

Legal Principles Governing the Processing of Personal Data in Information Exchange Networks

Abootaleb Koosha¹, Ali Akbar Farahzadi², Mahdi Naser^{3*}

1. Assistant Professor, Department of Private Law, Faculty of Judicial Law, University of Judicial Sciences and Administrative Services, Tehran, Iran.

2. Associate Professor, Department of Islamic Law, Faculty of Judicial Law, University of Judicial Sciences and Administrative Services, Tehran, Iran.

3. Doctoral student of private law, University of Judicial Sciences and Administrative Services, Tehran, Iran.



Article Type:

Original Research

Pages: 255-297

Received: 2023 August 13

Revised: 2023 August 30

Accepted: 2023 September 10



Abstract

Electronic data are divided into personal and non-personal data. Personal data is information that provides the basis for identifying real persons directly and indirectly. This type of information is always processed in information exchange networks. Privacy is the meeting point of protecting people's rights and processing their information by communication networks, and maintaining a balance in respect of privacy and managing a network will require processing under legal principles. The main question of this research is what are the principles governing the processing of personal data? In order to answer this question, the present research has started to study the regulations governing the legal system of the European Union and compared the results of its studies with the legal rules governing the legal system of Iran. In general, the principles governing the legal system of the European Union are placed in two general categories, the legal principle, the fairness and transparency of information processing, and the principle of limitation in information processing, which are explained in the first and second chapters of this research. In the conclusion part, the current research has tried to provide some policy recommendations to improve the implementation of these principles in Iran's legal system.

Keywords: Processing, Private data, Information exchange network, Legal principles

*Corresponding Author: Mn.ujasac0077@yahoo.com

اصول حقوقی حاکم بر پردازش داده‌های شخصی در شبکه‌های تبادل اطلاعات

ابوطالب کوشا^۱، علی اکبر فرحزادی^۲، مهدی ناصر^{۳*}

۱. استادیار گروه حقوق خصوصی، دانشکده حقوق قضایی، دانشگاه علوم قضایی و خدمات اداری، تهران، ایران.
۲. دانشیار گروه حقوق اسلامی، دانشکده حقوق قضایی، دانشگاه علوم قضایی و خدمات اداری، تهران، ایران.
۳. دانشجوی دکتری حقوق خصوصی دانشگاه علوم قضایی و خدمات اداری، تهران، ایران.



چکیده

داده‌های الکترونیکی به دودسته شخصی و غیرشخصی تقسیم می‌شوند. داده‌های شخصی به اطلاعاتی گفته می‌شوند که زمینه شناسایی اشخاص حقیقی را به صورت مستقیم و غیرمستقیم فراهم می‌آورند. این نوع اطلاعات همواره در شبکه‌های تبادل اطلاعات تحت پردازش قرار می‌گیرند. حریم خصوصی نقطه تلاقی حفظ حقوق اشخاص و پردازش اطلاعات آنها توسط شبکه‌های ارتباطی می‌باشد که حفظ تعادل در زمینه رعایت حریم خصوصی و مدیریت یک شبکه نیازمند انجام پردازش تحت اصول قانونی خواهد بود. سوالی اصلی این پژوهش آن است که اصول حاکم بر پردازش داده‌های شخصی چه می‌باشند؟ پژوهش حاضر برای پاسخ به این سوال به روش اسنادی مبادرت به مطالعه مقررات حاکم بر نظام حقوقی اتحادیه اروپا نموده و نتایج حاصل از مطالعات خود را با قواعد حقوقی حاکم بر نظام حقوقی ایران تطبیق داده است. بطور کلی اصول حاکم بر نظام حقوقی اتحادیه اروپا در دو دسته کلی، اصل قانونی، منصفانه بودن و شفافیت پردازش اطلاعات و اصل محدودیت در پردازش اطلاعات قرار می‌گیرند که در گفتارهای اول و دوم این پژوهش مورد تشریح قرار گرفته اند. پژوهش حاضر در قسمت نتیجه‌گیری نیز مبادرت به ارائه برخی توصیه‌های سیاست‌گذارانه در جهت بهبود اجرای این اصول در نظام حقوقی ایران نموده است.

نوع مقاله: علمی پژوهشی

صفحات: ۲۹۷-۲۵۵

تاریخ دریافت: ۱۴۰۲/۰۵/۲۲

تاریخ بازنگری: ۱۴۰۲/۰۶/۰۸

تاریخ پذیرش: ۱۴۰۲/۰۶/۱۹



تمامی حقوق انتشار این مقاله، متعلق به نویسنده است.

واژگان کلیدی: پردازش، داده‌های شخصی، شبکه تبادل اطلاعات، اصول حقوقی

درآمد

حریم خصوصی از جمله حقوق بنیادین بشر است که باید از طریق قانون حمایت گردد. (قناد و علینقی، ۱۳۹۹، ۲۹۹) این حق در ماده ۱۲ اعلامیه جهانی حقوق بشر تحت حمایت قرار گرفته و مستقیماً به کرامت انسانی و حق هر شخص بر حفاظت از آن مربوط می‌شود. (حبیبی، ۱۳۹۵، ۴۰) در عصر حاضر، مدیریت شبکه‌های ارتباطی در گرو پردازش اطلاعات قرار گرفته است. شبکه به رایانه‌های متصل به هم اطلاق می‌گردد که در محدوده هدف از پیش تعیین شده مبادرت به پردازش اطلاعات می‌نمایند. (Win-kelman²⁰²³) در شبکه‌های تبادل اطلاعات کاربران امکان برقراری ارتباط و تبادل اطلاعات با یکدیگر را برخوردار می‌باشند. (انصاری و عطار، ۱۳۹۲، ۱۱۸) بنابراین کشورهای توسعه یافته برای نظام مند نمودن فرایند جمع‌آوری و تحلیل اطلاعات اشخاص مبادرت به تنظیم مقرراتی نموده اند تا فرایند پردازش اطلاعات و ورود به حریم خصوصی اشخاص در چارچوب قوانین و مقررات مصوب صورت پذیرد. از جمله این مقررات می‌توان به مقررات عمومی حفاظت از اطلاعات مصوب ۲۰۱۶ اتحادیه اروپا، اشاره نمود. در نظام حقوقی ایران نیز اگرچه قوانین صریحی در زمینه حفاظت از اطلاعات توسط مجلس قانونگذاری تصویب نشده اند، اما مقرراتی در قوانین تجاری از جمله قانون تجارت الکترونیکی مصوب ۱۳۸۲ گنجانده شده اند که مسئله حفظ حریم خصوصی اشخاص را با اختصاص مقررات مواد ۵۸ و ۵۹ خود، در زمینه داده‌پیام‌های شخصی در دستور کار قرار داده است.

داده‌پیام به هر نمادی از واقعه، اطلاعات یا مفهوم که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود، اطلاق می‌گردد.^۲ داده‌پیام‌های الکترونیکی به دودسته داده‌پیام شخصی و غیرشخصی تقسیم می‌شوند. داده‌پیام شخصی به اطلاعاتی گفته می‌شود که به صورت مستقیم یا غیرمستقیم

1. General Data Protection Regulation

۲. ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲

زمینه شناسایی اشخاص حقیقی را فراهم می‌آورند. (2017,18,Sloot der van) اهمیت این نوع اطلاعات از آنجا نمایان می‌گردد که انجام وظایف نهادهای دولتی و غیردولتی در گرو پردازش این نوع اطلاعات بوده و داده‌پیام‌های غیرشخصی عموماً کاربردی در زمینه پردازش اطلاعات ندارند. اما سوال اینجاست که پردازش اطلاعات چه بوده و چه مصادیقی را میتواند در شمول خود داشته باشد.

پردازش به تعبیر بند دوم از ماده ۴ مقررات مصوب ۲۰۱۶ «به عملیاتی از جمله جمع‌آوری، ضبط، سازماندهی، ساختاربندی، ذخیره سازی، سازگاری یا تغییر، بازیابی، مشاوره، استفاده، افشای از طریق تبادل، انتشار یا استفاده دیگر، تراز یا ترکیب، محدودیت، پاک یا اصلاح کردن و تخریب داده اطلاق می‌گردد که از طریق وسایل خودکار یا غیرخودکار بر روی داده‌پیام‌ها انجام می‌شود». (Consulting²⁰²³ Intersoft) در نظام حقوقی ایران نیز، بند دوم از ماده ۲ طرح حمایت و حفاظت از داده و اطلاعات شخصی واصل شده به مجلس شورای اسلامی در تاریخ ۱۳۹۹/۰۷/۱۲ نیز با بیان تعریفی مشابه با آنچه در نظام حقوقی اتحادیه اروپا قید شده، مقرر می‌دارد «پردازش هرگونه عملیات دستی یا خودکار بر داده‌ها و اطلاعات شخصی، از قبیل ایجاد، ثبت، دریافت، گردآوری، نگهداری، جداسازی، تغییر، تجزیه و تحلیل، طبقه بندی، ساختاربندی، تطبیق، ذخیره سازی، اشتراک گذاری، فرستادن، توزیع و عرضه، انتشار و دردسترس قراردادن و پاک کردن آن‌ها می‌باشد». همانطور که در تعاریف مذکور مشاهده می‌گردد، گستردگی مصادیق مندرج در تعریف پردازش در مقررات مصوب ۲۰۱۶ و طرح فوق‌الذکر، منجر شده است تا تقریباً تمامی اعمال انجام شده بر روی داده‌پیام‌ها توسط اشخاص حقیقی یا حقوقی قابلیت ذکر، ذیل عنوان پردازش داده داشته باشند.

حریم خصوصی نقطه تزاخم حقوق قانونی اشخاص و پردازش اطلاعات آنها توسط شبکه‌های می‌باشد که انجام آن باید از یک طرف منجر به نقض حریم خصوصی نشده و از طرف دیگر به نحوی صورت نپذیرد که منجر به خلل در عملکرد یک شبکه

گردد. این موضوع ایجاب می نماید تا فرایند پردازش اطلاعات در چارچوب هایی که قانون معین می کند، صورت پذیرد. از جمله این چارچوب ها اصولی می باشند که قانونگذاران کشورها در قوانین مصوب خود پیش بینی می کنند. این اصول در ماده پنجم از مقررات مصوب ۲۰۱۶ مورد تصریح قانونگذار اتحادیه اروپا قرار گرفته اند. اما در نظام حقوقی ایران، ماده بخصوصی در این زمینه توسط قانونگذار مورد تصریح قرار نگرفته است. از این رو پژوهش حاضر با مطالعه و تحلیل اصول حقوقی پردازش اطلاعات در مقررات حاکم بر نظام حقوقی اتحادیه اروپا، سعی در تطبیق آن با قواعد حقوقی حاکم بر نظام حقوقی ایران نموده است. این موضوع از آن جهت اهمیت دارد که رعایت اصول پردازش اطلاعات مطابق با آنچه در این پژوهش بیان خواهد شد، مستقیماً با نظم عمومی در ارتباط می باشد.

به عبارت دیگر نظم عمومی دارای عناصری است که از جمله آنها می توان به حفظ امنیت عمومی و کرامت انسانی اشاره نمود. امنیت عمومی به حکم ماده ۸ اعلامیه حقوق بشر به حمایتی که جامعه برای حفظ شخصیت، حقوق و اموال اعضایش می کند، اطلاق می گردد. کرامت انسانی نیز به معنای احترام گذاری به حقوق قانونی اشخاص توسط دولت می باشد. (جلالی و کامیاب، ۱۳۹۴، ۱۴۰ و ۱۵۰) اطلاعات اشخاص جزو دارایی های آنها محسوب می گردند که باید از امنیت کافی در فرایند پردازش اطلاعات برخوردار باشند. همچنین فرایند پردازش آنها باید به نحو قانونی با احترام به حقوق و آزادی های قانونی اشخاص صورت پذیرد. بنابراین حفظ امنیت عمومی جامعه در فضای مجازی و کرامت انسانی اشخاص ایجاب می کند تا سازوکارهایی در جهت انجام پردازش اطلاعات پیش بینی گردد تا اولاً حقوق اشخاص در ارتباط با حریم خصوصی خود حفظ شده و ثانیاً فرایند پردازش به صورت نظام مند انجام گیرد. از جمله این سازوکارها اصول حاکم بر پردازش اطلاعات می باشند که ذیلاً به تبیین آنها اقدام خواهد شد. اگرچه در زمینه پردازش اطلاعات، مقالاتی توسط برخی نویسندگان مورد تالیف قرار گرفته اند، اما هیچ

کدام از پژوهش‌های پیشین صورت‌گرفته به موضوع اصول قانونی حاکم بر این فرایند نپرداخته و پژوهش حاضر در محوریت موضوعی خود، پژوهشی بدیع محسوب می‌گردد. اصول حاکم بر نظام حقوقی اتحادیه اروپا در دو دسته کلی، اصل قانونی، منصفانه بودن و شفافیت پردازش اطلاعات و اصل محدودیت در پردازش اطلاعات قرار می‌گیرند که در گفتارهای ذیل این پژوهش مورد تشریح قرار خواهند گرفت.

۱- اصل قانونی، منصفانه بودن و شفافیت پردازش اطلاعات

این اصل در بند اول ماده ۵ مقررات مصوب ۲۰۱۶ مورد تصریح قانونگذار این اتحادیه قرارگرفته است. بند مذکور مقرر می‌دارد: «پردازش داده‌های شخصی باید قانونی، منصفانه و شفاف در رابطه با موضوع داده صورت پذیرد.» سوالیکه در بدایت امر مطرح می‌گردد اینست که چرا این ماده، موضوع پردازش را تنها در خصوص داده‌های شخصی مطرح نموده است. در پاسخ به این سؤال باید به معنای پردازش اطلاعات توجه نمود. همانطورکه بیان شد کلیه اقدامات از جمله جمع‌آوری، ذخیره، تبادل و ارسال اطلاعات همگی در ذیل عنوان پردازش مطرح می‌شوند. بنابراین اطلاعات عمومی که در حالت عادی در دسترس مردم قرار داشته و آزادانه مورد تبادل قرار می‌گیرند، اصولاً نمی‌توانند واجد شرایطی برای چگونگی پردازش باشند. به همین جهت محوریت بحث در این ماده، بر روی داده‌های شخصی قرارگرفته است. این بند ماده ۵، دارای سه قسمت می‌باشد که ذیلاً به تشریح هر یک اقدام می‌شود.

- پردازش داده‌های شخصی به صورت قانونی
- پردازش داده‌های شخصی بر اساس قواعد عدل و انصاف
- پردازش شفاف داده‌های شخصی

۱-۱- قانونی بودن پردازش

در خصوص پردازش "قانونی" اطلاعات می‌توان بیان داشت، در نظام حقوقی اتحادیه اروپا تمامی مراحل پروسه پردازش اطلاعات جز در موارد مصرح قانونی باید با رعایت شرایط ماده ۶ مقررات مصوب ۲۰۱۶ انجام گیرد. از این رو شرایط مقرر در ماده ۶ می‌تواند به عنوان آستانه یا حداقل استانداردهای لازم قانونی برای پردازش داده‌های شخصی تلقی گردد. (Satori, 2023) ماده ۶ مقررات مصوب ۲۰۱۶ در بیان شرایط پردازش قانونی اطلاعات مقرر می‌دارد:

پردازش فقط در صورتی قانونی خواهد بود که حداقل یکی از موارد زیر اعمال شود:

- موضوع داده^۱ با پردازش داده‌های شخصی خود برای یک یا چند هدف خاص موافقت کرده باشد
- پردازش برای اجرای قراردادی که موضوع داده طرف آن است یا به منظور انجام اقداماتی بنا به درخواست موضوع داده قبل از انعقاد قرارداد ضروری باشد
- پردازش به منظور حفاظت از منافع حیاتی موضوع داده یا شخص حقیقی دیگر ضروری باشد
- پردازش برای انجام وظیفه‌ای که به نفع عمومی یا در اعمال اختیارات رسمی به کنترل‌کننده^۲ انجام می‌شود، ضروری باشد
- پردازش برای اهداف مشروعی که توسط کنترل‌کننده یا شخص ثالث دنبال می‌شود، ضروری باشد، به استثنای مواردی که این منافع تحت تأثیر منافع یا حقوق اساسی و آزادی‌های موضوع داده باشد که مستلزم حفاظت از داده‌های شخصی است،

۱. موضوع داده اصطلاحاً به شخصی اطلاق می‌گردد که اطلاعات شخصی او مورد پردازش واقع می‌شود.

۲. کنترل‌کننده شخصی است که در یک شبکه ارتباطی مبادرت به جمع‌آوری، تحلیل و نگهداری اطلاعات شخصی موضوع داده می‌نماید. البته این شخص میتواند فرایند پردازش اطلاعات را به شخص دیگری که تحت دستور و راهنمایی او مبادرت به این امر می‌نماید، محول نماید. این شخص اصطلاحاً پردازنده نامیده می‌شود.

به ویژه در مواردی که موضوع داده یک کودک باشد. همانطور که ملاحظه می‌گردد، ماده ۶ مقررات مصوب ۲۰۱۶، شش شرط برای تحقق پردازش قانونی اطلاعات پیش‌بینی نموده است. بنابراین در صورتیکه فرایند پردازش اطلاعات، در بردارنده یکی از شرایط فوق‌الذکر نباشد، اصولاً نمی‌تواند فرایند قانونی تلقی گردد.

۱-۱-۱- رضایت

شرط اول در پردازش قانونی اطلاعات، رضایت موضوع داده می‌باشد. نظام حقوقی ایران در مقایسه با نظام حقوقی اتحادیه اروپا دارای تفاوت‌هایی در شرایط اعلام رضایت می‌باشد. ماده ۵۸ از قانون تجارت الکترونیکی مصوب ۱۳۸۲، اعلام رضایت در پردازش داده‌های شخصی را منوط به ارائه رضایت «صریح» توسط موضوع داده نموده است. ماده فوق‌الذکر، در صورت عدم وجود رضایت صریح موضوع داده، پردازش اطلاعات را غیرقانونی تلقی کرده است. اما سؤال اینجاست که آیا صرف بیان واژه رضایت می‌تواند مثبت وجود رضایت صریح و قانونی موضوع داده باشد یا باید شرایطی نیز در این امر به عنوان شرایط مقدماتی وجود داشته باشد تا بتوان رضایت صریح موضوع داده را احراز نمود؟ برای پاسخ به سؤالات فوق باید ابتدا مفهوم «رضایت صریح» را تبیین کرد. در دیدگاه برخی که نگارندگان نیز قائل بر آن می‌باشند، اعلام رضایت باید در بردارنده سه شرط باشد:

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

بنابراین اولین شرط در اعلام رضایت صریح، علم به مفاد چیزی که بدان رضایت

داده شده می‌باشد. اگرچه قانونگذار ایران در باب اعلام شرایط و چگونگی انجام پردازش به موضوع داده حکمی در قانون تجارت الکترونیکی قید ننموده اما می‌توان با تدبیر در فلسفه استفاده از این واژه در ماده ۵۸ و همچنین اخذ وحدت ملاک از سایر متون، ضرورت این موضوع را ایجاب نمود. به عنوان مثال ماده ۳۳ طرح حمایت و حفاظت از داده و اطلاعات شخصی بر ضرورت ذکر کلیه جزئیات فرایند پردازش از جمله هدف پردازش، نحوه پردازش، شرایط فنی پردازش، سطح ایمنی موجود، حقوق موضوع داده و فرایند نظارت بر امر پردازش به موضوع داده تاکید نموده است. این موضوع در دستورالعمل‌های شماره ۴۲ و ۴۳ مقررات مصوب ۲۰۱۶ اتحادیه اروپا نیز مورد تصریح قانونگذار این اتحادیه قرار گرفته است. (ICO, 2023)

بنابراین صرف اعلام رضایت چه به صورت کتبی و چه به صورت شفاهی، برای احراز صریح بودن آن در فرایند پردازش اطلاعات کفایت نمی‌نماید. به عبارتی اعلام رضایت، شرط لازم بوده اما شرط کافی تلقی نمی‌گردد و باید علاوه بر اعلام، دو شرط دیگر که اطلاع از مفاد چیزی که بدان باید رضایت داده شود و همچنین وجود قصد بر اعلام وجود داشته باشد. نکته قابل توجه اینست که در احراز وجود یا عدم وجود شروط اول و دوم (علم و قصد) بنظر نگارنده، اصل بر عدم وجود شرط اول بوده و قاضی در مقام قضاوت باید نسبت به احراز علم رضایت دهنده بر مفاد چیزی که بدان رضایت داده اقدام نماید. از این رو در صورتیکه دلیلی بر اطلاع موضوع داده از چیزی که بدان رضایت داده کشف نگردد، نمی‌توان رضایت صریح وی را احراز نمود. اما در فرض احراز یا عدم احراز وجود قصد، ابراز آن که مثبت شرط سوم می‌باشد، می‌تواند مبین وجود قصد بر ابراز نیز بوده و شرایطی مانند اکراه یا اجبار یا اشتباه باید از سوی مدعی عدم وجود رضایت اثبات شده و به عبارتی باید به ظاهر امر در ابراز رضایت توجه داشت. این درحالی می‌باشد که بند یازدهم ماده ۴ مقررات مصوب ۲۰۱۶، واجد شرایط و احکام دیگری در احراز رضایت توسط موضوع داده می‌باشد. بند یازدهم ماده ۴ مقرر می‌دارد:

رضایت موضوع داده به معنای هرگونه اشاره آزادانه، مشخص، آگاهانه و بدون ابهام از خواسته‌هایی است که موضوع داده به موجب آن، با بیانیه‌ای یا با یک اقدام مثبت واضح، موافقت خود را با پردازش داده‌های شخصی خود نشان می‌دهد

سؤال اینجاست که آیا قانونگذار اتحادیه اروپا نیز همانند قانونگذار ایران، اعلام رضایت صریح را شرط دانسته یا رضایت ضمنی نیز در اتحادیه اروپا برای احراز رضایت موضوع داده کفایت می‌کند؟ منشاء طرح این سؤال اینست که قانونگذار اتحادیه اروپا در صدر ماده با تصریح به واژه «اشاره» که عموماً ظهور در اعلام قصد ضمنی بر انجام یا عدم انجام یک موضوع داشته، شرایط ابراز رضایت را قید و در ذیل این بند از واژه «اقدام مثبت واضح» بر اعلام موافقت در پردازش داده‌ها که ظهور در ضرورت اعلام صریح موضع دارد، پرده برداشته است. بنظر نگارنده این یک تعارض در متن ماده بوده و جایی برای توجیه توسل به قواعد حقوقی و حالت‌گزینی و ذکر وجوه افتراق این دو واژه وجود ندارد. اما در نظام حقوقی ایران طرح حمایت و حفاظت از داده‌ها و اطلاعات شخصی در مواد ۴ و ۵ خود، واجد شروط دیگری غیر از اعلام رضایت صریح می‌باشد. ماده ۴ این طرح بیان می‌دارد: پردازش اطلاعات شخصی اشخاص مربوط به وضعیت‌ها یا موقعیت‌های غیرعمومی منوط به اعلام رضایت آنها بوده و اعلام رضایت اشخاص موضوع داده باید با رعایت شرایط ذیل همراه باشد:

- پیش از پردازش باشد
- بیانگر آگاهی موضوع داده باشد
- استنادپذیر باشد

تصریح صورت‌گرفته در بند اول شرایط مقرر در ماده ۴ بر بیان رضایت پیش از پردازش، در انعقاد قراردادهای پردازشی نمود بیشتری دارد. براین مبنا، کنترل‌کنندگان و پردازندگان می‌توانند با اخذ امضا از موضوع داده، نسبت به اخذ رضایت وی اقدام نمایند. اما چالش موجود عموماً در شبکه‌هایی که متشکل از سایت‌های فروش و عرضه

محصولات یا شبکه‌های اجتماعی می‌باشند، جلوه می‌کند که در این سایت‌ها عموماً معرفی کالای متناسب با علایق یک مراجعه کننده برای خرید، پیش از پذیرش شرایط تعیین شده از سوی سایت صورت می‌پذیرد که خلاف مقررات مصرح در این طرح می‌باشد. برای حل این مشکل، گردانندگان سایت‌ها می‌توانند با ایجاد آیکنی که هنگام ورود کاربر به سایت بر روی شبکه باز شده و پیش از تأیید اطلاعات امکان ملاحظه محتویات سایت را به کاربر ندهد، نسبت به حل مشکل اقدام کنند. اما در شبکه‌های اجتماعی مانند اینستاگرام و فیس بوک و توییتر و... که ورود کاربر به شبکه منطبق با جمع‌آوری اطلاعات وی بوده و تنها دسترسی به مخاطبین تلفن همراه یا برخی اطلاعات دیگر وی منوط به اخذ رضایت می‌باشد، نقض این شرط جلوه بیشتری دارد.

بعلاوه ماده ۵ طرح، پردازش داده‌ها و اطلاعات شخصی مربوط به وضعیت‌ها یا موقعیت‌های عمومی را بدون رضایت شخص در صورتی بلامانع تلقی کرده که «یا خود وی داده‌ها را در معرض پردازش قرار داده یا پردازش داده‌ها را منع یا محدود نکرده باشد». سوالیکه می‌تواند مطرح گردد اینست که فردی که مبادرت به انتشار اطلاعات شخصی خود در شبکه‌های اجتماعی که میلیون‌ها بیننده دارد نموده و به عبارتی آنها را عمومی کرده باشد، چطور می‌تواند پردازش این داده‌ها را منع یا محدود نماید؟ در صورتیکه انتشار اطلاعات در شبکه خاص با کاربران خاصی صورت گرفته باشد، این مشکل جلوه کمتری دارد اما در شبکه‌های اجتماعی نمی‌توان به سادگی نسبت به این مهم اقدام کرد. سؤال دیگری که مطرح می‌گردد اینست که موضوع داده باید به چه طریقی نسبت به ایجاد منع یا محدودیت در پردازش اقدام کرده و در صورتیکه شخصی از این موضوع مطلع نشده و مبادرت به پردازش نماید، سازوکار و کمیت و کیفیت شناسایی مسئولیت برای وی به چه نحوی خواهد بود. نکته دیگر اینست که ماده ۱۰ این مقررات، مصادیق استثنا از اخذ رضایت موضوع داده را با عنایت به قواعدی مانند «انجام اقدام مهم نسبت به مهم» مورد تصریح قرار داده است. مصادیقی که در این ماده پردازش بدون اخذ رضایت موضوع داده

ذکر شده شامل موارد ذیل می‌باشد:

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

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

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

به ارائه تفسیر مضیق نمود و به عبارتی مصادیق شمول بندهای ماده ۱۰ را تا حد ممکن محدود کرد. ثانیاً بند دوم ماده ۱۰، در بیان این استثنا، به واژه «پیشگیری» تصریح کرده که نشان از پردازش اطلاعات بدون رضایت موضوع داده درحالتی دارد که هیچ ضرر و زیانی به دیگری وارد نشده که بتوان میزان شدید بودن یا نبودن آن را احراز نمود. براین مبنا چه دلیلی دارد با ارائه معیارهای نوعی و گسترش شمول مصادیق این ماده، به صرف پیشگیری از وقوع زیان، نسبت به پردازش بدون رضایت اطلاعات دیگران اقدام کرد.

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

دیدگاه اول براین استدلال استوار است که هدف از تدوین مقررات حمایت از داده‌های شخصی، حفظ و پیشگیری از نقض امنیت این اطلاعات می‌باشد. بنابراین در تقابل مقررات مواد این طرح، اولویت را باید نسبت به پذیرش موادی قرار داد که در جهت صیانت از امنیت داده پیام‌ها تصویب شده‌اند. از این رو مقررات ماده ۱۱ را باید در هر حال نسبت به مقررات ماده ۱۰ اولویت بندی نمود.

دیدگاه دوم که بنظر نگارنده نیز صحیح‌تر است این می‌باشد که مستفاد از اصل ۴۰ قانون اساسی یا موادی مانند ماده ۱۳۲ یا ۹۷۵ قانون مدنی می‌توان بیان داشت که اعمال حقوق اشخاص تا جایی جاری می‌باشد که با نظم عمومی یک کشور در تعارض نباشد. بنابراین در فرضی که ممکن است اعمال حق موضوع داده منجر به زیان شدید مالی به دیگران شود، طبیعتاً باید نسبت به حقوق موجود تعادل برقرار نمود. بعلاوه بندهای

سوم و چهارم ماده ۱۰ نیز مصادیق مهمی مانند حفظ امنیت کشور یا انجام تحقیقات قضایی را ذکر نموده‌اند که اگر قائل بر حکومت مقررات ماده ۱۱ بر ماده ۱۰ باشیم، در این زمینه نیز نمی‌توان نسبت به پردازش اطلاعات اشخاص برای حفظ امنیت ملی یک کشور به صرف وقوع زیان به آن‌ها اقدام کرد. درحالی‌که موادی مانند ماده ۱۱ قانون مسئولیت مدنی ایران، دولت را حتی از جبران خسارت در امور حاکمیتی که بر حسب ضرورت برای تأمین منافع اجتماعی انجام گیرد نیز معاف دانسته است.

۱-۱-۲- انعقاد قرارداد

درخصوص بند دوم ماده ۶ این مقررات می‌توان بیان داشت که این بند پردازش در انجام تعهدات قراردادی یا پیش از قرارداد را منوط به وجود عنصر «رضایت» نموده است. شق اول بند دوم این ماده دو شرط را برای پردازش اطلاعات موضوع داده پیش‌بینی کرده است. این دو شرط طرف قرارداد بودن موضوع داده و ضرورت پردازش برای اجرای مفاد قرارداد می‌باشند. بنابراین اطلاعات اشخاص در قراردادهایی که این افراد جزو طرفین قرارداد نباشند، غیرقانونی و ممنوع می‌باشد. مضاف بر آنچه بیان شد، ذکر عنوان «درخواست موضوع داده» درخصوص اقدامات پیش از قرارداد در دیدگاه نگارنده می‌تواند به صورت موسع تفسیر شود. به عبارت دیگر گاه جمع‌آوری اطلاعات اشخاص مسبوق بر درخواست صریح آنها مانند اشتراک اطلاعات در یک شبکه تبادل اطلاعات می‌باشد و گاه ورود یک شخص به یک سایت جهت خرید کالا می‌تواند به عنوان درخواست ضمنی وی بر جمع‌آوری اطلاعات از جمله آدرس، شماره کارت اعتباری و... تلقی گردد که برای ارسال کالای خریداری شده از آن سایت به خریدار ضروری شمرده شود.

درخصوص واژه ضرورت، می‌توان بیان داشت که پردازش در صورتی ضروری است که قرارداد بدون انجام آن تکمیل نگردد. (Voigt&Etc,2017,102) با این حال این بدان معنا نیست که تنها راه برای اجرای مفاد قرارداد، پردازش داده‌ها باشد، بلکه وجود یک گام

هدفمند و متناسب با تعهدات کفایت می‌کند، بنابراین وجود راه‌های دیگر مانع از احراز ضرورت نخواهد بود. (لطیف زاده و دیگران، ۱۴۰۱، ۳۴۶) سوالیکه در این جا مطرح می‌شود اینست که وجود راه‌های دیگر تا کجا می‌تواند مانع احراز ضرورت نباشد؟ آیا در صورت وجود گزینه‌های هم عرض می‌توان به صرف استناد به تناسب و وجود گام هدفمند نسبت به پردازش اطلاعات اقدام نمود یا باید معیار بخصوصی در این زمینه وجود داشته باشد؟ در دیدگاه نگارندگان صرف وجود گام هدفمند و تناسب با تعهدات در این خصوص کفایت نمی‌کند. چرا که در بیان دیدگاه فوق یکپارچگی میان اقدامات و تعهدات نیز شرطی است که مورد توجه قرار نگرفته است. به عبارت دیگر تناسب میان تعهدات و وجود گام هدفمند در صورتی می‌تواند افاده معنای ضرورت نماید که یکپارچگی میان تعهدات نیز وجود داشته باشد. بنابراین در یک موضوع خاص راهکارهای دیگر به عنوان راهکارهای طاقت فرسا یا مشقت پیش رو باشند و منطقاً پردازش اطلاعات به عنوان راهکاری معقول تلقی گردد. (Barrett&Etc,2023)

بعلاوه در دیدگاه برخی در این فرایند لازم نیست حتماً یک قرارداد رسمی یا مکتوب میان طرفین منعقد شود بلکه صرف توافق کفایت می‌کند. (لطیف زاده و دیگران، ۱۴۰۱، ۳۴۵) در نقد این دیدگاه نیز می‌توان بیان داشت که اولاً توافقات گاه به منزله قراردادهای شفاهی و گاه توافقات پیش از قرارداد می‌باشند. بر فرض اینکه منظور نویسندگان فوق‌الذکر، قراردادهای شفاهی باشد، سؤال اینجاست که آیا با وجود شرایط متعدد تعیین شده در مواد ۵ و ۶ مقررات مصوب ۲۰۱۶ و حساسیتی که قانونگذار اتحادیه اروپا در تعیین مورد به مورد شرایط پردازش داشته، می‌توان در قراردادهای شفاهی که هر طرف می‌تواند در مقام اثبات منکر تعهدات خود گردد، امر پردازش را مورد پذیرش قرار داد؟ برای پاسخ به این سوال می‌توان بیان داشت با توجه به اینکه قانونگذار اتحادیه اروپا با اختصاص یک فصل از مقررات مصوب ۲۰۱۶ از مواد ۷۷-۸۴ این قانون را به مسائل مرتبط با مسئولیت‌پذیری اشخاص فعال در فرایند پردازش اطلاعات در اتحادیه اروپا اختصاص

داده و این موضوع نشان از اهمیت موضوع در نظر قانونگذار بوده است. بنظر می‌رسد قانونگذار حکیم اتحادیه اروپا، اصولاً هر نوع قراردادی را به منزله قراردادی که موضوع پردازش اطلاعات نیز جزو فرایند اجرای تعهدات باشد، در نظر نگرفته و بنظر نگارنده منظور همان قراردادهای کتبی بوده است.

نکته دیگر آن است که در فرایند پردازش، امعان نظر از مفهوم ضرورت ایجاب می‌نماید که «اجرای قرارداد» تنها در محدوده تعهدات قراردادی تفسیر شده و امور فراتر جزو این عنوان تلقی نگردد. به عنوان مثال در اجرای مفاد یک قرارداد خرید کالا از یک سایت اینترنتی، مسئولین شبکه حق جمع‌آوری اطلاعات در خصوص علایق کاربر سایت در انتخاب نوع کالا و ارائه پیشنهادات مشابه را ندارند. (همان، ۳۴۶) چرا که این موضوع ارتباطی به اجرای مفاد قرارداد ندارد. ضمن اینکه آنچه بیان شد عموماً در محدوده پیش از انعقاد قرارداد قرار می‌گیرد که اصولاً هیچ کاربری درخواست ارائه کالاهای مشابه با علایق خود را از مسئولین شبکه مطرح نمی‌نماید.

شرط مقرر در بند دوم ماده ۶ مقررات مصوب ۲۰۱۶ اتحادیه اروپا، مقررات مشابهی در نظام حقوقی ایران ندارد و با امعان نظر از واژه ضرورت وجود رضایت «صریح» در ماده ۵۸ قانون تجارت الکترونیکی و اصولی مانند اصل عدم وجود رضایت، می‌توان به فقدان وجود مجوز در پردازش اطلاعات شخصی در فرایند انعقاد یا پیش از انعقاد قرارداد استناد کرد. مگر در مواردی که بنا بر ضرورت، راهی جز پردازش اطلاعات همانند آنچه در خصوص موضوع رضایت در مثال خرید کالا از سایت ذکر شد، وجود نداشته و این موضوع نیز در محدوده فرض رضایت قابل بحث می‌باشد. اما بنظر برخی توجه به قواعدی مانند «اذن در شیء اذن در لوازم آن می‌باشد» (نجفی، ۱۴۲۱، ۷۰) و با امعان نظر از این قاعده مبنی بر اینکه اگر کسی به دیگری نسبت به چیزی اذن دهد، گستره اذن به آن چه مورد تصریح اذن دهنده قرار گرفته محدود نشده بلکه لوازم عقلی، ذاتی، عرفی و قانونی آن را نیز دربر می‌گیرد، (شاهرودی، ۱۴۳۲، ۵۹ و محقق داماد، ۱۳۸۴، ۲۳۶-۲۳۷) اظهار نظر

کرده‌اند که رضایت شخصی افراد به انعقاد قرارداد به منزله اذن بر پردازش اطلاعات نیز می‌باشد. (قبولی درافشان و دیگران، ۱۴۰۱، ۳۴۷) اما سؤال اینجاست که اگر امکان توسل به چنین قواعدی در نظام حقوقی ایران امکان پذیر باشد، چرا قانونگذار از ضرورت اعلام رضایت صریح در مقررات ماده ۵۸ پرده برداشته است. با توجه به استثنایی بودن این مقررات و ضرورت تفسیر مضیق این ماده قانونی، بنظر نگارنده امکان توسل به قواعد فقهی و حقوقی برای توسعه مفهوم رضایت به قراردادها وجود نخواهد داشت.

۱-۱-۳- حفظ منافع حیاتی موضوع داده یا دیگری

درخصوص بند سوم ماده ۶ مقررات مصوب ۲۰۱۶، بنا بر نظر عده‌ای این بند تنها درخصوص حفظ جان و منافع حیاتی و زندگی اشخاص مانند پردازش اطلاعات وی در هنگام عمل جراحی در بیمارستان برای دستیابی به سوابق عمل جراحی یا گروه خونی و... کاربرد داشته و نمی‌توان به مسائل دیگر آن را تسری داد. بعلاوه درخصوص دیگران نیز باید به طریق اولی تنها درخصوص منافع حیاتی و زندگی مانند پردازش داده‌های شخصی والدین جهت حفاظت از منافع زندگی و حیاتی فرزند تفسیر نمود. اگرچه این بند نیز در مقررات مصوب در کشور ایران مورد تصریح قرار نگرفته اما مقررات پراکنده مانند بند سوم ماده ۴ منشور حقوق بیماران ایران درخصوص حریم خصوصی بیماران دارای مقرراتی دراین زمینه می‌باشد. (همان، ص ۳۵۱) ماده ۴ این منشور مقرر می‌دارد:

ارائه خدمات سلامت باید متبنی بر احترام به حریم خصوصی بیمار (حق خلوت) و رعایت اصل رازداری باشد- فقط بیمار و گروه درمانی و افراد مجاز از طرف بیمار و افرادی که به حکم قانون مجاز تلقی می‌شوند، می‌توانند به اطلاعات دسترسی داشته باشند.

اگرچه این مقرر می‌تواند به منزله توجیه‌کننده اقدامات مراکز درمانی در دسترسی

۱. ماده ۵۸- ذخیره، پردازش و یا توزیع «داده‌پیام» های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام» های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون ضایت صریح آنها به هر عنوان غیرقانونی است.

به اطلاعات شخصی بیماران بدون اخذ رضایت تلقی شود و منطقاً نیز در مواردی که صحبت از جان اشخاص مطرح می‌شود باید تمامی موانع قانونی کنار گذاشته شوند، اما سؤال اینجاست که آیا در تقابل این مقرر با مقررات ماده ۵۸ قانون تجارت الکترونیکی و این موضوع که قانونگذار در آن ماده از عبارت «بدون رضایت صریح آنها به هر عنوان غیرقانونی است» و توجه به این موضوع که قانونگذار صراحتاً از واژه به هر عنوان اشاره نموده، نمی‌توان عدم وجود استثنا در پردازش اطلاعات شخصی را از این ماده استناد و استثنای بیان شده در ماده ۴ منشور را فاقد وجهت قانونی تلقی نمود؟ بنظر نگارنده جواب این سؤال مثبت بوده و سیاستگذاران تقنینی باید نسبت به اصلاح این مقرر و رفع خلاء های قانونی آن اقدام نمایند.^۱

۱-۱-۴- حفظ منافع عمومی یا اعمال اختیارات رسمی

درخصوص بند چهارم مقررات مصوب ۲۰۱۶ می‌توان بیان داشت که واژه منفعت عمومی امری بسیط بوده و تفسیر موسع از آن می‌تواند آثار بندهای دیگر از جمله بند اول مبنی بر ضرورت اخذ رضایت را از بین ببرد. بنظر برخی، منفعت عمومی به امری اطلاق می‌گردد که در آن عموم مردم سهیم بوده و عبارتی به «آنچه که برای کل جامعه بهترین باشد» اطلاق می‌گردد. (Rekosh, ۲۰۲۳) این واژه می‌تواند حقوق آزادی اشخاص، حقوق مصرف‌کنندگان، حقوق سلامت و موارد مشابه را در برگیرد. شق دوم این بند نیز بر اعمال اختیارات رسمی به کنترل‌کننده اختصاص یافته است. اختیارات رسمی نیز به اختیاراتی گفته می‌شود که مقامات رسمی دولتی برای انجام وظایف قانونی اعطا می‌شود. (Cam-Dictionary²⁰²³ bridge) بنابراین می‌توان نتیجه‌گیری نمود که این اختیارات بیشتر جنبه حاکمیتی داشته و از مفهوم تصدی‌گری فاصله دارند. در این حالت نیز مقام دارای

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

اختیار، از اخذ رضایت موضوع داده یا هر الزام قانونی دیگر معاف می‌باشد. اگرچه مشابه این مقرر در قانون تجارت الکترونیکی ایران پیش‌بینی نشده، با این حال مفهوم آن از سایر مقررات قانونی از جمله ماده ۱۱ قانون مسئولیت مدنی مصوب ۱۳۳۹ و ماده ۸ قانون مدیریت خدمات کشوری مصوب ۱۳۸۶ قابل استنباط می‌باشد. التفات به مقررات ماده ۱۱ قانون مسئولیت مدنی که مقرر می‌دارد «... در مورد اعمال حاکمیت دولت، هرگاه اقداماتی که بر حسب ضرورت برای تأمین منافع اجتماعی طبق قانون به عمل می‌آید و موجب ضرر دیگری شود، دولت مجبور به پرداخت خسارت نخواهد بود» می‌تواند منتج به این نتیجه شود که دولت در مقام اعمال حاکمیت می‌تواند نسبت به اموری اقدام نماید که انجام آن از سوی اشخاص عادی امکان پذیر نیست و موجب مسئولیت می‌باشد. مصادیق اعمال حاکمیت در ماده ۸ قانون مدیریت خدمات کشوری ذکر شده که با امور عام المنفعه، هم پوشانی دارند. بنابراین در صورتیکه دولت یا هر مقام صلاحیت داری در مقام اعمال حاکمیت مبادرت به انجام فرایند پردازش اطلاعات نمایند، این موضوع استثنایی بر مقررات ماده ۵۸ قانون تجارت الکترونیکی تلقی و فاقد ضمانت اجرای مقرر در ماده ۷۱ همان قانون خواهد بود.^۱

۱-۱-۵- وجود اهداف مشروع

در خصوص بند آخر ماده ۶ مقررات مصوب ۲۰۱۶ نیز می‌توان بیان داشت این بند امکان پردازش اطلاعات را در صورتی پیش‌بینی نموده‌است که سه شرط ذیل به صورت توأمان وجود داشته باشند:

- هدف مشروع
- ضرورت

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

- تقابل منافع

درخصوص هدف مشروع عده‌ای بیان داشته‌اند که زمانی یک هدف از پردازش مشروع می‌باشد که هدف از لوازم و توابع حقوق آن شخص باشد. در فرایند تقابل منافع نیز باید منافع آن شخص بر منافع موضوع داده ارجحیت داشته باشد تا به حکم قاعده «تقدم منافع اهم بر مهم» امکان پردازش فراهم گردد. دراین راستا باید پیامدهای پردازش بر حقوق اشخاص ارزیابی شده و ملاک تشخیص نیز حکم عقل خواهد بود. این عده معتقدند که پردازش بر اساس این بند باید با در نظر گرفتن شرایط خاص پردازش مشروع بوده و بنابراین باید به صورت موسع تفسیر شود. (قبولی درافشان و دیگران، ۱۴۰۱، ۳۵۲) اما توجه به مفاد متن بند پنجم در دیدگاه نگارنده امری خلاف آنچه که اظهارنظر شده را به ذهن متبادر می‌سازد. چرا که قانونگذار از واژه «به استثنای» دراین ماده سخن گفته و تقابل حقوق موضوع داده با دیگران را از جمله مصادیق استثنا برای پردازش اطلاعات تعبیر نموده است. علت این موضوع نیز روشن است، دلیلی وجود ندارد که قانونگذار حکیم که در مقررات ماده ۵ این قانون شرایطی برای پردازش ذکر نموده و تنها استثنائاتی را برای حکم کلی مذکور در ماده ۶ مقرر داشته، به یکباره با ذکر جملاتی کلی، آثار احکام پیشین خود را از میان ببرد. بعلاوه، آنچه در باب تجویز پردازش در موارد اعمال حاکمیت نیز قید گردید، به جهت شرایط خاصی می‌باشد که امور حاکمیتی از آن برخوردار هستند. ازاین رو نمی‌توان به سایر مصادیق حکم کلی فوق‌الذکر را نسبت داده و از آن تفسیر موسع نمود.

۲-۱- منصفانه بودن پردازش

عنصر دوم در اصل پردازش قانونی، منصفانه و شفاف اطلاعات، منصفانه بودن پردازش می‌باشد. پردازشی، منصفانه می‌باشد که اطلاعات به روش‌های فریب کارانه یا گمراه کننده جمع‌آوری نشده باشند. دراین حالت تفاوتی میان داده‌های شخصی

موضوع داده یا داده‌های اشخاص ثالث وجود نداشته و بنابراین حتی در صورتیکه اطلاعات فرد الف تحت پردازش قرار گرفته و در این میان اطلاعاتی وجود داشته باشد که به صورت فریب کارانه از شخص ب جمع‌آوری شده و توأم با اطلاعات شخص الف پردازش شوند، پردازش اطلاعات شخص ب منجر به غیرقانونی تلقی شدن پردازش اطلاعات شخص الف نیز می‌گردند.

پرونده شرکت نوآوران (ارائه خدمات پستی) علیه مسئول حفاظت از اطلاعات^۱، مثالی عینی از جمع‌آوری غیرقانونی اطلاعات می‌باشد که همچنان به عنوان یکی از نمونه‌های بارز نقض عدالت و انصاف در جمع‌آوری اطلاعات شناخته می‌گردد. شرکت مذکور در ارائه خدمات پستی، سفارشات خود را از دو طریق دریافت سفارش از فروشگاه‌های خود و دریافت سفارش از طریق پاسخ به تبلیغات رسانه‌ای به دست می‌آورد. اشخاصی که از طریق تبلیغات رسانه‌ای مبادرت به دریافت خدمات پستی می‌نمودند، استفاده از جزئیات اطلاعات ارائه شده توسط آنها تنها پس از اطلاع دادن این مورد و دریافت "اجازه لیست" از سوی آنها امکان پذیر بود. در هنگام ثبت سفارش، شرکت، مشتریان را از تمامی جزئیات به دست آمده از آنها مطلع می‌نمود. بعدها شرکت با این استدلال که تبلیغات گسترده رسانه‌ای؛ عملاً منجر به ایجاد محدودیت‌های عملی در ارائه آگاهی بر مشتریان می‌شد، از ادامه این پروسه سر باز زد. دادگاه در رسیدگی به پرونده این موضوع را مورد اشعار قرار داد که عدم ارائه آگاهی از سوی شرکت به مشتریان، ممکن است در ذهن آنها به این شکل القا نماید که عدم ارائه هرگونه آگاهی در تبلیغات رسانه‌ای به منزله عدم انجام هرگونه تبادل یا پردازش یا هر استفاده دیگری از جزئیات اطلاعات داده شده از سوی آنها تلقی گردد. این موضوع مقدمه‌ای در دستیابی ناعادلانه به اطلاعات مردم تلقی شد. (2018,43,CAREY)

مقررات مصوب ۲۰۱۶، در زمینه پردازش منصفانه اطلاعات، دارای قواعدی

1. Innovations (Mail Order) Ltd v Data Protection Registrar) DA92 31/49/1)

می‌باشد که در بند دوم ماده ۱۳ مقرر شده است. این بند مقرر می‌دارد «کنترل‌کننده باید در زمانی که داده‌های شخصی به دست می‌آید، اطلاعات مرتبط با دوره نگهداری و حقوق موضوع داده را برای اطمینان از پردازش عادلانه و شفاف اطلاعات به وی اعطا کند». این بند پشتیبند مقررات بند اول ماده ۱۳ قید شده که پیش از شروع فرایند جمع‌آوری اطلاعات، برای حفظ اصل پردازش منصفانه، موضوع داده را محق بر اطلاع از حقوق قانونی خود نموده است. بنابراین می‌توان به نتیجه رسید که مهمترین الزام در پردازش منصفانه اطلاعات، اطلاع موضوع داده از حقوق قانونی خود می‌باشد.^۱ بعلاوه دستورالعمل شماره ۶۰ مقررات مصوب ۲۰۱۶ در انجام هر چه بهتر فرایند پردازش منصفانه ضرورت ارائه کلیه اطلاعات مرتبط با احراز منصفانه بودن را فراتر از حقوق قانونی مندرج در ماده ۱۳، به موضوع داده مورد تصریح قرار داده است. این دستورالعمل مقرر می‌دارد:

- اصل پردازش شفاف و منصفانه ایجاب می‌کند که موضوع داده از عملیات پردازش و اهداف آن مطلع شود. کنترل‌کننده باید هر اطلاعات دیگری را که برای اطمینان از پردازش شفاف و منصفانه با در نظر گرفتن شرایط خاص و زمینه پردازش داده‌ها لازم است، به موضوع داده ارائه دهد.... (Lex, 2016, 12-EUR) ۲

۳-۱- شفافیت در پردازش

عنصر سوم در اصل بیان شده در این گفتار شفافیت در پردازش اطلاعات می‌باشد. مقررات مربوط به این موضوع در ماده ۱۲ مقررات مصوب ۲۰۱۶ مورد تصریح قرار گرفته است. در این راستا، باید "اقدامات مناسب" در زمینه در اختیار گذاشتن اطلاعات قابل فهم و واضح در خصوص کیفیت جمع‌آوری و پردازش اطلاعات در اختیار موضوع داده گذاشته شده، صورت پذیرد. ضمن اینکه اطلاعات داده شده باید به سادگی

۱. مفاد این حقوق در مواد ۱۵-۲۱ مقررات مصوب ۲۰۱۶ مورد تصریح قرار گرفته است.

۲. نقل شده در قبولی درافشان، ۱۴۰۲، ص ۹۸۴

قابل فهم باشند. از این رو ارائه اطلاعات به زبان فنی یا استفاده از واژگان قانونی پیچیده در فهماندن مطالب خلاف اصل شفافیت تلقی می‌گردد. با استفاده از این نکته می‌تواند نتیجه‌گیری نمود، ارائه اطلاعات به موضوع داده باید به زبان محلی کشور متبوع فرد صورت پذیرد. (44, cit. op, CAREY)

در کنار موارد بیان شده، در صورتیکه اطلاعات جمع‌آوری شده، تلازم مستقیم یا غیرمستقیم با حقوق اشخاص ثالث داشته باشد، باید نسبت به ارائه آگاهی لازم در این خصوص به آن‌ها نیز اقدام گردد. ضمن اینکه از جمله نتایج ضروری اصل شفافیت، ارائه اطلاعات مرتبط با حقوق کاربران شبکه‌های تبادل اطلاعات در دسترسی و پردازش اطلاعات از جمله (تصحیح، پاک کردن، محدودیت، تبادل، حمل و...) می‌باشد تا آنها به خوبی از اختیارات سایر کاربران یا مدیران شبکه‌های ارتباطی در بررسی اطلاعات آگاهی یابند. ماده ۱۲ از مقررات مصوب ۲۰۱۶ برخی الزامات قانونی که در زمینه ایجاد شفافیت امکان مفید واقع شدن را داشته باشند، به شرح ذیل معین نموده است:

- باید دسترسی موضوع داده به اطلاعات و آگاهی از حقوق قانونی وی تسهیل گردد.

- باید در محدوده زمانی مشخص به درخواست‌های موضوع داده جهت اجرای حقوق قانونی وی پاسخ داده شود.

- باید دلایل منطقی مبنی بر عدم اجرای درخواست‌های موضوع داده به صورت دقیق به وی اطلاع داده شده و وی از چگونگی امکان اعتراض به تصمیم خود، آگاه گردد.

متداول‌ترین روش جهت ایجاد شفافیت در پروسه دسترسی و پردازش اطلاعات، تهیه اطلاعاتی متشکل از توضیحات جامع از تمامی الزامات حقوقی مرتبط با ایجاد شفافیت می‌باشد که اصطلاحاً با عنوانی از جمله "اعلامیه پردازش منصفانه"، "اعلامیه حفظ حریم خصوصی"، "خط مش حفظ حریم خصوصی" و یا "اعلامیه محافظت از داده" شناخته می‌شود. در اعلامیه بیان شده، شرایط ذیل مورد توجه قرار می‌گیرند:

- اطلاعات باید به هر طریق فیزیکی یا الکترونیکی به صورت کتبی تهیه و در اختیار موضوع داده قرار داده شود.
- ارائه اطلاعات شفاهی به موضوع داده تنها در صورتی است که اولاً به درخواست صریح وی صورت گرفته باشد و ثانیاً موضوع داده هویت خود را اثبات نماید.
- اطلاعات ممکن در مواردی مانند تبلیغات آنلاین از طریق یک وبسایت ارائه شود، به ویژه در مواردی که تعداد کنترل‌کنندگان و پردازندگان زیاد بوده و شناسایی اینکه چه کسی مبادرت به جمع‌آوری اطلاعات نموده و بطورکلی فرایند ارائه اطلاعات با پروسه پیچیده‌ای مواجه باشد.
- حتی در مواردی که داده‌های جمع‌آوری شده به صورت غیرخطی (مانند پر کردن فرم از طریق چهره نگاری) به دست آمده باشند، ارائه آنلاین اطلاعات نمی‌تواند جایگزینی برای اعلام مستقیم داده‌ها باشد.
- از آنجا که شرط اساسی در ایجاد شفافیت انجام اقدامات مناسب در راستای تسهیل دسترسی به اطلاعات توسط موضوع داده می‌باشد، باید تمامی اقدامات قانونی لازم در این خصوص بدون دریافت هرگونه هزینه از موضوع داده صورت پذیرد. (44-45,cit.op,CAREY)

۲- اصل ایجاد محدودیت در پردازش اطلاعات

اصل محدودیت در پردازش اطلاعات همانطور که از نام آن پیداست به معنای ایجاد محدودیت در پردازش اطلاعات می‌باشد تا داده‌پیام‌ها در چارچوب اهداف تعیین شده پردازش شوند. از نتایج این اصل می‌توان به سه نتیجه محدودیت هدف در پردازش اطلاعات، به حداقل رساندن اطلاعات و دقت در جمع‌آوری اطلاعات اشاره نمود که ذیلاً به تبیین هر یک اقدام می‌گردد.

۱-۲- محدودیت هدف در پردازش اطلاعات^۱

محدودیت هدف به معنای جمع‌آوری و پردازش داده‌ها بر اساس اهداف از پیش تعیین شده مشخص، صریح و قانونی می‌باشد. از این رو در صورتیکه اهداف مقرر واجد ویژگی‌های بیان شده نباشند، پردازش مذکور قانونی تلقی نمی‌گردد. با این حال استثنائاتی نیز در این زمینه پیش‌بینی شده است. در جمع مفاد این اصل و مفاد ماده ۸۹ مقررات مصوب ۲۰۱۶، در صورتیکه بر فرض مشخص نمودن اهداف پردازش، پردازش بیشتر در جهت حفظ منافع عمومی یا اهداف تحقیقاتی و علمی و جمع‌آوری داده‌های آمار صورت پذیرد، این موضوع به معنای نقض اصل مذکور تلقی نمی‌گردد. (coimisi-un, 2023)

در خصوص پردازش بر اساس منافع عمومی، در مطالب پیشین توضیحات مفصل ارائه گردید که در اینجا به جهت جلوگیری از تکرار مکررات از ذکر مجدد خودداری می‌گردد. اما نکته قابل توجه پردازش بیشتر بر اساس اهداف تحقیقاتی می‌باشد. سؤال اینجاست که آیا این استثنا مطلق اهداف تحقیقاتی را شامل می‌گردد یا اهداف تحقیقاتی باید بر اساس اصول و قواعدی صورت پذیرد؟ در پاسخ باید بیان داشت که اطلاعات اشخاص در هر مرجع و سازمانی بر اساس اهداف بخصوصی مورد جمع‌آوری و ذخیره قرار می‌گیرند. بنظر نگارنده، منظور از اهداف تحقیقاتی، اهدافی می‌باشند که در حوزه فعالیت آن سازمان باشند تا پس از تحقیقات صورت‌گرفته امکان بکارگیری آن‌ها در پروژه‌های کاربردی آن سازمان فراهم شود. بنابراین سازمانی که در حوزه نانو فناوری تشکیل و فعالیت نموده و اطلاعات عرضه شده این سازمان در شبکه‌های ارتباطی خود تنها در حوزه نانو فناوری باشد، امکان انجام پردازش اطلاعات با اهداف مرتبط با حوزه جراحی مغز و اعصاب را نخواهد داشت.

معیار بیان شده در فوق در خصوص داده‌های آماری نیز جاری می‌باشد. بنابراین

1. Purpose Limitation

داده‌های آماری جمع‌آوری شده نیز دقیقاً باید در حوزه فعالیت سازمانی باشند که نسبت به جمع‌آوری این داده‌ها اقدام می‌کنند. بنابراین سازمانی که در حوزه سرشماری جمعیت فعالیت می‌کند، اصولاً نمی‌تواند آمار مربوط به بیماران مبتلا به بیماری‌های خاص را جمع‌آوری نماید چرا که این حوزه مربوط به حوزه وزارت بهداشت و درمان یک کشور بوده و با آمار جمعیتی متفاوت است.

توضیحات بیان شده در فوق می‌تواند دربردارنده دو نتیجه باشد:

- منجر به تعیین دقیق اهداف و نظارت قانونی بر عملکرد اشخاص فعال در شبکه‌های ارتباطی می‌گردد. (نتیجه ایجابی)
 - از پردازش بی مورد داده‌ها یا مغایر با اهداف از پیش تعیین شده جلوگیری می‌نماید. (نتیجه سلبی) (CAREY, cit.Op, 34)
- همانطور که بیان شد در اصل فوق‌الذکر، ابتدا باید اهداف دقیق از پردازش اطلاعات تعیین و جز در مورد سه استثنای بیان شده، پردازش اطلاعات تنها در محدوده اهداف تعیین شده صورت پذیرد. اما سؤال اینجاست که تعیین انطباق پردازش با اهداف صورت‌گرفته به چه نحوی خواهد بود؟ در تعیین انطباق یا عدم انطباق پردازش صورت‌گرفته بر روی داده‌های شخصی با اهداف از پیش تعیین شده، در سال ۲۰۱۳ کارگروه ماده ۲۹ دستور العمل حفاظت از اطلاعات مصوب ۱۹۹۵ اتحادیه اروپا^۱ - این مرجع به عنوان مرجع راهنمای کمیسیون اتحادیه اروپا شناخته می‌شود- مبادرت به ارائه دستورالعملی با عنوان راهنمای ارزیابی انطباق به کنترل‌کنندگان اطلاعات نمود. در این دستورالعمل عوامل اصلی که باید در ارزیابی انطباق پردازش و اهداف از پیش تعیین شده باید در نظر گرفته شود، به قرار ذیل تعیین گردیده است: (Europa, ۲۰۲۳)
- رابطه بین اهداف جمع‌آوری داده‌های شخصی و اهداف پردازش

۱. این دستورالعمل پیش از مقررات عمومی حفاظت از اطلاعات اتحادیه اروپا به عنوان مقررات لازم الاجرا در سطح اتحادیه اروپا در زمینه حفاظت از اطلاعات محسوب می‌شد.

- زمینه جمع‌آوری داده‌های شخصی و ضروریات توجیه‌کننده نگهداری آنها
- ماهیت داده‌های شخصی و تأثیر پردازش بر روی موضوع داده
- اقدامات حفاظتی اتخاذ شده برای اطمینان از پردازش عادلانه و جلوگیری از هرگونه پردازش خلاف اصول (Ico(b),2023)

درخصوص عامل اول، باید خاطر نشان کرد اگرچه جمع‌آوری اطلاعات خود زیرمجموعه‌ای از پردازش می‌باشد، اما منظور از پردازش در این فرایند، انجام هرگونه اقدام اعم از تحلیل آماری یا فنی یا ذخیره یا تبدیل اطلاعات به انواع دیگر داده‌ها بر روی داده‌های جمع‌آوری شده می‌باشند.^{(۳۳) Thelin} بنابراین در صورتیکه نتیجه حاصل از اقدامات انجام شده با اهداف تعیین شده در جمع‌آوری اطلاعات سنخیتی نداشته باشند، نمی‌توان بر وجود محدودیت هدف در پردازش تاکید داشت. به عنوان مثال فرض کنید شخصی با نقل مکان به محدوده شرکت آب و برق منطقه خاصی از یک شهر مبادرت به ارائه اطلاعات به شرکت مذکور جهت دریافت خدمات می‌نماید. شرکت مذکور اطلاعات دریافت شده را برای کلیه اهداف مرتبط با آب و برق و ارائه خدمات مورد پردازش قرار داده و در نهایت جزئیات موجود را به یک اپراتور تلفن همراه برای بهبود بازاریابی شرکت ارسال می‌نماید. در این صورت اعمال حاصل از پردازش اطلاعات توسط شرکت آب و برق نمی‌تواند به عنوان نقض اصول حاکم بر حفاظت از اطلاعات تلقی گردد. اما ارسال اطلاعات به شرکت اپراتور تلفن همراه به منزله نقض اصل محدودیت هدف در پردازش می‌باشد. (35,cit.Op , CAREY)

این موضوع در بند ب ماده ۵۹ قانون تجارت الکترونیکی ایران نیز مورد تصریح قرار گرفته است. بند ب ماده ۵۹ مقرر می‌دارد:

«داده‌پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع «داده‌پیام» شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.

این بند از دو قسمت تشکیل شده است. بر مبنای قسمت اول جمع‌آوری اطلاعات اشخاص باید بر مبنای اهداف مشخصی صورت پذیرفته و خارج از این اهداف امکان جمع‌آوری اطلاعات وجود ندارند. و بر مبنای قسمت دوم، هرگونه اقدام پردازشی از جمله ذخیره، نگهداری، تحلیل و... بر روی اطلاعات جمع‌آوری شده نیز باید در راستای اهداف از پیش تعیین شده صورت پذیرد. شق دوم از این بند به نوعی می‌تواند مشمول عامل دومی باشد که بر انطباق مفهوم پردازش با جمع‌آوری اطلاعات تاکید دارد. با توجه به اینکه داده‌های شخصی بر اساس اهدافی جمع‌آوری می‌شوند، دلیلی برای نگهداری این اطلاعات در یک شبکه ارتباطی وجود ندارد. چرا که جمع‌آوری و هرگونه پردازش بر روی اطلاعات باید با اهداف بخصوصی و تحت شرایط بخصوصی از جمله اخذ رضایت موضوع داده و... صورت پذیرد. بنابراین در صورتیکه به هر نحو پس از جمع‌آوری، نیاز به نگهداری این اطلاعات جهت پردازش مجدد وجود داشته باشد، باید دلایل توجیهی لازم در این خصوص ارائه گردد.

عامل سوم بر نوع داده‌های شخصی تاکید دارد. داده‌های شخصی انواع مختلفی دارند که در دسته بندی‌های بخصوصی مانند داده‌های مربوط به بهداشت، اعتقادات مذهبی، منشاء قومی، عقاید سیاسی و... مطابق با ماده ۹ مقررات مصوب ۲۰۱۶ قرار می‌گیرند. پردازش هر کدام از این اطلاعات دارای آثار مختلفی می‌باشد. به عنوان مثال پردازش اطلاعات مذهبی، شناخت کلی در خصوص اعتقادات و رسوم و باورهای دینی یک موضوع داده ارائه می‌کند. بنابراین در صورتیکه به هر نحو داده‌ای بر اساس هدف خاصی جمع‌آوری و پردازش شود، باید آثار حاصل از پردازش مورد ارزیابی قرار گرفته و مشخص گردد که آیا اهداف معین محقق شده‌اند یا خیر. در خصوص عامل چهارم نیز باید بیان داشت که ملاک در اجرای اصل محدودیت هدف، تنها اقدامات ایجابی نبوده و باید اقدامات حفاظتی نیز در نظارت بر فرایند انجام شده صورت پذیرد. بر این مبنای اساس نوع و دسته ویژه داده‌های شخصی که در مطالب فوق بیان شد، اقدامات حفاظتی

بخصوص نیز باید اتخاذ گردد. (Law Data Golden, ۲۰۲۳)

۲-۲- به حداقل رساندن اطلاعات^۱

درخصوص به حداقل رساندن اطلاعات می‌توان بیان داشت، پردازش داده‌های شخصی باید به حد لزوم (کفایت)، مرتبط و محدود به آن چه با اهداف پردازش ضروری می‌باشد صورت پذیرد. (Ico, 2023, c) از آنچه از این نتیجه حاصل می‌گردد اینست که باید تنها داده‌هایی که برای اهداف تعیین شده ضروری باشد مورد جمع‌آوری واقع گردد. (Trend, 2023) این نتیجه در قسمت سوم بند اول ماده ۵ مقررات مصوب ۲۰۱۶ مورد تصریح قرار گرفته و به سه عامل "حد لزوم"^۲، "ارتباط"^۳ و "محدودیت"^۴ در پردازش اطلاعات تاکید دارد.^۵

معیار اول در عملیاتی نمودن به حداقل رساندن داده‌ها، کفایت می‌باشد. بر مبنای این معیار، اطلاعات جمع‌آوری شده باید به حد ضرورت جمع‌آوری و نگهداری آنها نیز باید تا حد نیاز و برای اهداف تعیین شده باشد. از این رو به عنوان مثال در جمع‌آوری داده‌های بیومتریک اشخاص مانند اثر انگشت، تنها باید به حد ضرورت اکتفا نموده و از جمع‌آوری داده‌های مربوط به شبکه چشم یا سایر اطلاعات بیومتریک خودداری کرد. بر این مبنا در صورت از میان رفتن ضرورت، نهادی که اطلاعات در دسترس وی باشد باید نسبت به حذف اطلاعات از شبکه خود یا ناشناس سازی آنها اقدام نماید. (Iapp²⁰²³) این موضوع اثرات مثبتی از جمله صرفه جویی در مصرف انرژی و هزینه با کاهش ذخیره سازی داده‌ها داشته و سرعت پردازش در سیستم را به حداکثر می‌رساند.

1. Data Minimization
2. adequate
3. relevant
4. limited

۵. معیار اول و سوم دارای آثار یکسانی می‌باشند که هر دو به جمع‌آوری اطلاعات در حد کفایت و ضرورت تاکید دارند. از این رو در توضیحات ارائه شده تنها به دو معیار اشاره می‌گردد.

بعلاوه از انباشت اطلاعات در یک شبکه جلوگیری نموده و خطرات سرقت اطلاعات را از شبکه کاهش می‌دهد. (Staff, 2023)

نکته قابل توجه اینست که درخصوص معیار مدت زمان نگهداری اطلاعات، در مقررات مصوب ۲۰۱۶ اتحادیه اروپا حکمی قید نشده و براین مبنا می‌توان تعیین این موضوع را بر صلاحدید شخصی قرار داد که داده‌ها را در اختیار داشته باشد. با این حال نکته قابل توجه اینست که مدت زمان نگهداری داده‌ها با توجه به ماهیت آنها، نباید از مدت زمانی که برای اهداف دادرسی به عنوان مواعد قانونی توسط قانونگذار مورد تاکید قرار گرفته است، کمتر باشد. بنابراین مطابق با مقررات حاکم بر نظام حقوقی اتحادیه اروپا سوابق تصادف در محل کار باید حداقل سه سال پس از تاریخ حادثه نگه داشته شوند. همچنین سوابق مصاحبه افراد نیز باید حداقل به مدت سه ماه از تاریخ مصاحبه نگهداری گردند. بعلاوه آنچه بیان شد از جمع‌آوری اطلاعات نیز می‌تواند به عنوان معیار موثری در شناسایی دوره نگهداری استفاده کرد. به عنوان مثال آدرس منزل یک کارمند، حداقل باید برای مدت زمان اشتغال وی حفظ گردد یا سندی که برای بررسی هویت شخص از وی مطالبه می‌گردد می‌تواند دوره نگهداری بسیار کوتاهی داشته باشد. (39, cit.Op, CAREY)

در نظام حقوقی ایران مدت زمانی نگهداری اطلاعات جمع‌آوری شده، دارای ضوابطی می‌باشد. این موضوع از مصوبات جلسات ۴۸۲-۴۸۸ شورای عالی انقلاب فرهنگی در زمینه حمایت از ارتباطات الکترونیکی و داده‌پیام‌های شخصی قابل برداشت می‌باشد که حذف اطلاعات در دسترس پس از شش ماه از زمان نگهداری را در صورت عدم وجود دستور مخالف از جانب مقامات قضایی مورد تصریح قرار داده است. (قناد و علینقی، ۱۳۹۹، ۳۱۸) بنابراین بر مبنای مصوبات فوق، حداکثر مدت نگهداری اطلاعات در نظام حقوقی ایران مدت زمان شش ماهه در نظر گرفته شده است. با این حال این موضوع با مقررات ماده ۶۶۷ قانون آیین دادرسی کیفری که حداقل مدت نگهداری

اطلاعات کاربران در سامانه ارائه دهندگان خدمات دسترسی را تا شش ماه پس از خاتمه اشتراک قرار داده دارای تعارض است. به عبارت دیگر مصوبات شورای عالی انقلاب فرهنگی مدت زمان مقرر شده را حداکثر شش ماه در حالی که ماده ۶۶۷ قانون آیین دادرسی کیفری مدت زمان مذکور را به حداقل زمان نگهداری اطلاعات تغییر داده است. سوال اینجاست که در مقام تعارض این دو حکم باید به چه نحوی عمل نمود؟ این موضوع از آن جهت اهمیت دارد که به حکم تبصره دوم ماده ۶۶۷، اطلاعات کاربران شامل هرگونه اطلاعات مربوط به یک کاربر بوده و بنابراین شامل اطلاعات شخصی وی نیز می‌گردد. از این رو با مفاد بند ب ماده ۵۹ قانون تجارت الکترونیکی که ذخیره اطلاعات را تنها به اندازه ضرورت متناسب با اهداف جمع‌آوری، امکان پذیر کرده است، دارای تعارض می‌باشد. برای رفع این تعارض به نظر می‌رسد با توجه به تعارض موجود، باید میان مقررات جمع برقرار نمود. به عبارت دیگر حکم مطلق ماده ۶۶۷ قانون آیین دادرسی کیفری در خصوص داده پیام‌های شخصی تنها در صورتی جاری می‌گردد که متناسب با اهداف جمع‌آوری، ضرورت این موضوع نیز وجود داشته باشد و در صورت عدم وجود ضرورت مطابق با مصوبات جلسات ۴۸۲-۴۸۸ شورای عالی انقلاب فرهنگی، باید تنها محدود زمان ضرورت و حداکثر تا شش ماه نسبت به نگهداری اطلاعات اقدام نمود. در خصوص داده پیام‌های غیرشخصی نیز باید مقررات قانون آیین دادرسی کیفری را ناسخ مصوبات فوق‌الذکر شورای عالی انقلاب فرهنگی قرار داد.

نکته دیگر اینست که قسمت پنجم بند اول ماده ۵ و بند اول ماده ۸۹ مقررات مصوب ۲۰۱۶، استثنائاتی را برای اجرای این نتیجه پیش‌بینی کرده‌اند. براین مبنا، اطلاعات شخصی را در صورتی می‌توان برای مدت طولانی نگهداری نمود که این اقدام تحت سه هدف، حفظ منافع عمومی، تحقیقات علمی یا تاریخی و جمع‌آوری داده‌های آماری صورت پذیرد. (Ombudsman Protection Data the of Office, ۲۰۲۳) بعلاوه در برخی

موارد، بیش از یک هدف برای نگهداری اطلاعات وجود دارد. در این شرایط تا زمانی که تمامی اهداف موجود محقق نگردد، باید اطلاعات موجود نگهداری شوند. به عنوان مثال در مواردی که سند مورد نیاز کپی کارت شناسایی فردی باشد که به عنوان راننده در یک شرکت مشغول بکار است، اگرچه مشاهده کپی کارت شناسایی فرد مدت زمان اندکی را نیاز دارد، اما به جهت مشغول بودن فرد به عنوان کارمند در شرکت مذکور، مدارک شناسایی وی باید به مدت خدمت وی نگهداری شوند.

معیار دوم ارتباط می‌باشد. بر مبنای این معیار، اطلاعات جمع‌آوری شده باید مرتبط با هدف پردازش باشند و در صورتیکه داده‌ای خارج از این موازین جمع‌آوری گردد، باید حذف شود. از این رو در صورتیکه یک خبرنامه الکترونیکی که با مشتریان خود به صورت الکترونیکی از طریق اشتراک تلفنی یا ایمیل در ارتباط می‌باشد، مبادرت به جمع‌آوری اطلاعات آدرس منزل آنها نماید، این موضوع به منزله نقض این نتیجه محسوب خواهد شد. حتی در صورتیکه این خبرنامه، از پیش اطلاعاتی در خصوص آدرس منزل مشترکین خود داشته باشد نیز باید نسبت به حذف اطلاعات از شبکه خود اقدام نماید. چرا که این اطلاعات ارتباطی به موضوع و هدف فعالیت این شبکه ندارد.

نتیجه بیان شده در فوق در بردارنده دو رکن تعیین اهداف مورد پردازش و میزان تقریبی اطلاعات قابل پردازش می‌باشد. به عنوان مثال در صورتیکه هدف از جمع‌آوری اطلاعات در فرم "درخواست اشتغال" باشد، تصمیم‌گیری در خصوص اینکه فرد مذکور مناسب برای یک شغل تمام وقت یا پاره وقت می‌باشد یا دقیقاً چه شغلی با چه درجه حساسیتی مدنظر متقاضی باشد می‌تواند در کمیت پردازش اطلاعات مؤثر واقع گردد. بعلاوه در اعمالی مانند بازاریابی، رفتارهای متعددی مانند پرداخت، تحویل کالا و ارسال اطلاعات در انجام فرایند می‌توانند مؤثر واقع شوند. دوم پس از تعیین اهداف مقرر، باید بررسی گردد هر فعالیت در زمینه پردازش آیا می‌تواند برای دستیابی به هدف اصلی مؤثر و مورد لزوم واقع گردد؟ (CAREY, Op. cit, 35-36) از این رو اگر

فعالیتی لزوماً جهت دستیابی به هدف تعیین شده در پردازش اطلاعات مورد استفاده واقع نگردد، انجام آن به منزله نقض اصل مذکور محسوب می‌شود. به عنوان مثال در صورتیکه شخصی برای کار در واحد ترابری یک شرکت در آن استخدام شود، پردازش و حتی نگهداری اطلاعات شخصی وی که به عنوان مثال مرتبط با انجام فعالیت در واحد حسابداری یا امور مالی بوده، به منزله نقض این اصل تلقی می‌گردد. بعلاوه عنصر زمان نیز در زمینه پردازش داده‌ها به عنوان رکنی مهم تلقی می‌گردد. چرا که پردازش طولانی مدت و نامتعارف داده‌ها و دسترسی بیش از حد به آن‌ها نیز خارج از عنصر حداقل رساندن داده‌ها می‌تواند باشد.

نکته قابل توجه در این موضوع اینست که اطلاعات جمع‌آوری شده توسط مدیران یک شبکه ارتباطی نمی‌تواند به بهانه این موضوع که موضوع داده نسبت به این امر رضایت داشته، از حد کفایت و ضرورت خارج گردد. به عبارت دیگر قواعد این اصل جزو قواعد آمره بوده و کسب رضایت از موضوع داده، نمی‌تواند به منزله مجوزی برای نقض قواعد ماده ۵ مقررات مصوب ۲۰۱۶ تلقی گردد. (Law, (b), 2023 Data Golden). نکته دیگر که بیان آن ضرورت دارد اینست که به حداقل رساندن اطلاعات تنها منحصر به مرحله تحلیل و بررسی اطلاعات نبوده و در مرحله جمع‌آوری داده‌های شخصی نیز باید مورد نظر قرار گیرد. از این رو اگر در هر یک از مراحل جمع‌آوری یا پردازش داده‌ها، از مفاد این نتیجه تخطی گردد، می‌توان آن را در تمامی مراحل دسترسی به اطلاعات نقض شده تلقی نمود. نکته دیگر اینست که در اجرای به حداقل رساندن اطلاعات، میزان دسترسی اشخاص و کارکنان یک شبکه نیز باید مورد نظر و توجه قرار گیرد. به عبارت دیگر بنا بر ماهیت داده‌های در دسترس که در خصوص داده‌های حساس ضرورت دسترسی کارکنان خاص را ایجاد می‌نماید؛ در صورتیکه تعداد غیرمتعارفی کارمند مبادرت به دسترسی به اطلاعات مذکور نمایند، نتیجه فوق‌الذکر می‌تواند مورد نقض واقع گردد.

۳-۲- دقت در جمع‌آوری و پردازش اطلاعات^۱

مطابق با این نتیجه که در قسمت چهارم بند اول ماده ۵ مقررات مصوب ۲۰۱۶ پیش‌بینی شده، اطلاعات جمع‌آوری شده باید دقیق و به روز بوده و شبکه‌های تبادل اطلاعات، داده‌های شخصی کاربران خود را هر ۳۰ روز یکبار به روز رسانی نمایند. هرچند در ماده ۱۷ مقررات فوق‌الذکر تاکید شده که یکی از حقوق اشخاص موضوع داده، حق اصلاح یا حذف (پاک کردن) اطلاعات می‌باشد، اما وجود این حق نافی وظیفه مدیران شبکه‌های تبادل اطلاعات یا هر سازمانی که اطلاعات نزد وی باشد، بر به روزرسانی اطلاعات شخصی در دسترس نخواهد بود. به عنوان مثال در صورتیکه اطلاعات شخصی کاربری در سامانه یک بانک، اطلاعات موقعیت مکانی وی در شهر مادرید باشد، با نقل مکان وی از آن محل، بانک موظف به به روزرسانی اطلاعات موقعیتی وی در سامانه خود خواهد بود. (Nelson, 2023)

البته نکته‌ای که باید بدان توجه گردد اینست که بنظر می‌رسد به روزرسانی اطلاعات اگرچه به عنوان یک اصل مورد پذیرش قرار گرفته، اما در موارد ضرورت نافی عدم انجام این کار در یک شبکه نخواهد بود. (Commission, 2023 European) به عنوان مثال، نگهداری سوابق یک شخص در سازمان‌هایی مانند ادارات مالیاتی، دادگستری و ... امری است که می‌تواند به منزله استثنایی بر حکم کلی این نتیجه تلقی گردد. دلیل این موضوع نیز روشن است، سازمان‌هایی مانند دادگستری برای رسیدگی به پرونده‌های خود نیازمند دسترسی به سوابق اشخاص می‌باشند تا با اطلاع از اطلاعات پیشین آنها امکان حل و فصل امور قضایی برای آنها میسر باشد. به عنوان مثال دسترسی به آدرس منزل یک شخص در جلب وی موضوعی است که نیازمند بررسی سوابق تردد فرد در مکان‌های مختلف می‌باشد. یا سازمان ثبت اسناد و املاک کشور، اگرچه ملزم به به روزرسانی اطلاعات مالکین املاک و اراضی در سطح کشور است، اما در بسیاری از موارد

1. Data Accuracy

حل پرونده‌های قضایی منوط به استعلام سوابق مالکیت املاک بوده و براین مبنا حذف این اطلاعات از سامانه این سازمان، عملاً حل پرونده‌های قضایی را با مشکل مواجه می‌کند. البته نگهداری سوابق نیز باید با رعایت سایر اصول از جمله ضرورت و در حد کفایت صورت پذیرد. نکته آخر اینست که به روز نمودن اطلاعات شخصی به دو عنصر نوع داده مورد پردازش و هدف پردازش بستگی دارد. به عنوان مثال داده‌هایی که مربوط به جلسه خاصی از هیئت مدیره یک شرکت می‌باشند، نیازی به به روزرسانی ندارند. درحالیکه داده‌های مربوط به وضعیت اقتصادی یک شخص ممکن است در فواصل زمانی معینی نیاز به به روزرسانی داشته باشند. (37,cit.Op ,CAREY)

در نظام حقوقی ایران نیز مفاد این نتیجه در بند ج ماده ۵۹ قانون تجارت الکترونیکی تصریح شده است. ماده ۵۹ قانون تجارت الکترونیکی مقرر می‌دارد: در صورت رضایت شخص موضوع «داده‌پیام» نیز به شرط آنکه محتوای داده‌پیام وفق قوانین مصوب مجلس شورای اسلامی باشد، ذخیره، پردازش و توزیع داده‌پیام‌های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:

بند ج: «داده‌پیام» باید صحیح و روزآمد باشد.

آنچه از واژه صحت در این ماده قانونی پرده برداشته شده، حذف اطلاعات نادرست از سامانه سازمان‌ها می‌باشد که می‌توان با توجه به صدر این ماده که بیان داشته «در صورت رضایت موضوع داده...»، وظیفه تصحیح و به روزرسانی را جزو وظایف مدیران شبکه‌های تبادل اطلاعات در نظر گرفت. به عبارت دیگر وجود عبارت «در صورت رضایت موضوع داده» گواه بر این موضوع است که شخصی از موضوع داده درخواستی داشته و موضوع داده نسبت به اعلام رضایت اقدام نموده است. بنابراین در صورتیکه اطلاعات صحیح در سامانه مراجع ذیربط ثبت نشده یا اطلاعات موجود به روز نباشند، در صورت جمع شرایط مسئولیت کیفری، می‌توان برای افراد مسئول، مسئولیت کیفری بر اساس ماده ۷۰ قانون تجارت الکترونیکی در نظر گرفت. این موضوع در خصوص اطلاعات حوزه

بهداشت و درمان که در سامانه مراکز درمانی ذخیره می‌باشد، نمود بیشتری دارد. سوالیکه درخصوص این بند قابلیت طرح دارد اینست که ملاک روزآمد بودن اطلاعات چه می‌باشد؟ آیا می‌توان دوره خاصی را برای به روزرسانی اطلاعات معین نمود؟ برای پاسخ به سؤال فوق باید بیان داشت که با توجه به اینکه قانونگذار ایران در این ماده معیار مشخصی را برای به روزرسانی اطلاعات در نظر نگرفته و در کنار آن، به روزرسانی اطلاعات امری مهم می‌باشد، انجام این امر در نظام حقوقی ایران را باید فوری قلمداد کرد. پس حتی در صورتیکه نیاز به بروزرسانی اطلاعات یک شخص بصورت چند باره در یک روز وجود داشته باشد، سازمان مجری باید نسبت به این مهم اقدام نماید.



برآمد

شبکه‌های تبادل اطلاعات از کامپیوترهای به هم متصل که مبادرت به تبادل داده پیام‌های الکترونیکی با یکدیگر می‌نمایند، تشکیل شده‌اند. این شبکه‌ها می‌توانند در محدوده اتصال چند کامپیوتر درون یک فروشگاه عرضه و فروش محصولات تا شبکه‌های راه اندازی شده در سازمان‌های دولتی و غیردولتی و حتی در مقیاس جهانی، اینترنت را شامل شوند. خصیصه اصلی عملکرد کامپیوترها در این نوع شبکه‌ها، انجام فرایند پردازش اطلاعات می‌باشد که همانطورکه بیان شد، کلیه مصادیق جمع‌آوری، ذخیره، نگهداری، تحلیل به روزرسانی و... اطلاعات را شامل می‌شود. عدم نظام مند نمودن این پروسه می‌تواند منجر به نقض امنیت کاربران این شبکه‌ها و اطلاعات آنها و نهایتاً کل شبکه گردد. از این رو نظام حقوقی کشورها با سیاستگذاری‌های تقنینی مبادرت به تصویب مقرراتی در این زمینه نموده‌اند.

مقررات عمومی حفاظت از اطلاعات اتحادیه اروپا مصوب ۲۰۱۶، جدیدترین قانونی است که نظام حقوقی اتحادیه اروپا در راستای حفاظت از داده پیام‌های الکترونیکی مورد تبادل در کشورهای عضو این اتحادیه به تصویب رسانده است. این قانون دربردارنده مواد مختلفی در موضوعات متفاوت می‌باشد که یکی از این موضوعات اصول حاکم بر پردازش اطلاعات خواهد بود. این اصول همانطورکه در متن این پژوهش نیز قید گردید به دو دسته کلی، اصل قانونی، منصفانه بودن و شفافیت پردازش اطلاعات و اصل محدودیت در پردازش اطلاعات تقسیم بندی می‌شوند.

در نظام حقوقی اتحادیه اروپا، پردازش اطلاعات در شبکه‌های ارتباطی بر مبنای این اصول قانونی صورت پذیرفته و عدم اجرای مفاد و نتایج این اصول می‌تواند منجر به غیرقانونی تلقی شدن فرایند پردازش و شمول ضمانت‌های مقرر در بخش پنجم از مقررات فوق‌الذکر گردد. اما در نظام حقوقی ایران، مقرراتی وجود ندارند که به صراحت به مفاد این اصول اشاره نمایند و آنچه از بررسی مقررات قابل برداشت

می‌باشد، وجود مصادیقی پرداخته از اجزا یا نتایج اصول بیان شده در فوق می‌باشد که در مقرراتی مانند ماده ۵۹ قانون تجارت الکترونیکی به تصویب رسیده است. آنچه اهمیت دارد، اصلاح مقررات حاکم بر نظام حقوقی ایران می‌باشد. چرا که شرایط موجود در ماده ۵۹ درخصوص داده‌پیام‌هایی اعمال می‌شوند که در ماده ۵۸ این قانون مورد تصریح قرار گرفته‌اند. اما متن ماده ۵۸ به گونه‌ای تنظیم شده است که پردازش داده‌های مبین ریشه‌های قومی، نژادی، عقیدتی، مذهبی، اخلاقی و داده‌های مربوط به وضعیت جسمی و روانی و جنسی اشخاص را منوط به شرایط مقرر در این ماده و ماده ۵۹ نموده و نص ماده‌گویی تفکیک میان این گروه از داده‌ها و دیگر داده‌های شخصی می‌باشد. به عبارت دیگر قانونگذار ایران در اقدامی نسنجیده، علیرغم تعریفی مشخص از داده‌پیام شخصی در ماده ۲، در ماده ۵۸ مبادرت به تفکیک داده‌پیام‌های شخصی به دودسته نموده که دسته‌های مشخص در ماده ۵۸ باید الزاماً با اخذ رضایت موضوع داده و دسته‌های غیرمصرح می‌توانند بدون رضایت موضوع داده پردازش و شامل شرایط ماده ۵۹ نشوند. اگرچه بنظر نگارندگان این موضوع ناشی از مسامحه قانونگذار بوده و وی پردازش انواع داده‌های شخصی را در متن این ماده مدنظر داشته و امکان‌الغای خصوصیت از مصادیق مذکور را به خواننده اعطا می‌نماید، اما نص مبهم ماده مذکور و البته نبود مقررره‌ای در زمینه کیفیت جمع‌آوری اطلاعات، ضرورت اصلاح این مقررات و توجه به انواع داده‌پیام‌های شخصی و اختصاص فصولی از این قانون به اصول پردازش اطلاعات را ایجاب می‌کند.

بعلاوه اجرای این اصول منوط به نظارت بر عملکرد اشخاص فعال در زمینه پردازش اطلاعات می‌باشد. امری که در حال حاضر به جهت نبود هرگونه سازمان ناظر یا اعطاکننده مجوز و عدم پیش‌بینی شرایط اخذ مجوز و فعالیت این اشخاص، در کشور ایران انجام نمی‌گیرد. براین مبنا لازم است وزارت صمت ابتدائاً مبادرت به تعیین سازوکار اخذ مجوز فعالیت شرکت‌ها و نظارت این سازمان بر فعالیت‌های آنها در حوزه

پردازش اطلاعات نموده و ثنیا شبکه‌های تبادل اطلاعاتی که همگان امکان دسترسی به آنها را دارند به نحوی تحت رصد قرار دهد که خارج از چارچوب قانونی مبادرت به جمع‌آوری، نگهداری، تحلیل و سایر مصادیق پردازش اطلاعات ننمایند.

توصیه آخر در این زمینه ضرورت آگاهی بخشی به مردم می‌باشد تا با اطلاع از قوانین و مقررات اولاً نسبت به اجرای حقوق قانونی خود اقدام و در صورت مشاهده مصادیق نقض مقررات، مبادرت به گزارش امر به مراجع ذیربط نمایند. این اقدام باید در وسایل ارتباط جمعی مانند تلویزیون با ایجاد برنامه‌های آموزشی صورت گیرد. بعلاوه ملزم نمودن مدیران شبکه‌های ارتباطی که مبادرت به پردازش اطلاعات می‌نمایند، خصوصاً سایت‌های عرضه و فروش محصولات، به ایجاد آیکن‌های پیش فرض که در بردارنده حقوق موضوع داده و الزامات قانونی پردازش اطلاعات بوده و به هنگام ورود کاربر پیش از نمایش اطلاعات شبکه، در کادری مجزا مبادرت به اعلام این مراتب به کاربر نموده و با پذیرش کاربر با زدن دکمه‌هایی مانند «مطلع شدم» و مشابه آن، نسبت به نمایش اطلاعات شبکه اقدام می‌نمایند، راهکاری مناسب در افزایش آگاهی بخشی به مردم تلقی می‌گردد.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

منابع

الف: فارسی

- انصاری، باقر، عطار، شیما، (۱۳۹۲)، *حریم خصوصی در شبکه های اجتماعی مجازی*، دوفصلنامه پژوهش های حقوقی، دوره ۲۳، شماره ۱، صص ۱۱۳-۱۳۷
- جلالی محمد، کامیاب، میثا، (۱۳۹۷)، *مقدمه ای بر شناخت مفهوم پلیس اداری در ایران با مطالعه تطبیقی در حقوق فرانسه*، دوفصلنامه مطالعات حقوق تطبیقی، دوره ۹، شماره ۱، صص ۶۷-۸۶
- حبیبی، همایون، (۱۳۹۵)، *حق بر حریم خصوصی در شبکه های اجتماعی*، فصلنامه تحقیقات حقوقی، دوره ۱۹، شماره ۷۵، صص ۳۹-۶۴
- قبولی درافشان، سید محمد مهدی، لطیف زاده، مهدیه، محسنی سعید، عابدی، محمد، (۱۴۰۲)، *حمایت از داده شخصی در اتحادیه اروپا و امکان سنجی آن در نظام حقوقی ایران*، فصلنامه مطالعات حقوق عمومی، دوره ۵۳، شماره ۲، صص ۹۸۱-۱۰۰۵
- قناد، فاطمه، علینقی، امیره، (۱۳۹۹)، *مفهوم و اهمیت داده های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی*، دوفصلنامه حقوق قراردادها و فناوریهای نوین، دوره ۱، شماره ۱، صص ۲۹۷-۳۳۲
- لاریجانی، مریم، (۱۳۸۷) *نظریه لاک: رضایت یا قرارداد*، فصلنامه پژوهش های فلسفی-کلامی، دوره ۹، شماره ۴، صص ۱۴۷-۱۷۸
- لطیف زاده، مهدیه، قبولی درافشان، سید محمد مهدی، محسنی، سعید، (۱۴۰۱) *تبیین اسباب مشروعیت پردازش داده های شخصی از منظر حقوق اتحادیه اروپا و ایران*، فصلنامه مطالعات حقوقی، صص ۳۳۵-۳۶۴
- محقق داماد، سید مصطفی، (۱۳۸۴) *قواعد فقه، بخش مدنی*، چاپ دوازدهم، مرکز نشر علوم اسلامی
- نجفی، محمد حسن، (۱۴۲۱)، *جواهرالکلام*، جلد سیزدهم، موسسه دارالمعارف

فقه اسلامی بر مذهب اهل بیت

هاشمی شاهرودی، محمود، (۱۴۳۲) *موسوعه الفقه الاسلامی المقارن*، جلد چهارم، موسسه دارالمعارف فقه اسلامی بر مذهب اهل بیت.

ب: انگلیسی

Albin Thelin),last visited (21/07/2023) ***The principle of purpose limitation***, <https://www.dporganizer.com/blog/gdpr-requirements-series/the-principle-of-purpose-limitation/>

An coimisiun um chosaint sonraí data protection commission,(Last visited 20/05/2023) Principles of Data Protection, <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>,

ARTICLE 29 DATA PROTECTION WORKING PARTY, (Last visited 22/06/2023) pinion 03/2013 on purpose limitation Adopted on 2 April 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Barrett Paula, Lorna Doggett, (last visited 14/07/2023), ***Shining a light on the meaning of “necessity” under GDPR Our eight point summary of the EDPB’s draft guidance***, online Edition: <https://www.eversheds-sutherland.com/documents/services/what-necessity-means-for-gdpr-our-eight-point-summary.pdf>

Cambridge Dictionary, (Last visited 22/07/2023), ***Authority***, <https://dictionary.cambridge.org/dictionary/english/authority>

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

European Commission, (Last Visited 12/06/2023), ***For how long***

can data be kept and is it necessary to update it?, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en

Golden Data Law, (last visited 21/07/2023) **What does “purpose limitation” mean under EU Data Protection Law?**, <https://medium.com/golden-data/what-is-purpose-limitation-under-eu-data-protection-law-fff4406ffe6>,

Golden Data Law, (b), (Last visited 21/07/2023), **What is “data minimization” under EU Data Protection Law?**, <https://medium.com/golden-data/what-is-data-minimization-under-eu-data-protection-law-b0e30fbb856e>,

Iapp, (Last visited 17/05/2023), **Storage Limitation**, <https://iapp.org/resources/article/storage-limitation/>

ICO Information Commissioners Office, (Last Visited 10/08/2023), What is valid consent?, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/#top>

Ico Commissioners Office, Principle (b): (Last visited 02/08/2023), Purpose limitation, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/purpose-limitation/>

Ico Commissioners Office, Principle (c): (Last visited 03/08/2023), Data minimization, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/>

Hunter Nelson, (Last Visited 21/07/2023), **GDPR Principles: Accuracy**, <https://tortoiseandharesoftware.com/blog/accuracy-principle-gdpr/>

Office of the Data Protection Ombudsman, (Last Visited 21/07/2023), Storage limitation, <https://tietosuoja.fi/en/storage-limitation>,

Osano Staff, (Last visited 15/08/2023), ***Less is more: the GDPR data minimization principle***, <https://www.osano.com/articles/less-is-more-the-data-minimization-principle-in-gdpr>

Peter Carey, (2018), ***Data Protection A Practical Guide to UK and EU Law***, Fifth Edition, Oxford University Press

Rekosh Edwin, (Last visited 22/07/2023), ***Who defines the public interest?***, international Journal of Human rights, online edition <https://sur.conectas.org/en/defines-public-interest/>

Roy Winkelman, (last visited 18/07/2023), ***Director, What is a Network?***, Florida Center for Instructional Technology College of Education, University of South Florida, <https://fcit.usf.edu/network/chap1/chap1.htm>

Satori, (last visited 22/07/2023), ***The Lawfulness of Processing***, <https://satoricyber.com/data-privacy/the-lawfulness-of-processing/>

Trend, (Last visited 13/07/2023), What is Data Minimization?, <https://www.trendmicro.com/vinfo/us/security/definition/Data-Minimization>

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

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