آموزه‌های فقه مدنی، دانشگاه علوم اسلامی رضوی، دورهٔ پانزدهم، شمارهٔ ۲۷، بهار ـ تابستان ۱۴۰۲
نوع مقاله: علمی ـ پژوهشی (۲۴۵ـ۲۸۶)

تعهدات پردازش‌کنندهٔ داده شخصی در اتحادیه اروپا

و امکان‌سنجی پذیرش آن در حقوق ایران*

□ مهدیه لطیف‌زاده[۱]
□ سیدمحمدمهدی قبولی درافشان[۲]
□ سعید محسنی[۳]
□ محمد عابدی[۴]

چکیده

با تصویب مقررات عمومی حفاظت از دادهٔ اتحادیه اروپا (GDPR)، تمامی

* تاریخ دریافت: ۱۴۰۰/۴/۲۱ ـ تاریخ پذیرش: ۱۴۰۱/۵/۹.
این اثر تحت حمایت مادی صندوق حمایت از پژوهشگران و فناوران کشور (INSF) برگرفته از طرح شماره ۹۸۰۲۸۶۸۹ انجام شده است.

۱. دانشجوی دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران (m.latifzadeh@mail.um.ac.ir).
۲. دانشیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران (نویسنده مسئول) (ghaboli@um.ac.ir).
۳. دانشیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران (s-mohseni@um.ac.ir).
۴. استادیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران (dr.m.abedi@um.ac.ir).

کشورهای عضو اتحادیه اروپا، ملزم به حمایت حداکثری نسبت به داده‌های شخصی هستند. در راستای تحقق کامل این حمایت‌ها، اشخاص پردازش کنندهٔ داده، ملزم به رعایت تعهدات مختلفی به موجب این مقررات هستند. این تعهدات در مواد مختلف GDPR به هدف حفاظت مؤثر از داده‌های شخصی و اشخاص موضوع داده بیان شده‌اند. با تبیین تعهدات مذکور از نگاه مقررات اروپاییِ مربوط به دادهٔ شخصی، مشخص شد که نظام حقوقی ایران چنین تعهداتی را مورد تصریح قرار نداده است و صرفاً کلیات این تعهدات از منابع مختلف حقوق ایران مانند قوانین موضوعه، مبانی حقوق ایران و فقه امامیه قابل استنباط است. باید گفت که این اشارات ضمنی در جهت تبیین دقیق تعهدات مختلفِ اشخاص پردازش کنندهٔ داده کافی نیست و شفافیت جزئیات این امر نیاز به تصریح قانون‌گذار دارد. در این راستا، این پژوهش مفاد پیشنهادی در خصوص تعهدات مختلف اشخاص پردازش کنندهٔ داده، از جمله در خصوص مسئولیت کنترل‌کننده نسبت به فرایند پردازش، تعهد کنترل‌کننده نسبت به انتخاب پردازنده مناسب، حفظ سوابق فعالیت‌های پردازش، همکاری با مراجع نظارتی، تضمین امنیت پردازش، اطلاع‌رسانی و ابلاغ نقض دادهٔ شخصی به مراجع نظارتی و اشخاص موضوع داده و انتصاب مأمور حفاظت از داده، ارائه نموده است.

واژگان کلیدی: دادهٔ شخصی، پردازنده، شخص موضوع داده، کنترل‌کننده، مقررات عمومی حفاظت از داده (GDPR).

مقدمه

حمایت جامع از داده‌های شخصی و اشخاص موضوع داده در برخی نظام‌های حقوقی مانند اتحادیه اروپا به گونه‌ای مناسب مورد توجه قانون‌گذار قرار گرفته است. در این راستا در سال ۲۰۱۶، پارلمان و شورای اروپا جامع‌ترین بستر قانونی در خصوص حمایت از داده‌های شخصی، یعنی مقررات عمومی حفاظت از داده (GDPR)[1] ـزین‌پس GDPRـ را تصویب نمودند. دادهٔ شخصی مطابق با 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 به طور مستقیم یا

1. General Data Protection Regulation (GDPR).

غیر مستقیم، به ویژه با ارجاع به یک شناسه از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه برخط 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). این مقررات از سال ۲۰۱۸ در تمامی کشورهای عضو اتحادیه اروپا لازم‌الاجرا شده است. گرچه اتحادیه اروپا در خصوص حفاظت از دادهٔ شخصی سابقاً نیز قانون‌گذاری کرده بود (دستورالعمل حفاظت از دادهٔ شخصی سال ۱۹۹۵)، لیکن GDPR به دلیل حمایت‌های بدیع و دقیق خود، کامل‌ترین بستر قانونی در خصوص حمایت از داده‌های شخصی است که به جنبه‌های مختلف حمایت از داده‌های شخصی ورود نموده است. این مقررات از یکسو در جهت حمایت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی‌شان، و از سویی دیگر در خصوص جریان آزاد چنین داده‌هایی در اتحادیه اروپاست. GDPR به اشخاص حقیقی، حقوق ویژه در مورد حفاظت از داده شخصی‌شان اعطا می‌نماید و در مقابل، اشخاص پردازش‌کنندهٔ داده‌های شخصی (کنترل‌کننده‌ها[۱] و پردازنده‌ها[۲]) را ملزم به رعایت تعهدات خاصی نسبت به پردازش[۳] می‌نماید (Jones, 2009). به عبارت دیگر با تصویب GDPR، تمامی کشورهای عضو اتحادیه اروپا ملزم به حمایت حداکثری از داده‌های شخصی و اشخاص موضوع داده شدند (با وجود اینکه این

۱. Controller؛ کنترل‌کننده به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که به تنهایی یا به طور مشترک با دیگران، اهداف و ابزار پردازشِ داده‌های شخصی را تعیین می‌کند (EUR-Lex, 2016: 33). اگر یک شخص ـاعم از حقیقی یا حقوقیـ یا یک مرجع عمومی یا یک نهاد تصمیم بگیرد که چرا و چگونه داده‌های شخصی باید پردازش شوند، کنترل‌کننده داده است (Colcelli, 2019: 1031).

۲. 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, 2018[D]).

۳. Processing؛ پردازش مطابق با GDPR، به معنای عملیات یا مجموعه‌ای از عملیات است که بر روی دادهٔ شخصی یا مجموعه 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 به وسیله 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).

مقررات مصوب اتحادیه اروپاست، لیکن به دلیل الزامات خاص خود، بر بسیاری از اشخاص خارج از اتحادیه اروپا نیز اثرگذار است و ضمانت اجراهای آن بر اشخاص خارج از اتحادیه اروپا نیز قابل اعمال است). حمایت‌های مقرر در GDPR نسبت به بسترهای قانونی سابقِ اتحادیه اروپا و سایر نظام‌های حقوقی در خصوص حمایت از داده‌های شخصی، دقیق‌تر، سختگیرانه‌تر و در مقام عمل کاربردی‌تر است.

خارج از اتحادیه اروپا، با وجود اهمیت حفاظت از داده‌های شخصی، بسیاری از کشورها سند قانونی در این خصوص ندارند یا هنوز پیش‌نویس سندهای خود را نهایی نکرده‌اند. ایران نیز یکی از کشورهایی است که قانون مستقل در خصوص حمایت از داده‌های شخصی و اشخاص موضوع داده ندارد؛ در حالی که نظام حقوقی ایران از ضرورت حمایت از داده‌های شخصی مستثنا نیست و اشخاص موضوع داده که در بسترهای مختلف داده‌هایشان پردازش می‌شوند، انتظار حمایت از خود و داده‌هایشان را دارند. در واقع، چنین حمایتی یکی از حقوق شهروندی است که هر نظام حقوقی ازجمله ایران باید از عهدهٔ این مهم برآید. البته حقوق ایران با ارائه پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» در تیرماه سال ۱۳۹۷ ـ منتشرشده در وبگاه وزارت ارتباطات و فناوری اطلاعات ـ[1] و طرح «حمایت و حفاظت از داده و اطلاعات شخصی»[2] اعلام وصول‌شده در صحن علنی مجلس در شهریورماه ۱۴۰۰، در این خصوص گامی برداشته است؛ لیکن این اقدامات در خصوص حمایت از این داده‌های شخصی کافی نیست. بدین‌جهت و با فقدان قانون در خصوص حمایت از دادهٔ شخصی در نظام حقوقی ایران، حمایت از داده‌های شخصی و اشخاص موضوع داده باید از خلال قوانین موضوعه، دکترین حقوقی، مبانی حقوق ایران و فقه امامیه استنباط شود.

با لحاظ مطالب پیش‌گفته و دامنهٔ موضوعی پژوهش حاضر باید گفت که در این پژوهش، تعهدات مختلف اشخاص پردازش‌کنندهٔ داده که در مواد مختلفی از GDPR مورد تصریح قرار گرفته است، تبیین خواهد شد (بند ۱)؛ سپس جریان تعهدات مذکور در نظام حقوقی ایران امکان‌سنجی می‌شود (بند ۲).

1. <https://www.ict.gov.ir/fa/newsagency/21691>.

2. See: <https://dotic.ir/news/10419>.

۱. تبیین تعهدات اشخاص پردازش‌کننده داده به موجب GDPR

تعهدات مختلف کنترل‌کننده‌ها و پردازنده‌ها در خلال مواد ۲۴ تا ۳۹ GDPR مطرح شده است. تمامی این تعهدات در خصوص کنترل‌کننده‌ها و برخی از آن‌ها برای پردازنده‌ها وجود دارد. این تکالیف به ترتیب عبارت‌اند از: پاسخ‌گویی کنترل‌کننده (بند ۱ـ۱)، تعهد کنترل‌کننده نسبت به انتخاب پردازنده مناسب (۱ـ۲)، حفظ سوابق فعالیت‌های پردازش (۱ـ۳)، همکاری با مراجع نظارتی (۱ـ۴)، تضمین امنیت پردازش (۱ـ۵)، اطلاع‌رسانی و ابلاغ نقض دادهٔ شخصی به مراجع نظارتی و اشخاص موضوع داده (۱ـ۶)، انتصاب مأمور حفاظت از داده (۱ـ۷). تفصیل این تعهدات به شرح زیر است.

۱ـ۱. کنترل‌کننده، پاسخ‌گو و مسئول اصلی پردازش

به موجب ماده ۲۴ GDPR و به عنوان یک قاعده کلی، مسئولیت و پاسخ‌گویی نسبت به پردازش دادهٔ شخصی با کنترل‌کننده است؛ چه پردازش توسط خود کنترل‌کننده یا از طرف کنترل‌کننده ـ به نمایندگی توسط پردازنده ـ انجام شده باشد (ICO, 2018[A]).

در هر پردازش ممکن است کنترل‌کننده منفرد یا مشترک باشد. اشخاص موضوع داده هنگامی که با تعدد کنترل‌کنندگان مواجه می‌شوند، نباید سطح حفاظت از داده‌ای که در GDPR برای آن‌ها تضمین شده است، کاهش یابد. قانون‌گذار اروپایی، مفهوم «کنترل‌کنندگان مشترک»[1] را در ماده ۲۶ مقرر کرده است. در خصوص چنین مفهومی باید گفت، صرف اینکه اشخاص مختلف به تنهایی در پردازش داده‌ها همکاری کنند، لزوماً آن‌ها را به کنترل‌کنندگان مشترک تبدیل نمی‌کند؛ زیرا تبادل داده‌ها بین طرفین بدون اهداف یا ابزار مشترک در یک مجموعهٔ مشترکِ از عملیات، صرفاً یک انتقال دادهٔ ساده بین کنترل‌کنندگان مجزاست. برای اینکه کنترل‌کننده‌ها به‌عنوان کنترل‌کنندگان مشترک به موجب ماده ۲۶ GDPR محسوب شوند، باید (۱) دو یا چند کنترل‌کننده (۲) به طور مشترک اهداف و ابزار پردازش را تعیین کنند. همچنین هر شخص درگیر باید الزامات لازم برای کنترل‌کننده بودن را داشته باشد. علاوه بر این، کنترل‌کننده‌ها باید جهت تعیین هدف یا عناصر اساسیِ ابزار پردازش داده که

1. Joint controllers.

مشخص‌کننده یک کنترل‌کننده است، با در نظر گرفتن عملیات پردازش، همکاری کنند. معیارِ نوعی تعیین خواهد کرد که آیا اشخاص مختلف به عنوان کنترل‌کنندهٔ مشترک، واجد شرایط هستند یا خیر. برای مثال، شرکت D تولیدکننده اتومبیل است و به منظور ارتقا خودروهای الکترونیکی، گروه D با دیگر تولیدکنندگان خودرو، یعنی شرکت‌های X، Y و Z همکاری می‌کند و یک وبگاه تجاری ایجاد کرده‌اند که داده‌های کاربر، مانند آدرس‌های IP را جمع‌آوری می‌کند. D، X، Y و Z به طور مشترک بر سر اینکه کدام داده‌ها به چه شیوه‌ای پردازش خواهند شد، توافق دارند. در این مثال، D، X، Y و Z به طور مشترک اهداف و ابزارهای پردازش داده را تعیین می‌کنند؛ بنابراین کنترل‌کنندگان مشترک به موجب ماده ۲۶ GDPR تلقی می‌شوند (Voigt & von dem Bussche, 2017: 34 & 35).

مطابق ماده ۲۶(۳) GDPR، شخص موضوع داده می‌تواند حقوق خود به موجب این مقررات را علیه هر یک از کنترل‌کنندگان مشترک اعمال کند. به علاوه در صورت بروز خسارت، هر کنترل‌کنندهٔ مشترک مسئول تمام خسارت است؛ گرچه قانون ملی کشورهای عضو اتحادیه می‌تواند مسئولیت را بین آن‌ها تقسیم کند. با وجود اینکه از نگاه GDPR هر کنترل‌کنندهٔ مشترک، مسئول جبران خسارت کامل نسبت به شخص موضوع داده است، اگر یک کنترل‌کنندهٔ مشترک، غرامت را به طور کامل پرداخت کند، می‌تواند اقداماتی را علیه دیگر کنترل‌کنندگان مشترک انجام دهد تا آن‌ها سهم خود از خسارت را پرداخت نمایند (Colcelli, 2019: 1041).

۱ـ۲. تعهد کنترل‌کننده به انتخاب پردازندهٔ مناسب

روشن شد که به عنوان یک قاعده کلی، کنترل‌کننده پاسخ‌گو و مسئول تعهدات حفاظت از داده است. با این حال، این بدان‌معنا نیست که کنترل‌کننده باید خود پردازش داده را انجام دهد؛ چرا که می‌تواند از یک پردازنده برای عمل کردن از جانب خود استفاده کند. لیکن باید گفت مطابق با ماده ۲۹ GDPR، پردازش توسط پردازنده صرفاً باید بر اساس دستور کنترل‌کننده صورت گیرد (ICO, 2018[A]).

مطابق ماده ۲۸(۱) GDPR:

«در صورتی 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، به گونه‌ای که پردازش مطابق با الزامات این مقررات باشد و حفاظت از حقوق اشخاص موضوع داده تضمین شود» (EUR-Lex, 2016: 49).

بنابراین کنترل‌کننده ملزم است قبل از انتخاب یک پردازنده خاص، ارزیابی کند که آیا پردازندهٔ موردنظر اقدامات حفاظت از دادهٔ فنی و سازمانی مناسب را فراهم می‌کند و کنترل‌کننده نیز به طور مداوم اطمینان حاصل کند که اقدامات حفاظت دادهٔ مذکور، در حال انجام است (ICO, 2018[C]). به منظور تعهد پردازنده نسبت به برآورده کردن شرایط مورد نظر کنترل‌کننده، هر دو طرف باید یک قرارداد منعقد کنند یا با دیگر اقدامات حقوقی چنین تعهدی را روشن سازند (EUR-Lex, 2016: 49).

۱ـ۳. حفظ سوابق فعالیت‌های پردازش

ماده ۳۰ GDPR، کنترل‌کننده، پردازنده و نمایندگان آن‌ها را ملزم به حفظ سابقه فعالیت‌های پردازش می‌کند. این تعهد مبیّن پاسخگویی کنترل‌کننده و پردازنده است. الزامات مربوط به محتوای سوابق تا حدودی بین کنترل و پردازنده متفاوت است. مسئولیت حفظ سوابق توسط کنترل‌کننده گسترده‌تر است؛ زیرا کنترل‌کننده مسئول اصلی حفاظت از داده به موجب GDPR است، البته برای مواردی که کنترل‌کننده طبق ماده ۳۰ GDPR ملزم به مستندسازی و حفظ سوابق است، اما پردازنده‌ها طبق ماده ۳۰ چنین الزامی ندارند، می‌توان چنین الزامی را در قرارداد بین کنترل‌کننده و پردازنده، برای پردازنده مقرر کرد و بدین‌ترتیب در عمل، تعهد حفظ سوابق برای کنترل‌کننده و پردازنده یکسان می‌شود (Hintze, 2018: 16).

مطابق با ماده ۳۰(۳) GDPR، سوابق باید کتبی، از جمله به صورت الکترونیکی باشد (EUR-Lex, 2016: 51). به علاوه برای جمع‌آوری اطلاعات لازم جهت حفظ سوابق، بخش‌های مختلف نهاد کنترل‌کننده و پردازنده که با داده‌های شخصی سروکار دارند، باید بررسی شوند. این کار می‌تواند از طریق نرم‌افزارهای تخصصی انجام شود

(Eija, 2018: 20). همچنین هر کنترل‌کننده و پردازنده ملزم به همکاری با مرجع نظارتی در صورت درخواست است و به محض درخواست باید سوابق فعالیت‌های پردازش را در اختیار مراجع نظارتی قرار دهد تا چنین مراجعی بر عملیات پردازش نظارت کنند (Kubben et al., 2019: 64).

۱ـ۴. همکاری با مراجع نظارتی

ماده ۳۱ GDPR، تعهد همکاری با مراجع نظارتی را مقرر می‌کند. این تعهد در مورد کنترل‌کننده، پردازنده و در صورت وجود نمایندگان آن‌ها وجود دارد. چنین مرجعی در منابع مرتبط با واژگان مرجع (ملی) حفاظت از داده[1] (DPA) یا مرجع نظارتی[2] (SA) ذکر شده است. این مراجع را کشورهای عضو اتحادیه اروپا مطابق با ماده ۸(۳) منشور حقوق اساسی اتحادیه اروپا ایجاد نموده‌اند (European Commission, 2016).

طبق ماده ۳۱ GDPR، همکاری باید بر اساس «درخواست» مراجع نظارتی صورت گیرد. این بدان‌معناست که کنترل‌کننده یا پردازنده مجبور نیست با ابتکارِ عمل خود همکاری کند. با وجود این، همکاری بدون درخواستِ مراجع نظارتی ممکن است مفید باشد؛ زیرا همکاری داوطلبانه ممکن است به یک عامل تخفیف‌دهنده تبدیل شود، در جایی که اشخاص پردازش‌کننده داده با جریمه‌ها یا سایر ضمانت اجراها به موجب GDPR مواجه می‌شوند (Voigt & von dem Bussche, 2017: 37). ضمانت اجراهای نقض GDPR در فصل نهایی بیان خواهد شد.

در خصوص ماده ۳۱ GDPR باید گفت، تعهد همکاری با مراجع نظارتی مصادیق مختلفی دارد که در مواد مختلف بدان اشاره شده است؛ مانند ماده ۳۰ که بیان شد. کنترل‌کننده و پردازنده ملزم به همکاری با مرجع نظارتی در صورت درخواست هستند و به محض درخواست باید سوابق فعالیت‌های پردازش را در اختیار مراجع نظارتی قرار دهند، اما خود تعهد همکاری به موجب ماده ۳۱ GDPR، قابلیت اجرایی ندارد؛ بدین‌توضیح که برای نقض آن ضمانت اجرایی در مقررات پیش‌بینی نشده است

1. Data Protection Authority.
2. Supervisory Authority.

و اگر کنترل‌کننده و پردازنده به دلیل عدم همکاری با مراجع نظارتی مورد توبیخ، جریمه یا مجازات قرار می‌گیرند، به دلیل عدم رعایت مصادیق متفاوت همکاری با مراجع نظارتی به موجب مواد دیگر است. بنابراین قابلیت اجرایی این ماده باید توسط سایر اصول حقوقیِ اتحادیه اروپا یا قوانین ملی کشورهای عضو اتحادیه اروپا مشخص شود؛ چرا که تعهد همکاری به موجب ماده ۳۱ GDPR فی‌نفسه الزامی ندارد (Ibid.: 37 & 38).

۱ـ۵. تضمین امنیت پردازش (اجرای اقدامات فنی و سازمانی مناسب)

اقدامات فنی و سازمانی (TOM)[1] مناسب باید حفاظت از داده‌های شخصی را تضمین کند. ماده ۳۲ GDPR، کنترل‌کننده و پردازنده را ملزم به انجام چنین اقداماتی در جهت حفظ امنیت داده‌های شخصی می‌کند. اقدامات فنی و سازمانی مناسب شامل هر گونه اقدام در ارتباط با جمع‌آوری، پردازش یا استفاده از داده‌های شخصی است که سطح مناسبی از حفاظت از داده‌ها را بر اساس GDPR فراهم می‌کند (Eija, 2018: 18). الزامات ماده ۳۲ GDPR به طور مساوی برای کنترل‌کننده‌ها و پردازنده‌ها اعمال می‌شود و کنترل‌کننده‌ها و پردازنده‌ها ملزم به «اجرای اقدامات فنی و سازمانی مناسب جهت تضمین سطح امنیت متناسب با خطر» هستند. البته کنترل‌کننده‌ها باید در قراردادهای خود با پردازنده‌ها، تعهدات لازم جهت اجرای مناسب ماده ۳۲ را مورد توجه قرار دهند. این تعهدات برای پردازنده‌های فرعی نیز جاری است و به هر پردازنده فرعی که درگیر پردازش است نیز منتقل می‌شود (Hintze, 2018: 11 & 12).

مطابق ماده ۳۲(۱) GDPR، اقدامات مختلفی به عنوان اقدامات فنی و سازمانی مناسب تلقی می‌شود: الف‌ـ مستعار ساختن و رمزگذاری داده‌های شخصی؛ ب‌ـ امکان نظارت اشخاص موضوع داده بر پردازش داده‌ها و دسترسی به داده‌های شخصی، همچنین توانایی بازیابیِ به موقع جهت دسترسی به داده‌های شخصی در صورت بروز حادثهٔ فیزیکی یا فنی؛ ج‌ـ حفظ محرمانگی و تمامیت داده‌های شخصی با مفاهیم بازدارندهٔ حفاظت از داده با طراحی و به طور پیش‌فرض؛ دـ فرایندی برای آزمایش منظم،

1. Technical and organisational measures.

ارزیابی و اثربخشی اقدامات فنی و سازمانی مناسب جهت اطمینان از امنیت پردازش (EUR-Lex, 2016: 51 & 52). برخی از اقدامات فنی و سازمانی مذکور نیاز به توضیح دارد:

ـ مستعارسازی[1] به موجب ماده ۴ GDPR:

«به معنای پردازش داده‌های شخصی به روشی است که داده‌های شخصی دیگر نتواند به یک شخص موضوع دادهٔ خاص بدون استفاده از اطلاعات اضافی نسبت داده شود؛ به شرطی که چنین اطلاعات اضافی به طور جداگانه و همراه با اقدامات فنی و سازمانی نگهداری شود تا اطمینان حاصل شود که داده‌ها به یک شخص حقیقی شناسایی‌شده یا قابل شناسایی نسبت داده نمی‌شوند» (Ibid.: 33).

داده‌های شخصی که مستعار هستند یا رمزگذاری[2] شده‌اند (کدگذاری تا فقط افراد مجاز بتوانند به دادهٔ شخصی دسترسی داشته باشند)، می‌توانند برای شناسایی مجددِ یک فرد استفاده شوند و بدین‌ترتیب در محدودهٔ GDPR قرار گیرند. در مقابل، داده‌های شخصی اگر به گونه‌ای ناشناس (ناشناس ساختن[3]) ارائه شوند که فرد قابل شناسایی نباشد یا دیگر قابل شناسایی نیست، داده‌های شخصی نیست (European Commission, 2019).

ـ حفاظت از داده با طراحی و به طور پیش‌فرض:[4] اشخاص پردازش‌کننده داده ملزم به اجرای اقدامات فنی و سازمانی مناسب جهت حفاظت از داده هستند. بدین‌منظور از همان مراحل اولیه، طراحی عملیات پردازش باید به گونه‌ای 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 در واقع اقدامات پیشگیرانه است که خطرات حریم خصوصی را پیش‌بینی و از آن‌ها جلوگیری می‌کند؛ بنابراین این نوع از حفاظت، راه حلّی برای معضلات ارائه نمی‌دهد، بلکه هدف آن جلوگیری از وقوع معضلات است (Ferrara & Spoto, 2018: 3).

به علاوه به طور پیش‌فرض، اشخاص پردازش‌کننده داده باید اطمینان حاصل کنند که دادهٔ شخصی با بالاترین سطح حفاظت از داده پردازش می‌شود. برای مثال تنها

1. Pseudonymisation.
2. Encryption.
3. Anonymisation.
4. Data Protection by Design and by Default.

داده‌های لازم باید پردازش شوند، دوره ذخیره‌سازی داده‌ها کوتاه و دسترسی محدود باشد و پردازش داده به طور پیش‌فرض باید به گونه‌ای باشد که دادهٔ شخصی برای تعداد زیادی از افراد قابل دسترس نباشد (حفاظت از داده به طور پیش‌فرض). با توجه به تعاریف مذکور، مثال‌های حفاظت از داده با طراحی مستعارسازی و رمزگذاری است و برای حفاظت از داده به طور پیش‌فرض می‌توان موردی را گفت که تنظیمات یک پیام‌رسان اجتماعی به گونه‌ای است که پروفایل کاربران از ابتدا و به طور پیش‌فرض، برای تعداد نامحدودی از افراد قابل دسترس نباشد (European Commission, 2018[C]).

۱ـ۶. اطلاع‌رسانی و ابلاغ نقض دادهٔ شخصی به مراجع نظارتی و اشخاص موضوع داده

مطابق ماده ۴ شماره ۱۲ GDPR:

«نقض داده شخصی، نقض امنیت است که منجر به تخریب اتفاقی یا غیر قانونی، از دست دادن، تغییر، افشای غیر مجاز یا دسترسی غیر مجاز به دادهٔ شخصیِ منتقل‌شده، ذخیره‌شده یا پردازش‌شده [به شیوه‌های دیگر] می‌شود» (EUR-Lex, 2016: 34).

نقض دادهٔ شخصی می‌تواند به صورت یک حادثه فنی یا فیزیکی رخ دهد. در واقع، دادهٔ مربوطه باید شخصی باشد و باید قبل از وقوع حادثه، منتقل شده، ذخیره شده یا به شیوه‌های دیگر پردازش شده باشد. تعریف مذکور از نقض، به عنصر قصد (عمد) یا سهل‌انگاری (غیر عمد) نیاز ندارد. بنابراین نسبت به هر گونه وقوع نقض داده، اعمال می‌شود ـو مهم نیست که نقض داده‌ها چگونه و چرا اتفاق افتاده است و حتی نقض تصادفی را نیز شامل می‌شودـ. همچنین مشخص نیست که آیا «افشای غیر مجاز یا دسترسی غیر مجاز»، مستلزم آن است که چنین افشا یا دسترسی واقعاً اتفاق افتاده باشد یا احتمال دسترسی نیز شامل تعریف است. با توجه به رویکرد مبتنی بر خطر GDPR، مورد اخیر باید مدّنظر باشد. در نتیجه و به طور کلی، حتی از دست دادن واسطهٔ داده یا دسترسی به پایگاه دادهٔ رمزگذاری‌شده، نقض دادهٔ شخصی است (Eija, 2018: 22 & 23).

GDPR برای زمانی که داده‌های شخصی نقض می‌شوند، تعهدی را برای کنترل‌کننده و پردازنده نسبت به مراجع نظارتی و اشخاص موضوع داده مقرر می‌کند.

این تعهد، اطلاع‌رسانی نقض دادهٔ شخصی به مرجع نظارتی (به موجب ماده ۳۳ GDPR) و ابلاغِ نقض به شخص موضوع داده (به موجب ماده ۳۴ GDPR) است. بنابراین در فراز نخست به تعهد اطلاع‌رسانی به مرجع نظارتی، و در فراز بعدی به ابلاغ به شخص موضوع داده، پرداخته خواهد شد.

۱ـ۶ـ۱. تعهد اطلاع‌رسانی به مرجع نظارتی

مطابق ماده ۳۳ GDPR:

«۱ـ در مورد نقض داده‌های شخصی، کنترل‌کننده باید بدون تأخیر غیر ضروری و در صورت امکان، ظرف ۷۲ ساعت پس از آگاهی، نقض داده‌های شخصی را به مرجع نظارتیِ صالح مطابق با ماده ۵۵ اطلاع دهد، مگر اینکه نقض داده‌های شخصی برای حقوق و آزادی‌های اشخاص حقیقی خطری ایجاد نکند. در صورتی که ظرف ۷۲ ساعت اطلاع‌رسانی به مرجع نظارتی انجام نشود، اطلاع‌رسانی با دلایل تأخیر همراه خواهد بود. ۲ـ پردازنده باید پس از آگاهی از نقض داده‌های شخصی، بدون تأخیرِ غیر ضروری کنترل‌کننده را مطلع سازد. ۳ـ اطلاع‌رسانی مذکور در بخش ۱ باید حداقل شامل موارد ذیل باشد: الف‌ـ توصیف ماهیت نقض داده‌های شخصی و در صورت امکان، دسته‌ها و تعداد تقریبی اشخاص موضوع دادهٔ مربوطه و دسته‌ها و تعداد تقریبی داده‌های شخصی مربوطه؛ ب‌ـ نام و جزئیات تماس مأمور حفاظت داده و یا سایر مسیرهای ارتباطی در صورتی که اطلاعات بیشتری می‌توان از آن‌ها به دست آورد؛ ج‌ـ پیامدهای احتمالی نقض داده‌های شخصی؛ د‌ـ توصیف اقدامات صورت‌گرفته یا پیشنهادشده توسط کنترل‌کننده برای رسیدگی به نقض داده‌های شخصی و در صورت لزوم، اقداماتی برای کاهش اثرات منفی احتمالی با نقض داده‌های شخصی...» (EUR-Lex, 2016: 52).

همان طور که ملاحظه می‌شود، مطابق ماده ۳۳(۲) GDPR، پردازنده تعهد ندارد که نقض داده‌ها را به مراجع نظارتی اطلاع دهد، بلکه تنها موظف است به کنترل‌کننده اطلاع می‌دهد. در واقع، گرچه GDPR تعهد اطلاع‌رسانی را مستقیماً برای کنترل‌کنندهٔ داده قرار می‌دهد نه پردازنده، با این حال، اگر پردازنده از نقض داده‌های شخصی آگاه شود، باید به کنترل‌کننده اطلاع دهد و بدین‌صورت پردازنده نیز متعهد است (Hintze, 2018: 12). برای پردازنده محدودیت زمانی ـ۷۲ ساعتـ نیز وجود ندارد؛ لیکن

باید گفت که مطابق مشروح GDPR ۸۷، چنین اطلاع‌رسانی باید بر اساس موقعیت هر پردازش، فوری باشد. این مشروح بیان می‌کند:

«... این امر که اطلاع‌رسانی باید بدون تأخیر غیر ضروری باشد، به طور خاص با درنظر گرفتن ماهیت و اهمیت نقض داده‌های شخصی، عواقب و اثرات منفی آن برای شخص موضوع داده تعیین می‌شود. چنین اطلاع‌رسانی ممکن است منجر به مداخلهٔ مرجع نظارتی، مطابق با وظایف و اختیارات مذکور در این مقررات شود» (EUR-Lex, 2016: 17).

به علاوه مطابق ماده ۳۳(۱) GDPR:

«کنترل‌کننده باید نقض داده را بدون تأخیر غیر ضروری و در صورت امکان، ظرف ۷۲ ساعت پس از آگاهی از نقض اطلاع‌رسانی کند».

با این حال، حتی اگر این اطلاع در ۷۲ ساعت داده شود، ممکن است «بدون تأخیر غیر ضروری» نباشد (Reini, 2019: 18)؛ زیرا همان طور که ذکر شد، مطابق مشروح ۸۷ GDPR، این فوریت باید با در نظر گرفتن ماهیت و اهمیت نقض داده‌های شخصی و عواقب و اثرات سوء آن برای اشخاص موضوع داده تعیین شود. بنابراین هرچه خطراتِ نقض داده برای حقوق و آزادی‌های اشخاص بیشتر باشد، اطلاع‌رسانی باید سریع‌تر صورت گیرد. از سوی دیگر در برخی موارد، اگر دلایل موجه وجود داشته باشد، این اطلاع‌رسانی ممکن است بیش از ۷۲ ساعت طول بکشد که در این صورت، کنترل‌کننده باید دلایل تأخیر را با اطلاع‌رسانی بیان نماید (BNA, 2016: 9).

همچنین مطابق مفاد مذکور (ماده ۳۳(۱) GDPR) باید گفت، دوره اطلاع‌رسانی با آگاهی کنترل‌کننده‌ها از نقضِ داده آغاز می‌شود؛ با این حال، GDPR مشخص نمی‌کند که کنترل‌کننده چقدر سریع باید از نقض دادهٔ در حال وقوع آگاه شود. با توجه به رویکرد مبتنی بر خطر GDPR و وظیفه اجرای اقدامات فنی و سازمانی ـ که در فراز سابق بیان شد ـ اطلاع‌رسانی نقض داده‌هایی که با پردازش، خطرات مهمی دارد، باید از مواردی که پردازش خطر کمتری دارد، سریع‌تر باشد. همچنین به موجب GDPR مشخص نیست که آیا آگاهی پردازنده به کنترل‌کننده نسبت داده خواهد شد یا خیر. اگر چنین باشد، دورهٔ اطلاع‌رسانی، با آگاهی پردازنده بدون توجه به زمان

آگاهی کنترل‌کننده از نقض داده آغاز می‌شود. البته با توجه به اینکه قاعده کلی این است که مسئول اصلی پردازش کنترل‌کننده است و باید اقدامات پردازنده را نیز برعهده بگیرد، بعید نیست که آگاهی پردازنده به کنترل‌کننده نسبت داده شود (Voigt & von dem Bussche, 2017: 66 & 67) و بتوان چنین امری را به قصد قانون‌گذار اروپایی منتسب کرد.

۱ـ۶ـ۲. تعهد ابلاغ به شخص موضوع داده

به موجب ماده ۳۴(۱) GDPR، به هنگام شناسایی احتمال خطر مهم از نقض داده‌ها برای حقوق و آزادی‌های اشخاص موضوع داده، کنترل‌کننده باید نقض دادهٔ شخصی را به اشخاص موضوع دادهٔ متأثر، بدون تأخیر غیر ضروری ابلاغ کند. این اطلاع‌رسانی به اشخاص موضوع داده اجازه می‌دهد تا اقدامات احتیاطی لازم را انجام دهند[۱] (European Commission, 2018[F]: 15). ماده ۳۴ GDPR مقرر می‌کند:

«۱ـ هنگامی که نقض داده‌های شخصی به احتمال زیاد منجر به خطر مهم برای حقوق و آزادی‌های اشخاص حقیقی می‌شود، کنترل‌کننده باید نقض داده‌های شخصی را بدون تأخیر غیر ضروری، به شخص موضوع داده ابلاغ کند. ۲ـ ابلاغ مذکور در بخش ۱ این ماده باید با زبانی روشن و واضح، ماهیت نقض داده‌های شخصی را شرح داده و حداقل حاوی اطلاعات و اقدامات اشاره‌شده در بندهای ب، ج و د ماده ۳۳(۳) باشد. ۳ـ در صورت وجود هر یک از شرایط ذیل، ابلاغ به شخص موضوع داده مذکور در بخش ۱ الزامی نیست: الف ـ کنترل‌کننده اقدامات فنی و سازمانی مناسب را انجام داده است و آن اقدامات بر روی داده‌های شخصی متأثر از نقض اعمال شده است، به خصوص اگر که داده‌های شخصی برای هر فردی که مجاز به دسترسی به آن نیست، غیر قابل فهم شده باشد، مانند رمزگذاری؛ ب ـ کنترل‌کننده اقدامات بعدی را اتخاذ کرده و اطمینان حاصل نموده است که خطر مهم برای حقوق و آزادی شخص موضوع داده مذکور در بخش ۱، دیگر احتمال تحقق ندارد؛ ج ـ ابلاغ مستلزم تلاش نامتناسب است. در چنین حالتی باید یک ابلاغ عمومی یا اقدامی مشابه انجام شود، به صورتی که به موجب آن، شخص

۱. اقدامات اصلاحی (جبرانی) که قادر به کاهش خسارت باشند، مانند حذف داده‌های شخصی از بسترهایی که موجب نقض شده یا در معرض نقض هستند (Singh, 2016: 131 & 132).

موضوع داده با روشی به همان اندازه مؤثر مطلع شود. ۴ـ اگر کنترل‌کننده نقض داده‌های شخصی را به شخص موضوع داده ابلاغ نکند، مرجع نظارتی با در نظر گرفتن اینکه نقض داده‌های شخصی ممکن است خطر مهمی داشته باشد، می‌تواند این کار را انجام دهد یا تصمیم بگیرد که هر یک از شرایط مذکور در بخش ۳ رعایت شود» (EUR-Lex, 2016: 52 & 53).

۱ـ۷. انتصاب مأمور حفاظت از داده

مأمور حفاظت از داده[1] (DPO)، مسئول نظارت و اعمال مقررات حفاظت از داده است که به طور مستقل بر رعایت چنین مقرراتی نظارت می‌کند. چنین مأموری نقشی کلیدی در انطباق با GDPR ایفا می‌کند (European Commission, 2016). مواد ۳۷ تا ۳۹ GDPR در خصوص مأمور حفاظت از داده مقرر شده است. تا زمان معرفی مأمور حفاظت از داده توسط GDPR، تعهد انتصاب مأمور حفاظت از داده به طور گسترده‌ای در بیشتر کشورهای عضو اتحادیه اروپا ناشناخته بود. با این حال، تعدادی از کشورهای عضو اتحادیه اروپا، مانند لهستان، فرانسه و سوئد، امکان تعیین داوطلبانهٔ مأمور حفاظت از داده را بیان کرده بودند. البته انتصاب اجباری چنین مأموری، بیش از ۳۰ سال است که در قانون حفاظت از دادهٔ آلمان ارائه شده و موفقیت آن به اثبات رسیده است (Voigt & von dem Bussche, 2017: 53).

به موجب GDPR، هم کنترل‌کننده و هم پردازنده در معرض تعهد انتصاب مأمور حفاظت از داده قرار دارند (Hintze, 2018: 4)؛ زیرا طبق ماده ۳۷(۱) بندهای ب و ج GDPR:

«در صورتی که فعالیت اصلی کنترل‌کننده یا پردازنده شامل پردازشی است که مستلزم نظارت منظم و نظام‌مند بر اشخاص موضوع داده در مقیاس وسیع با توجه به ماهیت، دامنه و اهداف پردازش است، یا فعالیت اصلی کنترل‌کننده یا پردازنده شامل پردازش دسته‌های خاص از داده‌های شخصی مذکور در ماده ۹ و داده‌های شخصی مرتبط با محکومیت‌های کیفری و جرائم مذکور در ماده ۱۰ در مقیاس وسیع است، کنترل‌کننده و پردازنده باید مأمور حفاظت از داده منصوب نمایند».

1. Data Protection Officer.

به علاوه مطابق ماده ۳۷(۱) بند الف GDPR:

«مراجع و نهادهای عمومی همیشه ملزم بـه انتـصاب مـأمور حفاظـت از داده هـستند، مگر دادگاه‌هایی که در صلاحیت قضایی خود عمل می‌کنند» (EUR-Lex, 2016: 55).

مثال برای لزوم انتصاب مـأمور حفاظـت از داده مـی‌توانـد ردیـابی بـرخط اشـخاص موضوع داده باشد؛ بدین‌توضیح که یک وبگاه مرکز خریـد، از الگـوریتم‌هـایی جهـت نظارت بـر جـستجوها و خریـدهای کـاربران خـود اسـتفاده مـی‌کنـد و بـر اسـاس ایـن اطلاعات به آن‌ها پیشنهادهایی را ارائه می‌دهد. از آنجایی که این امر به طور مداوم و بـا توجه به معیارهای از پیش تعریف‌شده رخ می‌دهد، می‌تواند بـه عنـوان نظـارت مـنظم و نظام‌مند اشخاص موضوع داده در مقیاس وسـیع تلقـی شـود یـا در خـصوص داده‌هـای حساس می‌توان مثالی را فرض نمود که یـک شـرکت بیمـهٔ سـلامت، طیـف وسـیعی از داده‌های شخـصی در مـورد تعـداد زیـادی از افـراد، از جملـه شـرایط پزشـکی و سـایر اطلاعات بهداشتی را پردازش می‌کند. این مورد می‌توانـد بـه عنـوان پـردازش داده‌هـای حساس در مقیاس وسیع در نظر گرفته شود (ICO, 2018[B]). در مثالی دیگر می‌توان گفت کـه چنانچـه یـک شـرکت، داده‌هـای شخـصی را بـه هـدف ارسـال تبلیغـات از طریـق موتورهای جستجو بر اساس رفتار برخط مردم پردازش می‌کند، بایـد مـأمور حفاظـت از داده داشته باشد؛ با این حال، اگر این شرکت تنهـا یـک بـار در سـال، مطالـب تبلیغـاتی بـرای مـشتریان خـود ارسـال مـی‌کنـد، بـه چنـین مـأموری نیـاز نخواهـد داشـت (European Commission, 2018[F]: 13).

مأمور حفاظت از داده می‌تواند کارمنـد سـازمان، شـرکت یـا نهـادِ کنتـرل‌کننـده یـا پردازندهٔ داده‌های شخصی باشد (مـأمور حفاظـت از دادهٔ داخلـی[1]) و یـا ممکـن اسـت براساس قرارداد خدماتی و به صورت خـارجی منـصوب شـود (مـأمور حفاظـت از دادهٔ خارجی[2]). نیز چنین مأموری می‌تواند شخص حقیقی یا حقوقی باشد (Id., 2018[A]).

GDPR الزامات برای دوره انتصاب و الزامات رسمی جهت انتـصاب ایـن مـأمور را تعیین نمی‌کند. با این حال، شکل کتبی توصیه می‌شود؛ زیرا به اهـداف مـستندسازی و

1. Internal DPO.
2. External DPO.

اثباتی کمک می‌کند. همچنین در حالی که در پیش‌نویس GDPR، یک دورهٔ انتصاب ۲ ساله برای مأمور حفاظت از داده تعیین شده بود، این الزام در متن نهایی GDPR وجود ندارد. اما به نظر می‌رسد که هنوز هم بهتر است مأمور حفاظت از داده برای حداقل ۲ سال منصوب شود تا استقلال آن تضمین شود و بتواند نظارت مداوم بر فعالیت‌های پردازشی داشته باشد (Voigt & von dem Bussche, 2017: 58).

فارغ از تعهد انتصاب مأمور حفاظت از داده، که کنترل‌کننده و پردازنده در موارد خاصی ملزم به چنین تعهدی هستند، در اینجا بیان مطالبی در خصوص مأمور حفاظت از داده نیز مفید است. مواد ۳۸ و ۳۹ GDPR، وظایف مأمور حفاظت از داده را بیان می‌کنند که عبارت‌اند از: آگاهی و مشاوره به کنترل‌کننده، پردازنده یا کارمندانی که به موجب این مقررات یا سایر قوانین مربوط به حفاظت از دادهٔ اتحادیه یا کشورهای عضو، پردازش را انجام می‌دهند؛ نظارت بر رعایت این مقررات یا سایر قوانین حفاظت از داده کشور عضو یا اتحادیه، همچنین نظارت بر سیاست‌های کنترل‌کننده یا پردازنده در ارتباط با حفاظت از داده‌های شخصی، از جمله تخصیص مسئولیت‌ها، افزایش آگاهی و آموزش کارکنان درگیر در عملیات پردازش و انجام بررسی‌ها مربوطه؛ در صورت درخواست، ارائه مشاوره در مورد ارزیابی تأثیر حفاظت از داده[1] و نظارت بر عملکرد آن مطابق ماده ۳۵؛ همکاری با مراجع نظارتی؛ عمل نمودن به عنوان نقطه ارتباطی برای مراجع نظارتی در مورد مسائل مربوط به پردازش، از جمله مشاوره قبلی مذکور در ماده ۳۶ و در صورت لزوم در مورد هر موضوع مهم دیگر؛ عمل نمودن به عنوان نقطه ارتباطی برای اشخاص موضوع داده تا اشخاص موضوع داده بتوانند در خصوص تمام مسائل مربوط به پردازشِ داده‌های شخصی خود و اِعمال حقوق خود به موجب GDPR با مأمور در تماس باشند.

---

۱. مطابق با ماده ۳۵ بخش ۱ GDPR، اگر نوعی از پردازش داده به ویژه با استفاده از فناوری‌های جدید، به احتمال زیاد منجر به خطر مهم برای حقوق و آزادی‌های افراد با در نظر گرفتن ماهیت، دامنه، زمینه و اهداف پردازش شود، کنترل‌کننده باید ارزیابی در مورد تأثیر فعالیت‌های پردازشی پیش‌بینی‌شده نسبت به حفاظت از داده‌ها انجام دهد. در واقع، مطابق با رویکرد کلی مبتنی بر خطر GDPR، کنترل‌کننده باید در صورت شناسایی احتمال خطر مهم، اثرات فعالیت‌های پردازشی خود را نسبت به آینده پیش‌بینی کند (European Commission, 2018[C]: 14).

مطابق ماده ۳۸(۶) GDPR، مـأمور حفاظـت از داده مـی‌توانـد وظـایف دیگـری را انجام دهد، لیکن کنترل‌کننده یا پردازنده باید اطمینان حاصل کنند که چنـین وظـایفی منجر بـه تعـارض منـافع نمـی‌شـود (EUR-Lex, 2016: 56). بنـابراین مطـابق بـا GDPR، کنترل‌کننده یا پردازنده می‌توانند وظایف و مسئولیت‌های بیشتری را ـعلاوه بـر وظـایفِ الزامی مذکورـ به مأمور حفاظـت از داده اختـصاص دهنـد؛ البتـه تـا زمـانی کـه چنـین تخصیص مسئولیت و وظایفی منجر به تضاد منافع با وظایف اولیه و الزامی مأمور حفاظت از داده نشود. برای مثال، ماده ۳۰ GDPR مستلزم آن است که کنترل‌کننده یا پردازنده باید سوابق عملیات پردازش را حفظ کنند و تخصیص این وظیفه به مأمور حفاظت از داده مانعی ندارد و تعارض منافعی ایجاد نمی‌کند. در مقابل، این مأمور نمی‌تواند در سازمان، نهاد یا شرکت کنترل‌کننده و پردازنده جایگـاهی داشـته باشـد کـه در تعیـین اهـداف و ابزارهای پردازش داده‌هـای شخـصی دخیـل باشـد؛ زیـرا اگـر مـأمور حفاظـت از داده، مسئول تعیین اهداف و ابزارهای پردازش داده یا تضمین مجاز بودن فعالیت‌های پردازش باشد، تضاد منافع رخ خواهد داد؛ چرا که این مأمور نمی‌تواند بر پیروی خود از GDPR نظارت کند. همچنین مأمور حفاظت از داده نمی‌تواند اهـداف رقـابتی‌ای داشـته باشـد که نقشی در منافع کسب و کار دارد و تأثیر بر حفاظت از داده‌ها می‌گذارد. برای مثال، رئیس بازاریابی یک شرکت، پویشی تبلیغاتی را برنامـه‌ریـزی مـی‌کنـد، از جملـه اینکـه کدام یک از مشتریان شرکت باید هدف قرار گیـرد یـا کـدام روش ارتبـاطی و جزئیـات شخصی باید مورد استفاده قرار گیرد. در ایـن صـورت، ایـن شـخص نمـی‌توانـد مـأمور حفاظت از داده شرکت باشد؛ چون وظایف او منجر به تعارض منافع بین اهداف پویش (استفاده از داده‌های شخصی برای اهداف تبلیغاتی) و تعهدات حفاظت از دادهٔ شرکت می‌شود (ICO, 2018[B]). به عنوان یک قاعده کلی، انتصاب هـر شخـصی بـا هـر یـک از نقش‌های مدیریتی (مدیر عامل، مدیر اجرایی)، رؤسای بخش‌هـای فنـاوری اطلاعـات، بازاریابی یا منابع انسانی و سایر نقـش‌هـای دیگـری کـه در سـاختار سـازمانی در مرتبـهٔ پایین‌تری قرار دارند، ولی به تعیین اهداف و ابزارهای پردازش داده می‌پردازند، به عنوان مأمور حفاظت از داده ممکن نیست (Kubben et al., 2019: 65).

با توجه به نقش کلیدی این مأمور در حفاظت از داده، نامزدهای ایـن موقعیـت بایـد

صلاحیت‌های قانونی مشخصی را داشته باشند. طبق ماده ۳۷(۵) GDPR، این مأمور باید خصوصیات حرفه‌ای، دانش تخصصی در زمینه قانون و رویه‌های حفاظت از داده و توانایی انجام وظایف قانونی مذکور را داشته باشد. از آنجایی که صلاحیت آن‌ها با توانایی انجام مسئولیت‌های قانونی‌شان مرتبط است، نامزد مأموریت حفاظت از داده، باید در ارتباط با فعالیت‌های پردازش داده شرکت، نهاد یا سازمان ارزیابی شود. سطح مورد نیاز دانش تخصصی نیز با توجه به عملیات پردازشی و حفاظت مورد نیاز برای داده‌های شخصی مشخص می‌شود (Voigt & von dem Bussche, 2017: 56 & 57).

در نهایت باید گفت مأمور حفاظت از داده، عملکرد مشاوره‌ای دارد و شخصاً مسئول عدم رعایت GDPR نیست؛ لیکن باید پاسخ‌گوی وظایف مخصوص به خود باشد (Kubben et al., 2019: 65). همچنین مطابق ماده ۳۸(۳) GDPR، مأمور حفاظت از داده نباید به خاطر انجام وظایف خود توسط کنترل‌کننده یا پردازنده اخراج یا جریمه شود. در مقابل، اخراج یا جریمه به دلایل دیگر ـبرای مثال، دلایل قراردادی یا اقتصادیـ در هر زمانی ممکن است. با وجود این، دلایل دیگری که ذکر شد، نباید منجر به اخراج یا جریمه این مأمور جهت انجام وظایفش شود؛ زیرا این کار، خلاف ماده ۳۸(۳) GDPR (قصد قانون‌گذار) است (Voigt & von dem Bussche, 2017: 60).

۲. بررسی تعهدات اشخاص پردازش‌کنندهٔ داده در نظام حقوقی ایران

جهت بررسی تعهدات اشخاص پردازش‌کنندهٔ داده در نظام حقوقی ایران، به دلیل عدم اشاره صریح به این امر در قوانین موضوعه و دکترین حقوقی، باید چنین تعهداتی از مبانی حقوق ایران و فقه امامیه استنباط شود. همچنین اسناد مرتبط یعنی پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» مورخ ۱۳۹۷ و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» اعلام وصول‌شده در مجلس به تاریخ شهریورماه ۱۴۰۰، در این خصوص قابل بررسی هستند. در این بند، موارد مذکور در فرازهای جداگانه مورد واکاوی قرار خواهند گرفت.

۲ـ۱. جستجوی تعهدات اشخاص پردازش‌کنندهٔ داده در مبانی حقوق ایران و فقه امامیه

از آنجایی که در مبانی حقوق ایران و فقه امامیه، تعهدات اشخاص پردازش‌کنندهٔ داده مورد تصریح قرار نگرفته است، باید چگونگی ید یعنی استیلا و تصرف اشخاص پردازش‌کننده داده نسبت به دادهٔ شخصی تبیین شود. در مرحلهٔ بعد و با کشف نوع استیلای اشخاص پردازش‌کنندهٔ داده نسبت به دادهٔ شخصی، تعهدات چنین اشخاصی قابل استنباط است.

تصرف یا ید به طور کلی به ید امانی و ید ضمانی قابل تقسیم است. به موجب قاعدهٔ استیمان (امانی بودن ید و عدم ضمان امین)، امین نسبت به مال امانتی که تلف شده یا دچار نقص گشته است، بدون تعدی و تفریط ضامن نیست: «عدمُ ضمان الأمین إلّا مع التعدّی أو التفریط» (هاشمی شاهرودی، ۱۳۸۲: ۲۷۸/۶). البته در مواردی ممکن است که تصرف غیر مجاز، موجب تلف یا نقص مال هم نشود، بلکه بر بهایش نیز بیفزاید، لیکن موجب ضمان است؛ زیرا این ضمان ناشی از آن است که ید مأذون به ید غیر مأذون و عدوانی تبدیل شده و اینجا مجرای قاعدهٔ «علی الید ما أخذت حتّی تؤدّیه» است (موسوی بجنوردی، ۱۳۷۹: ۱۹۲/۱). همچنین در مواردی، امانت در جهت مصلحت مالک است (مانند ودیعه) و در برخی موارد نیز برای مصلحت امین (مانند عاریه) و در سایر موارد ممکن است که هر دو از آن منتفع شوند (مانند اجاره) (لطفی، ۱۳۷۸: ۹۵). ملاک جریان قاعدهٔ استیمان، اذن و تسلیط مجانی بر مال مالک است که در این صورت، ضامن تلف و نقص نیز نیست؛ زیرا او امین است و بدون تعدی و تفریط، ضمان از وی ساقط است (ر.ک: موسوی بجنوردی، ۱۳۷۹: ۱۱۳/۱). ید امانی، اعم از ید مالکی و شرعی (قانونی) است. ید امانیِ مالکی آن است که خود مالک، شیء را به امانت نزد دیگری می‌گذارد و اذن در تصرف از جانب مالک می‌باشد؛ اعم از اینکه چنین اذنی بر اساس عقدی باشد که امانت موضوع اصلی آن است، مانند ودیعه،[۱] یا به وسیلهٔ عقودی باشد که امانت، مسئلهٔ تبعیِ آن عقود است و از ارادهٔ ضمنی اطراف عقد کشف می‌شود،

۱. حقیقت ودیعه استنابه در حفظ است (قزوینی، بی‌تا: ۲۱۷).

مانند اجاره، رهن، وکالت، عاریه، مضاربه، شرکت (موسوی خمینی، ۱۳۸۳: ۵۴۹/۲؛ موسوی گلپایگانی، بی‌تا: ۵/۳). ید امانی شرعی (قانونی) نیز آن است که خود مالک، آن را به امانت نگذاشته، ولی شارع یا قانون‌گذار آن را به عنوان امانت تلقی کرده است، مانند یابنده مال گمشده که شارع او را امین محسوب می‌نماید (مدرسی، ۱۳۹۳: ۳۲۷).

دو عنصر اذن و مجانی بودن برای جریان امانت در کلام برخی فقها قابل مشاهده است.[۱] برای نمونه، محقق خویی با عبارت «فهو طبعًا أمین من قبل المالك أی مجاز فی إبقاء المال عنده مجّانًا» به عنصر اذن و مجانی بودن اشاره نموده است. با لحاظ این امر، در مورد اجاره یا برخی از عقود امانی دیگر، ممکن است اشکالی به ذهن متبادر شود؛ بدین‌مضمون که این عقود معوض هستند و عنصر مجانی بودن که برای جریان یدِ امانی لازم است، در آن‌ها وجود ندارد. در پاسخ به این اشکال باید گفت که منظور از مجانی بودن این است که بقای عین در نزد امین به صورت مجانی و با اذن مالک باشد؛ برای نمونه در اجاره، اجرت در قبال منفعت باشد نه ذات عین؛ بدین‌جهت امانت که شامل اذن و مجانی بودن است، در خصوص اجاره وجود دارد (موسوی خویی، ۱۴۱۸: ۲۲۰/۳۰؛ تسخیری، ۱۴۳۱: ۶۲/۳). همچنین باید گفت که اثر اذن صرفاً اباحه است و مطلق اباحه، نفی ضمان نمی‌کند، بلکه تنها اباحهٔ مجانی رافع ضمان است (طباطبایی یزدی، ۱۴۱۰: ۳۹/۱؛ شهیدی تبریزی، بی‌تا: ۲۱۸/۲؛ حسینی روحانی، ۱۴۲۹: ۳۵۸/۲). بدین‌جهت است که برای جریان ید امانی، عنصر مجانی بودن ضروری است؛ البته با لحاظ نکته‌ای که ذکر شد.

با بیان این امر که نگهداری عین در برخی از عقود امانی مجانی است و بدین‌جهت ید امانی است، ممکن است اشکال دیگری پیش آید؛ بدین‌بیان که در برخی از مصادیقِ جریان ید ضمانی، مانند مأخوذ بالسوم نیز نگهداری از عین مجانی است و با اذن مالک نیز می‌باشد، در حالی که ید ضمانی است. در پاسخ باید گفت مسئله مأخوذ بالسوم

۱. گرچه از نظر بسیاری از فقها، مجرای قاعدهٔ استیمان، وجود اذن از جانب مالک یا شارع است (امین کسی است که مأذون از سوی مالک یا شارع باشد) و عنصر مجانی بودن مورد تصریح قرار نگرفته است (فاضل موحدی لنکرانی، ۱۳۸۳: ۲۸؛ موسوی بجنوردی، ۱۳۷۹: ۱۹۱/۱؛ مکارم شیرازی، ۱۳۷۰: ۲۶۹/۲)، لیکن به دلیل تفکیک دقیق مصادیق ید امانی از ید ضمانی و دخالت این عنصر در تقسیم ید ضمانی به عدوانی و غیر عدوانی ـ که بیان خواهد شد ـ تصریح به مجانی بودن برای جریان ید امانی، دقیق‌تر است.

خارج از عنوان امانت است؛ زیرا در این مورد، مشتری با قصد خرید عین، آن را در اختیار می‌گیرد و لذا ضامن عوض و ثمن آن است. به عبارت دیگر، اخذ شیء (عین) به وسیله مشتری، مقدمه‌ای برای خرید است که از امانت ـاعم از مالکی و شرعیـ خارج است و موجب ضمان می‌باشد (موسوی بجنوردی، ۱۳۷۹: ۲۱۴/۱).

در مقابل ید امانی، ضمان وجود دارد که اعم از ید ضمانی عدوانی و ید ضمانی غیر عدوانی است. ید ضمانی عدوانی در مواردی است که عنصر اذن مفقود، و علاوه بر آن عنصر عدوان موجود باشد، مانند غصب. ید ضمانی غیر عدوانی نیز در صورتی است که یکی از دو عنصر لازم برای تحقق ید امانی مفقود است و عنصر عدوان نیز وجود ندارد[1] (محقق داماد، ۱۳۸۴: ۱۰۲؛ ر.ک: نراقی، ۱۳۸۰: ۲۷/۱).

با توجه به تقسیم‌بندی مذکور، اگر پردازش مجانی باشد (مانند پردازش داده‌های شخصی توسط رسانه‌ها و شبکه‌های اجتماعی مجازی یا موتورهای جستجو)، رابطهٔ بین شخص موضوع داده و اشخاص پردازش‌کنندهٔ داده، رابطهٔ امانی است؛ زیرا در این موارد، اذن توسط شخص موضوع داده و مجانی بودن برای جریان رابطهٔ امانی موجود است. همچنین در صورتی که پردازش داده‌ها به موجب قرارداد باشد، ید امانی مالکی وجود دارد و در سایر موارد که پردازش به تجویز قانون است، می‌تواند ید امانی قانونی وجود داشته باشد (مانند پردازش داده‌های شخصی برای حفاظت از منافع حیاتی شخص موضوع داده یا دیگران یا پردازش به جهت منافع عمومی).

گرچه رابطهٔ بین اشخاص پردازش‌کننده داده و شخص موضوع داده در صورت وجود اذن و با وجود عنصر مجانی بودن، رابطه‌ای امانی است و در حالات مختلف،از انواع متفاوت رابطهٔ امانی می‌باشد، لیکن چنین رابطهٔ امانی حتی در صورت قراردادی بودن، قابلیت تطبیق کامل با هیچ یک از عقود امانی معین را ندارد و بدین‌جهت نمی‌توان به‌طور مطلق تعهدات اطراف عقود امانی معین را برای اشخاص پردازش‌کننده داده

۱. در اینجا ذکر نکته‌ای مفید است؛ بدین‌توضیح که در هر دو فرضِ ید ضمانی عدوانی و ید ضمانی غیرعدوانی، مسئولیت مدنی وجود دارد؛ لیکن در فرض وجود عنصر عدوان مانند غصب، علاوه بر مسئولیت مدنی، مسئولیت کیفری نیز وجود دارد، ولی در مورد ید ضمانی غیر عدوانی، چنین مسئولیتی محقق نیست (محقق داماد، ۱۳۸۴: ۶۸).

درنظر گرفت. البته در مواردی می‌توان تطبیقاتی داد؛ بدین‌توضیح که به نظر می‌رسد بتوان ماهیت ارتباط بین شخص موضوع داده و اشخاص پردازش‌کننده داده را رابطهٔ بین مودع و امین دانست و ارتباط بین این اشخاص را به نوعی عقد ودیعه تلقی نمود؛ زیرا ودیعه «عقدی است که به موجب آن، یک نفر مال خود را به دیگری می‌سپارد، برای آنکه آن را مجانی نگاه دارد». در بحث حاضر نیز داده‌های شخصی مال هستند[۱] و نگهداری[۲] نیز از مصادیق پردازش است که به آن در GDPR اشاره شده است (EUR-Lex, 2016: 33). بدین‌جهت در جایی که پردازش مجانی است، عناصر عقد ودیعه وجود دارد و می‌توان شخص موضوع داده را مودع و اشخاص پردازش‌کننده داده را مستودع یا امین دانست. با وجود امین بودن اشخاص پردازش‌کننده داده، تعهداتی که برای مستودع در مواد ۶۱۲ تا ۶۳۲ قانون مدنی مقرر شده است، در مواردی که موضوعیت دارد، قابل جریان است. موادی که بر بحث حاضر قابلیت جریان دارند، مواد زیر هستند:

«ماده ۶۱۲ـ امین باید مال ودیعه را به طوری که مالک مقرر نموده، حفظ کند و اگر ترتیبی تعیین نشده باشد، آن را به طوری که نسبت به آن مال متعارف است، حفظ کند؛ والا ضامن است.

ماده ۶۱۳ـ هر گاه مالک برای حفاظت مال ودیعه ترتیبی مقرر نموده باشد و امین از برای حفظ مال، تغییر آن ترتیب را لازم بداند، می‌تواند تغییر دهد؛ مگر اینکه مالک صریحاً نهی از تغییر کرده باشد که در این صورت ضامن است».

این دو ماده می‌توانند مبین تعهد «تضمین امنیت پردازش» به موجب GDPR باشند؛ زیرا اشخاص پردازش‌کننده داده به موجب GDPR باید اقدامات لازم جهت حفظ

۱. گرچه دادهٔ شخصی مانند آنچه در ودیعه متعارف است، شیء مادی قابل اشاره نیست، لیکن به جهت اینکه مجرای عقد ودیعه و قاعدهٔ امانت در جایی است که امرِ مورد امانت، مال باشد و شیء مادی بودن موضوعیت ندارد، همچنین داده‌های شخصی، ماهیتی دو جنبه‌ای دارند که مرکب از بعد مالی (ابعاد مالی دادهٔ شخصی، حق انحصاری هر گونه بهره‌برداری از دادهٔ شخصی است. بهره‌برداری متناسب با دادهٔ شخصی از طریق پردازش است که مصادیق آن در ماه ۴(۲) GDPR بیان شده است. این موارد از قبیل جمع‌آوری، ضبط، ذخیره‌سازی و... نسبت به دادهٔ شخصی است (EUR-Lex, 2016: 33)) و بعد معنوی‌اند، چنین داده‌هایی ارزشمند بوده، مال محسوب شده و می‌توانند مصداق مال‌الامانه باشند.

2. Storage.

امنیت پردازش را لحاظ نمایند، همان طور که امین باید ترتیبات لازم جهت حفظ مال‌الامانه را انجام دهد.

همچنین از ماده ۶۱۲ قانون مدنی، تعهد «کنترل‌کننده به انتخاب پردازنده مناسب» نیز قابل استنباط است؛ زیرا به موجب این ماده، امین باید مال‌الامانه را به صورت متعارف حفظ نماید. در خصوص بحث حاضر می‌توان گفت که عرف انتخاب پردازندهٔ مناسب توسط کنترل‌کننده را با توجه به مال بودن داده‌های شخصی و با لحاظ این امر که پردازنده، نماینده کنترل‌کننده در پردازش است، لازم می‌داند. بنابراین کنترل‌کننده در مقام امین باید اموری که عرف ضروری می‌داند، مانند انتخاب پردازندهٔ مناسب را رعایت نماید.

تعهد «ابلاغ نقض دادهٔ شخصی به شخص موضوع داده» نیز از عقد ودیعه قابل استنباط است؛ زیرا همان طور که در ودیعه، آسیب به مال‌الامانه منطقاً باید به اطلاع مودع رسانده شود، به موجب GDPR نیز نقض دادهٔ شخصی باید به شخص موضوع داده اطلاع داده شود.

به علاوه، مطابق با ماده ۶۱۴ قانون مدنی، «امین ضامن تلف یا نقصان مالی که به او سپرده شده است، نمی‌باشد، مگر در صورت تعدی یا تفریط»، و به موجب ماده ۶۱۵، «امین در مقام حفظ، مسئول وقایعی نمی‌باشد که دفع آن از اقتدار او خارج است». در واقع امین ید امانی دارد. ماده ۸۲ GDPR نیز مقرر می‌کند:

«... ۲ـ هر کنترل‌کنندهٔ درگیر در پردازش، مسئول آسیب ناشی از پردازش است که این مقررات را نقض کرده است. پردازنده تنها در صورتی مسئول آسیب ناشی از پردازش است که از الزامات این مقررات به طور خاص در مورد پردازنده‌ها پیروی نکرده باشد یا در صورتی که خارج یا بر خلاف دستورالعمل‌های قانونی کنترل‌کننده عمل کرده باشد. ۳ـ کنترل‌کننده یا پردازنده از مسئولیت بخش ۲ معاف هستند، اگر ثابت کنند که به هیچ وجه مسئول حادثهٔ موجب خسارت نیستند».

از آنچه در ماده ۸۲ مقرر شده، استنباط می‌شود که ید اشخاص پردازش‌کنندهٔ داده، ید امانی است و در صورت نقص مقررات یا عدم پیروی از دستورات و عمل نمودن برخلاف دستورات ـ که از مصادیق تعدی و تفریط هستند ـ مسئولیت وجود دارد. در

صورت مجانی بودن پردازش و با جریان رابطهٔ امانی بین اشخاص موضوع داده و اشخاص پردازش‌کننده داده، می‌توان گفت که در نظام حقوقی ایران، اشخاص پردازش‌کننده داده در صورت تعدی و تفریط (تقصیر) مسئولیت دارند و باید نسبت به شخص موضوع داده پاسخ‌گو باشند.

فارغ از تطبیق رابطهٔ بین شخص موضوع داده و اشخاص پردازش‌کننده داده با مودع و مستودع، باید گفت که رابطهٔ امانی بین اشخاص پردازش‌کننده داده و شخص موضوع داده، رابطه‌ای ویژه است که درک تعهدات کامل این رابطه، نیاز به تصریح قانون دارد. البته روشن است که به طور کلی با جریان رابطهٔ امانی، اشخاص پردازش‌کننده داده با تقصیر ضامن هستند و بدون تعدی و تفریط مسئولیتی ندارند.

تا کنون فرضی از پردازش بیان شد که با اذن شخص موضوع داده، پردازش مجانی است. در مقابل، اگر پردازش داده‌های شخصی مجانی نباشد (مانند پردازش داده‌های شخصی توسط بانک‌ها برای امور مالی)، ید اشخاص پردازش‌کنندهٔ داده نسبت به شخص موضوع داده، ید ضمانی غیر عدوانی است؛ زیرا با وجود اذن و عدم مجانی بودن ید ضمانی غیر عدوانی محقق است. همچنین اصل بر ضمانی بودن تصرف است و با فقدان یکی از عناصر ید امانی، به اصل رجوع می‌شود. ید ضمانی غیر عدوانی، مصادیق متفاوتی مانند مقبوض به عقد فاسد، مأخوذ بالسوم و... دارد که رابطهٔ حاضر، قابل تطبیق با هیچ یک از این مصادیق نیست و باز هم شفافیت تعهدات اشخاص پردازش‌کننده، تصریح قانون را می‌طلبد. در اینجا نیز از رابطهٔ ضمانی غیر عدوانی صرفاً می‌توان به این نتیجه دست یافت که با وجود ضمانی بودن رابطه، شخص پردازش‌کننده داده بدون تقصیر ضامن است.

۲ـ۲. بررسی تعهدات اشخاص پردازش‌کننده داده در پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» و طرح «حمایت و حفاظت از داده و اطلاعات شخصی»

فارغ از امور پیش‌گفته در خصوص تعهدات اشخاص پردازش‌کننده داده از مبانی حقوق ایران و فقه امامیه، می توان این تعهدات را از اسناد مرتبط یعنی پیش‌نویس لایحهٔ

«صیانت و حفاظت از داده‌های شخصی» منتشرشده در تیرماه ۱۳۹۷ و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» اعلام وصول‌شده در مجلس به تاریخ شهریورماه ۱۴۰۰ نیز بررسی نمود.

پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» در تیرماه سال ۱۳۹۷ در وبگاه وزارت ارتباطات و فناوری اطلاعات ایران در خصوص حمایت از دادهٔ شخصی منتشر شده است. چنین سندی پیش‌نویس است و تا کنون حتی نسخه نهایی برای این پیش‌نویس منتشر نشده است. البته به نظر می‌رسد با ارائهٔ طرح «حمایت و حفاظت از داده و اطلاعات شخصی» که در ۲۴ شهریورماه ۱۴۰۰ در صحن علنی مجلس اعلام وصول شده است، پیش‌نویس مذکور در همین مرحله رها شده باشد؛ به ویژه که طرح مذکور گزیده‌ای از پیش‌نویس سابق است. در واقع این طرح که با چند سال فاصله از ارائهٔ پیش‌نویس، به تازگی در خصوص حمایت از دادهٔ شخصی و اشخاص موضوع داده، در مجلس وصول شده است، در محتوا نسبت به مواد استفاده‌شده از پیش‌نویس تغییری نکرده است و با عدم شفافیت و فقدان افزایش حمایت از دادهٔ شخصی و اشخاص موضوع داده، با همان کیفیتِ مقرر در پیش‌نویس، به حمایت از داده‌های شخصی و اشخاص موضوع داده پرداخته است. حتی پیش‌نویس سال ۱۳۹۷ متضمن ۷۸ ماده، مفاد آن در جهت حمایت مفصل‌تر و مواد مختلف آن نیز با عناوین و زیرعنوان‌های مختلف و جزئی جدا شده‌اند؛ در حالی که طرح مذکور در ۵۶ ماده تنظیم و به صورت کلی‌تری ارائه شده است. بدین‌جهت طرحی که به تازگی به مجلس ارائه شده است، نسبت به پیش‌نویس سال ۱۳۹۷ ضعیف‌تر است. البته از سوی دیگر، پیش‌نویس به دلیل اینکه حتی به صورت لایحه مطرح نشده است، نسبت به طرح در مرحله پایین‌تری قرار دارد. با لحاظ مطالب پیش‌گفته و توجه به این امر که حمایت‌های طرح و پیش‌نویس یکسان است و در عین حال پیش‌نویس به جنبه‌هایی در خصوص داده‌های شخصی اشاره نموده است که از نگاه طرح مورد غفلت واقع شده‌اند، مبنای بررسی، پیش‌نویس است؛ لیکن در مطالب مرتبط، علاوه بر ارجاع به پیش‌نویس، به شماره ماده طرح نیز جهت دسترسی بهتر اشاره می‌شود (در موضوع‌های واحد، شماره مواد در پیش‌نویس و طرح متفاوت است).

اکنون باید گفت که باب سوم پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» در چندین ماده، دامنهٔ تعهدات کنترل‌کننده‌ها و پردازنده‌ها را مشخص می‌کند. مواد مذکور به شرح ذیل هستند:

ماده ۱۵ پیش‌نویس (مفاد این ماده در طرح وجود ندارد):

«تعهدات مقرر در این باب به عهده کنترلگر است؛ مگر اینکه به موجب قانون یا توافق یا قرارداد، پردازشگر عهده‌دار آن‌ها شود».

ماده ۱۶ پیش‌نویس (ماده ۲۷ طرح):

«همه کارکردهای فرایند پردازش داده‌های شخصی باید بر پایه دستور یا درخواست مستند کنترلگر باشد؛ در غیر این صورت، پردازشگر به عنوان کنترلگر پردازش هم شناخته می‌شود».

ماده ۱۷ پیش‌نویس (تبصره ۱ ماده ۲۷ طرح):

«چنانچه هر یک از کارکردهای پردازش، کنترلگر یا پردازشگر مختص به خود را داشته باشد، تنها نسبت به همان کارکرد تعهد خواهند داشت».

ماده ۱۸ پیش‌نویس (تبصره ۲ ماده ۲۷ طرح):

«در صورت تعدد کنترلگران یا پردازشگران در هر کارکرد، فرض بر تعهد برابر آن‌هاست؛ مگر اینکه خلاف آن ثابت شود».

با توجه به ماده ۱۵ پیش‌نویس، کنترل‌کننده مسئول اصلی پردازش است و پاسخ‌گویی بر عهده اوست، مانند آنچه در GDPR مقرر شده است؛ لیکن ماده ۱۵ با مواد GDPR در خصوص مسئولیت کنترل‌کننده تفاوت دارد، بدین‌توضیح که به موجب GDPR، اصل بر مسئولیت کنترل‌کننده است و تنها در صورتی که پردازنده بدون مشورت با کنترل‌کننده، عملی مستقل در مورد فعالیت‌های پردازشِ داده داشته باشد، پردازنده به عنوان کنترل‌کنندهٔ داده‌ها در نظر گرفته خواهد شد و به عبارت دیگر، تمام مسئولیت‌ها و تعهدات یک کنترل‌کننده با پردازنده خواهد بود (Eija, 2018: 17-18). در واقع از نگاه GDPR، تجاوز پردازنده از دستورات کنترل‌کننده تنها استثنا بر اصل مسئولیت کنترل‌کننده است. گرچه چنین استثنایی در ماده ۱۶ پیش‌نویس مقرر شده است، لیکن ماده ۱۵ پیش‌نویس نیز استثنایی دیگر بر اصل مسئولیت کنترل‌کننده دارد و مسئولیت را با پردازنده

می‌داند اگر که «به موجب قانون یا توافق یا قرارداد، پردازشگر عهده‌دار آن‌ها باشد». همچنین به موجب بند ت ماده ۲ این پیش‌نویس:

«... در صورت نبود کنترلگر یا عدم امکان اتصاف پردازش به آن، پردازشگر به عنوان کنترلگر نیز شناخته می‌شود».

در خصوص دو استثنای اخیر بر اصل مسئولیت کنترل‌کننده که در GDPR وجود ندارد باید گفت که گرچه این دو استثنا با افزایش دامنهٔ تعهدات پردازنده‌ها موجب تقویت حمایت از داده‌های شخصی و اشخاص موضوع داده است، لیکن در بند ت ماده ۲، فرض دقیقی بیان نشده است؛ چرا که کنترل‌کننده در اصل، مسئول پردازش است و نمی‌توان حالتی را فرض کرد که پردازش متصف به کنترل‌کننده نباشد؛ زیرا کنترل‌کننده شخصی است که پردازش را به پردازنده واگذار کرده است و پردازنده نماینده کنترل‌کننده است، مگر اینکه عدم اتصاف پردازش به کنترل‌کننده به دلیل این باشد که پردازنده بر خلاف یا بدون دستور کنترل‌کننده عمل کرده است که این امر در ماده ۱۶ پیش‌نویس مورد تصریح قرار گرفته و در این بند نیاز به اشاره به آن با عبارات دیگر نیست.

همچنین نسبت به ماده ۱۸ پیش‌نویس (تبصره ۲ ماده ۲۷ طرح) که «در صورت تعدد کنترلگران یا پردازشگران در هر کارکرد، فرض را بر تعهد برابر آن‌ها می‌داند؛ مگر اینکه خلاف آن ثابت شود» نیز ابهامی وجود دارد و آن عبارت «تعهد برابر» است. در واقع معلوم نیست که تعهد برابر به چه معناست و با بروز خسارت، روشن نیست که نحوهٔ جبران به صورت مساوی یا به صورت نسبی است. بدین‌جهت مناسب بود که از عبارت دقیق‌تری استفاده می‌شد. برای نمونه، همان طور که ذکر شد، GDPR مسئولیت اشخاص پردازش‌کنندهٔ داده را در زمانی که مشترک باشند، تضامنی دانسته و بر این امر در ماده ۲۶(۳)[1] تصریح نموده است؛ گرچه به موجب مفهوم مخالف ماده ۴۰۳ قانون تجارت[2]

۱. «شخص موضوع داده می‌تواند حقوق خود به موجب این مقررات را در خصوص و علیه هر یک از کنترل‌کننده‌ها اعمال کند» (EUR-Lex, 2016: 48).

۲. «در کلیه مواردی که به موجب قوانین یا موافق قراردادهای خصوصی، ضمانت تضامنی باشد، طلبکار می‌تواند به ضامن و مدیون اصلی مجتمعاً رجوع کرده یا پس از رجوع به یکی از آن‌ها و عدم وصول طلب خود، برای تمام یا بقیه طلب به دیگری رجوع نماید».

و اصل عدم که مبیّن عـدم تـضامن اسـت، مـسئولیت تـضامنی در نظـام حقـوقی ایـران خلاف قاعده و اصل است و وجود مسئولیت تضامنی نیاز به تصریح دارد و بدین‌جهت مسئولیت تضامنی منتفی است، لیکن عبارت ماده ۱۸ پیش‌نویس بین مسئولیت مـساوی و نسبی مجمل است.

همچنین به موجب ماده ۳۱ پیش‌نویس (ماده ۳۸ طرح):

«کنترلگران در برابر اشخاص موضوع داده از پاسخ‌گویی کامل برخوردارنـد؛ اعـم از آنکه تعهداتشان با آن‌ها پیرو عقد لازم منعقد شده یـا در تفـاهم‌نامـه یـا اسـنادی ماننـد خط‌مشی‌های حریم خصوصی مندرج باشد».

این ماده نیز مبیّن اصل مسئولیت کنترل‌کننده بر اساس GDPR است، با این تفاوت که ماده ۳۱ پیش‌نویس به بستری که چنین تعهداتی را الزامی می‌سازد نیز اشـاره نمـوده است. گرچه اشاره به این امر مناسب است، لیکن جای حکم قانون بین این موارد خالی است؛ زیرا ممکن است تعهدات مختلف کنترل‌کننده در مقابل اشخاص موضـوع داده به موجب حکم قانون باشد که جدای از قرارداد، تفاهم‌نامه یـا اسـناد مربـوط بـه حـریم خصوصی است.

در این راستا ماده ۵۹ پیش‌نویس (ماده ۴۵ طرح) نیز بیان می‌کند:

«کنترلگر و پردازشگر در برابر تعهدات خود مسئولیت مستقل دارند».

این امر در GDPR نیز پیش‌بینی شده است و اشاره پیش‌نویس به ایـن امـر مناسـب است. به علاوه به موجب ماده ۶۰ پیش‌نویس (ماده ۴۵ طرح):

«پردازشگر در صورتی معاف از مسئولیت است که: الف- اقدام وی با دستور یا درخواست کنترلگر مغایرت نداشته باشد؛ ب- در صورت غیر قانونی دانستن دستور یا درخواسـت مورد نظر، آگاهی لازم را به کنترلگر داده باشد».[1]

۱. ماده ۴۵ طرح در این خصوص، بند زیر را اضافه نموده است: «کنترلگر و پردازشـگر در برابـر تعهـدات خود مسئولیت مستقل دارند و زیان‌دیده همزمان می‌تواند به کنترلگر یا پردازشگر مراجعـه و جبـران همـه زیان‌ها را مطالبه نماید. پردازشگر در صورتی معاف از مسئولیت است که: الف- اقـدام وی بـا دسـتور یـا درخواست کنترلگر مغایرت نداشته باشد؛ ب- در صورت غیر قانونی دانستن دستور یـا درخواسـت مـورد نظر، هشدار لازم را به کنترلگر داده باشد؛ پـ در صورت زیانبار دانستن پـردازش، از نـاظر ویـژه کـسب تکلیف کرده باشد».

به نظر می‌رسد مفاد مذکور غیر دقیق تدوین شده است؛ زیرا مبنای معافیت از مسئولیت، اموری مانند عدم تقصیر است (با توجه به مبانی مختلف مسئولیت، مبنای معافیت هم متفاوت می‌گردد) و عدم مغایرت با دستورات کنترل‌کننده از موجبات معافیت نیست. از این ماده استنباط می‌شود در فرضی که پردازنده تقصیر نموده، لیکن از دستورات کنترل‌کننده تجاوز نکرده است، مسئولیتی ندارد که این امر صحیح به نظر نمی‌رسد. بند ب نیز همین اشکال را دارد؛ زیرا اطلاع‌رسانی به کنترل‌کننده نمی‌تواند مبنای معافیت از مسئولیت باشد.

پیش‌نویس و طرح به نوعی به تعهد «حفظ سوابق فعالیت‌های پردازش» نیز اشاره نموده‌اند؛ بدین‌توضیح که به موجب ماده ۳۳ پیش‌نویس (ماده ۴۰ طرح):

«کنترلگر یا پردازشگر موظف است همه یا هر یک از داده‌ها و اطلاعات ذیل را تا حداقل تا شش ماه پس از پاک شدن داده‌های شخصی نگهداری کند:[1] الف- داده‌های رخداد نگار (Log (Files و داده‌های ترافیک حاصل از پردازش داده‌های شخصی؛ ب- اطلاعات هویتی اشخاص موضوع داده‌ها؛ پ- انواع پردازش‌های انجام‌شده بر روی داده موردنظر و هدف یا اهداف آن؛ ت- اطلاعات هویتی کنترلگران یا پردازشگران مرتبط با پردازش مورد نظر. تبصره[2] - کمیسیون می‌تواند زمان نگهداری و حفاظت از اطلاعات و داده‌های موضوع این ماده را حسب مورد تا دو سال افزایش دهد».

این مفاد نیز خالی از اشکال نیست، بدین‌توضیح که اولاً حفظ سوابق را منوط به وضعیتی نموده که داده‌های شخصی پاک شده است. ثانیاً به طور کلی باید گفت که عبارت این ماده غیر دقیق است: «همه یا هر یک از داده‌ها را بعد از پاک شدن دادهٔ شخصی نگه دارد». این عبارت به چه معناست؟ در واقع در زمانی که داده‌ها پاک شده است، چگونه می‌توان همه یا هر یک از داده‌ها را حفظ نمود؟ مگر اینکه بیان شود بعد از پاک کردن داده‌ها، که بدین‌معناست که با حذف داده‌های شخصی باید داده‌ها و اطلاعاتی حفظ شوند. با این فرض هم باز اشکال وجود دارد؛ زیرا در زمانی که

۱. ابتدای ماده در طرح بدین‌صورت تغییر نموده است: «کنترلگر یا پردازشگر موظف است اطلاعات ذیل را تا ۱۸ ماه پس از پردازش داده‌ها و اطلاعات را شخصی نگهداری کند».

۲. تبصره طرح نیز به این محتوا تغییر یافته است: «تبصره- داده‌ها و اطلاعات و اطلاعات موضوع این گفتار علیه کنترلگر و پردازشگر آن قابل استناد است».

داده‌ها باید حذف شوند و هدف از پردازش حاصل شده و دیگر مبنای حقوقی برای حفظ داده‌ها و پردازش وجود ندارد، با چه مبنایی باید داده‌ها حفظ شوند. (البته به دلیل اینکه ابتدای ماده در طرح بدین‌صورت تغییر کرده است: «کنترلگر یا پردازشگر موظف است اطلاعات ذیل را تا ۱۸ ماه پس از پردازش داده‌ها و اطلاعات را شخصی نگهداری کند»، این اشکال بر قسمت ابتدایی طرح وارد نیست؛ هرچند ایراد دیگری مانند نارسایی معنایی دارد.)

همچنین این اشکال در مورد بند ب نیز وجود دارد (پیش‌نویس و طرح) که بیان کرده باید «اطلاعات هویتی اشخاص موضوع داده‌ها» نگه‌داری شود. اطلاعات هویتیِ چنین اشخاصی، مصداق بارز دادهٔ شخصی است و با پاک کردن داده‌ها و عدم مبنای حقوقی برای پردازش، به چه دلیل باید اطلاعات هویتی اشخاص موضوع داده حفظ شوند؟ در اینجا باید گفت که اگر حفظ چنین اطلاعاتی ضروری است، این اطلاعات هویتی باید به صورت مستعار و رمزگذاری‌شده نگه‌داری شوند تا ضرورت قانونی در کنار حقوق اشخاص موضوع داده رعایت گردد.

تعهد «تضمین امنیت پردازش» نیز در مواد ۲۸ تا ۳۰ پیش‌نویس (مواد ۳۵ تا ۳۷ طرح) بیان شده است. مواد مذکور مقرر می‌کنند:

ماده ۲۸:

«هر یک از کارکردها و مراحل پردازش، باید از تمهیدات ایمنی و امنیتی ویژه خود برخوردار باشد. این تمهیدات باید هر سه سطح ذیل را در بر گیرد: الف- ایمنی و حفاظت فیزیکی، شامل زیرساخت‌ها، سازه‌ها و سامانه‌های سخت‌افزاری مرتبط؛ ب- ایمنی و حفاظت اطلاعات، شامل انواع پردازنده‌های سخت‌افزاری و نرم‌افزاری؛ و پ- ایمنی و حفاظت انسانی، شامل همه کنترلگران و پردازشگران اصلی و مرتبط».

ماده ۲۹:

«سازوکارها و ابزارهای سخت‌افزاری و نرم‌افزاری ایمنی و حفاظتی مقرر یا پیشنهادی باید با شرایط ذیل سازگار باشد: الف- نوع و میزان آسیب‌زایی تهدیدهای بالقوه و بالفعل از نگاه اشخاص موضوع داده؛ ب- تأمین‌پذیری آن‌ها؛ و پ- توانمندی فنی و اجرایی».

ماده ۳۰:

«اشخاص موضوع داده تنها در صورتی می‌توانند کنترلگر یا پردازشگر را به رعایت تمهیدات ایمنی و حفاظتی فراتر از ضوابطِ مراجع صلاحیت‌دار ملزم کنند که اجرای آن تمهیدات، ایفای تعهدات آن‌ها را مختل نکرده و هزینه‌های آن را نیز عهده‌دار شوند».

مواد مذکور مناسب هستند؛ لیکن بهتر بود که مصادیقی برای «تمهیدات ایمنی و امنیتی» نیز بیان می‌شد، مانند آنچه در GDPR وجود دارد و یکی از مصادیق چنین تمهیداتی را مستعار ساختن و رمزگذاری داده‌های شخصی می‌شمارد.

همچنین مشابه با مأمور حفاظت از داده به موجب GDPR، در پیش‌نویس به ناظر ویژه اشاره شده است. بند ث ماده ۲ پیش‌نویس (بند ث ماده ۲ این طرح) مقرر می‌کند:

«ناظر ویژه کسی است که پیرو حکم صادره از سوی کمیسیون، صلاحیت نظارت بر پردازش داده‌های شخصی را می‌یابد».

به موجب GDPR، مأمور حفاظت از داده توسط کنترل‌کننده و پردازنده در موارد مشخصی منصوب می‌شود؛ اما به موجب این پیش‌نویس، ناظر ویژه را کمیسیون صیانت از داده‌های شخصی[۱] تعیین می‌کند. به نظر می‌رسد اعطای اختیار تعیین چنین ناظری به کنترل‌کننده‌ها و پردازنده‌ها، برای هدف تعیین چنین ناظری یعنی نظارت بر پردازش داده‌های شخصی و حفاظت از چنین داده‌هایی مناسب‌تر است؛ زیرا در مواردی که وجود چنین ناظری ضروری است، یک کنترل‌کننده یا پردازنده بهتر می‌تواند ناظر متخصص و مناسب با فعالیت‌های پردازشی را انتخاب نماید. در واقع، چنین ناظری

۱. به موجب ماده ۴۰ پیش‌نویس (ماده ۱۴ طرح)، اعضای کمیسیون به شرح ذیل هستند: «کمیسیون از اعضای ذیل تشکیل می‌شود: وزیر ارتباطات و فناوری اطلاعات به عنوان رئیس کمیسیون؛ وزیر اطلاعات؛ وزیر کشور؛ وزیر دادگستری؛ وزیر فرهنگ و ارشاد اسلامی؛ وزیر اقتصاد و امور دارایی؛ دبیر شورای عالی و رئیس مرکز ملی فضای مجازی؛ معاون پیشگیری از وقوع جرم قوه قضاییه؛ رئیس کمیسیون اصل ۹۰ مجلس شورای اسلامی؛ دادستان کل کشور؛ و دبیر شورای اجرایی فناوری اطلاعات به عنوان دبیر کمیسیون». در طرح، بند دوازدهم نیز وجود دارد که بیان می‌کند: «دو نفر از صاحب‌نظران دارای سوابق مرتبط با مدیریت، سیاستگذاری، حکمروایی داده‌ها و اطلاعات به پیشنهاد دبیر و تأیید رئیس کمیسیون» از اعضای کمیسیون هستند.

مانند داور است که طرفین یک دعوی خود بهتر می‌توانند داور مناسب را جهت حل و فصل انتخاب نمایند.

به علاوه بر اساس ماده ۵۴ پیش‌نویس (ماده ۲۳ طرح)، وجود ناظر ویژه در موارد خاصی ضروری است. این موارد عبارت‌اند از:

«الف- پردازش داده‌های شخصی حیاتی و حسّاس؛ ب- پردازش کلان‌داده‌های شخصی؛[۱] پ- زیان‌ها و آسیب‌های جدی یا پرشمار بالقوه و بالفعل پردازش‌ها به داده‌های شخصی؛ ت- سایر موارد به تشخیص هیئت نظارت و تأیید کمیسیون».

مفاد مذکور مناسب است و لزوم وجود چنین ناظری در برخی موارد مشابه با GDPR است؛ زیرا بندهای الف و ب پیش‌نویس مطابق با ماده ۳۷(۱)ب و ج GDPR ـ که بیان شد ـ است.

همچنین به موجب ماده ۵۵ پیش‌نویس (ماده ۲۴ طرح)، شرایط احراز صلاحیت ناظر ویژه عبارت‌اند از:

«الف- نداشتن سوءپیشینه کیفری و انتظامی؛ ب- داشتن حسن شهرت؛ پ- دارا بودن تجربه و تخصص لازم؛ ت- نداشتن تعارض منافع با موضوع نظارت».

شرایط مذکور مناسب و مشابه با مفاد مربوطه در GDPR است. به موجب ماده ۳۷(۵) GDPR، مأمور حفاظت از داده باید خصوصیات حرفه‌ای، دانش تخصصی در زمینه قانون و رویه‌های حفاظت از داده و توانایی انجام وظایف قانونی مذکور را داشته باشد. به علاوه بر اساس ماده ۳۸(۶) GDPR، مأمور حفاظت از داده می‌تواند وظایف

۱. کلان‌داده‌ها مجموعه عظیمی از داده‌ها مانند ابرداده‌ها در جستجوهای اینترنتی، تراکنش کارت‌های اعتباری، داده‌های موجود در پیام‌رسان‌های اجتماعی، داده‌های موقعیت تلفن همراه، داده‌های حسگرها در خودروها و دیگر دستگاه‌ها و... هستند. کلان‌داده‌ها در حال حاضر، موضوع اصلی در زمینهٔ مدیریت، بازاریابی و تحقیقات علمی هستند و هر دو بخش عمومی و خصوصی در حال استفاده مکرر از کلان‌داده‌ها هستند؛ برای مثال، یک سازمان سلامت از روش‌های تحلیلی برای کاهش بستری مجدد بیماران بستری‌شده به دلیل حمله قلبی استفاده می‌کند. این سازمان از داده‌های جمع‌آوری‌شده در طول مدت اقامت بیماران در بیمارستان استفاده می‌کند. با تحلیل چنین داده‌هایی، این سازمان می‌تواند ویژگی‌ها یا رفتارهای مرتبط را که موجب بستری مجدد بیمار می‌شوند، تشخیص دهد و اگر یک بیمار خاص، این رفتارها را نشان دهد، سازمان سلامت می‌تواند در موقعیت مناسب از بیمار حفاظت کند تا مانع بستری مجدد وی شود (Information Commissioner's Office, 2014: 6-8).

دیگری را انجام دهد، لیکن کنترل‌کننده یا پردازنده باید اطمینان حاصل کنند که چنین وظایفی منجر به تعارض منافع نمی‌شود (EUR-Lex, 2016: 56).

با وجود شباهت‌های بیان‌شده بین مأمور حفاظت از داده به موجب GDPR و ناظر ویژه بر اساس پیش‌نویس و طرح ایرانی، تفاوت‌هایی نیز وجود دارد؛ برای نمونه، مطابق با ماده ۵۶ پیش‌نویس (ماده ۲۵ طرح):

«مدت فعالیت ناظر ویژه به دو شکل تعیین می‌شود: الف- موردی متناسب با موضوع نظارت واگذارشده به وی؛ ب-[1] دوره‌ای برای مدت سه سال و قابل تمدید برای دوره‌های مشابه».

همان طور که از ماده مذکور روشن است، در صورت عدم تعیین مدت در موارد خاص، دورهٔ نظارت سه سال است؛ لیکن به موجب GDPR ـهمان طور که بیان شدـ برای نظارت مأمور حفاظت از داده، بازهٔ زمانی مقرر نشده است و این امر می‌تواند به‌عنوان نقص GDPR تلقی شود. از دیگر تفاوت‌ها می‌توان به عدم اشاره پیش‌نویس و طرح به وظایف ناظر ویژه اشاره کرد؛ در حالی که مواد ۳۸ و ۳۹ GDPR به طور خاص و تفصیلی، وظایف مأمور حفاظت از داده را بیان کرده‌اند ـهمان طور که بیان شدـ. این امر نیز از نواقص پیش‌نویس و طرح ایرانی است و ضرورت بیان وظایف ناظر ویژه احساس می‌شود.

تا بدینجا در مقام قیاس پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» با GDPR، نقدهای مختلفی نسبت به دو سند ایرانی بیان شد. ضروری است که قانون‌گذار اشکالات پیش‌گفته را رفع نماید. همچنین مناسب است با توجه به حمایت‌های GDPR، مفاد مناسبی در خصوص تعهدات اشخاص پردازش‌کنندهٔ داده ارائه نماید که حمایت‌های مؤثر و کافی از داده‌های شخصی و اشخاص موضوع داده نماید.[2]

۱. این بند در طرح بدین‌صورت است: «ب- دوره‌ای برای مدت چهار سال و قابل تمدید برای دوره‌های مشابه بر اساس شیوه‌نامه مصوب کمیسیون».

۲. مفاد پیشنهادی این پژوهش در خصوص تعهدات مذکور با توجه به حمایت‌های موجود در GDPR در «پیوست شماره ۱» قابل دسترسی است.

نتیجه‌گیری

تعهدات اشخاص پردازش‌کنندهٔ داده در میان مواد ۲۴ تا ۳۹ GDPR مقرر شده است. مواد مذکور متضمن تعهدات خاصی هستند؛ ماده ۲۴ GDPR، مبیّن اصل مسئولیت و پاسخ‌گویی کنترل‌کننده است، چه پردازش توسط خود کنترل‌کننده یا از طرف کنترل‌کننده انجام شده باشد. ماده ۳۰ GDPR، کنترل‌کننده، پردازنده و نمایندگان آن‌ها را ملزم به حفظ سابقه فعالیت‌های پردازش می‌کند. ماده ۳۱ GDPR، تعهد همکاری با مراجع نظارتی را مقرر می‌کند. ماده ۳۲ GDPR، کنترل‌کننده و پردازنده را ملزم به انجام اقدامات فنی و سازمانی مناسب در جهت حفظ امنیت داده‌های شخصی می‌کند. ماده ۳۳(۱) GDPR در مورد نقض داده‌های شخصی، کنترل‌کننده را ملزم می‌نماید که بدون تأخیر غیر ضروری و پس از آگاهی، نقض داده‌های شخصی را به مرجع نظارتیِ صالح اطلاع دهد. همچنین ماده ۳۴(۱) GDPR به هنگام شناسایی احتمال خطر مهم از نقض داده‌ها برای حقوق و آزادی‌های اشخاص موضوع داده، کنترل‌کننده را ملزم به اطلاع‌رسانی برای اشخاص موضوع داده می‌نماید و در نهایت مواد ۳۷ تا ۳۹ GDPR در خصوص مأمور حفاظت از داده و تعهد انتصاب این مأمور توسط اشخاص پردازش‌کننده است. جهت بررسی تعهدات مذکور در نظام حقوقی ایران، به دلیل عدم اشاره قوانین موضوعه و دکترین حقوقی به این امر، با جستجو در مبانی حقوق ایران و فقه امامیه روشن شد که با توجه به نوع تصرف اشخاص پردازش‌کنندهٔ داده نسبت به دادهٔ شخصی، چگونگی تعهدات اشخاص پردازش‌کنندهٔ داده متفاوت می‌گردد. در این خصوص، این نتیجه حاصل شد که اگر پردازش مجانی باشد، رابطهٔ بین شخص موضوع داده و اشخاص پردازش‌کنندهٔ داده، رابطهٔ امانی است و در مقابل، اگر پردازش داده‌های شخصی مجانی نباشد، ید اشخاص پردازش‌کنندهٔ داده نسبت به شخص موضوع داده، ید ضمانی غیر عدوانی است. با تبیین نوع تصرف اشخاص پردازش‌کنندهٔ داده باید گفت در مواردی که ید امانی است، تعهدات اشخاص پردازش‌کنندهٔ داده مانند امین است و در سایر موارد که محل جریان ید ضمانی است، اشخاص پردازش‌کنندهٔ داده ضامن هستند. فارغ از بحث مبنایی پیش‌گفته، پیش‌نویس

لایحهٔ «صیانت و حفاظت از داده‌های شخصی» و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» نیز به تعهدات کنترل‌کننده‌ها و پردازنده‌ها در مواد مختلفی اشاره نموده‌اند؛ لیکن سندهای مذکور علاوه بر عدم اعتبار قانونی، اشکالات مختلفی نیز دارند که از کارآمد بودن آن‌ها می‌کاهد. بدین‌جهت تبیین دقیق تعهدات اشخاص پردازش‌کنندهٔ داده نیاز به تصریح قانون‌گذار دارد. در این خصوص مفاد پیشنهادی در «پیوست شماره ۱» قابل استفاده‌اند.

پیوست شماره ۱

ماده نخست- مسئولیت و پاسخ‌گویی کنترل‌کننده: با در نظر گرفتن ماهیت، دامنه، زمینه و اهداف پردازش و همچنین خطرات احتمالی و شدت خطر برای حقوق و آزادی‌های اشخاص حقیقی، کنترل‌کننده باید اقدامات فنی و سازمانی مناسبی را برای تضمین و اثبات اینکه پردازش مطابق با این قانون است، انجام دهد. این اقدامات در صورت لزوم باید بازبینی و به‌روزرسانی شوند.

ماده دوم- کنترل‌کنندگان مشترک: در صورتی که دو یا چند کنترل‌کننده به طور مشترک، اهداف و ابزار پردازش را تعیین کنند، آن‌ها کنترل‌کنندگان مشترک هستند که باید به طور شفاف، مسئولیت‌های مربوط به خود را در قبال تعهدات مندرج در این قانون مشخص کنند، به ویژه در مورد اِعمال حقوق اشخاص موضوع داده. این امر به موجب قرارداد بین کنترل‌کنندگان مشخص می‌شود، مگر اینکه مسئولیت‌های مربوط به کنترل‌کنندگان توسط قانون تعیین شده باشد.

تبصره ۱- قرارداد مذکور در این ماده باید به طور مناسب، نقش‌ها و روابط کنترل‌کنندگان مشترک را در مقابل اشخاص موضوع داده منعکس نماید. مفاد اصلی این قرارداد باید در دسترس شخص موضوع داده قرار گیرد.

تبصره ۲- صرف‌نظر از روابط مقرر در قرارداد به موجب تبصره ۱، شخص موضوع داده می‌تواند حقوق خود را بر اساس این قانون در خصوص و علیه هر یک از کنترل‌کنندگان اعمال کند.

ماده سوم- انتخاب پردازنده مناسب توسط کنترل‌کننده: در صورتی که پردازش از

طرف کنترل‌کننده انجام می‌شود، کنترل‌کننده باید صرفاً از پردازنده‌هایی استفاده نماید که اقدامات کافی جهت تضمین امنیت پردازش ارائه می‌کنند، به گونه‌ای که پردازش مطابق با الزامات این قانون باشد و حفاظت از حقوق اشخاص موضوع داده تضمین شود.

ماده چهارم- حفظ سوابق فعالیت‌های پردازش: هر کنترل‌کننده و در صورت وجود نمایندهٔ کنترل‌کننده، باید سوابق فعالیت‌های پردازش را تحت مسئولیت خود حفظ کند. این سوابق باید شامل تمام اطلاعات ذیل باشد: الف- نام و جزئیات تماس کنترل‌کننده و در صورت وجود، کنترل‌کنندگان مشترک، نمایندهٔ کنترل‌کننده و ناظر ویژه؛ ب- هدف از پردازش؛ ج- توصیف دسته‌های اشخاص موضوع داده و طبقه‌بندی داده‌های شخصی؛ د- گروه‌های دریافت‌کنندهٔ داده‌های شخصی از جمله دریافت‌کنندگان در کشورهای ثالث که داده‌های شخصی برای آن‌ها افشا خواهد شد؛ هـ در صورت انتقال داده‌های شخصی به کشور ثالث، بیان آن کشور ثالث؛ و- در صورت امکان، محدوده زمانی پیش‌بینی‌شده برای حذف دسته‌های مختلف داده؛ ز- در صورت امکان، توضیحات کلی در مورد اقدامات امنیتی فنی و سازمانی. همچنین هر پردازنده و در صورت وجود، نمایندهٔ پردازنده باید تمام سوابق فعالیت‌های پردازشی انجام‌شده از طرف کنترل‌کننده را که شامل موارد زیر است، نگهداری نماید: ۱- نام و جزئیات تماس پردازنده یا پردازنده‌ها و هر کنترل‌کننده‌ای که پردازش از طرف آن انجام شده است و در صورت وجود، نمایندهٔ کنترل‌کننده یا پردازنده و ناظر ویژه؛ ۲- دسته‌بندی پردازش انجام‌شده از طرف هر کنترل‌کننده؛ ۳- در صورت انتقال داده‌های شخصی به کشور ثالث، بیان آن کشور ثالث؛ ۴- در صورت امکان، توضیحات کلی در مورد اقدامات امنیتی فنی و سازمانی.

ماده پنجم- همکاری و مشورت با مرجع نظارتی: کنترل‌کننده و پردازنده و در صورت وجود، نمایندگان آن‌ها باید در صورت درخواست با مرجع نظارتی در انجام وظایف همکاری کنند. کنترل‌کننده قبل از پردازش باید با مرجع نظارتی مشورت کند، چنانچه با ارزیابی پردازش، متوجه خطرات مهم در خصوص حقوق و آزادی اساسی اشخاص موضوع داده می‌گردد؛ به طوری که در صورت عدم توجه به این امر توسط

کنترل‌کننده و عدم اقدام وی در جهت کاهش خطرات، پردازش پیامدهای منفی مهمی را به دنبال دارد. همچنین در این شرایط ممکن است به موجب قانون، نیاز به دریافت مجوز قبلی از مرجع نظارتی باشد.

ماده ششم- تضمین امنیت پردازش: با در نظر گرفتن وضعیت پردازش، هزینه‌های انجام آن، ماهیت، دامنه، زمینه و اهداف پردازش و همچنین خطرات با احتمال و شدت متفاوت برای حقوق و آزادی‌های اشخاص حقیقی، کنترل‌کننده و پردازنده باید اقدامات فنی و سازمانی مناسب را جهت تضمین سطح امنیت که متناسب با خطرات است، انجام دهند. این اقدامات عبارت‌اند از: الف- مستعارسازی و رمزگذاری داده‌های شخصی؛ ب- تضمین محرمانگی، تمامیت، در دسترس بودن و انعطاف‌پذیری دستگاه‌ها و خدمات پردازش؛ ج- بازیابی به موقع جهت دسترسی به داده‌های شخصی در صورت بروز حادثهٔ فیزیکی یا فنی؛ د- فرایندی برای آزمایش منظم، ارزیابی و اثربخشی اقدامات فنی و سازمانی مناسب جهت اطمینان از امنیت پردازش.

ماده هفتم- اطلاع‌رسانی نقض داده‌های شخصی به مرجع نظارتی: در مورد نقض داده‌های شخصی، کنترل‌کننده باید بدون تأخیر غیر ضروری و در صورت امکان، ظرف ۷۲ ساعت پس از آگاهی، نقض داده‌های شخصی را به مرجع نظارتی اطلاع دهد؛ مگر اینکه نقض داده‌های شخصی برای حقوق و آزادی‌های اشخاص حقیقی خطری ایجاد نکند. در صورتی که ظرف ۷۲ ساعت اطلاع‌رسانی به مرجع نظارتی انجام نشود، همراه با اطلاع‌رسانی، دلایل تأخیر نیز باید بیان شود. پردازنده باید پس از آگاهی از نقض داده‌های شخصی، بدون تأخیر غیر ضروری، کنترل‌کننده را مطلع سازد.

ماده هشتم- ابلاغ نقض داده‌های شخصی به شخص موضوع داده: هنگامی که نقض داده‌های شخصی به احتمال زیاد منجر به خطر مهم برای حقوق و آزادی‌های اشخاص حقیقی می‌شود، کنترل‌کننده باید نقض داده‌های شخصی را بدون تأخیر غیرضروری به شخص موضوع داده نیز ابلاغ کند. ابلاغ مذکور باید با زبانی روشن و واضح باشد.

ماده نهم- انتصاب ناظر ویژه: کنترل‌کننده و پردازنده باید ناظر ویژه را در موارد

ذیل منصوب کنند: الف- پردازش توسط مرجع یا نهاد عمومی انجام می‌شود، مگر برای دادگاه‌هایی که در صلاحیت قضایی خود عمل می‌کنند؛ ب- فعالیت اصلی کنترل‌کننده یا پردازنده که مجموعه عملیات پردازشی آن‌ها را تشکیل می‌دهد، شامل پردازشی است که مستلزم نظارت منظم و نظام‌مند بر اشخاص موضوع داده در مقیاس وسیع با توجه به ماهیت، دامنه و اهداف پردازش است؛ یا ج- فعالیت اصلی کنترل‌کننده یا پردازنده که مجموعه عملیات پردازشی آن‌ها را تشکیل می‌دهد، شامل پردازش دسته‌های خاص از داده‌های شخصی -شامل داده‌های شخصی حساس، داده‌های مربوط به امور کیفری و داده‌های شخصی کودکان- در مقیاس وسیع است.

کتاب‌شناسی

۱. پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی تیرماه سال ۱۳۹۷ ش.، منتشرشده در وبگاه وزارت ارتباطات و فناوری اطلاعات به نشانی: <https://www.ict.gov.ir/fa/newsagency/21691>.

۲. تسخیری، محمدعلی، ***القواعد الاصولیة و الفقهیة علی مذهب الامامیه***، تهران، المجمع العالمی للتقریب بین المذاهب الاسلامیه، المعاونیة الثقافیه، ۱۴۳۱ ق.

۳. حسینی روحانی، سیدمحمدصادق، ***منهاج الفقاهه***، چاپ پنجم، قم، انوار الهدی، ۱۴۲۹ ق.

۴. شهیدی تبریزی، میرزا فتاح، ***هدایة الطالب الی اسرار المکاسب***، قم، دار الکتاب، بی‌تا.

۵. طباطبایی یزدی، سیدمحمدکاظم بن عبدالعظیم، ***حاشیة المکاسب***، قم، اسماعیلیان، ۱۴۱۰ ق.

۶. طرح «حمایت و حفاظت از داده و اطلاعات شخصی» اعلام وصول شده در مجلس مورخ شهریورماه ۱۴۰۰ ش.، قابل دسترس در پایگاه ملی اطلاع‌رسانی قوانین و مقررات کشور به نشانی: <https://dotic.ir/news/10419>.

۷. فاضل موحدی لنکرانی، محمد، ***القواعد الفقهیه***، قم، مرکز فقهی ائمهٔ اطهار علیهم‌السلام، ۱۳۸۳ ش.

۸. قانون تجارت مصوب ۱۳۱۱ ش.

۹. قانون مدنی مصوب ۱۳۰۷ ش.

۱۰. قزوینی، ملاعلی بن محمد، ***صیغ العقود و الایقاعات***، حاشیه و شرح محمدعلی بن احمد قراچه‌داغی تبریزی، قم، شکوری، بی‌تا.

۱۱. لطفی، اسدالله، «قاعده استیمان در سقوط ضمان»، ***مجله دانشکده حقوق و علوم سیاسی***، دانشگاه تهران، شماره ۴۴، تابستان ۱۳۷۸ ش.

۱۲. محقق داماد، سیدمصطفی، ***قواعد فقه (بخش مدنی ـ مالکیت، مسئولیت)***، تهران، مرکز نشر علوم اسلامی، ۱۳۸۴ ش.

۱۳. مکارم شیرازی، ناصر، ***القواعد الفقهیه***، قم، مدرسة الامام علی بن ابی‌طالب علیه‌السلام، ۱۳۷۰ ش.

۱۴. موسوی بجنوردی، سیدمحمد بن حسن، ***قواعد فقهیه***، تهران، مؤسسه تنظیم و نشر آثار امام خمینی، مؤسسه چاپ و نشر عروج، ۱۳۷۹ ش.

۱۵. موسوی خمینی، سیدروح‌الله، ***ترجمه تحریر الوسیله***، ترجمه علی اسلامی و محمد قاضی‌زاده، قم، دفتر انتشارات اسلامی، ۱۳۸۳ ش.

۱۶. موسوی خویی، سیدابوالقاسم، ***موسوعة الامام الخوئی***، قم، مؤسسة احیاء آثار الامام الخوئی، ۱۴۱۸ ق.

۱۷. موسوی گلپایگانی، سیدمحمدرضا، ***مجمع المسائل***، قم، دار القرآن الکریم، بی‌تا.

۱۸. نراقی، احمد بن محمدمهدی، ***رسائل و مسائل؛ شامل هشتصد و پانزده سؤال و جواب و دوازده رساله فقهی و غیره***، گردآوری رضا استادی، قم، کنگره بزرگداشت محققان ملامهدی و ملااحمد نراقی، ۱۳۸۰ ش.

۱۹. هاشمی شاهرودی، سیدمحمود، ***فرهنگ فقه مطابق مذهب اهل بیت علیهم‌السلام***، قم، مؤسسه دائرةالمعارف فقه اسلامی بر مذهب اهل بیت علیهم‌السلام، ۱۳۸۲ ق.

20. Bureau of National Affairs (BNA), “The Final European Union General Data Protection Regulation”, ***Privacy & Security Law Report***, 15 PVLR 153, 2016.

21. Colcelli, Valentina, “Joint Controller Agreement Under Gdpr”, ***EU and Comparative Law Issues and Challenges Series (ECLIC 3): “Eu and Member States – Legal and Economic Issues”***, 2019.

22. Eija, Saaranen, ***Applying General Data Protection Regulation in Small Organizations; Simplified Framework and Templates for Managing a Privacy***, Bachelor's Thesis, School of Business and Culture, 2018.
23. EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), ***Official Journal of the European Union***, L 119, 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.
24. European Commission, "Data protection in the EU", 2016, <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en>.
25. Id., "Does my company/organisation need to have a Data Protection Officer (DPO)?", 2018[A], <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/does-my-company-organisation-need-have-data-protection-officer-dpo_en>.
26. Id., "The GDPR: new opportunities, new obligations", 2018[B], <https://op.europa.eu/en/publication-detail/-/publication/44d8441b-5fc5-11e8-ab9c-01aa75ed71a1/language-en>.
27. Id., "What does data protection 'by design' and 'by default' mean?", 2018[C], <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>.
28. Id., "What is a data controller or a data processor?", 2018[D], <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>.
29. Id., "What is personal data?", European Commission Policies, Information and Services, 2019, <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en>.
30. Ferrara, Pietro & Fausto Spoto, "Static Analysis for GDPR Compliance", ***CEUR Workshop Proceedings***, Vol. 2058, 2018.
31. Hintze, Mike, "Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR", ***Journal of Internet Law (Wolters Kluwer)***, 2018, <https://ssrn.com/abstract=3192721>.
32. Information Commissioner's Office (ICO), "Controllers and processors", 2018[A], <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors>.

33. Information Commissioner's Office (ICO), "Data protection officers", 2018[B], <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers>.
34. Information Commissioner's Office (ICO), "What responsibilities and liabilities do controllers have when using a processor?", 2018[C], <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor>.
35. Jones, E., "Data protection", ***Journal of Direct, Data and Digital Marketing Practice***, 2009, <https://edps.europa.eu/data-protection/data-protection_en>.
36. Kubben, Pieter, Michel Dumontier & Andre Dekker (Eds.), ***Fundamentals of Clinical Data Science***, Springer International Publishing, 2019.
37. Reini, Pasi, ***GDPR implementation, Case: Headpower Oy***, Master's thesis, University of Transport and Communications, March 2019, <https://www.theseus.fi/bitstream/handle/10024/166514/Reini_k7696_thesis_versio4.1.pdf?sequence=2>.
38. Singh, Atul, "Protecting Personal Data as a Property Right", ***ILI (The Indian Law Institute) Law Review***, Winter Issue, 2016.
39. Voigt, Paul & Axel von dem Bussche, ***The EU General Data Protection Regulation (GDPR)***, Springer International Publishing, 2017, <https://doi.org/10.1007/978-3-319-57959-7>.