جستاری در ماهیت‌شناسی داده‌های خصوصی در سازوکار عملکرد ابزارهای فناوری اینترنت‌اشیاء

حسین صادقی[*]
دانشگاه تهران، تهران، ایران
hosadeghi@ut.ac.ir

مهدی ناصر[**]
دانشگاه علوم قضایی، تهران، ایران
Mn.ujsasac0077@yahoo.com

تاریخ دریافت: ۱۳۹۹/۰۳/۱۷
تاریخ اصلاحات: ۱۳۹۹/۰۷/۱۰
تاریخ پذیرش: ۱۳۹۹/۰۸/۲۴

چکیده

ابداع فناوری اینترنت‌اشیاء و به‌کارگیری آن منجر به توسعه صنعت و تجارت کشورها شده است. ابزارهای دربردارنده فناوری اینترنت‌اشیاء، ابزارهایی هستند که در آنها با تعبیه محرک‌ها و سنسورهای متعدد، امکان شبیه‌سازی عملکرد انسان توسط ابزار فراهم می‌گردد. اما سازوکار عملکرد این ابزارها واجد چالش‌هایی در زمینه حفظ امنیت اطلاعات خصوصی اشخاص می‌باشد. اولین مسأله در این زمینه ضرورت ماهیت‌شناسی و تفکیک داده‌های خصوصی از نوع غیرخصوصی است. در نظام حقوقی ایران تنها سند قانونی موجود در این زمینه ماده ۵۸ قانون تجارت الکترونیکی می‌باشد که نص مبهم این ماده شناسایی این نوع داده‌ها را با چالش مواجه نموده است. در ماده مذکور به دلیلی نامشخص با تفکیک میان انواع داده‌های خصوصی، نه تنها ماهیت‌شناسی این داده‌ها خلل ایجاد نموده است بلکه تنها دسته خاصی از این داده‌ها را مشمول شرایط ماده برای پردازش نموده و درخصوص دیگر انواع داده‌ها حکمی مقرر ننموده است. این درحالی است که در اتحادیه اروپا مقررات نسبتاً جامعی در این زمینه وجود دارد که در زمینه شناسایی ماهیت داده‌های خصوصی، چهار معیار شناسایی براساس ماهیت داده‌های مورد پردازش، اهداف استفاده از داده‌های مورد پردازش، مفهوم داده‌های نام مستعار و اطلاعات رمزنگاری‌شده مورد تبادل در بسترهای نامتمرکز (از جمله فناوری بلاک‌چین) به‌عنوان معیار تشخیص این نوع داده‌ها معین شده است. بکارگیری این معیارها توسط سیاست‌گذاران کشور ایران می‌تواند راهگشای بسیاری از چالش‌های پیش‌رو باشد.

واژگان کلیدی

داده‌های خصوصی؛ فناوری اینترنت‌اشیاء؛ پردازش؛ فناوری بلاک‌چین؛ معیارهای شناسایی؛ حقوق اتحادیه اروپا.

۱- مقدمه

داده‌های خصوصی و سازوکار حفاظت از این نوع اطلاعات همواره یکی از مسائل چالش برانگیز در حوزه بین‌الملل بوده است. در سال‌های اخیر با ابداع فناوری اینترنت‌اشیاء و به‌وجودآمدن ابزارهای دربردارنده این فناوری، ضرورت سیاستگذاری‌های تقنینی جهت تحلیل ابعاد حقوقی این موضوع بیش از پیش جلوه می‌نماید. اینترنت‌اشیاء فناوری ارتباط میان ابزارهای الکترونیکی با یکدیگر یا عامل انسانی جهت انجام وظایف محوله می‌باشد. ابزارهای دربردارنده این فناوری واجد سنسورها و محرک‌های متعددی می‌باشند تا با جمع‌آوری اطلاعات از محیط پیرامون و پردازش آنها توسط پردازنده ابزار، مبادرت به انجام وظایف محوله نمایند. اطلاعات جمع‌آوری‌شده توسط این ابزارها، شامل انواع داده‌ها از جمله داده‌های خصوصی اشخاص می‌گردد. چگونگی حفاظت از داده‌های خصوصی در این سازوکار از جمله مسائل مهم در اتحادیه اروپا بوده است.

اتحادیه اروپا یکی از نظامات پیشرو در جهت سیاست‌گذاری‌های تقنینی در این زمینه تلقی می‌گردد. تاریخچه طرح این موضوع و تلاش برای رفع آن به سال ۱۹۸۱ باز می‌گردد. در سال ۱۹۸۱ به دنبال پیدایش مسأله تبادل داده‌های خصوصی اروپاییان در میان کشورهای عضو اتحادیه پیش‌نویس دستورالعمل‌های حفظ حریم خصوصی اروپاییان[1] مورد تصویب سران اتحادیه قرار گرفت. اما عدم پاسخگویی دستورالعمل مذکور به مسائل حادث در دهه ۱۹۹۰ از جمله مبادلات فرامرزی داده‌های خصوصی و ایجاد مسائل مستحدث مرتبط با بسترهای متمرکز[2] مانند صفحه گسترده جهانی[3] منجر به تصویب دستورالعمل پارلمان اروپا در حفاظت از اشخاص در سازوکار پردازش اطلاعات خصوصی و آزادی تبادل آنها در

1. OECD Privacy Directive
2. Centralized Ledgers
3. World Wide Web

[*] نویسنده مسئول- دانشیار گروه کسب و کار، دانشکده کارآفرینی دانشگاه تهران، تهران، ایران
[**] دانشجوی دکترای حقوق خصوصی دانشگاه علوم قضایی، تهران، ایران

سال ۱۹۹۵ شد.[1] اما مسائلی از قبیل کیفیت شناسایی داده‌های خصوصی از یک طرف و پیدایش بسترهای نامتمرکز[2] مانند بلاک‌چین[3] و ابداع ابزارهای اینترنت‌اشیاء، بازنگری مقررات را در دستورکار سیاست‌گذاران قرار داد. آیین‌نامه عمومی حفاظت از داده‌های خصوصی[4] مصوب ۲۰۱۶، مقررات جدیدی است که پس از دو سال مذاکره درخصوص کم و کیف مفاد آن، در ماه می سال ۲۰۱۸ به مرحله اجرایی درآمده است.

در نظام حقوقی ایران نیز تنها سند قانونی در زمینه پیش‌بینی مقررات حفاظت از اطلاعات خصوصی قانون تجارت الکترونیکی مصوب ۱۳۸۲ می‌باشد. مواد ۵۸ و ۵۹ این قانون در بردارنده مقرراتی در زمینه کیفیت پردازش داده‌های خصوصی اشخاص هستند. علی‌رغم وجود این دو ماده، نه در این قانون و نه در قوانین دیگر مصوب مجلس هیچ مقرره دیگری در زمینه مفهوم‌شناسی متغیرهای مورد بحث یا دیگر احکام مرتبط با این سازوکار وجود ندارد. این امر منجر به متروک‌شدن مقررات این دو ماده و عدم شناسایی دقیق کاربرد عملی صحیح این دو ماده توسط پژوهشگران شده است. یکی از ابهاماتی که نظام حقوقی ایران در مسأله پردازش داده‌های خصوصی با آن مواجه است، مسأله شناسایی مفهوم و انوع داده‌های خصوصی می‌باشد. اهمیت این موضوع به شکلی است که شناسایی انواع داده‌های خصوصی به منزله مقدمه پردازش این اطلاعات و شمول مقررات مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی بر آنها می‌باشد. از آنجا که در نظام حقوقی ایران این مسأله با ابهام مواجه است، تدبر در مقررات مصوب اتحادیه اروپا می‌تواند راهکارهای مفیدی در این زمینه پیش‌روی پژوهشگران قرار داده تا با تبیین سازوکارهای شناسایی این نوع داده‌ها و تحلیل آنها در نظام حقوقی ایران، گام‌هایی در جهت بهبود روند سیاست‌گذاری تقنینی در این زمینه برداشته شود.

سؤال اصلی که پژوهش حاضر به دنبال پاسخگویی به آن می‌باشد این است که ابهامات موجود در نظام حقوقی ایران در مواجهه با تشخیص ماهیت داده‌های خصوصی چه بوده و چه معیارهایی در حقوق اتحادیه اروپا در زمینه شناسایی داده‌های خصوصی اشخاص در سازوکار پردازش اطلاعات آنها وجود دارد؟ فرضیه تحقیق ابهام موجود در ماده ۵۸ قانون تجارت الکترونیکی ایران و وجود چهار معیار کلی شناسایی داده‌های خصوصی براساس ماهیت داده‌ها، براساس اهداف استفاده از داده‌ها، براساس ماهیت داده‌های نام مستعار و براساس بستر تبادل داده‌ها در حقوق اتحادیه اروپا می‌باشد. برای پاسخگویی به سؤال فوق، پژوهش حاضر با نگاهی تحلیلی به مقررات مصوب اتحادیه اروپا از جمله آیین‌نامه مصوب ۲۰۱۶، تبیین معیارهای مذکور در این آیین‌نامه و تحلیل آنها مبادرت به رفع این مسأله نموده است.

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
2. Decentralized Ledgers
3. Blockchain
4. General Data Protection Regulation (GDPR)

۲- چارچوب نظری و مبانی پژوهش

داده‌های خصوصی از جمله اطلاعاتی هستند که حفاظت از آنها به‌عنوان یکی از مهم‌ترین مسائل عصر جدید در حوزه تجارت الکترونیکی تلقی می‌گردد. این موضوع مسائلی مانند اسرار تجاری تجار را تحت شمول خود قرار داده است. این امر موجب شده است تا موادی از قانون تجارت الکترونیکی مصوب ۱۳۸۲ به این مبحث اختصاص پیدا نماید. مسأله مفهوم‌شناسی و بیان قمرو شمول داده‌های خصوصی در اتحادیه اروپا از اهمیت وافری برخوردار بوده است به‌طوری‌که در مقررات عدیده‌ای به بیان دقیق معنای این عبارت پرداخته شده است. اگرچه در حال حاضر آیین‌نامه عمومی حفاظت از اطلاعات اتحادیه اروپا به‌عنوان قانون مبنا در شناسایی داده‌های خصوصی در اتحادیه اروپا شناخته می‌شود، اما مقررات دیگری از جمله بند الف از ماده ۲ دستورالعمل حفاظت از اطلاعات و حتی مقررات داخلی کشورهای عضو اتحادیه اروپا از جمله ماده ۱ قانون حفاظت از اطلاعات انگلستان نیز به صورت دقیق به این مفهوم اشاره نموده‌اند [۲].

براساس مفاد ماده ۲ دستورالعمل حفاظت از اطلاعات، داده‌های شخصی به هرگونه اطلاعات مربوط به شخص حقیقی شناخته شده یا قابل شناسایی که اصطلاحاً موضوع داده نامیده می‌شوند، اطلاق می‌گردد. فرد قابل شناسایی شخصی است که با بررسی شماره شناسایی یا عوامل زیستی منتسب به اشخاص از جمله خصوصیات هویت جسمی، فیزیولوژیکی، روحی، مبادلات اقتصادی یا رفتارهای فرهنگی یا اجتماعی به‌طور مستقیم یا غیرمستقیم شناسایی گردد.[5]

براساس بند اول از ماده ۱ قانون حفاظت از اطلاعات انگلستان نیز داده‌های شخصی به هرگونه اطلاعات مربوط به یک فرد زنده که از قابلیت شناسایی برخوردار باشد اطلاق می‌گردد، به گونه‌ای که:

الف: از آن داده‌ها

ب: یا هر داده‌ای که کنترل‌کننده در اختیار نهاد شناسایی‌کننده قرار داده یا خود موضوع داده پیشتر مبادرت به ارائه آن اطلاعات به نهاد مذکور نموده است، شامل هرگونه اطلاعاتی که در تطبیق آنها با یک فرد و تمیز آن از افراد دیگر به‌کار گرفته شود، موضوع داده قابل شناسایی باشد.[6]

مفاد مواد مرقوم به صورت کلی خصوصیات داده‌های شخصی را در شناسایی موضوع داده قرار داده است. به نظر می‌رسد تعیین این مصداق از اطلاعات نمی‌تواند راهکار مناسبی در شناسایی داده‌های خصوصی باشد.

5. Article 2(a) Data Protection Directive
Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
6. Section 1(1) Data Protection Act Data which relate to a living individual who can be identified— (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

چرا که حتی در مواردی مقایسه رنگ موی میان دو نفر می‌تواند معیاری در تشخیص آن دو از یکدیگر باشد. به همین جهت نمی‌توان معیار بیان شده در این ماده قانونی را به‌عنوان معیاری قابل اطمینان در شناسایی داده‌های مذکور و تمایز آنها از داده‌های غیرخصوصی تلقی نمود [۳].

از دیگر مبانی تعیین معیارهای شناسایی داده‌های خصوصی می‌تواند به ضرورت طرح این موضوع در ارتباط با سازوکار عملکرد نهادهای دولتی و غیردولتی اشاره نمود. در ارگان‌های دولتی و خصوصی به‌کارگیری هر کدام از نیروها نیازمند دسترسی به اطلاعات آنها سوی دیگر کارمندان و پرسنل اداره است. دسته‌بندی این نوع اطلاعات و تشخیص محرمانگی آنها نیز نیازمند تعیین دقیق معیارهای شناسایی داده‌های خصوصی می‌باشد. علاوه بر آن توسعه فناوری اطلاعات و ایجاد ابزارهایی مانند اینترنت‌اشیاء که در راستای انجام وظایف از پیش تعیین‌شده نیازمند جمع‌آوری اطلاعات از محیط پیرامون خود هستند نیز ضرورت تعیین معیارهایی جهت تمایز میان داده‌های خصوصی و غیرخصوصی و تعیین درجه و کیفیت دسترسی این ابزارهای و کنترل‌کنندگان آنها به این اطلاعات را ضرورت می‌بخشد که در پژوهش حاضر نیز به تفصیل به این موضوع پرداخته شده است.

۳- بیان مسأله

کارکردهای فراوان ابزارهای اینترنت‌اشیاء در بخش‌های مختلف صنعت و تجارت ضرورت اهتمام بر تصویب قوانین کارآمد در راستای پیش‌بینی ابعاد مختلف حقوقی مسائل حوزه سازوکار عملکرد این ابزارها را تحکم می‌بخشد. در این سازوکار کنترل‌کنندگان ابزار و پردازندگان اطلاعات دارای نقشی غیرقابل انکار می‌باشند. کنترل‌کننده‌های ابزارهای اینترنت‌اشیاء، طراحان و تولیدکنندگان آنها می‌باشند که وظیفه نظارت بر عملکرد ابزار را بر عهده دارند. علاوه بر آن اطلاعات جمع‌آوری‌شده توسط ابزار، در قالب ابرداده به این اشخاص ارسال و آنها وظیفه ارسال اطلاعات به شرکت‌های پردازنده اطلاعات را بر عهده دارند. پردازندگان اطلاعات نیز شرکت‌هایی جهت پردازش اطلاعات ارسالی از سوی کنترل‌کننده و باز ارسال آن می‌باشند. مسأله موجود ضرورت حفاظت از اطلاعات در این فرایند است. گاه به جهت آنکه کنترل‌کننده یا پردازنده دارای تابعیت کشوری غیر از کشور متبوع دارنده اطلاعات می‌باشد، دسترسی این اشخاص به اطلاعات خصوصی دارنده، می‌تواند زمینه سوءاستفاده از آنها را فراهم آورد. دسترسی اشخاص غیرمجاز به اطلاعات خصوصی اتباع یک کشور می‌تواند منجر به ورود خسارات جبران‌ناپذیری از جمله ساخت سلاح‌های بیومتریک یا بیولوژیک گردد.

بر همین اساس نیز تصویب مقررات جامع در جهت چگونگی پردازش اطلاعات خصوصی و جهت‌دهی بر فعالیت اشخاص دخیل در این پروسه، امری ضروری می‌باشد که متأسفانه در حقوق ایران نه قانون جامعی در این زمینه تصویب شده است و به جهت ابهامات موجود در تفسیر مقررات مصوب نیز امکان اجرای مناسب آنها فراهم نیست. لذا انجام پژوهش‌های تحلیلی با محوریت حقوق غرب و بیان تجربیات یا تبیین مفاد مقررات مصوب کشورهای توسعه‌یافته در جهت رفع خلاءهای قانونی موجود در نظام حقوقی ایران می‌تواند راهگشای بسیاری از مسائل موجود در این زمینه باشد. در حقوق ایران، آنچه از تدبر در مقررات مصوب مشاهده می‌گردد، این است که ماده ۵۸ قانون تجارت الکترونیکی در زمینه مفهوم‌شناسی داده‌های خصوصی تنها با بیان مصادیقی، به صورت گذرا سعی در شناسایی این اطلاعات به خوانندگان داشته است. اما محوریت موضوع و اهمیت آن در حوزه تجارت الکترونیکی ضرورت تحلیل موشکافانه این موضوع و ارائه معیارهایی جهت شناسایی این اطلاعات را ضرورت می‌بخشد.

۴- ضرورت انجام پژوهش

اولین بحث در زمینه پردازش اطلاعات خصوصی، شناسایی این اطلاعات است. این در حالی است که تنها مقرره مصوب در نظام حقوقی ایران به صورتی کاملاً مبهم و چند پهلو تبیین مصادیق این اطلاعات را در دستور کار خود قرار داده است.

ماده ۵۸ قانون تجارت الکترونیکی مقرر می‌دارد: «ذخیره، پردازش و یا توزیع داده پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است.»

در نگاه اول نص ماده قانونی مزبور این امر را به ذهن القاء می‌نماید که تنها پردازش آن دسته از اطلاعات خصوصی اشخاص که در متن ماده بیان شده است نیازمند اخذ رضایت صریح دارنده اطلاعات بوده و سایر اطلاعات شخصی وی قابلیت هرگونه پردازش بدون هر محدودیتی را دارا می‌باشند. چنین مقرره‌ای به این کیفیت نه تنها هیچ مشکلی از نظام حقوقی ایران را حل و فصل نمی‌نماید، بلکه چند پهلوبودن مفاد ماده بر ابهامات موجود در این زمینه و فلسفه تصویب آن بیش از پیش دامن می‌زند. به عبارت دیگر فلسفه تصویب مقررات حوزه حفاظت از اطلاعات، پردازش تمامی انواع داده‌های خصوصی طی قیود بخصوص می‌باشد. از این‌رو تفکیک میان این نوع اطلاعات نمی‌تواند اهداف حاصل از تصویب این نوع مقررات را محقق نماید. اگر اطلاعات خصوصی اشخاص، داده‌هایی واجد ارزش تلقی می‌شوند که ماده ۵۹ قانون تجارت الکترونیکی[1]، علاوه بر مفاده ماده ۵۸، شرایط خاص دیگری را

---

۱ ماده ۵۹ - درصورت رضایت شخص موضوع «داده پیام» نیز به شرط آنکه محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع «داده پیام»های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:

الف - اهداف آن مشخص بوده و به‌طور واضح شرح داده شده باشند.

ب - «داده پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام‌جمع‌آوری برای شخص موضوع «داده پیام» شرح داده شده جمع‌آوری گردد و تنها برای‌اهداف تعیین شده مورد استفاده قرار گیرد.

ج - «داده پیام» باید صحیح و روزآمد باشد.

د - شخص موضوع «داده پیام» باید به پرونده‌های رایانه‌ای حاوی «داده پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده پیام»های ناقص و یا نادرست رامحو یا اصلاح کند.

هـ - شخص موضوع «داده پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه‌ای «داده پیام»های شخصی مربوط به خود را بنماید.

نیز برای پردازش آنها پیش‌بینی نموده است، چرا در نص ماده تنها دسته‌ای از اطلاعات خصوصی اشخاص در شمول این مقررات قرار گرفته‌اند.

مشکل دیگر این است که معیار دقیق شناسایی یک داده شخصی چه می‌باشد که بتوان در محدوده موضوعی این ماده مصادیق مورد شمول یا غیرقابل شمول ماده ۵۸ را شناسایی نمود. صرف‌نظر از آنکه حقیقتاً قصد سیاست‌گذاران از تصویب این ماده احصا یا بیان مصادیق داده‌های خصوصی بوده و در تألیف متن آن اشتباهات نگارشی منجر به تصویب ماده‌ای قانونی با متنی مبهم شده است که در زمینه پردازش اطلاعات جمع‌آوری شده در سازوکار عملکرد ابزارهای اینترنت‌اشیاء نیز تفسیر این ماده می‌تواند مشکلات فراوانی را برای دستگاه‌های اجرایی و نهادهای دخیل در این فرایند ایجاد نماید، نبود آیین‌نامه یا دستورالعمل اجرایی این ماده نیز یکی دیگر از خلاءهای قانونی نظام قانون‌گذاری ایران می‌باشد. از این‌رو تدبر در مقررات مصوب اتحادیه اروپا از جمله آیین‌نامه مصوب ۲۰۱۶ به‌عنوان جدیدترین سند قانونی مصوب در سطح بین‌الملل و مطالعه پژوهش‌های منتشره در معتبرترین پایگاه‌های علمی این قاره می‌تواند منبع مناسبی برای قانون‌گذاری صحیح در این زمینه تلقی گردد.

۵- پیشینه پژوهش

در زمینه پردازش داده‌های خصوصی و مباحث مرتبط در حقوق ایران پیشینه‌ای در مقالات منتشره در نشریات معتبر علمی مشاهده نمی‌گردد. تنها پژوهش صورت گرفته در این زمینه مقاله فرحزادی و ناصر منتشره در سال ۱۳۹۸ می‌باشد. نویسندگان مقاله مذکور با تحلیل سازوکار جبران جمعی خسارات ناشی از نقض قواعد حفاظت از داده‌های خصوصی در اتحادیه اروپا به‌عنوان مکانیسمی در زمینه کیفیت جبران خسارات وارده به اشخاص در این پروسه، بر ضرورت پیاده‌سازی این سازوکار در حقوق ایران تأکید نموده‌اند [۱].

اما در سطح بین‌الملل مقالاتی در حوزه‌های مرتبط با این موضوع در نشریات تخصصی حوزه حقوق فناوری به چاپ رسیده‌اند. ارگارد و لاگ در مقاله منتشره در سال ۲۰۱۹ پس از بیان کلیاتی درخصوص مقررات مصوب ۲۰۱۶ اتحادیه اروپا، محوریت بحث مقاله مزبور را بر سازوکار مسئولیت‌پذیری نهادهای فعال در فرایند پردازش اطلاعات قرار داده است [۴]. علاوه بر آن وانگر در مقاله منتشره در سال ۲۰۱۹ با بیان ضرورت اخذ تضامین مالی از شرکت‌های فراملی پردازنده اطلاعات مبادرت به ارائه پیشنهاداتی در جهت جلوگیری از سوءاستفاده از داده‌های در دسترس و وجود امکان جبران خسارات وارده ناشی از اعمال پردازندگان اقدام نموده است [۵].

فینک و پالاس نیز در مقاله منتشره در سال ۲۰۲۰ بهبود نظارت بر عملکرد ابزارهای اینترنت‌اشیاء را منوط به ایجاد سیاستگذاری‌های تقنینی مبنی بر مشخص‌نمودن تمایز میان اطلاعات شخصی و غیرشخصی دارنده اطلاعات نموده و عدم وجود مشخصه واحد در حال حاضر را به‌عنوان یکی از دلایل عدم اجرای صحیح مقررات مصوب ۲۰۱۶ تلقی کرده است [۶]. مضاف بر آن رینگاک و ون ایجک در مقاله منتشره در سال ۲۰۱۹ با اشاره خطرات سوءاستفاده از اطلاعات شخصی افراد، ضرورت پیش‌بینی مراجعی جهت نظارت بر عملکرد نهادهای فعال در این زمینه را که دارای تابعیت کشوری خارج از اتحادیه اروپا باشند نیز بیان نموده است [۷] و نهایتاً آلتمان و همکاران در مقاله منتشره در سال ۲۰۱۸ با اشاره به نقش و ابعاد حقوقی حاکم بر تبادل ابرداده‌ها در سازوکار عملکرد ابزارهای اینترنت‌اشیاء، مبادرت به ارائه مدلی با به‌کارگیری بسترهای نامتمرکز در تأمین امنیت این داده‌ها در فرایند تبادل اقدام نموده است [۸].

تدبر در مقالات منتشره فوق‌الذکر نشان می‌دهد که اهمیت حوزه حقوق حاکم بر پردازش داده‌های خصوصی در اتحادیه اروپا منجر به انجام تحقیقات متعددی در ابعاد مختلف حقوقی مرتبط با این حوزه شده است. مسأله‌ای که در جامعه علمی ایران در میان پژوهشگران امری بسیار نادر بوده و تاکنون تنها پژوهش مستقلی که در این زمینه منتشر شده است مقاله منتشره در فصلنامه حقوق خصوصی می‌باشد که تدبر در متن این پژوهش نشان می‌دهد که نویسندگان هیچ‌گونه ورودی به مباحث مفهوم‌شناسی داده‌های خصوصی و ارائه معیارهای شناسایی این داده‌ها از نوع غیرخصوصی آن ارائه ننموده و با تألیف پژوهشی شکلی، بر تبیین جایگاه سازوکار جبران جمعی خسارات تأکید نموده‌اند. لذا پژوهش حاضر در محدوده موضوعی خود یک تحقیق کاملاً نوین در جامعه علمی ایران تلقی می‌گردد.

۶- روش‌شناسی پژوهش

مقاله حاضر، پژوهشی با روش تحقیق کیفی می‌باشد که روش جمع‌آوری اطلاعات آن از منابع اسنادی موجود در پایگاه داده‌های Heinonline, Springer, Elsevier, Oxford Journals و تقریرات منتشره در سایت‌های معتبر خارجی استخراج شده است.

قلمرو مکانی مقاله حاضر منحصر به نظام حقوقی اتحادیه اروپا و مقالات منتشره در مجلات معتبر این اتحادیه بوده و بر مقالات منتشره در نشریات معتبر خارجی نیز نگاهی صورت گرفته است.

از نظر قلمرو زمانی نیز محدودیتی میان مطالب این پژوهش متصور نیست. اما عمده مطالب مورد تحلیل از نوین‌ترین مقالات منتشره در پایگاه‌های فوق‌الذکر در سال ۲۰۱۹-۲۰۲۰ استخراج و اسناد قانونی مصوب مورد تشریح نیز مقررات آیین‌نامه عمومی حفاظت از داده‌های خصوصی اتحادیه اروپا مصوب ۲۰۱۶ می‌باشد.

۷- تعریف متغیرهای پژوهش

آنچه در پژوهش حاضر به‌عنوان متغیر ضرورت تعریف دارد، عنوان «داده‌های خصوصی» اشخاص و فناوری «اینترنت‌اشیاء» می‌باشد. همانطور که بیان شد در نظام حقوقی ایران تعریف مشخصی از این اصطلاح وجود نداشته و قانون‌گذار تنها با ارائه برخی مصادیق این مفهوم مبادرت به پیش‌بینی شرایط پردازش این اطلاعات نموده است. این در حالی است که نظام حقوقی اتحادیه اروپا در ماده۴ مقرره جدیدالتصویب خود در سال ۲۰۱۶ به تعریف این مفهوم پرداخته است.

ماده ۴ آیین‌نامه عمومی حفاظت از اطلاعات خصوصی اتحادیه اروپا مقرر می‌دارد: «اطلاعات خصوصی به هرگونه اطلاعاتی که به صورت مستقیم یا غیرمستقیم امکان شناسایی وی را فراهم آورد اطلاق می‌گردد. این داده‌ها می‌توانند انواع داده‌های شناسایی مانند نام و شماره شناسنامه، یا داده‌های مکانی یا شناسه‌های آنلاین برای شناسایی وضعیت هویتی فرد از جمله عوامل خاص جسمی، فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی آن شخص طبیعی باشند.»[1]

مطابق با مفاد ماده فوق داده‌های شخصی داده‌هایی هستند که در شناسایی مستقیم یا غیرمستقیم یک شخص حقیقی می‌توانند به‌کار گرفته شوند. از این‌رو اطلاعات مربوط به اشخاص حقوقی در نظام حقوقی اتحادیه اروپا جزو مجموعه داده‌های شخصی محسوب نشده و در ذیل مقررات حاکم بر این عنوان قرار نمی‌گیرند [۹]. علاوه بر آن مطابق با پاراگراف ششم از اعلامیه کارگروه ماده ۲۹ این مقررات[2] که در راستای رفع ابهامات ناشی از اجرای مقررات این آیین‌نامه مورد تصویب کمیسیون اتحادیه اروپا قرار گرفته است، در مقام تفسیر مفاد ماده ۴ آیین‌نامه، در مواجهه با نوع و کیفیت داده‌های مورد پردازش باید نهادهای فعال با ارائه تفسیرهای بسط و گسترده، در موارد وجود ابهام، هرگونه داده‌ای که شمول یا عدم شمول آن ذیل مقررات داده‌های خصوصی با اختلاف مواجه باشد را جزو داده‌های خصوصی محسوب نمایند.

علاوه بر آنچه بیان شد، داده‌های شخصی و معیارهای شناسایی این داده‌ها در نظام حقوقی اتحادیه اروپا منحصر به داده‌های مربوط به خود شخص نمی‌گردد. بلکه مطابق با مفاد پاراگراف ۳۱ از اعلامیه کارگروه ماده ۲۹ این اطلاعات صرف‌نظر از ماهیت شکلی خود از نوع داده، فیلم، تصویر، عدد و حتی صوت که قابلیت دستیابی به آنها از طریق ابزارها تحت اختیار دارنده اطلاعات از جمله گوشی تلفن‌همراه یا خودرو وجود داشته باشد نیز قابلیت قرارگیری در ذیل عنوان داده‌های خصوصی را برخوردار می‌باشند [۶].

درخصوص مفهوم‌شناسی اینترنت‌اشیاء نیز در نظام حقوقی اتحادیه اروپا تنها تعریفی که با تدبر در اسناد مصوب این اتحادیه می‌توان یافت، تعریف مقرر در ماده ۲۹ اعلامیه مرکز نظارت بر داده پیام‌های اتحادیه اروپا مصوب ۲۰۱۰ با الحاقات و اصلاحات ۲۰۱۵،[3] می‌باشد. مطابق با مفاد ماده مذکور، «اینترنت‌اشیاء، زیرساخت‌هایی می‌باشند که در آن میلیاردها حسگر تعبیه‌شده در دستگاه‌های کاربردی روزمره برای ضبط، پردازش، ذخیره و انتقال داده‌ها طراحی‌شده و همان‌طور که از قابلیت ارتباط با عامل انسانی برخوردار هستند، با بهره‌مندی از شناسه‌های منحصر به فرد، با دستگاه‌ها یا سیستم‌های دیگر با استفاده از قابلیت‌های شبکه تعامل برقرار می‌کنند» همان‌طور که در تعریف مذکور بیان شد، اینترنت‌اشیاء ابزارهایی هستند که انواع مختلف حسگرها با تعبیه بر بدنه این ابزارها امکان انجام وظایف تعیین‌شده برای آنها را فراهم می‌نمایند. این ابزارها واجد پردازنده‌ای می‌باشند که با ارائه دستورالعمل‌هایی توسط طراح آنها در راستای چگونگی بهره‌مندی از حسگرهای مذکور برنامه‌ریزی می‌شوند. این ابزارها قادر به اتصال به بسترهای متمرکز مانند صفحه گسترده جهانی و یا بسترهای نامتمرکز مانند بلاک‌چین می‌باشند. اتصال به این بسترها قابلیت ارسال داده پیام‌های جمع‌آوری‌شده از سوی آنها را به یکدیگر یا کنترل‌کنندگان آنها و دریافت داده‌های پردازش‌شده را فراهم می‌آورند.

کنترل کنندگان این ابزارها، همان‌گونه از نامشان پیداست، اشخاصی می‌باشند که وظیفه کنترل و نظارت بر عملکرد ابزارهای مذکور را بر عهده دارند. از آنجا که کنترل‌کنندگان ابزارهای اینترنت‌اشیاء، عموماً تولیدکنندگان آنها نیز می‌باشند، وظیفه ارائه خدمات پس از فروش به خریداران این ابزارها را نیز بر عهده دارند. تدبر در مفاد بند هفتم از ماده چهارم از مقررات مصوب ۲۰۱۶ اتحادیه اروپا می‌تواند تعریف قانونی ارائه‌شده از این اشخاص را ارائه دهد. ماده مذکور مقرر می‌دارد: «کنترل‌کننده شخص حقیقی یا حقوقی، مرجع عمومی، نمایندگی یا هر نهاد دیگری است که به تنهایی یا به‌طور مشترک با دیگران اهداف و وسایل پردازش داده‌های شخصی را تعیین می‌کند.» مطابق با ماده مذکور، فراهم‌آوردن مقدمات پردازش داده‌های جمع‌آوری‌شده توسط کنترل‌کنندگان ابزارهای اینترنت‌اشیاء صورت می‌پذیرد.

ابزارهای اینترنت‌اشیاء برای انجام تمامی وظایف ارائه‌شده به پردازنده خود، نیاز به جمع آوری اطلاعات از محیط پیرامون خود، ذخیره و ارسال آنها به کنترل‌کننده را دارند. این اطلاعات می‌تواند انواع داده پیام‌های الکترونیکی از جمله اطلاعات خصوصی اشخاص باشد. کنترل‌کنندگان ابزارهای مذکور نیز برای پردازش این اطلاعات به زبان ارائه‌شده به پردازنده ابزار، آنها را به شرکت‌های پردازنده اطلاعات ارسال می‌نمایند. به تعبیر بند هشتم از ماده چهارم آیین‌نامه مرقوم، پردازنده «شخصی حقیقی یا حقوقی، مقامات دولتی یا هر نهاد دیگری است که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند.» از این‌رو پردازندگان اطلاعات، تحت مکانیسم تعیین‌شده از سوی کنترل‌کننده مبادرت به پردازش اطلاعات و ارسال آن به کنترل‌کننده می‌نمایند.

مقررات مصوب ۲۰۱۶ در راستای جهت بخشی بر سازوکار عملکرد ابزارهای اینترنت‌اشیاء، علاوه بر پیش‌بینی مکانیسم‌های نظارتی بر عملکرد کنترل کنندگان و پردازندگان این ابزارها از جمله ضرورت شفافیت مکانیسم پردازش و ارائه کامل گزارش فرایند مذکور به دارنده ابزار و دولت متبوع وی

1. Article 4 (1) GDPR: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

۲- پس از لازم‌الاجراشدن آیین‌نامه مصوب ۲۰۱۶، کارگروهی تحت عنوان کارگروه ماده ۲۹ این دستورالعمل متشکل از نمایندگان کشورهای عضو اتحادیه در ۲۵ می ۲۰۱۸ تشکیل گردید. هدف اصلی این کارگروه استخراج مقررات کاربردی دستورالعمل‌ها، اعلامیه‌ها و دیگر اسناد قانونی مصوب اتحادیه و پیشنهاد آن به کمیسیون اتحادیه اروپا بود تا در صورت تصویب کمیسیون، مقدمات ابلاغ آن به کشورهای عضو و لازم‌الاجراشدن آن صورت پذیرد. (۱۰)

3. European Data Protection Supervisory

(ماده ۵) و اخذ مجوزهای لازم در فعالیت اشخاص مذکور از نهادهای صلاحیت‌دار کشور متبوع دارنده (ماده ۴۲)، مبادرت به پیش‌بینی برخی حقوق اساسی برای دارندگان این ابزارها در جهت نظارت بر نحوه جمع‌آوری اطلاعات و پردازش آنها توسط کنترل‌کنندگان و پردازندگان نموده است. از جمله این حقوق، حق رضایت صریح و دسترسی به تمامی اطلاعات در سازوکار جمع‌آوری و پردازش آنها می‌باشد. (ماده ۶) علاوه بر آن مطابق با نص صریح ماده ۱۶ این مقررات، دارنده در هر مرحله از پردازش، قادر به جلوگیری و ایجاد محدودیت در کمیت و کیفیت پردازش اطلاعات خصوصی می‌باشد. اما محقق‌شدن این حق و اجرایی‌شدن مقررات آیین‌نامه مرقوم، پس از ماهیت‌شناسی داده‌های خصوصی امکان‌پذیر می‌گردد. امری که در ادامه این پژوهش به‌عنوان یافته‌ها مورد تحلیل و بررسی قرار خواهد گرفت.

۸- یافته‌ها

در کنار تحلیل مفاد ماده ۴ آیین‌نامه فوق‌الذکر جهت مشخص‌شدن ابعاد دقیق و شاخصه‌های شناسایی داده‌های خصوصی، دستورالعمل‌ها و دیگر مقررات مصوب اتحادیه با ارائه معیارهایی چهارگانه هرگونه اطلاعاتی که در زمره هر یک معیارهای ذیل قرار گرفته باشد را به‌عنوان داده‌های شخصی محسوب نموده‌اند.

۸-۱- شناسایی براساس ماهیت داده‌های مورد پردازش

اولین معیار در شناسایی داده‌های شخصی، تشخیص این نوع داده‌ها براساس ماهیت داده مورد پردازش می‌باشد. به عبارتی گروهی از داده‌ها می‌باشند که ماهیتاً به‌عنوان داده‌های شخصی محسوب می‌شوند. از جمله این داده‌ها همانطور که در متن ماده ۴ آیین‌نامه نیز به برخی از آنها اشاره شد می‌توان به داده‌های بیومتریک اشخاص از جمله خصوصیات زیستی و شخصیتی، داده‌های شناسایی از جمله نام و مشخصات هویتی را نام برد. علاوه بر آن داده مکان‌ها یا آدرس‌های آی‌پی همراه با اطلاعات در صفحات وب بازیابی‌شده نیز در آرایی از دادگاه عالی عدالت اتحادیه اروپا از جمله پرونده پیتر نواک[1] به‌عنوان داده‌های شخصی معرفی شده‌اند.

نکته‌ای که درخصوص این نوع داده‌ها خاطر نشان می‌گردد این است که مطابق با بیانیه تفسیری شماره ۲۶ منتشره درخصوص آیین‌نامه، وجود این داده‌ها به همراه انواع دیگر داده پیام‌های مورد پردازش، درصورتی‌که امکان انفکاک داده‌ها از یکدیگر موجود نبوده و پردازنده به هر صورت ملزم به پردازش همتا به همتای اطلاعات باشد، تمامی داده‌ها صرف‌نظر از اینکه ذیل عنوان داده‌های شخصی قرار گرفته یا قرار نگرفته باشند، مشمول مقررات حاکم بر داده‌های خصوصی قرار می‌گیرند [۱۱]. این امر در سازوکار عملکرد ابزارهای اینترنت‌اشیاء جلوه بیشتری می‌یابد. همانطور که بیان شد، اطلاعات جمع‌آوری‌شده از سوی این ابزارها در قالب ابرداده‌هایی به کنترل‌کنندگان و از طریق آنها به شرکت‌های پردازنده اطلاعات ارسال می‌گردد. از آنجا که پردازش اطلاعات مربوط به هر ابزار به صورت یکجا توسط پردازنده صورت می‌پذیرد، توأمان بودن داده‌های شخصی و غیرشخصی، تمامی این اطلاعات را مشمول مقررات حاکم بر داده‌های شخصی می‌گرداند.

اما سؤال پیش‌رو این است که اگر به هر طریق ابرداده ارسال شده به پردازنده، در مسیر دریافت در بستر به هر طریق از جمله وجود بدافزارها دچار اختلال شده و داده‌های شخصی آن از داده‌های غیرشخصی جدا گردند، آیا کماکان می‌توان این مجموعه داده را در شمول مقررات حاکم بر داده‌های شخصی محسوب نمود؟ به نظر نگارندگان فلسفه ارائه چنین مقرره‌ای از سوی کمیسیون اتحادیه اروپا، رعایت حداکثری امنیت داده‌های مورد پردازش است. از این‌رو وجود خصوصیت «توأمان‌بودن» داده‌های شخصی و غیرشخصی نیز در هنگام وقوع فرایند پردازش داده باید مورد توجه قرار گیرد نه در زمان ارسال داده. به همین جهت درصورتی‌که در ابتدای وقوع فرایند پردازش، خصوصیتی از حیث توأمان‌بودن داده‌های شخصی و غیرشخصی وجود نداشته باشد، دلیلی بر شمول این نوع داده‌ها بر مقررات داده‌های شخصی وجود نخواهد داشت.

سؤال دیگری که در این زمینه می‌تواند مورد طرح قرار گیرد این است که اگر پردازنده اطلاعات در صورت وجود دستور از سوی قوای حکومتی ملزم به تقدیم داده‌های خام دریافت‌شده به آنها شده و پیش از آغاز فرایند پردازش اطلاعات برای کنترل‌کننده، ملزم به پردازش قسمتی از اطلاعات به دستور قوای حکومتی شده باشد، اگر اطلاعات مورد پردازش ماهیتاً داده‌های شخصی تلقی نگردد، آیا می‌توان مقررات حاکم بر داده‌های شخصی را بر این نوع داده‌ها اعمال نمود؟ سؤال بیان‌شده از این جهت حائز اهمیت است که اگر پردازنده اطلاعات دارای تابعیت کشوری غیر از کشور متبوع دارنده اطلاعات باشد، مطابق با ماده ۴۵ آیین‌نامه مصوب ۲۰۱۶ و پروتکل الحاقی به آن جهت پردازش اطلاعات خصوصی اروپاییان باید تضامین مالی به‌عنوان وثیقه جبران خسارات وارده به نهادهای صلاحیت‌دار کشور متبوع دارنده تقدیم نماید [۱۲].

از این‌رو اگر داده‌هایی که در سؤال فوق‌الذکر مورد پردازش واقع می‌گردند، داده‌های شخصی باشند، عدم رعایت مقررات حاکم بر داده‌های شخصی می‌تواند وثایق سپرده شده را در معرض ضبط قرار دهد. به نظر نگارندگان مورد اخیرالذکر ماهیتاً با سؤال پیشین دارای تفاوت‌هایی می‌باشد که شمول مقررات حاکم بر داده‌های شخصی را بر این نوع داده‌ها هر چند ماهیتاً داده شخصی نباشند تقویت می‌نماید. چرا که از بین رفتن بخشی از داده‌های مورد پردازش به دلایلی که مربوط به عامل انسانی نباشد ارتباطی با ضرورت پردازش قسمتی از داده‌های مورد تبادل در قالب یک ابرداده ندارد. از این‌رو هرگونه نقض عهد از سوی شرکت پردازنده، هر چند به اجبار مقامات دولتی کشور متبوع وی باشد، می‌تواند زمینه ضبط وثایق مالی وی را توسط کشور متبوع دارنده فراهم آورد. در این صورت اگر خسارتی نیز به شرکت پردازنده وارد گردد، وی ملزم به اقامه دعوی علیه دولت متبوع خویش خواهد بود.

1. Cases C-293/12 and C-594/12 Digital Rights Ireland [2016] EU:C:2016: 238

۸-۲- شناسایی براساس اهداف استفاده از داده‌های مورد پردازش

دومین مقوله در شناسایی داده‌های شخصی، اهداف پردازش این نوع داده‌ها می‌باشد. به عبارت دیگر اگر داده‌ای ماهیتاً یک داده شخصی نباشد، اما برای شناسایی موضوع داده مورد پردازش واقع گردد، براساس مفاد پاراگراف ۱۶ از اعلامیه کارگروه ماده ۲۹ آیین‌نامه، داده‌های مذکور زیرمجموعه داده‌های شخصی قلمداد می‌شوند. این نوع داده‌ها معمولاً در پردازش اطلاعات اشخاصی مورد نظر قرار می‌گیرند، که اطلاعات کثیری از آنها در اختیار پایگاه‌های داده قرار گرفته باشد. به‌عنوان مثال می‌توان به شرکت‌های گوگل، یاهو، فیس‌بوک و ... اشاره نمود که اطلاعات بی‌شماری از دارندگان پست‌های الکترونیکی در اختیار این شرکت‌ها قرار دارد که در صورت پردازش داده‌های اشخاص به هر قصد و نیتی می‌توانند، اطلاعات بسیار دقیقی از خصوصیات شخصیتی آنها را به‌دست آورند [۱۳].

علاوه بر آن پردازش داده‌ها در سازوکار اعطای مجوز امکان تبادل یا تملک ارزهای مجازی براساس مفاد ماده ۲ کنوانسیون یکنواخت‌سازی معاملات مبتنی بر ارزهای مجازی[1] یا مجوز بهره‌مندی از امضائات دیجیتالی نیز می‌تواند داده‌های مورد پردازش را در وضعیت داده‌های شخصی قرار دهد. مطابق با ماده قانون مرقوم، افراد برای دریافت مجوز تبادل ارزهای مجازی در نظام حقوقی اتحادیه اروپا ملزم به دریافت این مجوز از کشور مبتوع خود یا از کشوری که با کشور متبوع آنها دارای قرارداد متقابل باشد، می‌باشند. دریافت این مجوز نیز منوط به تقدیم مدارک شناسایی از سوی متقاضی و بررسی اطلاعات موجود از وی توسط سازمان‌های صلاحیت‌دار حکومتی می‌باشد.[2] این سازوکار در تخصیص مجوز بهره‌مندی از امضائات دیجیتالی نیز در کشورهای اتحادیه موجود است [۱۴].

اما سؤال پیش‌رو این است که در مواردی که پردازش اطلاعات توسط شرکت‌های خصوصی صورت پذیرد، دریافت رضایت صریح دارنده می‌تواند امری ضروری باشد. اما درصورتی‌که این امر همانطور که در بند اخیر بیان شد، توسط نهادهای حکومتی صورت پذیرد کیفیت دریافت رضایت از دارنده اطلاعات به چه شکلی خواهد بود؟ چالش بیان‌شده از این حیث آن است که نهادهای حکومتی امکان پردازش هرگونه اطلاعاتی از اشخاص در طی این پروسه را داشته و توسل به استدلالاتی از جمله وجود رضایت ضمنی در پردازش اطلاعات به جهت اقدام دارنده به دریافت مجوز از حکومت نمی‌تواند در تمامی موارد توجیه‌کننده اقدامات دولت تلقی گردد.

چه بسا نهاد دولتی در ذیل رضایت دریافت‌شده درخصوص اعطای مجوزهای بیان‌شده، مبادرت به دسترسی و پردازش انواع اطلاعات شخصی متقاضی حتی اطلاعاتی که هیچ ارتباطی به دریافت مجوز مذکور از سوی وی نداشته باشند، نماید که این امر به منزله نقض حریم خصوصی فرد تلقی می‌گردد. از این‌رو جهت پیشگیری از مشکل بیان‌شده، مشخص‌نمودن دقیق کمیت و کیفیت اطلاعات مورد بررسی نهاد مذکور و اطلاع دارنده از این امر و ارائه رضایت صریح جزو ضروریات تلقی می‌گردد.

۸-۳- شناسایی براساس مفهوم داده‌های نام مستعار

داده‌های نام مستعار همانطورکه در بند پنجم از ماده ۴ آیین‌نامه مرقوم نیز تأکید شده است، داده‌هایی هستند که بدون استفاده از اطلاعات اضافی قابلیت اختصاص به شخص معینی را نداشته باشند.[3] از این‌رو اگر داده‌ای باشد که به همراه دیگر اطلاعات به‌دست آمده یا در دسترس قابلیت اختصاص به شخص معینی را داشته باشد، نه تنها داده مذکور، بلکه تمامی اطلاعات موجود نیز به تبع ذیل عنوان داده‌های خصوصی قرار داده می‌شوند. این نوع داده‌ها عموماً شناسه‌های کوکی یا اطلاعات ژنتیکی آزمایشگاهی را شامل می‌گردند که مشترک میان انسان‌ها و حیوانات بوده و هرگونه تغییر مختصر بر آن قابلیت اختصاص داده انسان به حیوان یا برعکس را شامل می‌گردد.

اختصاص احکام داده‌های شخصی به داده‌های نام مستعار نیز الزاماً باید در ابتدای پردازش توسط پردازنده صورت پذیرد. به عبارت دیگر اگر داده‌ای جهت پردازش به پردازنده اطلاعات ارسال گردد و در بررسی اولیه داده مذکور، پردازنده امکان اختصاص این نوع داده به دو گونه زیستی موجود در طبیعت از جمله حیوان و انسان را داشته باشد، باید شرایط حاکم بر پردازش داده‌های خصوصی موجود در مقررات مصوب ۲۰۱۶ رعایت گردد. اما سؤال پیش‌رو این است که کسب رضایت دارنده اطلاعات در این خصوص به چه شکلی باید صورت پذیرد؟ آنچه درخصوص ماهیت داده‌های نام مستعار به ذهن متبادر می‌گردد امکان اختصاص این داده‌ها به یک انسان می‌باشد نه یک شخص معین. چرا که اگر این داده‌ها قابلیت اختصاص به شخصی معین را داشته باشند اصولاً باید در دسته‌بندی‌های دیگر بیان شده در این مقاله مورد بررسی قرار گیرند. ضمن اینکه کسب رضایت دارنده اطلاعات نیز باید پیش از وقوع فرایند پردازش انجام شود نه پس از آن‌که امکان شناسایی دقیق مشخصات دارنده اطلاعات فراهم می‌گردد.

1. Uniform Regulation Virtual Currency Business Act,July2017
2. -(URVCBA Article2): A person may not engage in virtual-currency business activity, or hold itself out as being able to engage in virtual-currency business activity, with or on behalf of a resident unless the person is:
(1) licensed in this state by the department under Section 202;
(2) licensed in another state to conduct virtual-currency business activity by a state with which this state has a reciprocity agreement and has qualified under Section 203;
(3) registered with the department and operating in compliance with Section 207; or
(4) exempt from licensure or registration under this [act] by Section 103(b) or (c).

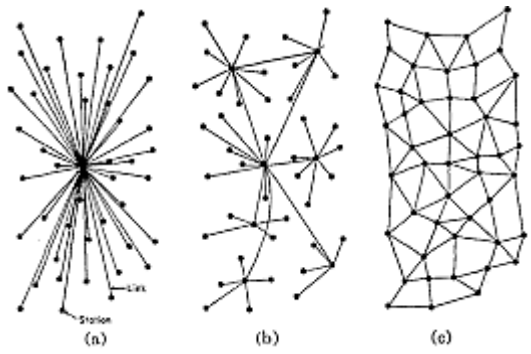
3. 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

ضمن اینکه امکان کسب رضایت از کشور دارنده اطلاعات نیز فراهم نمی‌باشد. چرا که اولاً در هر کشور افرادی که دارای تابعیت کشورهای دیگر باشند نیز به دلایلی از جمله شغل دائم یا مأموریت کاری یا به‌عنوان توریست وجود داشته و کشور میزبان امکان ارائه رضایت کلی بر پردازش تمامی داده‌ها را ندارد. ضمن اینکه اگر داده‌خام برای پردازش از سوی حاکمیت کشور به پردازنده ارسال گردد، اختصاص رضایت بر پردازش داده‌های نام مستعار بر همان حکومت نیز به منزله دور باطل و عمل خلاف قانون تلقی می‌گردد. به نظر نگارندگان این مسأله چالشی است که جز با تعیین تکلیف امر توسط قانون‌گذار امکان ارائه راه‌حل نخواهد داشت.

۸-۴- شناسایی براساس اطلاعات رمزنگاری شده مورد تبادل در بسترهای نامتمرکز

محیط اینترنت از دو نوع بستر متمرکز و نامتمرکز تشکیل می‌گردد. بسترهای متمرکز، بسترهایی هستند که آنها مرکزیت داده وجود داشته و ذخیره و تبادل اطلاعات تحت نظارت کنترل‌کننده مرکزی رخ می‌دهد که هرگونه خلل در عملکرد این کنترل‌کننده، منجر به اخلال کل سیستم می‌گردد. از جمله بسترهای متمرکز می‌توان به صفحه گسترده جهانی اشاره نمود. درحالی‌که در بسترهای نامتمرکز کنترل‌کننده‌ای وجود ندارد. بلاک‌چین از جمله بسترهای نامتمرکز است که داده‌های مورد تبادل جهت ذخیره در آن در بلوک‌های این زنجیره ذخیره می‌شوند. این داده‌ها ابتدا باید از طریق توابع هش به صفر و یک‌هایی تبدیل شوند که امکان ذخیره در بلاک‌ها را داشته باشند. بازخوانی این اطلاعات نیز از طریق ورود مجدد داده‌های تبدیل‌یافته به توابع هش ممکن می‌گردد. در شکل ذیل تمایز ماهیتی میان بسترهای متمرکز و نامتمرکز مشخص می‌باشد:

۸-۵- تمایز بسترهای متمرکز و نامتمرکز:



شکل ۱- تمایز بسترهای متمرکز و نامتمرکز

Picture Source: Http:// www.medium.com › centralized-ledgers-vs-distributed-ledgers

بسترهای نامتمرکز از جمله فناوری بلاک‌چین از پتانسیل بهره‌مندی از قراردادهای هوشمند برخوردارند. این قراردادها، قراردادهایی هستند که تحت نظارت هوش مصنوعی منعقد شده و در آنها پس از تأیید و امضای قرارداد توسط متعاملین، مفاد قرارداد توسط هوش مصنوعی مورد بازخوانی قرار گرفته و درصورتی‌که مفاد آن مغایرتی با دستورالعمل داده شده به هوش مصنوعی نداشته باشد، در بلاک‌چین ذخیره و مفاد آن نیز جهت مشاهده عموم، در این بستر ذخیره می‌گردد [۱۵]. افراد برای انعقاد این قراردادها الزاماً باید دارای امضائات دیجیتالی باشند. امضائات دیجیتالی امضائاتی هستند که از کلید خصوصی برای تولید داده پیام و کلید عمومی برای بازخوانی آن برخوردار می‌باشند. داده پیام‌های تولید و ارسال‌شده توسط کلید خصوصی همواره از طریق توابع هش به صفر و یک‌های غیرقابل خواندن تبدیل می‌گردد که تنها بازخوانی ان از طریق کلید عمومی و ورود آن داده به تابع هش اتفاق می‌افتد [۱۶].

رمزنگاری داده پیام‌های قابل تبادل در بسترهای نامتمرکز مبین قصد دارنده این اطلاعات بر «شخصی‌سازی ارادی» این داده پیام‌ها می‌باشد که پردازش آنها را جز با رضایت صریح آنها امکان‌پذیر نمی‌کند. از این‌رو به‌عنوان قاعده‌ای کلی در نظام حقوقی اتحادیه اروپا، درصورتی‌که به هر ترتیب دارنده اطلاعات، مبادرت به شخصی‌سازی اطلاعات خود نماید، هرگونه پردازش در این خصوص ممنوع می‌باشد [۱۷]. در حقوق ایران نیز دسترسی غیرمجاز به اطلاعات رمزنگاری‌شده مطابق با مفاد ماده ۷۲۹ قانون مجازات اسلامی جرم تلقی و واجد مجازات است. از این‌رو به طریق اولیه پردازش داده‌های رمزنگاری‌شده در حقوق ایران نیز جز با رضایت صریح دارنده می‌تواند ممنوع باشد. اما نکته قابل توجه این است که آنچه در نظام حقوقی اتحادیه اروپا پردازش این اطلاعات را ممنوع می‌نماید، ماهیت شخصی این اطلاعات است. اما در حقوق ایران سند قانونی مبنی بر شخصی‌بودن این اطلاعات وجود نداشته و جرم‌انگاری این عمل به جهت رمزنگاری داده می‌باشد نه ماهیت شخصی یا غیر شخصی آن.

۹- نتیجه‌گیری

توسعه روزافزون فناوری اطلاعات منجر به ابداع ابزارهای جدیدی با کاربردهای فراوان شده است. ابزارهای اینترنت‌اشیاء، ابزارهایی هستند که با برخورداری از فناوری نوین اینترنت‌اشیاء، کاربردهای فراوان در توسعه صنعت و تجارت کشورها دارند. اما سازوکار عملکرد آنها واجد چالش‌هایی در زمینه پردازش اطلاعات نیز می‌باشد. این ابزارها برای انجام وظایف از پیش تعیین‌شده نیازمند جمع‌آوری اطلاعات از محیط پیرامون خود می‌باشند. این اطلاعات شامل انواع داده پیام‌ها از جمله داده‌های شخصی افراد می‌باشد. مسأله حفاظت از داده‌های شخصی اشخاص جزو مهم‌ترین مسائل پیش‌روی سیاست‌گذاران هر کشور می‌باشد. سهل‌انگاری در جهت بخشی بر کیفیت پردازش این نوع اطلاعات می‌تواند زمینه دسترسی بیگانگان به اطلاعات خصوصی اتباع کشورها و سوءاستفاده از آن را پدید آورد.

اولین و مهم‌ترین مقدمه در محقق‌نمودن هدف بیان‌شده، شناسایی مفهوم داده‌های خصوصی و تفکیک این عنوان از دیگر انواع داده‌ها می‌باشد. در نظام حقوقی ایران تنها سند قانونی که مبادرت به ارائه معیارهای کلی در این زمینه نموده است، ماده ۵۸ قانون تجارت

الکترونیکی است. ماده مذکور با ارائه مصادیقی از داده‌های خصوصی، پردازش آن گروه از اطلاعات را در گروه کسب رضایت صریح دارنده نموده است. مشکل موجود در این ماده آن است که اولاً نه معیاری دقیق از امکان شناسایی داده‌های خصوصی به مخاطب ارائه می‌دهد و نه با ارائه مصادیقی احصایی امکان پیشگیری از ارائه تفاسیر متعدد را مفسرین منع می‌نماید. ضمن اینکه دلیلی بر عدم ضرورت کسب رضایت صریح دارنده در دیگر انواع داده‌های خصوصی مشاهده نمی‌گردد که نص ماده مذکور مبادرت به تفکیک نموده است.

وجود ابهامات بیان‌شده منجر می‌گردد تا مسأله سازوکار قانونی نحوه نظارت بر پردازش داده‌های خصوصی در مکانیسم عملکرد ابزارهای اینترنت‌اشیاء در حقوق ایران با چالش‌هایی مواجه گردد. اما نظام حقوقی اتحادیه اروپا متأثر از آخرین سند قانونی مصوب خود در سال ۲۰۱۶، معیارهای نسبتاً شفافی در زمینه شناسایی داده‌های خصوصی از نوع غیرخصوصی دارد. این معیارها در چهار دسته شناسایی داده‌های خصوصی براساس ماهیت داده‌ها، براساس اهداف حاصل از پردازش داده‌ها، براساس مفهوم داده‌های نام مستعار و براساس اطلاعات رمزنگاری‌شده مورد تبادل در بسترهای نامتمرکز استوار است. توجه به این معیارها می‌تواند زمینه بهبود روند شناسایی انواع داده‌های خصوصی در حقوق ایران و سیاست‌گذاری تقنینی در جهت پیش‌بینی سایر ابعاد حقوقی حاکم بر سازوکار پردازش اطلاعات در این کشور را بهبود بخشد. اما در حال حاضر نظام قانون‌گذاری این کشور نیازمند طی دو پروسه می‌باشد.

پروسه اول اصلاح قوانین موجود است. همانطور که بیان گردید، قانون تجارت الکترونیکی نه در این زمینه دارای احکام قانونی جامع و کافی می‌باشد و نه احکام موجود به صورت شفاف امکان برطرف‌نمودن نیازهای جامعه حقوقی را برخوردار هستند. این امر نیازمند اصلاح این قانون در حوزه مورد بررسی است. پروسه دوم نیز تصویب قوانین کارآمد در این حوزه می‌باشد. در حال حاضر بسیاری از جنبه‌های حقوقی مرتبط با سازوکا عملکرد ابزارهای اینترنت‌اشیاء از جمله چگونگی شناسایی مسئولیت ناقضان این قواعد، سازوکار تقسیم مسئولیت، سازوکار جبران و اقامه دعوی، آیین رسیدگی، داوری‌پذیری، قانون حاکم بر این دعاوی، سازوکار انعقاد قراردادهای پردازش، چگونگی اعطای مجوز به نهادهای فعال در این پروسه نیز علاوه بر چالش‌های موجود در حوزه مفهوم‌شناسی داده‌های خصوصی واجد خلاء قانونی در ایران می‌باشند که ضرورت هرچه سریع‌تر تصویب قانونی جامع در این خصوص احساس می‌گردد.

۱۰- مراجع

۱- فرحزادی، علی اکبر، ناصر، مهدی، سازوکار جبران جمعی خسارات ناشی از نقض قواعد امنیتی آیین‌نامهٔ عمومی حفاظت از اطلاعات اتحادیهٔ اروپا و امکان سنجی اجرای آن در حقوق ایران، دو فصلنامه حقوق خصوصی، دوره ۱۶، شماره ۲،صص ۴۱۳-۴۳۳، ۱۳۹۸

2- PETER CAREY, Data Protection, A Practical Guide to UK and EU Law, First Edition, Oxford Publisher, 2018.

3- Diane Rowland & Etc, Information Technology Law, Fifth Edition, Taylor Fransis, 2017.

4- Lachlan Urquhart, Tom Lodge, Andy Crabtree, Demonstrably doing accountability in the Internet of Things,International Journal of Law and Information Technology,Volume27, Issue1, pp 1-33, 2019.

5- Wagner Julian, The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?,International Data Privacy Law, online Edition:https://academic.oup.com › advance-article-pdf › doi › idpl › ipy008 › ipy008, 2019.

6- Finck Michèle,Pallas Frank, «They who must not be identified—distinguishing personal from non-personal data under the GDPR», International Data Privacy Law, Volume 10, Issue 1, February, pp11–36, 2020.

7- Ryngaert C &van Eijk N, "International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees", International Data Privacy Law, Volume 9, Issue 1, February, pp 61–73, 2019.

8- Altman, Micah & Etc, "Practical approaches to big data privacy over time", International Data Privacy Law, Volume 8, Issue 1, February, pp 29–51, 2018.

9- Van der Sloot, Bart, 'Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System', 31 Computer Law and Security Review, Volume 13, Issue 8, pp 18-34, 2017.

10- European Commission, The Article 29 Working Party Ceased to Exist as of 25 May 2018, https://ec.europa.eu/newsroom/article29/item detail. Cfm ? item id=629492, (accessed 13 Nov 2019).

11- Data Protection Commission, 'Guidance on Anonymisation and Pseudonymisation' https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf , (accessed 9 January 2020)

12- European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, online Edition: https://ec.europa.eu › newsroom › document, (accessed 12 May 2020).

13- Deliberation of the Restricted Committee SAN-2019-001, pronouncing a financial sanction against GOOGLE LLC, ONLINE Edition available at: http//:www.cnil.fr, (accessed 12 May 2020).

14- E. Blythe Stephen, "Hungary's Electronic Signature Act: Enhancing Economic Development with Secure Electronic Commerce Transactions", School of Management, New York Institute of Technology, USA, Volume 8, Issue 3, Automn, pp 47-58, 2007.

15- Levy, Karen E. C., Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law, online Edition available at: www.SSRN.com, pp 1-11, 2017.

16- O'Shields Reggie, Smart Contracts: Legal Agreements for the Blockchain, North Carolina Banking Institute,volume 21, Issue 4, pp 1-13, 2017.

17- Kuan Hon, 'The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated? - The Cloud of Unknowing' 1 International Data Privacy Law, Volume 3, Issue 2, March, pp 11–36, 2017