیقـی، فـارغ از ملیـت یـا محـل اقامتـش می‌توانـد از حمایـت تحـت GDPR برخـوردار شـود و به‌طـور کلـی، همـهٔ افـراد صـرف نظـر از سنشـان از حفاظـت تحـت GDPR بهـره می‌برنـد. بـا ایـن حـال، کـودکان از حفاظـت خـاص و تقویت‌شـده‌ای تحـت ایـن مقـررات بهره‌منـد هسـتند، زیـرا ممکـن اسـت نسـبت بـه خطـرات، پیامدهـا و تدابیـر حفاظتـی مربوطـه و حقـوق خودشـان نسـبت بـه پـردازش دادهٔ شـخصی آگاهـی کمتـری داشـته باشـند (Voigt & von dem Bussche 2017, 17 & 20-21).

بـه لحـاظ دامنـهٔ جغرافیایـی نیـز بایـد گفـت، GDPR در مـاده ۳ خـود بـه ایـن دامنـه[1] به‌شـرح زیـر اشـاره می‌کنـد:

الـف) ایـن مقـررات در مـورد پـردازش دادهٔ شـخصی در زمینـهٔ فعالیت‌هـای کنترل‌کننـده یـا پردازنـده‌ای کـه محـل استقرارشـان (مقـر) در اتحادیـهٔ اروپاسـت، صـرف نظـر از اینکـه آیـا پـردازش در اتحادیـه رخ می‌دهـد یـا خیـر، اعمـال می‌شـود؛

ب) ایـن مقـررات بـرای پـردازش دادهٔ شـخصیِ اشـخاص موضـوع داده‌ای کـه در اتحادیـهٔ اروپاسـت و پـردازش داده‌هایـش توسـط کنترل‌کننـده یـا پردازنـده‌ای کـه در اتحادیـهٔ اروپـا

1. territorial scope

مستقر نشده، انجام می‌شود نیز اعمال می‌شود؛ درصورتی‌که فعالیت‌های پردازش مربوط به موارد زیر باشد:

- □ ارائهٔ کالا یا خدمات به اشخاص موضوع داده‌ای که در اتحادیهٔ اروپا هستند، فارغ از اینکه آیا پرداخت شخص موضوع داده در اتحادیهٔ اروپاست یا خیر؛ یا
- □ نظارت بر رفتار اشخاص موضوع داده‌ای که در اتحادیهٔ اروپا هستند تا جایی که رفتار آن‌ها در داخل اتحادیهٔ اروپا صورت می‌گیرد.

ج) این مقررات برای پردازش دادهٔ شخصی، توسط کنترل‌کننده‌ای که در اتحادیهٔ اروپا مستقر نشده، اما در محلی واقع شده است که قانون کشور عضو اتحادیهٔ اروپا به موجب حقوق بین‌الملل عمومی اعمال می‌شود، نیز کاربرد دارد (EUR-Lex 2016, 32 & 33).

در ۷ ژانویهٔ سال ۲۰۲۰، هیئت حفاظت از دادهٔ اتحادیهٔ اروپا[1] نسخهٔ نهایی دستورالعمل خود را در خصوص قلمرو جغرافیایی GDPR تحت ماده ۳ بیان نمود[2]. این دستورالعمل برای کمک به مراجع حفاظت از داده، در خصوص فعالیت‌های پردازش داده و ارائهٔ تفسیری مشترک از GDPR در هنگام ارزیابی اینکه آیا پردازشِ خاصی توسط یک کنترل‌کننده یا یک پردازنده در محدودهٔ قلمرو GDPR قرار می‌گیرد یا خیر، است. چنین دستورالعملی به‌طور خاص، معیارهای کاربردی را برای ماده ۳ GDPR، تعیین و روشن می‌کنند (Olivi 2019, 1). این معیارها «مقر»[3] و «هدف»[4] هستند (EDPB 2019, 3)، که همراه با شرح بخش‌های مختلف ماده ۳ (در سه بند الف، ب، و ج) به آن‌ها اشاره خواهد شد.

الف) مطابق با ماده ۳ بخش ۱ GDPR، این مقررات برای پردازش داده‌های شخصی در زمینهٔ فعالیت‌های کنترل‌کننده یا پردازنده‌ای که در اتحادیهٔ اروپا مستقر شده، قابل اجراست؛ صرف نظر از اینکه پردازش در اتحادیه رخ می‌دهد یا خیر. این ماده اصل استقرار (مقر) را اعمال می‌کند که طبق آن انتخاب قانون به جایی که یک نهاد مقر دارد، بستگی دارد. بنابراین، برای کاربرد GDPR ضرورتاً لازم نیست مشخص شود که

1. European Data Protection Board (EDPB)

۲. این دستورالعمل از لینک زیر قابل دسترسی است:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_0.pdf

3. establishment
4. targeting

داده‌ها در کجا پردازش می‌شوند.

در خصوص اولین معیار (مقر) باید گفت که مقر مفهومی انعطاف‌پذیر دارد، زیرا مطابق مشروح[1] GDPR ۲۲، مقر دال بر اعمال مؤثر و واقعی فعالیت‌ها از طریق ترتیبات پایدار[2] است. شکل حقوقی چنین ترتیباتی، چه از طریق یک شعبه و چه از طریق یک شرکت تابعه با شخصیت حقوقی، عامل تعیین‌کننده نیست (EUR-Lex 2016, 4). همچنین، مکان ثبت با مقر به‌طور خودکار یکسان نیست، اما مکان ثبت ممکن است نشان‌دهندهٔ مقر باشد. به‌علاوه باید گفت که مطابق رأی دیوان دادگستری اتحادیهٔ اروپا (ECJ)[3] به شمارهٔ C-131/12 مورخ ۱۳ ماه می ۲۰۱۴، جهت اطمینان از سطح بالای حفاظت از داده‌های شخصی، اصطلاح «مقر» را نمی‌توان به‌طور محدود تفسیر کرد (CURIA 2014b, 13). درجهٔ پایداری چنین ترتیباتی باید با توجه به ماهیت فعالیت‌های اقتصادی و خدمات ارائه‌شده تعیین شود. هر دو عنصرِ تعریف -اعمال مؤثر و واقعی فعالیت‌ها و به‌وسیلهٔ ترتیبات پایدار- باید در ارتباط با یکدیگر تفسیر شوند، حتی حضور یک نمایندگی در یک کشور عضو می‌تواند برای تشکیل یک مقر کافی باشد، اگر نمایندگی مذکور خدمات خود را با درجهٔ معینی از پایداری ارائه دهد و وجود یک «مقر» به شرایط هر مورد بستگی دارد. حتی داشتن یک حساب بانکی یا صندوق پستی در یک کشور عضو می‌تواند یک ترتیب پایدار باشد. پایداری باید در ارتباط با ماهیت خاص فعالیت‌ها مشخص شود. به‌عنوان مثال، اگر یک شرکت خدمات را منحصراً روی اینترنت ارائه دهد، وجود مقدمه‌ای برای ارائه یا اجرای چنین خدماتی در یک کشور عضو اتحادیهٔ اروپا ممکن است «مقر» محسوب شود. هم پایداری ترتیبات و هم سهم فعالیت در پردازش داده‌ها باید وجود داشته باشد. فعالیت اقتصادی در چارچوب ترتیبات پایدار در نهایت می‌تواند یک فعالیت کوچک باشد؛ به‌عنوان مثال، ادارهٔ یک وب‌گاه برای ارائهٔ خدمات. بنابراین، هم منابع

---

1. recital

چنین مشروحاتی در ابتدای یک قانون یا مقررهٔ اتحادیهٔ اروپا می‌آید تا مفاد آن قانون یا مقرره را روشن‌تر سازد و در عین حال، بیان الزامی ندارد. بنابراین، باید گفت مشروحات، در قوانین و مقررات اتحادیهٔ اروپا به‌خودی خود از نظر حقوقی مانند مواد قانونی لازم‌الاجرا نیستند. با این حال، در جایی که آن قانون یا مقرره مبهم است، چنین مشروحاتی می‌تواند در تفسیر موارد مبهم استفاده شود (Practical Law, n.d.-b).

2. stable arrangement

3. European Court of Justice

انسانی و هم منابع مادی ممکن است به‌عنوان ترتیبات پایدار در نظر گرفته شوند. به‌عنوان مثال، یک شرکت غیرعضو اتحادیهٔ اروپا، دارای یک حساب بانکی، یک صندوق پستی و یک نمایندگی در کشور عضو اتحادیهٔ اروپاست که به‌عنوان نقطهٔ ارتباطی[1] انحصاری برای مشتریان در کشور عضو اتحادیهٔ اروپا عمل می‌کند. در این مثال، منابع انسانی و مادی، در کشور عضو اتحادیهٔ اروپا باید به‌عنوان ترتیبات پایدار محسوب شود و در نتیجه، شرایط «مقر» حاصل است (Voigt & von dem Bussche 2017, 22 & 23).

ب) مطابق ماده ۳ بخش ۲ GDPR، اگر کنترل‌کننده و پردازنده در اتحادیهٔ اروپا مستقر نشده باشند، با وجود این، GDPR می‌تواند اعمال شود. قانون‌گذار اتحادیهٔ اروپا به‌منظور حصول اطمینان از اینکه افراد از حقوق حفاظت از دادهٔ خود محروم نمی‌شوند، دامنهٔ کاربرد قانون حفاظت از دادهٔ اروپا را با معرفی اصل «قانون محل ایفای تعهد یا اجرای قرارداد»[2] گسترش داده است. با توجه به این اصل، قانونِ قابل‌اجرا بستگی به محلی دارد که اجرای قرارداد مربوطه ایجاب می‌شود. به‌طور کلی، مشخص است که ایجاب (پیشنهاد) قرارداد در کجا رخ می‌دهد. بنابراین، بر نهادهایی که مصرف‌کنندگان را در بازار داخلی اتحادیهٔ اروپا هدف قرار می‌دهند، تأثیر خواهد گذاشت. شرکت‌ها باید به خاطر داشته باشند تا زمانی که اشخاص موضوع داده در اتحادیهٔ اروپا هستند، ملیت مشتریانشان اهمیتی ندارد (Voigt & von dem Bussche 2017, 26).

ج) توضیح قسمت سوم نیز در مشروح GDPR ۲۵ بیان شده است؛ بدین‌شرح که: در صورتی که قانون کشور عضو به‌موجب حقوق بین‌الملل عمومی اعمال می‌شود، این مقررات باید در مورد کنترل‌کننده‌ای که در اتحادیهٔ اروپا مستقر نشده است، مانند مأموریت دیپلماتیک یک کشور عضو یا پست کنسولی، نیز اعمال شود (EUR-Lex 2016, 5).

برای درک بیشتر دامنهٔ جغرافیایی GDPR، به‌عنوان مثال باید گفت یک مؤسسهٔ آموزش عالی کوچک به‌صورت آنلاین و مستقر در خارج از اتحادیهٔ اروپا فعالیت می‌کند و عمدتاً دانشگاه‌های زبان اسپانیایی و پرتغالی در اتحادیهٔ اروپا را هدف قرار می‌دهد. خدمات این مؤسسهٔ مشاورهٔ رایگان در مورد تعدادی از دوره‌های دانشگاهی است و

1. contact point
2. lex loci solutionis

دانشجویان برای دسترسی به مطالب آنلاین به یک نام کاربری و رمز عبور نیاز دارند که زمانی که دانشجویان فرم ثبت نام را پر می‌کنند، شرکت نام کاربری و رمز عبور مذکور را ارائه می‌دهد. بنابراین، این مؤسسه داده‌های شخصی اشخاص حقیقیِ مستقر در اتحادیهٔ اروپا را با هدف ارائهٔ خدمات مورد پردازش قرار می‌دهد، پس GDPR بر این مؤسسه اعمال می‌شود. در مقابل، یک شرکت ارائه‌دهندهٔ خدمات مستقر در خارج از اتحادیهٔ اروپا به مشتریان خارج از اتحادیهٔ اروپا خدمات ارائه می‌دهد. مشتریان این شرکت می‌توانند هنگام سفر به کشورهای دیگر، از جمله کشورهای عضو اتحادیهٔ اروپا از خدمات آن استفاده کنند و اگر این شرکت به‌طور خاص برای خدمات خود اشخاص در اتحادیهٔ اروپا را مورد هدف قرار ندهد، مشمول مقررات GDPR نیست (European Commission 2018b). با توجه به مثال مذکور که توسط کمیسیون اتحادیهٔ اروپا بیان شده، می‌توان معیار دیگرِ هیئت حفاظت از دادهٔ اتحادیهٔ اروپا (هدف) را درک نمود؛ با این توضیح که، در فرضی که کنترل‌کننده و پردازنده در اتحادیهٔ اروپا مستقر نیستند، لیکن به اشخاص موضوع دادهٔ موجود در اتحادیهٔ اروپا ارائهٔ کالا یا خدمات دارند یا بر رفتار آن‌ها نظارت می‌کنند، چنین ارائهٔ کالا یا خدماتی یا نظارتی باید توسط کنترل‌کننده و پردازنده هدف‌گیری شده باشد و در صورت فقدان چنین هدف‌گیری، پردازش صرف داده‌های شخصی افراد در اتحادیهٔ اروپا به‌خودی خود برای اعمال GDPR کافی نیست. همچنین، صرف اینکه افراد در اتحادیهٔ اروپا باشند، کافی است و شهروند اتحادیه یا مقیم و ساکن بودن اهمیتی ندارد (Baker McKenzie 2019, 2). بنابراین، روشن شد که قابلیت اجرای GDPR ارتباطی به ملیت یک کشور عضو یا شهروند اتحادیهٔ اروپا ندارد و در مورد تمام اشخاص موضوع داده واقع در اتحادیهٔ اروپا صدق می‌کند (Kubben, Dumontier & Dekker 2019, 61).

شاخص‌های هدف قرار دادن افراد در اتحادیهٔ اروپا می‌تواند موارد زیر باشد: استفاده از زبانی که عموماً در یک یا چند کشور عضو اتحادیهٔ اروپا به‌کار می‌رود، دریافت ارزهای پذیرفته‌شده (به‌خصوص یورو)، ذکر مشتریان یا کاربران اتحادیهٔ اروپا، و امکان تحویل به یک یا چند کشور عضو اتحادیهٔ اروپا یا نام دامنهٔ وب‌گاه که به یک یا چند کشور عضو اتحادیهٔ اروپا اشاره دارد (‘xxx.com/de’, ‘xxx. es’, ...). به‌عنوان مثال، شرکت H در استرالیا یک فروشگاه آنلاین دارد. این شرکت هیچ شرکت تابعه یا نمایندگی در خارج از استرالیا ندارد و فروشگاه آنلاین‌ش تنها به زبان انگلیسی موجود است. H داده‌های

مشتری را ذخیره می‌کند. پرداخت به دلار استرالیا و همچنین یورو را می‌پذیرد و تحویل به آلمان، فرانسه و ایتالیا را ممکن می‌داند. اگر مشتریان کشورهای عضو اتحادیهٔ اروپا وب‌گاه H را فرا بخوانند، از دامنه "H.au" به "H.com/de"، "H.com/fr" و غیره هدایت می‌شوند. در این مثال، نام دامنهٔ جداگانه برای مشتریان اروپایی، امکان پرداخت به یورو و امکان تحویل به کشورهای عضو اتحادیهٔ اروپا دال بر این است که H مشتریان واقع در اتحادیهٔ اروپا را مورد هدف قرار داده است (Voigt & von dem Bussche 2017, 26 & 27). بنابراین، روشن است که ارائهٔ کالا و خدمات یا نظارت باید قصدشده و به‌طور عمدی باشد و ارائه یا نظارت اتفاقی و غیرعمدی برای اعمال GDPR کافی نیست (Futter & Shivarattan 2020, 3).

۶-۲. استثنائات از اعمال GDPR (دامنهٔ سلبی)

در این قسمت به مواردی پرداخته خواهد شد که از دامنهٔ کاربرد GDPR خارج هستند و این مقررات بر این موارد حمایتی ندارد. بر اساس مادهٔ ۲ بخش ۲ GDPR، این مقررات در مورد پردازش داده‌های شخصی زیر اعمال نمی‌شود:

الف) در جریان فعالیتِ خارج از دامنهٔ قانون‌گذاری اتحادیهٔ اروپا: این مقررات در مورد مسائل مربوط به حمایت از حقوق اساسی و آزادی‌های اساسی یا جریان آزاد داده‌های شخصیِ مربوط به فعالیت‌هایی که در صلاحیت قانون‌گذاری اتحادیهٔ اروپا نیست (Gabel & Hickman 2019, 2) و مربوط به قوانین ملی کشورهای عضو است، مانند فعالیت‌های مربوط به امنیت ملی، اعمال نمی‌شود. همچنین، این مقررات در مورد پردازش داده‌های شخصی توسط کشورهای عضو، هنگامی که فعالیت‌های خود را در رابطه با سیاست مشترک خارجی و امنیتی اتحادیه انجام می‌دهند، نیز اعمال نمی‌شود (EUR-Lex 2016, 3).

ب) اقدام شخص حقیقی در طی فعالیت صرفاً شخصی یا خانگی: این مفهوم باید بر اساس افکار عمومی اجتماعی تفسیر شود و شامل داده‌های شخصی است که برای فعالیت‌های اوقات فراغت، تفریح، تعطیلات، اهداف سرگرمی یا برای استفاده از یک شبکهٔ اجتماعی پردازش می‌شوند. لازم به ذکر است که اگر پردازش مربوط به داده‌های شخصی در بستر فعالیت‌های تجاری باشد، استثنا قابل اجرا نخواهد بود و در نتیجه، جهت حصول استثنای فعالیت‌ها، هیچ ارتباطی به فعالیت‌های حرفه‌ای یا تجاری نباید داشته باشند (European Parliament 2018, 1). کلمهٔ «صرفاً» به چنین تفسیر

مضیقی از این استثنا اشاره دارد. فعالیت تجاری شامل هرگونه فعالیت اقتصادی است، بدون توجه به اینکه آیا پرداختی وجود دارد یا خیر، و همچنین اقدامات آماده‌سازی برای امور مذکور، مانند اقدامات بازاریابی یا تجارت داده‌های شخصی برای دریافت خدمات. به‌عنوان مثال، مطابق با رأی دیوان دادگستری اتحادیهٔ اروپا (ECJ) به شماره C-۱۳/۲۱۲ مورخ ۱۱ دسامبر ۲۰۱۴، عملیات دوربین نظارتی که در آن محتوای ویدیوئی ضبط‌شده بر روی یک دستگاهِ ضبط، به‌طور مداوم ذخیره می‌شود که توسط یک فرد در خانه‌اش به‌منظور حفاظت از اموال، سلامت و زندگی صاحبان خانه نصب شده است و همچنین بر یک فضای عمومی (مانند خیابان یا پیاده‌رو عمومی) نظارت می‌کند، پردازش داده‌ها در دورهٔ فعالیت صرفاً شخصی یا خانگی محسوب نمی‌شود (CURIA 2014a, 6).

کنترل‌کننده‌ها یا پردازنده‌هایی که ابزار را برای چنین پردازش داده‌های شخصی فراهم می‌کنند، نمی‌توانند از این استثنا بهره‌مند شوند (Voigt & von dem Bussche 2017, 17).

ج) اقدام مراجع ذی‌صلاح در خصوص مسائل کیفری: به این استثنا مشروحات ۱۹ و ۲۰ GDPR اشاره کرده است، با این توضیح که حفاظت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی توسط مراجع ذی‌صلاح برای اهداف پیشگیرانه، بازرسی، تشخیص و یا تعقیب کیفری جرایم جنایی، از جمله حفاظت در برابر تهدیدات علیه امنیت عمومی و جابه‌جایی آزاد چنین داده‌هایی، موضوع یک مقررهٔ قانونی خاص اتحادیه است[1] و GDPR در خصوص فعالیت‌های پردازشی برای چنین اهدافی اعمال نمی‌شود. بنابراین، داده‌های شخصی که توسط مراجع عمومی تحت این مقررات مورد پردازش قرار می‌گیرند، زمانی که برای چنین اهدافی مورد استفاده قرار گیرند باید توسط مقررهٔ قانونی خاص اتحادیه –دستورالعمل 2016/680 (EU) – اداره شود.

1. is the subject of a specific Union legal act

این مقررهٔ قانونی خاص در بخش ۲ این پژوهش بیان شده است: دستورالعمل اتحادیه اروپا به شماره ۶۸۰/۲۰۱۶ مصوب پارلمان و شورای اروپا در تاریخ ۲۷ آوریل ۲۰۱۶ در مورد حفاظت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی توسط مقامات ذی‌صلاح به‌منظور پیشگیری، تحقیق، کشف یا تعقیب جرایم کیفری یا اجرای مجازات‌های جنایی، همچنین جریان آزاد این‌گونه داده‌ها و لغو تصمیمات شورا به شماره JHA/۹۷۷/۲۰۰۸.

د) داده‌های شخصی اشخاص متوفی: این مقررات بر داده‌های شخصی اشخاص متوفی نیز اعمال نمی‌شود. البته، کشورهای عضو ممکن است قواعد مربوط به پردازش داده‌های شخصی افراد متوفی را ارائه کنند (EUR-Lex 2016, 5).

۷. بررسی حمایت از دادهٔ شخصی توسط سایر کشورها با اثرپذیری از مقررات عمومی حفاظت از داده (GDPR)

حفاظت از داده‌های شخصی توسط کشورهای مختلف با اصطلاحات متفاوتی مورد اشاره قرار گرفته است. چنین اصطلاحاتی شامل حریم خصوصی اطلاعاتی[1]، حریم خصوصی داده[2] یا قوانین حفاظت از داده[3] هستند که تمامی آن‌ها برای یک هدف عمل می‌کنند و چارچوب‌های قانونی جهت حمایت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی هستند. تعداد و تنوع جغرافیایی قوانین حفاظت از داده از سال ۲۰۰۰ رو به گسترش است. با بررسی‌های انجام‌شده تا سال ۲۰۱۲، بیش از ۸۰ کشور از جمله تقریباً همهٔ کشورهای اروپایی قوانین جامع حفاظت از داده را تصویب کرده‌اند[4] (Greenleaf 2012, 2 & 3). در حال حاضر و با توجه به مقررات GDPR هر یک از کشورهای عضو اتحادیهٔ اروپا باید قوانین حفاظت از دادهٔ خود را بر اساس این مقررات تصویب کنند. فارغ از کشورهایی که بستری جامع در خصوص حمایت از داده‌های شخصی دارند، سایر کشورهایی که فاقد قانون و مقررات جامع برای حفاظت از داده‌ها هستند، از ترکیب اصول کلی حقوقی، قوانین و مقررات حوزه‌های دیگر جهت حفاظت از داده‌های شخصی استفاده می‌کنند (Singh 2016, 126).

روشن است که چنین حمایت‌هایی به‌صورت موردی و جزئی است؛ با این توضیح که این کشورها بستر مستقلی در خصوص حمایت ندارند، بلکه از طریق سایر قوانین و مقررات که در مفادی خاص یا در قسمتی جزئی به داده‌های شخصی و حریم خصوصی اطلاعاتی پرداخته‌اند، از چنین داده‌هایی حمایت می‌کنند. به‌عنوان نمونه، ایالات متحدهٔ آمریکا به‌دلیل فقدان قانونی جامع برای حریم خصوصی اطلاعاتی، از داده‌های شخصی به‌صورت جزئی و در خلال سایر بسترهای قانونی حمایت می‌کند؛ مانند قانون حریم خصوصی مصرف‌کنندهٔ کالیفرنیا[5]. این قانون مفاد جامعی را برای حریم خصوصی

1. information privacy 2. data privacy 3. data protection laws

۴. در منبع مذکور و در قالب جدول، فهرست این کشورها بیان شده است (Greenleaf 2012:10- 14).

5. California Consumer Privacy Act (CCPA)

مصرف‌کننده تصویب کرده است که مشابه با برخی از الزامات GDPR است. این قانون مجموعه‌ای از حقوق جدید حریم خصوصی مصرف‌کننده را ایجاد کرده است که بر اساس آن بسیاری از شرکت‌هایی که از داده‌های شخصی استفاده می‌کنند، باید فرایندهای تجاری خود را جهت تطبیق با چنین حقوق جدیدی برای مصرف‌کنندگان تغییر دهند (California's Consumer Privacy Act and Other State Privacy & Security Laws n.d.).

از میان کشورهایی که از داده‌های شخصی به‌صورت جزئی حمایت می‌کنند، می‌توان ایران را نام برد. حقوق موضوعهٔ ایران از طریق برخی مفاد قانونی، از جمله قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۸، به‌صورت موردی و جزئی از داده‌های شخصی حمایت می‌کند. توضیح اینکه در این قوانین احکامی وجود دارد که می‌توان از اطلاق و عموم آن‌ها در خصوص حمایت از داده‌های شخصی استفاده نمود.

به‌عنوان نمونه، مطابق ماده ۱۷ قانون جرایم رایانه‌ای: «هر کس به‌وسیلهٔ سیستم‌های رایانه‌ای یا مخابراتی، صوت یا تصویر یا فیلم خصوصی و خانوادگی یا اسرار دیگری را بدون رضایت او منتشر نماید یا در دسترس دیگران قرار دهد، به‌نحوی‌که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد». رضایت شخص موضوع داده جهت انتشار و دسترسی به اطلاعات خصوصی و داده‌های شخصی او لازم است، بدین‌جهت دسترسی و انتشار بدون رضایت جرم است.

همچنین، مطابق ماده ۱۴ قانون انتشار و دسترسی آزاد به اطلاعات: «چنانچه اطلاعات درخواست‌شده مربوط به حریم خصوصی اشخاص باشد و یا در زمرهٔ اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود». گرچه اصل، بر دسترسی آزاد به اطلاعات عمومی است، لیکن اگر چنین اطلاعاتی حاوی داده‌های شخصی و اطلاعات خصوصی باشد، قابل دسترسی نیستند. در واقع، این ماده به تعادل بین آزادی اطلاعات و حفاظت از دادهٔ شخصی اشاره می‌کند.

فارغ از چنین حمایت‌های جزئی، می‌توان گفت که ایران با تنظیم پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» - در تیرماه سال ۱۳۹۷ منتشرشده در سایت وزارت

ارتباطات و فناوری اطلاعات ایران[۱]- به‌عنوان سندی مستقل، در جهت حمایت از داده‌های شخصی گام برداشته است. لیکن باید گفت چنین سندی هنوز پیش‌نویس است و تاکنون حتی نسخهٔ نهایی برای این پیش‌نویس منتشر نشده است. بدین جهت استدلال و استناد به چنین سندی از قوت کافی برخوردار نیست. در عین حال، با بررسی این سند روشن است که پیش‌نویس مذکور از شفافیت و دقت کافی نیز برخوردار نیست و بدین‌جهت در مقام عمل، استفاده از آن دشوار است. به‌عنوان نمونهٔ طبق بند الف ماده ۲ این پیش‌نویس، دادهٔ شخصی این‌گونه تعریف شده است: «دادهٔ شخصی عبارت است از داده‌ای که به‌تنهایی یا به همراه داده‌های دیگر، مستقیم یا غیرمستقیم شخصِ موضوع داده را از طریق ارجاع به یک شناسه می‌شناساند». اگر این تعریف با تعریف دادهٔ شخصی در همین پژوهش مقایسه شود، غیردقیق بودن آن واضح است، چرا که از این ماده معلوم نیست که دادهٔ شخصی منحصر در اشخاص حقیقی است یا اشخاص حقوقی را نیز دربردارد، در حالی که در بسترهای قانونی کشورهای مختلف حمایت از داده‌های شخصی ناظر بر اشخاص حقیقی است و به این امر در چنین بسترهای قانونی اشاره شده است و دامنهٔ اعمال واضح است، چرا که مجمل و مبهم بودن یک سند قانونی مسیر را برای تفسیرهای گوناگون و در نتیجه، اختلاف عملی هموار می‌سازد.

همچنین، مطابق بند ب ماده ۳ این پیش‌نویس، در خصوص دامنهٔ شمول: «اتباع خارجی حقیقی یا حقوقی عمومی یا خصوصی که داده‌های شخصی آن‌ها از سوی کنترل‌کننده یا پردازشگر ایرانی پردازش می‌شود» تحت دامنهٔ این سند هستند. اگر این مفاد با بند مربوطه این پژوهش در خصوص دامنهٔ ایجابی GDPR مقایسه شود، روشن می‌شود که دامنهٔ اعمال باید دقیق‌تر باشد و صراحت داشته باشد و ابهامی ایجاد نکند. به‌عنوان نمونه، در مورد اتباع خارجی اگر کنترل‌کنندگان مشترک باشند و تنها یکی از آن‌ها ایرانی باشد یا حالتی که کنترل‌کننده خارجی و پردازنده ایرانی باشد، محل ابهام این دامنه است و معلوم نیست که تحت شمول این سند ایرانی است یا خیر. گرچه دامنهٔ اعمال GDPR

---

۱. لینک دسترسی به پیش‌نویس لایحه:
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

نیـز در مـاده ۳، توسـط هیئـت حفاظـت از دادهٔ اتحادیـهٔ اروپـا کامـل شـده اسـت، امـا ایـن هیئـت توسـط GDPR ایجادشـده و نهـادی مسـتقل بـا وظایفـی واضـح اسـت –چنیـن وظایفـی در مـاده ۷۰ GDPR بیـان شـده اسـت کـه شـامل تفسـیر و شفاف‌سـازی ایـن مقـررات اسـت– (EUR-Lex, 2016: 76-78)؛ در حالـی کـه مشـابه ایـن هیئـت در سـند ایرانـی –جهـت شفاف‌سـازی مفـاد ایـن سـند– بیـان نشـده و صرفـاً در مـادهٔ ۳۹ پیش‌نویـس، مراجـع و نهادهایـی بـرای تنظیـم و نظـارت بـر پـردازش داده‌هـای شـخصی معرفی‌شـده اسـت کـه چنیـن مراجـع و نهادهایـی به‌صـورت تخصصـی و مسـتقل در زمینـهٔ حفاظـت از داده عمـل نمی‌کننـد و بدیـن ترتیـب، بـه نظـر می‌رسـد کـه در زمینـهٔ شفاف‌سـازی سـند ایرانـی کمـک چندانـی نخواهنـد کـرد.

همچنیـن، می‌تـوان گفـت ضمانـت اجراهـای مناسـبی نیـز بـرای تعـرض بـه داده‌هـای شـخصی پیش‌بینـی نشـده اسـت. به‌عنـوان نمونـه، مجـازات در بخـش مسـئولیت کیفـری ایـن پیش‌نویـس –مـواد ۶۵ الـی ۶۸– بـه تعزیـرات قانـون مجـازات اسـلامی ارجـاع داده شـده. گرچـه چنیـن ارجاعـی بـدون ایـراد اسـت، لیکـن ایـن امـر زمانـی مناسـب اسـت کـه تعزیـرات قانـون مجـازات اسـلامی مطابـق بـا مـاده ۲۸ ایـن قانـون[1] در خصـوص جـزای نقـدی اثـر بازدارندگـی داشـته باشـد، در حالـی کـه بازدارندگـی جـزای نقـدی در تعزیـرات قانـون مجـازات خـود محـلِ بحـث بسـیار اسـت. بدیـن جهـت بهتـر بـود ماننـد مـادهٔ ۸۳ GDPR مبالغـی کـه متناسـب بـا تـورم موجـود در جامعـه کافـی باشـد، معیـن گـردد تـا اثـر بازدارندگـی بهتـری داشـته باشـد. البتـه، ذکـر مبلـغ معیـن بایـد همـراه بـا تعدیـل متناسـب بـا تـورم باشـد تـا جنبـهٔ بازدارندگـی حفـظ شـود یـا تعییـن جـزای نقـدی بـر اسـاس و بـه میـزان ضـرر وارده بـه شـخص موضـوع داده در جهـت جبـران هرچـه بهتـر خسـارت و برگردانـدن زیان‌دیـده بـه حالـت قبـل از نقـض دادهٔ شـخصی، نظیـر آنچـه در مـادهٔ ۱ قانـون تشـدید مجـازات مرتکبیـن ارتشـا و اختـلاس و کلاهبـرداری[2] بیـان شـده اسـت.

---

۱. مـاده ۲۸ قانـون مجـازات اسـلامی: «کلیـهٔ مبالـغ مذکـور در ایـن قانـون و سـایر قوانیـن از جملـه مجـازات نقـدی، بـه تناسـب نـرخ تـورم اعلام‌شـده به‌وسـیلهٔ بانـک مرکـزی هـر سـه سـال یک‌بـار بـه پیشـنهاد وزیـر دادگسـتری و تصویـب هیئـت وزیـران تعدیـل و در مـورد احکامـی کـه بعـد از آن صـادر می‌شـود، لازم‌الاجـرا می‌گـردد».

۲. مـاده ۱ قانـون تشـدید مجـازات مرتکبیـن ارتشـا و اختـلاس و کلاهبـرداری: «هـر کـس از راه حیلـه و تقلـب مـردم را به‌وجـود شـرکت‌ها یـا تجارتخانه‌هـا یـا کارخانه‌هـا یـا مؤسسـات موهـوم یـا بـه داشـتن امـوال و اختیـارات واهـی فریـب دهـد یـا بـه امـور غیرواقـع امیـدوار نمایـد یـا از حـوادث و پیش‌آمدهـای غیرواقـع بترسـاند و یـا اسـم و یـا عنـوان مجعـول اختیـار کنـد و بـه یکـی از وسـایل مذکـور و یـا وسـایل تقلبـی دیگـر وجـوه و یـا امـوال یـا اسـناد یـا حوالجـات یـا قبـوض یـا مفاصـا حسـاب و امثـال آن‌هـا تحصیـل کـرده و از ایـن راه مـال دیگـری را ببـرد، کلاهبـردار محسـوب و عـلاوه بـر رد اصـل مـال بـه صاحبـش، بـه حبـس از یـک تـا ۷ سـال و پرداخـت جـزای نقـدی معـادل مالـی کـه اخـذ کـرده اسـت، محکـوم می‌شـود».

در نهایت، باید گفت که پیش‌نویس لایحهٔ ایرانی متخذ از GDPR بوده و در واقع، ترجمه‌ای غیردقیق و مختصر از این مقررات است. اما باید به این نکته توجه نمود که یک سند قانونی وقتی کامل و کارآمد است که متناسب با ظرفیت‌ها و نواقص یک نظام حقوقی خاص تنظیم شود و صرف ترجمه کفایت نمی‌کند.

۸. مهم‌ترین نقاط قوت مقررات عمومی حفاظت از داده (GDPR)

در سال‌های اخیر پیشرفت‌های عمده‌ای که در فناوری اطلاعات رخ‌داده، تغییرات اساسی در روش‌هایی که اشخاص و سازمان‌ها با یکدیگر ارتباط برقرار می‌کنند و داده‌های شخصی و اطلاعات را به اشتراک می‌گذارند، به ارمغان آورده است. با وجود این تحولات، حمایت‌های جامعی از افرادی که اطلاعات و داده‌های شخصی آن‌ها در موارد مختلف استفاده می‌شد، وجود نداشت و ضرورت حمایت قانونی مؤثر از این امر احساس می‌شد تا اینکه مقررات جدید حفاظت از داده، GDPR، تصویب شد.

با مقایسه و بررسی مفاد اسناد قانونیِ کشورهای مختلف، که غالباً از GDPR تأثیر گرفته‌اند، و سند قانونی سابقِ اتحادیهٔ اروپا در خصوص حفاظت از دادهٔ شخصی روشن شد که این مقررات نقاط قوت برجسته‌ای دارد که در عمل موجب شفاف‌سازی پردازش داده‌های شخصی و کنترل بیشتر افراد بر روی داده‌های شخصی خود شده است. چنین نتایجی بر اساس منطق حقوقی که مستلزم ایجاد عدالت و انصاف است، دارای اعتبار است. مهم‌ترین نقاط قوت مذکور که این مقررات را متمایز می‌سازد، به‌شرح زیر است:

الف) وحدت قانونی (یک قاره، یک قانون): یک قانون واحد اروپایی برای حفاظت از داده، جای‌گزین قوانین کنونی ملی شده و تمام شرکت‌ها، نهادها، سازمان‌ها و افراد با یک قانون سروکار دارند (EC n.d.).

ب) توجه خاص نسبت به داده‌های حساس[1]: دسته‌های خاصی از داده‌های شخصی، «حساس» تلقی می‌شوند و بر اساس GDPR حفاظت خاص می‌شوند. داده‌هایی که مبیّن ریشهٔ نژادی یا قومی، عقاید سیاسی، باورهای دینی یا فلسفی، عضویت در اتحادیهٔ صنفی[2] زندگی جنسی یا جهت‌گیری جنسی، داده‌های ژنتیکی، داده‌های زیست‌شناختی[3] به‌منظور شناسایی منحصربه‌فرد یک شخص حقیقی، و داده‌های

1. sensitive data
2. trade union membership
3. biometric data

مربوط به سلامت، حساس تلقی می‌شوند. به چنین داده‌هایی در ماده ۹ بخش ۱ GDPR اشاره شده است (EUR-Lex 2016, 38). به‌عنوان یک قاعدهٔ کلی، پردازش انواع داده‌های مذکور ممنوع است. البته، بر این ممنوعیت استثناهایی نیز وجود دارد؛ مانند قانونی که نوع خاصی از پردازش داده‌های حساس را برای هدفی خاص در ارتباط با منافع عمومی یا سلامت، مجاز بداند (European Commission, n.d.-b).

ج) معرفی ابزارهای جدید جهت تقویت حفاظت از دادهٔ شخصی: GDPR چند ابزار جدید برای کمک به کنترل‌کنندگان داده جهت نشان دادن انطباق با مفاد این مقررات ارائه می‌دهد. منشورهای رفتاری[1] مقرر در مواد ۴۰ و ۴۱ GDPR و مکانیسم گواهینامه[2] مقرر در مواد ۴۲ و ۴۳، از جملهٔ این ابزارهای جدید است (EC.European Commission 2019, 15).

در خصوص تعریف این ابزارها باید گفت که منشور رفتاری در نگاه GDPR از ابزارهای پاسخگویی داوطلبانه است که به ماهیت‌های پردازش‌کنندهٔ داده این امکان را می‌دهد که چالش‌های کلیدی در زمینهٔ حفاظت از داده را در شرکت، سازمان و نهاد خود شناسایی کند و در جهت رفع آن، اقدامات مناسب را در نظر گیرد. با وجود منشور رفتاری، کنترل‌کننده‌ها و پردازنده‌ها می‌توانند اطمینان حاصل کنند که آن‌ها GDPR را به‌طوری مؤثر اعمال می‌کنند (ICO 2018a). مکانیسم گواهینامه نیز روشِ صدور گواهی برای یک محصول، فرایند یا سرویس خاصی است. بر اساس GDPR[3]، گواهینامه‌ها نیز ابزاری داوطلبانه برای کنترل‌کننده‌ها یا پردازنده‌ها جهت افزایش شفافیت و نشان دادن انطباق با GDPR در راستای اصل پاسخگویی و قادر ساختن افراد به ارزیابی سریعِ سطح حفاظت از دادهٔ کالاها و خدمات مربوط هستند (Practical Law n.d.-a).

د) حمایت‌های فرامرزی: با وجود این مقررات، شرکت‌های اروپایی باید به استانداردهای سخت‌تری نسبت به شرکت‌های خارج از اتحادیهٔ اروپا پای‌بند باشند و همچنین، در بازار واحد، تجارت انجام دهند. لیکن این مقررات بر شرکت‌های مستقر در خارج از اتحادیهٔ اروپا، در زمانی که به اتحادیهٔ اروپا ارائهٔ کالا یا خدمات دارند، نیز جاری

1. codes of conduct (COC) 2. certification mechanism

۳. البته، GDPR، اصطلاحات مربوط به مکانیسم گواهینامه را تعریف نکرده است و این تعاریف از منابع دیگر و با توجه به رویکرد GDPR استنباط می‌شود (European Commission 2019a, 4).

است[1] (Ganotra 2018, 4).

ه) پاسخ‌گویی بیشتر: طبق این مقررات، کنترل‌کننده و پردازنده‌ها نسبت به افرادی که داده‌هایشان را جمع‌آوری و پردازش می‌کنند، باید پاسخگویی حداکثری داشته باشند و این مقررات مجازات سخت‌تری را نسبت به قوانین سابق حفاظت از داده، برای کسانی که از GDPR پیروی نمی‌کنند، وضع می‌کند؛ مانند وضع جریمه‌های نقدی مطابق ماده ۸۳ GDPR – (EUR-Lex 2016, 82).

و) پیگیری مستمر: پردازش داده‌های شخص تنها بر اساس رضایت اشخاص حقیقی یا مبانی قانونی مجاز است. بدین جهت کنترل‌کننده و پردازنده باید سابقهٔ زمانی و چگونگی رضایت شخص حقیقی و سایر مبانی قانونی را در نظر بگیرند و به‌طور مستمر وجود مبانی قانونی پردازش را بررسی کنند (Reini 2019, 32).

ز) وجود حقوق مختلف برای اشخاص موضوع داده: شخص موضوع داده از نگاه GDPR حقوق مختلفی دارد. چنین حقوقی در مواد ۱۲ الی ۲۳ GDPR بیان شده است. برخی از این حقوق در قوانین سابق حفاظت از دادهٔ اروپا موجود بوده، لیکن توسط GDPR تقویت شده است؛ مانند حق حذف (فراموش شدن) مقرر در ماده ۱۷. برخی نیز توسط GDPR برای اولین بار، مانند حق انتقال داده مقرر در ماده ۲۰، معرفی شده است. برخی از این حقوق عبارت‌اند از:

- حق حذف (فراموش‌شدن): اگر اشخاص موضوع داده رضایت خود را نسبت به پردازش پس بگیرند و در عین حال، هیچ مبنای مشروع و قانونی برای پردازش وجود نداشته باشد، پردازش غیرقانونی است و باید تمامی داده‌ها حذف و فراموش شود (Politou, Alepis & Patsakis 2018, 11).
- حق تصحیح: حق تصحیح مبین «اصل صحت»، به موجب ماده ۵ بخش ۱ بند د GDPR است. طبق این اصل داده‌های پردازش‌شده، در هر زمان معین باید واقعیت را منعکس کنند (Finck 2018, 29).
- حق انتقال داده: حقی جدید بر اساس GDPR است. بر اساس این حق اشخاص موضوع داده می‌توانند درخواست انتقال داده‌هایشان را به کنترل‌کنندهٔ دیگری بدهند. به‌طوری که شخص موضوع داده بتواند بهتر از داده‌های خود استفاده کند

۱. تفصیل دامنهٔ اعمال GDPR، در بخش ششم این پژوهش بیان شد.

(Chassang et al. 2018, 297).

□ حق شفافیت جمع‌آوری داده و حق دسترسی: کنترل‌کننده‌ها و پردازنده‌ها باید روشن کنند که چگونه داده‌های شخصی افراد را جمع‌آوری می‌کنند، برای چه هدفی از آن استفاده می‌کنند و چگونه داده‌ها را پردازش می‌کنند. این موارد باید به‌طور واضح و با زبانی قابل فهم برای شخص موضوع داده بیان شود. همچنین، اشخاص موضوع داده حق دسترسی به هرگونه اطلاعات و داده‌های خود را دارند (Consumers International 2019, 3).

۹. نتیجه‌گیری

بستهٔ اصلاحات قوانین حفاظت از دادهٔ اتحادیهٔ اروپا که در ماه ژانویه ۲۰۱۲ آغاز شده بود، منجر به سه بخش کلیدی در قانون‌گذاری در مورد حمایت از داده‌ها شد. یکی از این بخش‌ها، مقررات عمومی حفاظت از داده (GDPR) است که در خصوص حفاظت از اشخاص حقیقی نسبت به پردازش دادهٔ شخصی آن‌ها و جریان آزاد چنین داده‌هایی است.

مطابق یافته‌های این پژوهش، دادهٔ شخصی در تعریف GDPR، به معنای هر اطلاعاتی است که مربوط به شخص حقیقی شناخته‌شده یا قابل شناسایی (شخص موضوع داده) است. یک فرد حقیقی قابل شناسایی کسی است که به‌طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به یک شناسه از جمله نام، شمارهٔ شناسایی، اطلاعات مکانی، شناسهٔ آنلاین یا به یک یا چند ویژگی خاص مانند هویت فیزیکی، فیزیولوژیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی شناسایی شود. پردازش نیز به معنای عملیات یا مجموعه‌ای از عملیات است که بر روی دادهٔ شخصی یا مجموعهٔ داده‌های شخصی، چه با وسایل خودکار و چه غیر آن صورت گیرد.

افزون بر این، در این پژوهش روشن شد که GDPR دامنهٔ اعمال مشخصی دارد که شامل دامنهٔ ایجابی و سلبی است. در خصوص دامنهٔ ایجابی باید گفت که مطابق GDPR، این مقررات در مورد پردازش دادهٔ شخصی در زمینهٔ فعالیت‌های کنترل‌کننده یا پردازنده‌ای که در اتحادیهٔ اروپا مستقر هستند، اعمال می‌شود که در واقع، مبین معیار «مقر» است. همچنین، این مقررات برای پردازش دادهٔ شخصیِ اشخاصِ موضوع داده‌ای که در اتحادیهٔ اروپا هستند و پردازش داده‌هایشان توسط کنترل‌کننده یا پردازنده‌ای که در اتحادیهٔ اروپا مستقر نشده‌اند، انجام می‌شود، نیز اعمال می‌شود؛ درصورتی‌که فعالیت‌های پردازش،

مربوط به ارائهٔ کالا یا خدمات به اشخاص موضوع داده در اتحادیهٔ اروپا یا نظارت بر رفتار اشخاصِ موضوع داده در اتحادیهٔ اروپا باشد و مشروط به اینکه چنین ارائهٔ کالا و خدمات یا نظارتی هدفمند باشد که مبین معیار «هدف» است. در خصوص دامنهٔ سلبی نیز می‌توان از مواردی یاد نمود که از قلمرو GDPR خارج هستند و این موارد، فعالیت‌های خارج از قلمرو قانون‌گذاری اتحادیهٔ اروپا، اقدام شخص حقیقی در طی فعالیت صرفاً شخصی یا خانگی و اقدامات مراجع ذی‌صلاح در خصوص مسایل کیفری است.

GDPR در مقایسه با سندهای مشابه در اتحادیهٔ اروپا (مقررات و دستورالعمل‌های سابق) و سایر کشورها، دارای نقاط قوت برجسته‌ای است که این مقررات را از سندهای دیگر متمایز می‌سازد. چنین نقاط قوتی شامل ایجاد وحدت قانونی، توجه خاص نسبت به داده‌های شخصی حساس، معرفی ابزارهای جدید جهت حمایت حداکثری از داده‌های شخصی، پاسخ‌گویی بیشتر، حمایت‌های فرامرزی، پیگیری‌های مستمر و اعطای حقوق مختلف به اشخاص موضوع داده است.

سرانجام باید گفت که شفاف‌سازی مفاد GDPR و مباحث مذکور در این پژوهش می‌تواند جهت تقویت پیش‌نویس لایحهٔ ایرانی در خصوص حمایت از داده‌های شخصی و رفع خلأهای موجود مؤثر باشد.

فهرست منابع

ابن ادریس حلی، محمدبن احمد. ۱۳۸۷. *موسوعهٔ ابن إدریس الحلی*. قم: دلیل ما.

حسینی عاملی، محمدجواد بن محمد. بی‌تا. *مفتاح الکرامهٔ فی شرح قواعد العلامهٔ*. بیروت: دار إحیاء التراث العربی.

سیستانی، علی. ۱۴۱۵ ه.ق. *منهاج الصالحین*. قم: مکتب آیه‌الله العظمی السید السیستانی.

شهید ثانی، زین‌الدین. ۱۴۱۰ ه.ق. *الروضهٔ البهیهٔ فی شرح اللمعهٔ الدمشقیهٔ*. قم: مکتبهٔ الداوری.

شیخ طوسی، محمدبن حسن. ۱۳۸۷ ه.ق. *المبسوط فی فقه الإمامیهٔ*. تهران: مکتبهٔ المرتضویهٔ.

علامه حلی، حسن بن یوسف. ۱۴۲۰ ه.ق. *تحریر الأحکام الشرعیهٔ علی مذهب الإمامیهٔ*. قم: مؤسسهٔ الإمام الصادق علیه‌السلام.

کاتوزیان، ناصر. ۱۳۹۶. *عقود معین ۲*. تهران: گنج دانش.

References

Ahmed, J. U. 2010. Documentary Research Method: New Dimensions. *Indus Journal of Management & Social Science (IJMSS)* 4 (1): 1–14.

Allison, S. 2009. the Concept of Personal Data Under the Data Protection Regime. *Edinburgh Student Law Review* 1: 48–65.

Baker McKenzie. 2019. *EDPB - Guidelines on the Territorial Scope of the GDPR (Art. 3) and on Representatives (Art. 27) – Now adopted after public consultation* (pp. 1–6). https://www.bakermckenzie.com/en/insight/publications/2019/12/guidelines-on-the-territorial-scope-of-gdpr (accessed June 16, 2020)

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

California's Consumer Privacy Act and Other State Privacy & Security Laws. (n.d.). Morgan Lewis. Retrieved from https://www.morganlewis.com/topics/ccpa-and-state-privacy-security-laws (accessed Oct. 4, 2020)

Chassang, G., T. Southerington, M. Boeckhout, & S. Slokenberga. 2018. Data Portability in Health Research and Biobanking: Legal Benchmarks for Appropriate Implementation. *European Data Protection Law Review* 3: 297–307.

Colcelli, V. 2019. Joint Controller Agreement Under Gdpr. *Eu and Member States – Legal and Economic Issues* 3: 1030–1047.

Consumers International. 2019. *The state of data protection rules around the world* (pp. 1–7). https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf (accessed April 8, 2020)

Curia. 2014a. *František Ryneš v Úřad pro ochranu osobních údajů,In Case C-212/13* (Issue December).

Curia. 2014b. *Google Spain v. Agencia Española de Protección de Datos (AEPD) and Costeja González,In Case C-131/12* (Issue May).

EC. European Commission. (n.d.). *Can someone else process the data on my organisation's behalf? | European Commission*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/can-someone-else-process-data-my-organisations-behalf_en (accessed March 12, 2020)

_____. 2019. *Data Protection Certification Mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679* (pp. 1–255).

EC, E. C. (n.d.). *Questions and Answers – General Data Protection Regulation*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387 (accessed Feb. 13, 2020)

EDPB. 2019. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*. *November*, 1–23. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_0.pdf (accessed May 9, 2020)

_____. (n.d.). *The History of the General Data Protection Regulation*. Retrieved from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (accessed Feb. 11, 2020)

EUR-Lex. 2012a. 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 (accessed March 18, 2020)

_____. 2012b. Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union*, 47–390. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN (accessed Mrch 18, 2020)

_____. 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 (accessed July 21, 2020)

European Commission. (n.d.-a). Data protection in the EU. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (accessed Jan. 16, 2021)

_____. (n.d.-b). How is data on my religious beliefs/sexual orientation/health/political views protected? Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-data-my-religious-beliefs-sexual-orientation-health-political-views-protected_en (accessed March 9, 2020)

_____. 2016. Data protection in the EU | European Commission. Data Protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (accessed Feb. 14, 2020)

_____. 2018a. What is a data controller or a data processor? | European Commission. Ec.Europa.Eu. 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 (accessed Dec. 19, 2019)

_____. 2018b. Who does the data protection law apply to? Ec.Europa.Eu. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en (accessed April 1, 2020)

_____. 2019a. What constitutes data processing? | European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en (accessed July 7, 2020)

_____. 2019b. What is personal data. European Commission Policies, Information and Services. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (accessed Aug. 6, 2020)

European Data Protection Supervisor. (n.d.). Legislation. Retrieved from https://edps.europa.eu/data-protection/data-protection/legislation_en (accessed Feb. 11, 2020)

European Parliament. 2018. Petition No 0497/2018 by D.B. (German) on the General Data Protection Regulation (GDPR) (pp. 1–2). https://www.europarl.europa.eu/doceo/document/PETI-CM-631840_EN.pdf?redirect (accessed Dec. 17, 2019)

Feijóo, C., J. L. Gómez-Barroso, & P. Voigt. 2014. Exploring the economic value of personal information from firms' financial statements. *International Journal of Information Management*, 34 (2): 248–256. https://doi.org/10.1016/j.ijinfomgt.2013.12.005

Finck, M. 2018. Blockchains and Data Protection in the European Union. *European Data Protection Law Review* 4 (1): 17–35.

Futter, D., & G. Shivarattan. 2020. *Territorial scope of the GDPR - Where does the boundary lie ?* (pp. 1–5). https://www.ashurst.com/en/news-and-insights/legal-updates/territorial-scope-of-the-gdpr---where-does-the-boundary-lie/ (accessed August. 6, 2020)

Gabel, D., & T. Hickman. 2019. Chapter 3: Subject matter and scope – Unlocking the EU General Data Protection Regulation. *White & Case*, 1–3. https://www.whitecase.com/publications/article/chapter-3-subject-matter-and-scope-unlocking-eu-general-data-protection (accessed Feb. 3, 2020)

Ganotra, S. 2018. *GDPR Compliant or Not Court Uncourt 5* (6): 1–4

Goethem, A. van. 2018. *The Effects of Brexit on Gdpr Implementation An Investigation into Data Protection Legislation within the United Kingdom* (pp. 1–62). U.K.: Leiden University.

Greenleaf, G. 2012. Global Data Privacy Laws: 89 Countries, and Accelerating. *Privacy Laws & Business International Report* 115: 1–14.

Information Commissioner's Office. 2018a. 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/ (accessed June. 5, 2020)

_____. 2018b. What are 'controllers' and 'processors'? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/ (accessed Dec. 16, 2020)

Jan Philipp, A. 2016. How the GDPR Will Change the World. In *European Data Protection Law Review* 2 (3): 287–289.

Korpisaari, P. 2019. Finland: A Brief Overview of the GDPR Implementation. *European Data Protection Law Review* 5 (2): 232–237.

Kubben, P., M. Dumontier, & A. Dekker. (Eds.). 2019. *Fundamentals of Clinical Data Science*. Cham :Springer International Publishing.

Legifrance. (n.d.). french Code civil. Retrieved from https://www.legifrance.gouv.fr/affichCode.do;jsessionid=529DE05A50A7DBD1C42C6A0C93B4F259.tplgfr34s_2?idSectionTA=LEGISCTA000006136404&cidTexte=LEGITEXT000006070721 &dateTexte=20200812 (accessed Aug. 12, 2020)

Marelli, L., & G. Testa. 2018. Scrutinizing the EU General Data Protection Regulation How will new decentralized governance impact research? *Science*, 496–498. https://doi.org/10.1126/science.aar5419 (accessed Feb. 15. 2020)

OECD. 2010. The economics of personal data and privacy: 30 years after the OECD guidelines. http://www.oecd.org/internet/ieconomy/theeconomicsofpersonaldataandprivacy30yearsaftertheoecd privacyguidelines.htm (accessed April 25, 2020)

Olivi, G. 2019. Are we subject to GDPR ? The territorial scope criteria under the new EDPB Guidelines. Mondaq. https://www.mondaq.com/italy/privacy-protection/871206/are-we-subject-to-gdpr-the-territorial-scope-criteria-under-the-new-edpb-guidelines (accessed August 22, 2021)

Politou, E., E. Alepis, & C. Patsakis. 2018. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* 4 (1): 1–20. https://doi.org/10.1093/cybsec/tyy001

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

_____. (n.d.-b). *Recital (EU)*. Retrieved August 11, 2020, from https://uk.practicallaw.thomsonreuters.com/w-009-6368?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (accessed June 10, 2020)

Purtova, N. 2018. The law of everything Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 40–81. https://doi.org/10.1080/17579961.2018.1452176 (accessed July 6, 2020)

Reini, P. 2019. *GDPR implementation Case: Headpower Oy* [University of Transport and Communications]. https://www.theseus.fi/bitstream/handle/10024/166514/Reini_k7696_thesis_versio4.1.pdf?sequence=2 (accessed May 19, 2020)

Sabti, S. A., & Y. R. Subbaiah. 2017. Conceptual analysis of sub Delegation: An overview. *International Journal of Law*, 3 (3): 75–79. www.lawjournals.org

Serzhanova, V. 2012. *Personal Data Protection in the European Union under the Treaty of Lisbon*. Poland: University of Rzeszow (Poland).

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

Spindler, G., & P. Schmechel. 2016. Personal Data and Encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7177–163 :.

Taylor, M. J. 2006. Data Protection: Too Personal to protect? *SCRIPT-Ed*, 381–71 :(1) . https://doi.org/10.2966/scrip.030106.71

University of Oxford. 2018. *Data Protection and Research* (Issue March, pp. 1–17). https://researchsupport.admin.ox.ac.uk/sites/default/files/researchsupport/documents/media/data_protection_and_researchpdf (accessed Dec. 12, 2019)

Viorescu, R. 2017, 2018. Reform Of Eu Data Protection Rules. In *European Journal of Law and Public Administration* (pp. 27–39). https://doi.org/10.18662/eljpa/11 (accessed Feb. 28, 2019)

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

مهدیه لطیف‌زاده

متولد سال ۱۳۷۱، دانشجوی دکتری حقوق خصوصی دانشگاه فردوسی مشهد است.

حفاظت از داده و حریم خصوصی، حقوق مدنی و نیز فقه امامیه از جمله علایق پژوهشی وی است.

سید محمدمهدی قبولی درافشان

متولد سال ۱۳۵۶، دارای مدرک تحصیلی دکتری در رشتهٔ حقوق خصوصی از دانشگاه تهران است. ایشان هم‌اکنون دانشیار گروه حقوق خصوصی دانشگاه فردوسی مشهد است.

حوزه‌های مختلف حقوق خصوصی از قبیل حقوق قراردادها، مسئولیت مدنی، حقوق خانواده و نیز حقوق مالکیت‌های فکری از جمله علایق پژوهشی وی است.

سعید محسنی

متولد سال ۱۳۵۴، دارای مدرک تحصیلی دکتری در رشتهٔ حقوق خصوصی از دانشگاه امام صادق علیه‌السلام است. ایشان هم‌اکنون دانشیار گروه حقوق خصوصی دانشگاه فردوسی مشهد است.

حقوق تجارت و حقوق مالکیت فکری از جمله علایق پژوهشی وی است.

محمد عابدی

متولد سال ۱۳۵۳، دارای مدرک تحصیلی دکتری در رشتهٔ حقوق خصوصی از دانشگاه تهران است. ایشان هم‌اکنون استادیار گروه حقوق خصوصی دانشگاه فردوسی مشهد است.

تحقیق در زمینهٔ حقوق مسئولیت مدنی، حقوق قراردادها و حقوق بشر و خانواده از جمله علایق پژوهشی وی است.