Culminatin of Law Quarterly

15nd Year, No. 2, Summer 2024

http://dx.doi.org/10.22034/THDAD.2023.1987539.2353

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

Abootaleb Koosha[1], Ali Akbar Farahzadi[2], 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.ujsasac0077@yahoo.com

فصلنامه تعالی حقوق

سال پانزدهم، شماره ۲، تابستان ۱۴۰۳

http://dx.doi.org/10.22034/THDAD.2023.1987539.2355

اصول حقوقی حاکم بر پردازش داده‌پیام‌های 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 دکترای حقوق خصوصی دانشگاه علوم قضایی و خدمات اداری، تهران، ایران.

نوع مقاله: علمی پژوهشی

صفحات: ۲۹۷-۲۵۵

تاریخ دریافت: ۱۴۰۲/۰۵/۲۲

تاریخ بازنگری: ۱۴۰۲/۰۶/۰۸

تاریخ پذیرش: ۱۴۰۲/۰۶/۱۹

چکیده

داده‌پیام‌های الکترونیکی به دودسته شخصی و غیرشخصی تقسیم می‌شوند. داده‌پیام‌های 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 داده‌پیام‌های شخصی چه می باشند؟ 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. بطورکلی اصول حاکم بر نظام حقوقی اتحادیه اروپا در دو دسته کلی، اصل قانونی، منصفانه‌بودن و شفافیت پردازش اطلاعات و اصل محدودیت در پردازش اطلاعات قرار می‌گیرند که درگفتارهای اول و دوم این پژوهش مورد تشریح قرارگرفته اند. پژوهش حاضر در قسمت نتیجه‌گیری نیز مبادرت به ارائه برخی توصیه های سیاستگذارانه در جهت بهبود اجرای این اصول در نظام حقوقی ایران نموده‌است.

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

* نویسنده مسئول: Mn.ujsasac0077@yahoo.com

درآمد

حریم‌خصوصی 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 قرارگرفته و مستقیما به کرامت انسانی و حق هرشخص بر حفاظت از آن مربوط می‌شود.(حبیبی،۱۳۹۵، ۴۰) در عصر حاضر، مدیریت شبکه‌های‌ارتباطی درگرو پردازش‌اطلاعات قرارگرفته است. شبکه به رایانه های متصل به هم اطلاق می‌گردد که در محدوده هدف از پیش تعیین‌شده مبادرت به پردازش‌اطلاعات می نمایند.(Win-kelman،2023[1]) در شبکه‌های‌تبادل‌اطلاعات کاربران امکان برقراری ارتباط و تبادل اطلاعات با یکدیگر را برخوردار می باشند.(انصاری و عطار، ۱۳۹۲، ۱۱۸) بنابراین کشورهای توسعه یافته برای نظام مند نمودن فرایند جمع‌آوری و تحلیل اطلاعات‌اشخاص مبادرت به تنظیم مقرراتی نموده اند تا فرایندپردازش‌اطلاعات و ورود به حریم‌خصوصی اشخاص در چارچوب قوانین و مقررات مصوب صورت پذیرد. ازجمله این مقررات می‌توان به مقررات عمومی حفاظت‌ازاطلاعات مصوب ۲۰۱۶ اتحادیه‌اروپا[1]، اشاره نمود. در نظام‌حقوقی‌ایران نیز اگرچه قوانین صریحی در زمینه حفاظت‌ازاطلاعات توسط مجلس قانونگذاری تصویب نشده اند، اما مقرراتی در قوانین تجاری ازجمله قانون‌تجارت‌الکترونیکی مصوب ۱۳۸۲ گنجانده شده اند که مسئله حفظ حریم‌خصوصی اشخاص را با اختصاص مقررات مواد ۵۸ و ۵۹ خود، در زمینه داده‌پیام‌های‌شخصی در دستورکار قرار داده است.

داده‌پیام به هر نمادی از واقعه، اطلاعات یا مفهوم که با وسائل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود، اطلاق می‌گردد.[2] داده‌پیام‌های‌الکترونیکی به دودسته داده‌پیام‌شخصی و غیرشخصی تقسیم می‌شوند. داده‌پیام‌شخصی به اطلاعاتی گفته می‌شودکه به صورت مستقیم یا غیرمستقیم

---

1. General Data Protection Regulation

۲. ماده ۲ قانون‌تجارت‌الکترونیکی 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 داده‌پیام‌های‌غیرشخصی عموما کاربردی در زمینه پردازش‌اطلاعات ندارند. اما سوال اینجاست که پردازش‌اطلاعات 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 ازجمله 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». (Consulting,2023 Intersoft)[1] در نظام‌حقوقی‌ایران نیز، بند دوم از ماده ۲ طرح حمایت و حفاظت از داده و اطلاعات‌شخصی واصل شده به مجلس شورای اسلامی در تاریخ ۱۳۹۹/۰۷/۱۲ نیز با بیان تعریفی مشابه با آنچه در نظام‌حقوقی‌اتحادیه‌اروپا قید شده، مقرر می‌دارد «پردازش هرگونه عملیات دستی یا خودکار بر داده‌ها و اطلاعات‌شخصی، 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». همانطورکه 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.

حریم‌خصوصی نقطه تزاحم حقوق قانونی اشخاص و پردازش‌اطلاعات آنها توسط شبکه های می‌باشدکه انجام آن باید از یک طرف منجر به نقض حریم‌خصوصی نشده و از طرف دیگر به نحوی صورت نپذیرد که منجر به خلل در عملکرد یک شبکه

گردد. این موضوع ایجاب می نماید تا فرایندپردازش‌اطلاعات در چارچوب هایی که قانون معین می کند، صورت پذیرد. ازجمله این چارچوب ها اصولی می باشند که قانونگذاران کشورها در قوانین مصوب خود پیش‌بینی می کنند. این اصول در ماده پنجم از مقررات مصوب ۲۰۱۶ مورد تصریح قانونگذاراتحادیه‌اروپا قرارگرفته اند. اما در نظام‌حقوقی‌ایران، ماده بخصوصی دراین زمینه توسط قانونگذار مورد تصریح قرار نگرفته است. ازاین‌رو پژوهش حاضر با مطالعه و تحلیل اصول حقوقی پردازش‌اطلاعات در مقررات حاکم بر نظام‌حقوقی‌اتحادیه‌اروپا، سعی در تطبیق آن با قواعدحقوقی حاکم بر نظام‌حقوقی‌ایران نموده‌است. این موضوع از آن جهت اهمیت دارد که رعایت اصول پردازش‌اطلاعات مطابق با آنچه در این پژوهش بیان خواهد شد، مستقیما 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 می‌کند، اطلاق می‌گردد. کرامت انسانی نیز به معنای احترام گذاری به حقوق قانونی اشخاص توسط دولت می‌باشد. (جلالی و کامیاب، ۱۳۹٤، ۱٤۰و ۱۵۰) اطلاعات اشخاص جزو دارایی‌های آنها محسوب می‌گردند که باید از امنیت کافی در فرایند پردازش اطلاعات برخودار 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 می‌کند 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 ذیلا به تبیین آنها اقدام خواهد شد. اگرچه در زمینه پردازش‌اطلاعات، مقالاتی توسط برخی نویسندگان مورد تالیف قرارگرفته اند، اما هیچ

کدام از پژوهش های پیشین صورت‌گرفته به موضوع اصول قانونی حاکم براین فرایند نپرداخته و پژوهش حاضر در محوریت موضوعی خود، پژوهشی بدیع محسوب می‌گردد. اصول حاکم بر نظام‌حقوقی‌اتحادیه‌اروپا در دو دسته کلی، اصل قانونی، منصفانه‌بودن و شفافیت پردازش‌اطلاعات و اصل محدودیت در پردازش‌اطلاعات قرار می‌گیرند که در گفتارهای ذیل این پژوهش مورد تشریح قرار خواهند گرفت.

۱- اصل قانونی، منصفانه‌بودن و شفافیت پردازش‌اطلاعات

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

- پردازش‌داده‌های‌شخصی به صورت قانونی
- پردازش‌داده‌های‌شخصی بر اساس قواعد عدل و انصاف
- پردازش شفاف داده‌های‌شخصی

۱-۱- قانونی بودن پردازش

درخصوص پردازش "قانونی" اطلاعات می‌توان بیان‌داشت، در نظام‌حقوقی‌اتحادیه‌اروپا تمامی مراحل پروسه پردازش‌اطلاعات جز در موارد مصرح قانونی باید با رعایت شرایط ماده ۶ مقررات مصوب ۲۰۱۶ انجام گیرد. ازاین‌رو شرایط مقرر در ماده ۶ می‌تواند به عنوان آستانه یا حداقل استانداردهای لازم قانونی برای پردازش‌داده‌های‌شخصی تلقی‌گردد.(Satori,2023) ماده ۶ مقررات مصوب ۲۰۱۶ دربیان شرایط پردازش‌قانونی‌اطلاعات مقرر می‌دارد:

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

- موضوع‌داده[۱] با پردازش‌داده‌های‌شخصی خود برای یک یا چند هدف خاص موافقت کرده باشد
- پردازش برای اجرای قراردادی که موضوع‌داده طرف آن‌است یا به منظور انجام اقداماتی بنا به درخواست موضوع‌داده قبل از انعقادقرارداد ضروری باشد
- پردازش به منظور حفاظت از منافع‌حیاتی موضوع‌داده یا شخص حقیقی دیگر ضروری باشد
- پردازش برای انجام وظیفه‌ای که به نفع عمومی یا در اعمال اختیارات‌رسمی به‌کنترل‌کننده[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 موضوع‌داده باشد که مستلزم حفاظت از داده‌های‌شخصی است،

---

۱. موضوع داده اصطلاحا به شخصی اطلاق می‌گردد که اطلاعات‌شخصی او مورد پردازش واقع می‌شود.

۲. کنترل‌کننده شخصی است که دریک شبکه ارتباطی مبادرت به جمع‌آوری، تحلیل و نگهداری اطلاعات‌شخصی موضوع داده می نماید. البته این شخص میتواند فرایندپردازش اطلاعات را به شخص دیگری که تحت دستورو راهنمایی او مبادرت به این امر می نماید، محول نماید. این شخص اصطلاحا پردازنده نامیده می‌شود.

به ویژه در مواردی که موضوع‌داده یک کودک باشد.

همانطورکه ملاحظه می‌گردد، ماده ۶ مقررات مصوب ۲۰۱۶، شش شرط برای تحقق پردازش‌قانونی‌اطلاعات پیش‌بینی نموده‌است. بنابراین درصورتیکه فرایندپردازش‌اطلاعات، دربردارنده یکی از شرایط فوق‌الذکر نباشد، اصولاً نمی‌تواند فرایند قانونی تلقی‌گردد.

۱-۱-۱- رضایت

شرط اول در پردازش‌قانونی‌اطلاعات، رضایت موضوع‌داده می‌باشد. نظام‌حقوقی‌ایران در مقایسه با نظام‌حقوقی‌اتحادیه‌اروپا دارای تفاوت‌هایی در شرایط اعلام‌رضایت می‌باشد. ماده ۵۸ از قانون‌تجارت‌الکترونیکی مصوب ۱۳۸۲، اعلام‌رضایت در پردازش‌داده‌های‌شخصی را منوط‌به ارائه رضایت «صریح» توسط موضوع‌داده نموده‌است. ماده فوق‌الذکر، درصورت عدم‌وجود رضایت‌صریح‌موضوع‌داده، پردازش‌اطلاعات را غیرقانونی تلقی کرده است. اما سؤال اینجاست که آیا صرف بیان واژه رضایت می‌تواند مثبت وجود رضایت‌صریح و قانونی موضوع‌داده باشد یا باید شرایطی نیز دراین امر به عنوان شرایط مقدماتی وجود داشته باشد تا بتوان رضایت‌صریح‌موضوع‌داده را احراز نمود؟ برای پاسخ به سؤالات فوق باید ابتدا مفهوم «رضایت‌صریح» را تبیین کرد. در دیدگاه برخی که نگارندگان نیز قائل بر آن می‌باشند، اعلام‌رضایت باید دربردارنده سه شرط باشد:

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

بنابراین اولین شرط در اعلام‌رضایت‌صریح، علم به مفاد چیزی‌که بدان رضایت

داده شده می‌باشد. اگرچه قانونگذارایران در باب اعلام شرایط و چگونگی انجام پردازش به موضوع‌داده حکمی در قانون‌تجارت‌الکترونیکی قید ننموده اما می‌توان با تدبر در فلسفه استفاده از این واژه در ماده ۵۸ و همچنین اخذ وحدت ملاک از سایر متون، ضرورت این موضوع را ایجاب نمود. به عنوان مثال ماده ۳۳ طرح حمایت و حفاظت از داده و اطلاعات‌شخصی بر ضرورت ذکر کلیه جزئیات فرایندپردازش ازجمله هدف پردازش، نحوه پردازش، شرایط فنی پردازش، سطح ایمنی موجود، حقوق موضوع‌داده و فرایند نظارت بر امر پردازش به موضوع‌داده تاکید نموده‌است. این موضوع در دستورالعمل‌های شماره ۴۲ و ۴۳ مقررات مصوب ۲۰۱۶ اتحادیه‌اروپا نیز مورد تصریح قانونگذار این اتحادیه قرارگرفته است.(2023,ICO)

بنابراین صرف اعلام‌رضایت چه به صورت کتبی و چه به صورت شفاهی، برای احراز صریح بودن آن در فرایندپردازش‌اطلاعات کفایت نمی‌نماید. به‌عبارتی اعلام‌رضایت، شرط لازم بوده اما شرط کافی تلقی نمی‌گردد و باید علاوه بر اعلام، دو شرط دیگر که اطلاع از مفاد چیزی‌که بدان باید رضایت داده شود و همچنین وجود قصد بر اعلام وجود داشته باشد. نکته‌قابل‌توجه اینست که در احراز وجود یا عدم‌وجود شروط اول و دوم (علم و قصد) بنظر نگارنده، اصل بر عدم‌وجود شرط اول بوده و قاضی در مقام قضاوت باید نسبت‌به احراز علم رضایت دهنده بر مفاد چیزی‌که بدان رضایت داده اقدام‌نماید. ازاین‌رو درصورتیکه دلیلی بر اطلاع موضوع‌داده از چیزی‌که بدان رضایت داده کشف نگردد، نمی‌توان رضایت‌صریح 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 ازسوی مدعی عدم‌وجود رضایت اثبات شده و به‌عبارتی 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 احرازرضایت توسط موضوع‌داده می‌باشد. بند یازدهم ماده ۴ مقرر می‌دارد:

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

سؤال اینجاست که آیا قانونگذاراتحادیه‌اروپا نیز همانند قانونگذارایران، اعلام‌رضایت‌صریح را شرط دانسته یا رضایت ضمنی نیز در اتحادیه‌اروپا برای احرازرضایت موضوع‌داده کفایت می‌کند؟ منشاء طرح این سؤال اینست که قانونگذاراتحادیه‌اروپا در صدر ماده با تصریح به واژه «اشاره» که عموما 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 پردازش‌داده‌ها 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 قواعدحقوقی و حالت گزینی و ذکر وجوه افتراق این دو واژه وجود ندارد.

اما در نظام‌حقوقی‌ایران طرح حمایت و حفاظت از داده‌ها و اطلاعات‌شخصی در مواد ۴ و ۵ خود، واجد شروط دیگری غیر از اعلام‌رضایت‌صریح می‌باشد. ماده ۴ این طرح بیان می‌دارد: پردازش اطلاعات‌شخصی اشخاص مربوط به وضعیت‌ها یا موقعیت‌های غیرعمومی منوط‌به اعلام‌رضایت آنها بوده و اعلام‌رضایت اشخاص موضوع‌داده باید با رعایت شرایط ذیل همراه باشد:

- پیش‌از پردازش باشد
- بیانگر آگاهی موضوع‌داده باشد
- استنادپذیر باشد

تصریح صورت‌گرفته در بند اول شرایط مقرر در ماده ۴ بر بیان رضایت پیش‌از پردازش، در انعقاد قراردادهای پردازشی نمود بیشتری دارد. براین‌مبنا، کنترل‌کنندگان و پردازندگان می‌توانند با اخذ امضا از موضوع‌داده، نسبت‌به 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 دراین سایت‌ها عموماً معرفی کالای متناسب با علایق یک مراجعه کننده برای خرید، پیش‌از پذیرش شرایط تعیین‌شده ازسوی سایت صورت می‌پذیرد که خلاف مقررات مصرح دراین طرح می‌باشد. برای حل این مشکل، گردانندگان سایت‌ها می‌توانند با ایجاد آیکنی که هنگام ورود کاربر به سایت بر روی شبکه باز شده و پیش‌از تأیید اطلاعات امکان ملاحظه محتویات سایت را به کاربر ندهد، نسبت‌به حل مشکل اقدام کنند. اما در شبکه‌های اجتماعی مانند اینستاگرام و فیس بوک و توییتر و... که ورود کاربر به شبکه منطبق با جمع‌آوری‌اطلاعات وی بوده و تنها دسترسی به مخاطبین تلفن همراه یا برخی اطلاعات دیگر وی منوط‌به اخذ رضایت می‌باشد، نقض این شرط جلوه بیشتری دارد.

بعلاوه ماده ۵ طرح، پردازش‌داده‌ها و اطلاعات‌شخصی مربوط به وضعیت‌ها یا موقعیت‌های عمومی را بدون‌رضایت شخص درصورتی بلامانع تلقی کرده که «یا خود وی داده‌ها را در معرض پردازش قرار داده یا پردازش‌داده‌ها را منع یا محدود نکرده باشد». سوالیکه می‌تواند مطرح گردد اینست که فردی که مبادرت به انتشار اطلاعات‌شخصی خود در شبکه‌های اجتماعی که ملیون ها بیننده دارد نموده و به‌عبارتی آنها را عمومی کرده باشد، چطور می تواند پردازش این داده‌ها را منع یا محدود نماید؟ درصورتیکه انتشار اطلاعات در شبکه خاص با کاربران خاصی صورت‌گرفته باشد، این مشکل جلوه کمتری دارد اما در شبکه‌های اجتماعی نمی‌توان به سادگی نسبت‌به این مهم اقدام کرد. سؤال دیگری که مطرح می‌گردد اینست که موضوع‌داده باید به چه طریقی نسبت‌به ایجاد منع یا محدودیت در پردازش اقدام کرده و درصورتیکه 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 موضوع‌داده را با عنایت به قواعدی مانند «انجام اقدام اهم نسبت‌به مهم» مورد تصریح قرار داده است. مصادیقی که دراین ماده پردازش بدون اخذ رضایت موضوع‌داده

ذکر شده شامل موارد ذیل می‌باشد:

- برای صیانت از حیثیت، جان یا مال موضوع‌داده ضروری باشد
- برای صیانت از حیثیت یا جان دیگری یا پیشگیری از زیان‌مالی 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 به‌آن توجه نمود اینست که بند دوم این ماده، شرط پردازش بدون‌رضایت را در وقوع‌زیان‌مالی به دیگران، «زیان مالی شدید» قلمداد کرده است. حال سؤال اینجاست که منظور از زیان مالی شدید چیست؟ آیا دراین 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 درنظر گرفت یا معیار درنظر 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 دراین بند خواهد بود. دلیل ارائه این نظر نیز آن‌است که اولاً پردازش بدون‌رضایت اطلاعات‌شخصی دیگران که برمبنای آن طرحی مشتمل بر ۵۶ ماده در دستورکار بررسی مجلس شورای اسلامی قرارگرفته، امری استثنایی بوده و در تفسیر استثنائات این قاعده نیز باید مبادرت

به ارائه تفسیر مضیق نمود و به‌عبارتی مصادیق شمول بندهای ماده ۱۰ را تا حدممکن محدود کرد. ثانیاً بند دوم ماده ۱۰، دربیان این استثنا، به واژه «پیشگیری» تصریح کرده که نشان از پردازش‌اطلاعات بدون‌رضایت موضوع‌داده درحالتی دارد که هیچ ضرر و زیانی به دیگری وارد نشده که بتوان میزان شدید بودن یا نبودن آن‌را احراز نمود. براین‌مبنا چه دلیلی دارد با ارائه معیارهای نوعی و گسترش شمول مصادیق این ماده، به صرف پیشگیری از وقوع‌زیان، نسبت‌به پردازش بدون‌رضایت اطلاعات دیگران اقدام کرد.

نکته آخر اینست که ماده ۱۱ از طرح فوق‌الذکر، انجام پردازش‌اطلاعات بدون اخذ رضایت را منوط‌به وجود سه شرط «حفظ گمنامی اطلاعات، عدم‌وجود زیان مادی یا معنوی برای موضوع‌داده و عدم امکان اخذ رضایت» نموده‌است. چالشی که در ارتباط با این ماده نیز می‌تواند مطرح شود اینست که در تقابل میان پیشگیری از وقوع‌زیان‌مالی شدید به دیگران و وقوع‌زیان‌مادی بسیار خفیف به موضوع‌داده یا زیان معنوی به وی، کدام حالت را باید نسبت‌به 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 داده‌های‌شخصی، حفظ و پیشگیری از نقض امنیت این اطلاعات می‌باشد. بنابراین در تقابل مقررات مواد این طرح، اولویت را باید نسبت‌به پذیرش موادی قرار داد که در جهت صیانت از امنیت داده‌پیام‌ها تصویب شده‌اند. ازاین‌رو مقررات ماده ۱۱ را باید در هر حال نسبت‌به 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 بیان‌داشت که اعمال حقوق‌اشخاص تا جایی جاری می‌باشد که با نظم عمومی یک کشور در تعارض نباشد. بنابراین در فرضی که ممکن است اعمال حق موضوع‌داده منجر به زیان شدیدمالی به دیگران شود، طبیعتاً باید نسبت‌به 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، دراین زمینه نیز نمی‌توان نسبت‌به پردازش‌اطلاعات‌اشخاص برای حفظ امنیت ملی یک کشور به صرف وقوع‌زیان به‌آن‌ها 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- انعقادقرارداد

درخصوص بند دوم ماده ۶ این مقررات می‌توان بیان‌داشت که این بند پردازش در انجام تعهدات قراردادی یا پیش‌از قرارداد را منوط به وجود عنصر «رضایت» نموده‌است. شق اول بند دوم این ماده دو شرط را برای پردازش‌اطلاعات موضوع‌داده پیش‌بینی کرده است. این دو شرط طرف قرارداد بودن موضوع‌داده و ضرورت پردازش برای اجرای مفاد قرارداد می‌باشند. بنابراین اطلاعات‌اشخاص در قراردادهایی که این افراد جزو طرفین قرارداد نباشند، غیرقانونی و ممنوع می‌باشد. مضاف بر آنچه بیان شد، ذکر عنوان «درخواست موضوع‌داده» درخصوص اقدامات پیش‌از قرارداد در دیدگاه نگارنده می‌تواند به صورت موسع تفسیر شود. به عبارت دیگر گاه جمع‌آوری‌اطلاعات‌اشخاص مسبوق بر درخواست صریح آنها مانند اشتراک اطلاعات در یک شبکه‌تبادل‌اطلاعات می باشد و گاه ورود یک شخص به یک سایت جهت خرید کالا می‌تواند به عنوان درخواست ضمنی وی بر جمع‌آوری‌اطلاعات ازجمله آدرس، شماره کارت اعتباری و... تلقی‌گردد که برای ارسال کالای خریداری شده از آن سایت به خریدار ضروری شمرده شود.

درخصوص واژه ضرورت، می‌توان بیان‌داشت که پردازش درصورتی 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، پردازش‌داده‌ها 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 دراین جا مطرح می‌شود اینست که وجود راه‌های دیگر تاکجا می‌تواند مانع احراز ضرورت نباشد؟ آیا درصورت وجود گزینه‌های هم عرض می‌توان به صرف استناد به تناسب و وجود گام هدفمند نسبت‌به پردازش‌اطلاعات اقدام نمود یا باید معیار بخصوصی دراین زمینه وجود داشته باشد؟ در دیدگاه نگارندگان صرف وجود گام هدفمند و تناسب با تعهدات دراین خصوص کفایت نمی‌کند. چراکه دربیان 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 درصورتی 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 پردازش‌اطلاعات به عنوان راهکاری معقول تلقی‌گردد.(Barrett&Etc,2023)

بعلاوه در دیدگاه برخی دراین 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 بیان‌داشت که اولاً توافقات گاه به منزله قراردادهای شفاهی و گاه توافقات پیش‌از قرارداد می‌باشند. بر فرض اینکه منظور نویسندگان فوق‌الذکر، قراردادهای شفاهی باشد، سؤال اینجاست که آیا با وجود شرایط متعدد تعیین‌شده در مواد ۵ و ۶ مقررات مصوب ۲۰۱۶ و حساسیتی که قانونگذاراتحادیه‌اروپا 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 بیان‌داشت با توجه به اینکه قانونگذاراتحادیه‌اروپا با اختصاص یک فصل از مقررات مصوب ۲۰۱۶ از مواد ۷۷-۸۴ این قانون را به مسائل مرتبط با مسئولیت‌پذیری اشخاص فعال در فرایندپردازش‌اطلاعات در اتحادیه‌اروپا اختصاص

داده و این موضوع نشان از اهمیت موضوع درنظر قانونگذار بوده است، بنظر می‌رسد قانونگذار حکیم اتحادیه‌اروپا، اصولاً هر نوع قراردادی را به منزله قراردادی که موضوع پردازش‌اطلاعات نیز جزو فرایند اجرای تعهدات باشد، درنظرنگرفته و بنظر نگارنده منظور همان قراردادهای کتبی بوده است.

نکته دیگر آن‌است که در فرایندپردازش، 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 جمع‌آوری‌اطلاعات درخصوص علایق کاربر سایت در انتخاب نوع کالا و ارائه پیشنهادات مشابه را ندارند.(همان، ۳۴۶) چراکه این موضوع ارتباطی به اجرای مفاد قرارداد ندارد. ضمن اینکه آنچه بیان شد عموماً در محدوده پیش‌از انعقادقرارداد 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 اتحادیه‌اروپا، مقررات مشابهی در نظام‌حقوقی‌ایران ندارد و با امعان نظر از واژه ضرورت وجود رضایت «صریح» در ماده ۵۸ قانون‌تجارت‌الکترونیکی و اصولی مانند اصل عدم‌وجود رضایت، می‌توان به فقدان وجود مجوز در پردازش‌اطلاعات‌شخصی در فرایند انعقاد یا پیش‌از انعقادقرارداد استناد کرد. مگر در مواردی که بنا بر ضرورت، راهی جز پردازش‌اطلاعات همانند آنچه درخصوص 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 براینکه اگر کسی به دیگری نسبت‌به چیزی اذن دهد، گستره اذن به‌آن‌چه مورد تصریح اذن دهنده قرارگرفته محدود نشده بلکه لوازم عقلی، ذاتی، عرفی و قانونی آن‌را نیز دربر می‌گیرد،(شاهرودی، ۱۴۳۲، ۵۹ و محقق داماد، ۱۳۸۴، ۲۳۶-۲۳۷) اظهارنظر

کرده‌اند که رضایت شخصی افراد به انعقادقرارداد به منزله اذن بر پردازش‌اطلاعات نیز می‌باشد. (قبولی درافشان و دیگران، ۱۴۰۱، ۳۴۷) اما سؤال اینجاست که اگر امکان توسل به چنین قواعدی در نظام‌حقوقی‌ایران امکان پذیر باشد، چرا قانونگذار از ضرورت اعلام‌رضایت‌صریح در مقررات ماده ۵۸ پرده برداشته است.[۱] 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 موضوع‌داده یا دیگری

درخصوص بند سوم ماده ۶ مقررات مصوب ۲۰۱۶، بنا بر نظر عده‌ای این بند تنها درخصوص حفظ جان و منافع‌حیاتی و زندگی اشخاص مانند پردازش‌اطلاعات وی در هنگام عمل جراحی در بیمارستان برای دستیابی به سوابق عمل جراحی یا گروه خونی و... کاربرد داشته و نمی‌توان به مسائل دیگر آن‌را تسری داد. بعلاوه درخصوص دیگران نیز باید به طریق اولی تنها درخصوص منافع‌حیاتی و زندگی مانند پردازش‌داده‌های‌شخصی 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 حریم‌خصوصی بیماران دارای مقرراتی دراین زمینه می‌باشد. (همان، ص ۳۵۱) ماده ۴ این منشور مقررمی‌دارد:

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

اگرچه این مقرره می‌تواند به منزله توجیه کننده اقدامات مراکز درمانی دردسترسی

---

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 بدون‌رضایت‌صریح آنها به هر عنوان غیرقانونی است.

به اطلاعات‌شخصی بیماران بدون اخذ رضایت تلقی شود و منطقاً نیز در مواردی که صحبت از جان اشخاص مطرح می‌شود باید تمامی موانع قانونی کنار گذاشته شوند، اما سؤال اینجاست که آیا در تقابل این مقرره با مقررات ماده ۵۸ قانون‌تجارت‌الکترونیکی و این موضوع که قانونگذار در آن ماده از عبارت «بدون‌رضایت‌صریح آنها به هر عنوان غیرقانونی است» و توجه به این موضوع که قانونگذار صراحتاً از واژه به هر عنوان اشاره نموده، نمی‌توان عدم‌وجود استثنا در پردازش‌اطلاعات‌شخصی را از این ماده استناد و استثنای بیان شده در ماده ۴ منشور را فاقد وجاهت قانونی تلقی نمود؟ بنظر نگارنده جواب این سؤال مثبت بوده و سیاستگذاران تقنینی باید نسبت‌به اصلاح این مقرره و رفع خلاء های قانونی آن اقدام نمایند.[۱]

۱-۱-۴- حفظ منافع عمومی یا اعمال اختیارات‌رسمی

درخصوص بند چهارم مقررات مصوب ۲۰۱۶ می‌توان بیان‌داشت که واژه منفعت عمومی امری بسیط بوده و تفسیر موسع از آن می‌تواند آثار بندهای دیگر ازجمله 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 بودهو به‌عبارتی به «آنچه که برای کل جامعه بهترین باشد» اطلاق می‌گردد. (Rekosh,۲۰۲۳)این واژه می‌تواند حقوق آزادی اشخاص، حقوق مصرف کنندگان، حقوق سلامت و موارد مشابه را در برگیرد. شق دوم این بند نیز بر اعمال اختیارات‌رسمی به کنترل‌کننده اختصاص یافته است. اختیارات‌رسمی نیز به اختیاراتی گفته می‌شود که مقامات رسمی دولتی برای انجام وظایف قانونی اعطا می‌شود.(Cam-bridge Dictionary،2023) بنابراین می‌توان نتیجه گیری نمود که این اختیارات بیشتر جنبه حاکمیتی داشته و از مفهوم تصدی گری فاصله دارند. دراین حالت نیز مقام دارای

---

۱. نکته جالب توجه در پردازش اطلاعات پزشکی اینست که ماده ۶۰ قانون‌تجارت‌الکترونیکی ، فرایند ذخیره، پردارش و توزیع داده‌پیام‌های مربوط به سوابق پزشکی و بهداشتی را تابع آیین نامه ماده ۷۹ این قانون قرارداده، درحالیکه آیین نامه ماده ۷۹، فاقد هرگونه مقرره دراین زمینه می‌باشد.

اختیار، از اخذ رضایت موضوع‌داده یا هر الزام قانونی دیگر معاف می‌باشد.

اگرچه مشابه این مقرره در قانون‌تجارت‌الکترونیکی ایران پیش‌بینی نشده، با این حال مفهوم آن از سایر مقررات قانونی ازجمله 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 مقررمی‌دارد«... 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 نسبت‌به اموری اقدام‌نماید که انجام آن ازسوی 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 درصورتیکه دولت یا هر مقام صلاحیت داری در مقام اعمال حاکمیت مبادرت به انجام فرایندپردازش‌اطلاعات نمایند، این موضوع استثنایی بر مقررات ماده ۵۸ قانون‌تجارت‌الکترونیکی تلقی و فاقد ضمانت اجرای مقرر در ماده ۷۱ همان قانون خواهد بود.[۱]

۱-۱-۵- وجود اهداف مشروع

درخصوص بند آخر ماده ۶ مقررات مصوب ۲۰۱۶ نیز می‌توان بیان‌داشت این بند امکان پردازش‌اطلاعات را درصورتی پیش‌بینی نموده‌است که سه شرط ذیل به صورت توامان وجود داشته باشند:

- هدف مشروع
- ضرورت

---

۱. ماده ۷۱- هرکس دربستر مبادلات الکترونیکی شرایط مقرردرمواد (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 بیان‌داشته‌اند 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 موضوع‌داده ارجحیت داشته باشد تا به حکم قاعده «تقدم منافع اهم بر مهم» امکان پردازش فراهم گردد. دراین راستا باید پیامدهای پردازش بر حقوق‌اشخاص ارزیابی شده و ملاک تشخیص نیز حکم عقل خواهد بود. این عده معتقدند که پردازش بر اساس این بند باید با درنظرگرفتن 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 موضوع‌داده با دیگران را ازجمله مصادیق استثنا برای پردازش‌اطلاعات تعبیر نموده‌است. 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. ازاین‌رو نمی‌توان به سایر مصادیق حکم کلی فوق‌الذکر را نسبت داده و از آن تفسیر موسع نمود.

۲-۱- منصفانه‌بودن پردازش

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

موضوع‌داده یا داده‌های اشخاص ثالث وجود نداشته و بنابراین حتی درصورتیکه اطلاعات فرد الف تحت‌پردازش قرارگرفته و دراین میان اطلاعاتی وجود داشته باشد که به صورت فریب کارانه از شخص ب جمع‌آوری شده و توام با اطلاعات شخص الف پردازش شوند، پردازش‌اطلاعات شخص ب منجر به غیرقانونی تلقی شدن پردازش‌اطلاعات شخص الف نیز می‌گردند.

پرونده شرکت نوآوران (ارائه خدمات پستی) علیه مسئول حفاظت‌ازاطلاعات[1]، مثالی عینی از جمع‌آوری غیرقانونی اطلاعات می‌باشد که همچنان به عنوان یکی از نمونه‌های بارز نقض عدالت و انصاف در جمع‌آوری‌اطلاعات 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" ازسوی آنها امکان پذیرد 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 ازسوی 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 ازسوی آنها تلقی‌گردد. 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 مقررمی‌دارد «کنترل‌کننده باید در زمانی که داده‌های‌شخصی به دست می‌آید، اطلاعات مرتبط با دوره نگهداری و حقوق موضوع‌داده را برای اطمینان از پردازش عادلانه و شفاف اطلاعات به وی اعطا کند». این بند پشتبند مقررات بند اول ماده ۱۳ قید شده که پیش‌از شروع فرایند جمع‌آوری‌اطلاعات، برای حفظ اصل پردازش منصفانه، موضوع‌داده را محق بر اطلاع از حقوق قانونی خود نموده‌است. بنابراین می‌توان به نتیجه رسید که مهمترین الزام در پردازش منصفانه اطلاعات، اطلاع موضوع‌داده از حقوق قانونی خود می‌باشد.[۱] بعلاوه دستور العمل شماره ۶۰ مقررات مصوب ۲۰۱۶ در انجام هر چه بهتر فرایندپردازش منصفانه ضرورت ارائه کلیه اطلاعات مرتبط با احراز منصفانه‌بودن را فراتر از حقوق قانونی مندرج در ماده ۱۳، به موضوع‌داده مورد تصریح قرار داده است. این دستورالعمل مقررمی‌دارد:

- اصل پردازش شفاف و منصفانه ایجاب می‌کند که موضوع‌داده از عملیات پردازش و اهداف آن مطلع شود. کنترل‌کننده باید هر اطلاعات دیگری راکه برای اطمینان از پردازش شفاف و منصفانه با درنظرگرفتن شرایط خاص و زمینه پردازش‌داده‌ها لازم است، به موضوع‌داده ارائه دهد.... (Lex,2016,12-EUR) ۲

۳-۱- شفافیت در پردازش

عنصر سوم در اصل بیان شده دراین گفتار شفافیت در پردازش‌اطلاعات می‌باشد. مقررات مربوط به این موضوع در ماده ۱۲ مقررات مصوب ۲۰۱۶ مورد تصریح قرارگرفته است. دراین راستا، باید "اقدامات مناسب" در زمینه در اختیار گذاشتن اطلاعات قابل فهم و واضح درخصوص کیفیت جمع‌آوری و پردازش‌اطلاعات در اختیار موضوع‌داده 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 قرارگرفته است.

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

قابل فهم باشند. ازاین‌رو 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 نتیجه گیری نمود، ارائه اطلاعات به موضوع‌داده باید به زبان محلی کشور متبوع فرد صورت پذیرد.(44,cit.op,CAREY)

در کنار موارد بیان شده، درصورتیکه اطلاعات جمع‌آوری شده، تلازم مستقیم یا غیرمستقیم با حقوق‌اشخاص ثالث داشته باشد، باید نسبت‌به ارائه آگاهی لازم دراین خصوص به‌آن‌ها نیز اقدام گردد. ضمن اینکه ازجمله نتایج ضروری اصل شفافیت، ارائه اطلاعات مرتبط با حقوق کاربران شبکه‌های تبادل‌اطلاعات دردسترسی و پردازش‌اطلاعات ازجمله (تصحیح، پاک کردن، محدودیت، تبادل، حمل و...) می‌باشد تا آنها به خوبی از اختیارات سایر کاربران یا مدیران شبکه‌های ارتلاطی 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 نموده‌است:

- باید دسترسی موضوع‌داده به اطلاعات و آگاهی از حقوق قانونی وی تسهیل گردد.
- باید در محدوده زمانی مشخص به درخواست‌های موضوع‌داده جهت اجرای حقوق قانونی وی پاسخ داده شود.
- باید دلایل منطقی مبنی بر عدم اجرای درخواست‌های موضوع‌داده به صورت دقیق به وی اطلاع داده شده و وی از چگونگی امکان اعتراض به تصمیم خود، اگاه گردد.

متداول‌ترین روش جهت ایجاد شفافیت در پروسه دسترسی و پردازش‌اطلاعات، تهیه اطلاعیه‌ای متشکل از توضیحات جامع از تمامی الزامات حقوقی مرتبط با ایجاد شفافیت می‌باشد که اصطلاحاً با عناوینی ازجمله " اعلامیه پردازش منصفانه"، " اعلامیه حفظ حریم‌خصوصی"، " خط مش حفظ حریم‌خصوصی" 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 موضوع‌داده قرار داده شود.
- ارائه اطلاعات شفاهی به موضوع‌داده تنها درصورتی است که اولاً به درخواست صریح وی صورت‌گرفته باشد و ثانیاً موضوع‌داده 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 جمع‌آوری‌اطلاعات 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 موضوع‌داده می‌باشد، باید تمامی اقدامات قانونی لازم دراین خصوص بدون دریافت هرگونه هزینه از موضوع‌داده صورت پذیرد. (44-45,cit.op,CAREY)

۲- اصل ایجاد محدودیت در پردازش‌اطلاعات

اصل محدودیت در پردازش‌اطلاعات همانطورکه از نام آن پیداست به معنای ایجاد محدودیت در پردازش‌اطلاعات می‌باشد تا داده‌پیام ها در چارچوب اهداف تعیین‌شده پردازش شوند. از نتایج این اصل می‌توان به سه نتیجه محدودیت هدف در پردازش‌اطلاعات، به حداقل رساندن اطلاعات و دقت در جمع‌آوری‌اطلاعات اشاره نمود که ذیلا به تبیین هر یک اقدام می‌گردد.

۱-۲- محدودیت هدف در پردازش‌اطلاعات[1]

محدودیت هدف به معنای جمع‌آوری و پردازش‌داده‌ها بر اساس اهداف از پیش تعیین‌شده مشخص، صریح و قانونی می‌باشد. ازاین‌رو درصورتیکه اهداف مقرر واجد ویژگی‌های بیان شده نباشند، پردازش مذکور قانونی تلقی نمی‌گردد. با این حال استثنائاتی نیز دراین زمینه پیش‌بینی شده است. در جمع مفاد این اصل و مفاد ماده ۸۹ مقررات مصوب ۲۰۱۶، درصورتیکه 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-2023,un)

درخصوص پردازش بر اساس منافع عمومی، در مطالب پیشین توضیحات مفصل ارئه گردید که دراینجا به جهت جلوگیری از تکرار مکررات از ذکر مجدد خودداری می‌گردد. اما نکته‌قابل‌توجه 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 بیان‌داشت که اطلاعات‌اشخاص 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 نانوفناوری تشکیل و فعالیت نموده و اطلاعات عرضه شده این سازمان در شبکه‌های ارتباطی خود تنها در حوزه نانوفناوری باشد، امکان انجام پردازش‌اطلاعات با اهداف مرتبط با حوزه جراحی مغز و اعصاب را نخواهد داشت.

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

---

1. Purpose Limitation

داده‌های آماری جمع‌آوری شده نیز دقیقاً باید در حوزه فعالیت سازمانی باشند که نسبت‌به 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 تعیین‌شده جلوگیری می‌نماید. (نتیجه سلبی) (34,cit.Op ,CAREY)

همانطورکه بیان شد در اصل فوق‌الذکر، ابتدا باید اهداف دقیق از پردازش‌اطلاعات تعیین و جز در مورد سه استثنای بیان شده، پردازش‌اطلاعات تنها در محدوده اهداف تعیین‌شده 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 داده‌های‌شخصی با اهداف از پیش تعیین‌شده، در سال ۲۰۱۳ کارگروه ماده ۲۹ دستور العمل حفاظت‌ازاطلاعات مصوب ۱۹۹۵ اتحادیه‌اروپا[1] - این مرجع به عنوان مرجع راهنمای کمیسیون اتحادیه‌اروپا شناخته می‌شود- مبادرت به ارائه دستورالعملی با عنوان راهنمای ارزیابی انطباق به کنترل‌کنندگان اطلاعات نمود. دراین دستورالعمل عوامل اصلی که باید در ارزیابی انطباق پردازش و اهداف از پیش تعیین‌شده باید درنظرگرفته شود، به قرار ذیل تعیین گردیده است:(۲۰۲۳,Europa)

- رابطه بین اهداف جمع‌آوری داده‌های‌شخصی و اهداف پردازش

۱. این دستورالعمل پیش‌ازمقررات عمومی حفاظت‌ازاطلاعات اتحادیه اروپا به عنوان مقررات لازم الاجرا درسطح اتحادیه اروپا در زمینه حفاظت‌ازاطلاعات محسوب می‌شد.

- زمینه جمع‌آوری داده‌های‌شخصی و ضروریات توجیه کننده نگهداری آنها
- ماهیت داده‌های‌شخصی و تأثیر پردازش بر روی موضوع‌داده
- 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 جمع‌آوری‌اطلاعات خود زیرمجموعه‌ای از پردازش می‌باشد، اما منظور از پردازش دراین فرایند، انجام هرگونه اقدام اعم از تحلیل آماری یا فنی یا ذخیره یا تبدیل اطلاعات به‌انواع دیگر داده‌ها بر روی داده‌های جمع‌آوری شده می‌باشند.(Thelin[۲۰۲۳]) بنابراین درصورتیکه نتیجه حاصل از اقدامات انجام شده با اهداف تعیین‌شده در جمع‌آوری‌اطلاعات 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. دراین صورت اعمال حاصل از پردازش‌اطلاعات توسط شرکت آب و برق نمی‌تواند به عنوان نقض اصول حاکم بر حفاظت‌ازاطلاعات تلقی‌گردد. اما ارسال اطلاعات به شرکت اپراتور تلفن همراه به منزله نقض اصل محدودیت هدف در پردازش می‌باشد.(CAREY, Op.cit,35)

این موضوع در بند ب ماده ۵۹ قانون‌تجارت‌الکترونیکی ایران نیز مورد تصریح قرارگرفته است. بند ب ماده ۵۹ مقررمی‌دارد:

«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 تعیین‌شده مورد استفاده قرار گیرد.

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

عامل سوم بر نوع داده‌های‌شخصی تاکید دارد. داده‌های‌شخصی 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 پردازش‌اطلاعات مذهبی، شناخت کلی درخصوص اعتقادات و رسوم و باورهای دینی یک موضوع‌داده ارائه می‌کند. بنابراین درصورتیکه به هر نحو داده‌ای بر اساس هدف خاصی جمع‌آوری و پردازش شود، باید آثار حاصل از پردازش مورد ارزیابی قرارگرفته و مشخص گردد که آیا اهداف معین محقق شده‌اند یا خیر. درخصوص عامل چهارم نیز باید بیان‌داشت که ملاک در اجرای اصل محدودیت هدف، تنها اقدامات ایجابی نبوده و باید اقدامات حفاظتی نیز در نظارت بر فرایند انجام شده صورت پذیرد. براین‌مبنا بر اساس نوع و دسته ویژه داده‌های‌شخصی که در مطالب فوق بیان شد، اقدامات حفاظتی

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

۲-۲- به حداقل رساندن اطلاعات[1]

درخصوص به حداقل رساندن اطلاعات می‌توان بیان‌داشت، پردازش‌داده‌های‌شخصی باید به حد لزوم (کفایت)، مرتبط و محدود به‌آن‌چه با اهداف پردازش ضروری می‌باشد صورت پذیرد.(Ico(c),2023) از آنچه از این نتیجه حاصل می‌گردد اینست که باید تنها داده‌هایی که برای اهداف تعیین‌شده ضروری باشد مورد جمع‌آوری واقع گردد.(Trend,2023) این نتیجه در قسمت سوم بند اول ماده ۵ مقررات مصوب ۲۰۱۶ مورد تصریح قرارگرفته و به سه عامل "حد لزوم"[2]، " ارتباط"[3] و " محدودیت"[4] در پردازش‌اطلاعات تاکید دارد.[5]

معیار اول در عملیاتی نمودن به حداقل رساندن داده‌ها، کفایت می‌باشد. برمبنای این معیار، اطلاعات جمع‌آوری شده باید به حد ضرورت جمع‌آوری و نگهداری آنها نیز باید تا حد نیاز و برای اهداف تعیین‌شده باشد. ازاین‌رو 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. براین‌مبنا درصورت از میان رفتن ضرورت، نهادی که اطلاعات دردسترس وی باشد باید نسبت‌به حذف اطلاعات از شبکه خود یا ناشناس سازی آنها اقدام‌نماید. (Iapp,2023)[1] این موضوع اثرات مثبتی ازجمله 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 جمع آوری اطلاعات در حد کفایت و ضرورت تاکید دارند. ازاین‌رو 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)

نکته‌قابل‌توجه اینست که درخصوص معیار مدت زمان نگهداری اطلاعات، در مقررات مصوب ۲۰۱۶ اتحادیه‌اروپا حکمی قید نشده و براین‌مبنا می‌توان تعیین این موضوع را بر صلاحدید شخصی قرار داد که داده‌ها را در اختیار داشته باشد. با این حال نکته‌قابل‌توجه 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 قرارگرفته است، کمتر باشد. بنابراین مطابق با مقررات حاکم بر نظام‌حقوقی‌اتحادیه‌اروپا 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 جمع‌آوری‌اطلاعات 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 جمع آوری شده، دارای ضوابطی می باشد. این موضوع از مصوبات جلسات ۴۸۲-۴۸۸ شورای عالی انقلاب فرهنگی در زمینه حمایت از ارتباطات الکترونیکی و داده‌پیام‌های‌شخصی قابل برداشت می باشد 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 می گردد. از این رو با مفاد بند ب ماده ۵۹ قانون تجارت الکترونیکی که ذخیره اطلاعات را تنها به اندازه ضرورت متناسب با اهداف جمع آوری، امکان پذیر کرده است، دارای تعارض می باشد. برای رفع این تعارض به نظر می رسد 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 پیام های شخصی تنها در صورتی جاری می گردد که متناسب با اهداف جمع آوری، 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 پیام های غیرشخصی نیز باید مقررات قانون آیین دادرسی کیفری را ناسخ مصوبات فوق الذکر 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. براین‌مبنا ، اطلاعات‌شخصی را درصورتی 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. دراین 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. برمبنای این معیار، اطلاعات جمع‌آوری شده باید مرتبط با هدف پردازش باشند و درصورتیکه داده‌ای خارج ازاین موازین جمع‌آوری گردد، باید حذف شود. ازاین‌رو درصورتیکه یک خبرنامه الکترونیکی که با مشتریان خود به صورت الکترونیکی از طریق اشتراک تلفنی یا ایمیل در ارتباط می‌باشد، مبادرت به جمع‌آوری‌اطلاعات آدرس منزل آنها نماید، این موضوع به منزله نقض این نتیجه محسوب خواهد شد. حتی درصورتیکه این خبرنامه، از پیش اطلاعاتی درخصوص آدرس منزل مشترکین خود داشته باشد نیز باید نسبت‌به حذف اطلاعات از شبکه خود اقدام‌نماید. چراکه این اطلاعات ارتباطی به موضوع و هدف فعالیت این شبکه ندارد.

نتیجه بیان شده در فوق دربردارنده دو رکن تعیین اهداف مورد پردازش و میزان تقریبی اطلاعات قابل پردازش می‌باشد. به عنوان مثال درصورتیکه هدف از جمع‌آوری‌اطلاعات در فرم " درخواست اشتغال" باشد، تصمیم گیری درخصوص 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 پردازش‌اطلاعات 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,36-35) ازاین‌رو اگر

فعالیتی لزوماً جهت دستیابی به هدف تعیین‌شده در پردازش‌اطلاعات مورد استفاده واقع نگردد، انجام آن به منزله نقض اصل مذکور محسوب می‌شود. به عنوان مثال درصورتیکه شخصی برای کار در واحد ترابری یک شرکت در آن استخدام شود، پردازش و حتی نگهداری اطلاعات‌شخصی 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 پردازش‌داده‌ها به عنوان رکنی مهم تلقی می‌گردد. چرا که پردازش طولانی مدت و نامتعارف داده‌ها و دسترسی بیش از حد به‌آن‌ها نیز خارج از عنصر حداقل رساندن داده‌ها می‌تواند باشد.

نکته‌قابل‌توجه دراین موضوع اینست که اطلاعات جمع‌آوری شده توسط مدیران یک شبکه ارتباطی نمی‌تواند به بهانه این موضوع که موضوع‌داده نسبت‌به 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 موضوع‌داده، نمی‌تواند به منزله مجوزی برای نقض قواعد ماده ۵ مقررات مصوب ۲۰۱۶ تلقی‌گردد.(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 داده‌های‌شخصی نیز باید مورد نظر قرار گیرد. ازاین‌رو اگر در هر یک از مراحل جمع‌آوری یا پردازش‌داده‌ها، از مفاد این نتیجه تخطی گردد، می‌توان آن‌را 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 دردسترس که درخصوص داده‌های حساس ضرورت دسترسی کارکنان خاص را ایجاب می‌نماید؛ درصورتیکه تعداد غیرمتعارفی کارمند مبادرت به دسترسی به اطلاعات مذکور نمایند، نتیجه فوق‌الذکر می‌تواند مورد نقض واقع گردد.

۳-۲- دقت در جمع‌آوری و پردازش‌اطلاعات[1]

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 شبکه‌های‌تبادل‌اطلاعات، داده‌پیام‌های شخصی کاربران خود را هر ۳۰ روز یکبار به روز رسانی نمایند. هرچند در ماده ۱۷ مقررات فوق‌الذکر تاکید شده که یکی از حقوق‌اشخاص موضوع‌داده، حق اصلاح یا حذف (پاک کردن) اطلاعات می‌باشد، اما وجود این حق نافی وظیفه مدیران شبکه‌های‌تبادل‌اطلاعات یا هر سازمانی که اطلاعات نزد وی باشد، بر به روزرسانی اطلاعات‌شخصی دردسترس نخواهد بود. به عنوان مثال درصورتیکه اطلاعات‌شخصی 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,۲۰۲۳)

البته نکته‌ای که باید بدان توجه گردد اینست که بنظر می‌رسد به روزرسانی اطلاعات اگرچه به عنوان یک اصل مورد پذیرش قرارگرفته، 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 تلقی‌گردد. 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 براین‌مبنا 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 ازجمله ضرورت و در حد کفایت صورت پذیرد. نکته آخر اینست که به روز نمودن اطلاعات‌شخصی 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 روز رسانی 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 قانون‌تجارت‌الکترونیکی مقررمی‌دارد: درصورت 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 دراین ماده قانونی پرده برداشته شده، حذف اطلاعات نادرست از سامانه سازمان‌ها می‌باشد که می‌توان با توجه به صدر این ماده که بیان‌داشته «درصورت رضایت موضوع‌داده...»، وظیفه تصحیح و به روزرسانی را جزو وظایف مدیران شبکه‌های‌تبادل‌اطلاعات درنظرگرفت. به عبارت دیگر وجود عبارت «درصورت رضایت موضوع‌داده» گواه براین موضوع است که شخصی از موضوع‌داده درخواستی داشته و موضوع‌داده نسبت‌به اعلام‌رضایت اقدام نموده‌است. بنابراین درصورتیکه اطلاعات صحیح در سامانه مراجع ذیربط ثبت نشده یا اطلاعات موجود به روز نباشند، درصورت جمع شرایط مسئولیت کیفری، می‌توان برای افراد مسئول، مسئولیت کیفری بر اساس ماده ۷۰ قانون‌تجارت‌الکترونیکی درنظرگرفت. این موضوع درخصوص 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 بیان‌داشت که با توجه به اینکه قانونگذارایران دراین ماده معیار مشخصی را برای به روزرسانی اطلاعات درنظرنگرفته و در کنار آن، به روزرسانی اطلاعات امری مهم می‌باشد، انجام این امر در نظام‌حقوقی‌ایران را باید فوری قلمداد کرد. پس حتی درصورتیکه نیاز به بروزرسانی اطلاعات یک شخص بصورت چند باره در یک روز وجود داشته‌باشد، سازمان مجری باید نسبت‌به این مهم اقدام‌نماید.

برآمد

شبکه‌های تبادل اطلاعات از کامپیوترهای به هم متصل که مبادرت به تبادل داده‌پیام‌های الکترونیکی با یکدیگر می نمایند، تشکیل شده اند. این شبکه ها می توانند در محدوده اتصال چند کامپیوتر درون یک فروشگاه عرضه و فروش محصولات تا شبکه های راه اندازی شده در سازمان های دولتی و غیردولتی و حتی در مقیاس جهانی، اینترنت را شامل شوند. خصیصه اصلی عملکرد کامپیوتر ها دراین نوع شبکه ها، انجام فرایندپردازش‌اطلاعات 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 شبکه ها و اطلاعات آنها و نهایتا کل شبکه گردد. ازاین‌رو نظام‌حقوقی کشورها با سیاستگذاری های تقنینی مبادرت به تصویب مقرراتی دراین زمینه نموده اند.

مقررات عمومی حفاظت‌ازاطلاعات اتحایه اروپا مصوب ۲۰۱۶، جدیدترین قانونی است که نظام‌حقوقی‌اتحادیه‌اروپا در راستای حفاظت از داده‌پیام‌های‌الکترونیکی مورد تبادل در کشورهای عضو این اتحادیه به تصویب رسانده است. این قانون دربردارنده مواد مختلفی در موضوعات متفاوت می‌باشد که یکی ازاین موضوعات اصول حاکم بر پردازش‌اطلاعات خواهد بود. این اصول همانطورکه در متن این پژوهش نیز قید گردید به دو دسته کلی، اصل قانونی، منصفانه‌بودن و شفافیت پردازش‌اطلاعات و اصل محدودیت در پردازش‌اطلاعات تقسیم بندی می‌شوند.

در نظام‌حقوقی‌اتحادیه‌اروپا، پردازش‌اطلاعات در شبکه‌های‌ارتباطی برمبنای این اصول قانونی صورت پذیرفته و عدم اجرای مفاد و نتایج این اصول میتواند منجر به غیرقانونی تلقی شدن فرایندپردازش و شمول ضمانت اجراهای مقرر در بخش پنجم از مقررات فوق‌الذکر گردد. اما در نظام‌حقوقی‌ایران، مقرراتی وجود ندارند که به صراحت به مفاد این اصول اشاره نمایند و آنچه از بررسی مقررات قابل برداشت

می‌باشد، وجود مصادیقی پرداکنده از اجزا یا نتایج اصول بیان شده در فوق می‌باشد که در مقرراتی مانند ماده ۵۹ قانون‌تجارت‌الکترونیکی به تصویب رسیده است. آنچه اهمیت دارد، اصلاح مقررات حاکم بر نظام‌حقوقی‌ایران می‌باشد. چرا که شرایط موجود در ماده ۵۹ درخصوص داده‌پیام‌هایی اعمال می‌شوند که در ماده ۵۸ این قانون مورد تصریح قرارگرفته اند. اما متن ماده ۵۸ به گونه ای تنظیم شده است که پردازشِ داده هایِ مبین ریشه های قومی، نژادی، عقیدتی، مذهبی، اخلاقی و داده هایِ مربوط به وضعیت جسمی و روانی و جنسی اشخاص را منوط‌به شرایط مقرر دراین ماده و ماده ۵۹ نموده و نص ماده گویای تفکیک میان این گروه از داده ها و دیگر داده های شخصی می‌باشد. به عبارت دیگر قانونگذارایران در اقدامی نسنجیده، علیرغم تعریفی مشخص از داده‌پیام‌شخصی در ماده ۲، در ماده ۵۸ مبادرت به تفکیک داده‌پیام‌های‌شخصی به دودسته نموده که دسته های مشخص در ماده ۵۸ باید الزاما با اخذ رضایت موضوع‌داده و دسته های غیرمصرح می توانند بدون‌رضایت موضوع‌داده پردازش و شامل شرایط ماده ۵۹ نشوند. اگرچه بنظر نگارندگان این موضوع ناشی از مسامحه قانونگذار بوده و وی پردازش انواع داده های شخصی را در متن این ماده مدنظر داشته و امکان الغای خصوصیت از مصادیق مذکور را به خواننده اعطا می نماید، اما نص مبهم ماده مذکور و البته نبود مقرره ای در زمینه کیفیت جمع‌آوری‌اطلاعات، ضرورت اصلاح این مقررات و توجه به‌انواع داده‌پیام‌های‌شخصی و اختصاص فصولی ازاین قانون به اصول پردازش‌اطلاعات را ایجاب می کند.

بعلاوه اجرای این اصول منوط‌به نظارت بر عملکرد اشخاص فعال در زمینه پردازش‌اطلاعات می‌باشد. امری که در حال حاضر به جهت نبود هرگونه سازمان ناظر یا اعطا کننده مجوز و عدم پیش‌بینی شرایط اخذ مجوز و فعالیت این اشخاص، در کشور ایران انجام نمی گیرد. براین‌مبنا لازم است وزارت صمت ابتدائا مبادرت به تعیین سازوکار اخذ مجوز فعالیت شرکت ها و نظارت این سازمان بر فعالیت های آنها در حوزه

پردازش‌اطلاعات نموده و ثانیا شبکه‌های‌تبادل‌اطلاعات‌ی که همگان امکان دسترسی به‌آنها را دارند به نحوی تحت رصد قرار دهد که خارج از چارچوب قانونی مبادرت به جمع‌آوری، نگهداری، تحلیل و سایر مصادیق پردازش‌اطلاعات ننمایند.

توصیه آخر دراین زمینه ضرورت آگاهی بخشی به مردم می‌باشد تا با اطلاع از قوانین و مقررات اولا نسبت‌به اجرای حقوق قانونی خود اقدام و درصورت مشاهده مصادیق نقض مقررات، مبادرت به گزارش امر به مراجع ذیربط نمایند. این اقدام باید در وسایل ارتباط جمعی مانند تلویزیون با ایجاد برنامه های آموزشی صورت گیرد. بعلاوه ملزم نمودن مدیران شبکه‌های‌ارتباطی‌که مبادرت به پردازش‌اطلاعات می نمایند، خصوصا سایت های عرضه و فروش محصولات، به ایجاد آیکن های پیش فرض که دربردارنده حقوق موضوع‌داده و الزامات قانونی پردازش‌اطلاعات بوده و به هنگام ورود کاربر پیش‌از نمایش اطلاعات شبکه، در کادری مجزا مبادرت به اعلام این مراتب به کاربر نموده و با پذیرش کاربر با زدن دکمه هایی مانند «مطلع شدم» و مشابه‌آن، نسبت‌به نمایش اطلاعات شبکه اقدام می نمایند، راهکاری مناسب در افزایش آگاهی بخشی به مردم تلقی می‌گردد.

منابع

الف: فارسی

انصاری، باقر، عطار، شیما،(۱۳۹۲)، ***حریم خصوصی در شبکه های اجتماعی مجازی***، دوفصلنامه پژوهش های حقوقی، دوره ۲۳، شماره۱، صص ۱۱۳-۱۳۷

جلالی محمد، کامیاب، میثا،(۱۳۹۷)،***مقدمه‌ای بر شناخت مفهوم پلیس‌اداری 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 اتحادیه‌اروپا و امکان سنجی آن در نظام‌حقوقی‌ایران***، 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***، دوفصلنامهٔ حقوق قراردادها و فناوریهای نوین، دوره ۱، شماره ۱، صص ۲۹۷-۳۳۲

لاریجانی، مریم،(۱۳۸۷)***نظریه لاک: رضایت یا قرارداد***، فصلنامه پژوهش‌های فلسفی-کلامی، دوره ۹، شماره ۴، صص ۱۴۷-۱۷۸

لطیف زاده، مهدیه، قبولی درافشان، سید محمد مهدی، محسنی، سعید،(۱۴۰۱) ***تبیین اسباب مشروعیت پردازش‌داده‌های‌شخصی از منظر حقوق اتحادیه‌اروپا و ایران***، فصلنامه مطالعات حقوقی، صص ۳۳۵-۳۶۴

محقق داماد، سید مصطفی،(۱۳۸٤)***قواعد فقه، بخش مدنی***، چاپ دوازدهم، مرکز نشر علوم اسلامی

نجفی، محمد حسن،(۱٤۲۱)، ***جواهرالکلام***، جلد سیزدهم، موسسه دارالمعارف

فقه اسلامی بر مذهب اهل بیت

هاشمی شاهرودی، محمود،(۱٤۳۲) ***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 sonrai 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