دوماهنامه بررسی‌های بازرگانی
سال نوزدهم، شماره ۱۰۹، مهر و آبان ۱۴۰۰، ۱۲۹-۱۱۵

Commercial Surveys Bimonthly
Vol.19, No.109, Oct-Nov 2021, 115-129

مقاله پژوهشی (تحلیلی)

حق بر تبادل داده‌های خصوصی و راه‌کارهای رفع چالش‌های آن در سازوکار عملکرد ابزارهای اینترنت اشیا

دریافت: ۹۸/۱۲/۱۶ پذیرش: ۹۹/۸/۷

علی‌اکبر فرحزادی [۱]، نویسنده مسئول
مهدی ناصر [۲]

چکیده

هدف از پژوهش حاضر تحلیل یکی از حقوق بیان شده با عنوان «حق بر تبادل داده‌های خصوصی» است. سوال اصلی پژوهش بررسی چیستی‌شناسی این حق و چالش‌های اجرای آن است. فرضیه این پژوهش بر این امر استوار است که مطابق با مفاد ماده (۲۰) آیین‌نامه عمومی حفاظت از اطلاعات اتحادیه اروپا مصوب ۲۰۱۶ حق بر تبادل داده‌های خصوصی به‌منزله انتقال حق نظارت و کنترل اطلاعات جمع‌آوری شده از سوی ابزار اینترنت اشیا از کنترل‌کننده اولیه به ثانویه است. اجرای این حق با چالش‌هایی از جمله محدوده اجرای مقررات حق مزبور، استثنائات حاکم بر اصول مقدماتی اجرای حق مزبور و سازوکار تبادل بدون بازگشت پردازش داده‌های خصوصی اشخاص از یک کنترل‌کننده به کنترل‌کننده دیگر استوار است. اجرای این حق در نظام حقوقی ایران منوط به اجرای برخی سیاست‌گذاری‌های تقنینی از جمله اصلاح قوانین موجود، پیاده‌سازی زیرساخت‌های به‌کارگیری ابزارهای اینترنت اشیا، آگاهی بخشی به مردم و نظارت مراجع صلاحیت‌دار می‌باشد.

طبقه‌بندی JEL: Q11 ,E22

ابزارهای اینترنت اشیا/ حق بر تبادل داده/ آیین‌نامه عمومی حفاظت از اطلاعات اتحادیه اروپا مصوب ۲۰۱۶/ چالش‌ها و راه‌کارها

۱. دانشیار دانشگاه علوم قضایی. aliakbar.farahzadi@yahoo.com
۲. دانشجوی دکترای حقوق خصوصی دانشگاه علوم قضایی.

۱. مقدمه: طرح مسأله

آیین‌نامه عمومی حفاظت از اطلاعات اتحادیه اروپا [۱] مقررات جدیدی است که پس از چهار سال مذاکره میان سران این اتحادیه در مورخه ۲۷ آوریل سال ۲۰۱۶ مورد تصویب قرار گرفته و در ۲۵ می سال ۲۰۱۸ در مرحله لازم‌الاجرا شدن برای تمامی کشورهای عضو اتحادیه قرار گرفته است. آیین‌نامه مذکور با هدف رفع خلاءهای قانونی دستورالعمل حفاظت از داده‌های اتحادیه اروپا مصوب ۱۹۹۵ [۲] واجد مقررات جدیدی است که ابتدا با تقویت اصول مسلم مورد تأکید در دستورالعمل مصوب ۱۹۹۵ از جمله رضایت بر پردازش داده‌های شخصی و پردازش داده‌ها با هدف مشخص و به میزان معین، ضمن اهتمام بر مقررات پیشین، واجد تعاریف و مقررات جدیدی از جمله حق دسترسی [۳] (ماده ۱۵)، حق حمل و تبادل داده (ماده۲۰) برای دارنده مطرح شده است [۱].

هدف اصلی از تصویب مقررات آیین‌نامه اخیر در حفاظت از دادهای خصوصی اشخاص، حفظ حریم خصوصی آنها است. حریم خصوصی در حوزه امنیت اطلاعات به حق بر جلوگیری از تحت کنترل قرارگرفتن تعبیر شده است [۵]. امروزه با ابداع ابزارهای هوشمند مانند گوشی‌های تلفن همراه، ابزارهای واقعیت مجازی، ابزارهای اینترنت اشیا و موارد مشابه، ضرورت حفاظت حریم خصوصی اشخاص بیش از پیش احساس می‌شود. آنچه در زمینه حفاظت از داده‌ها در فضای مجازی مورد بررسی قرار می‌گیرد دو گروه از داده‌ها با عنوان داده‌های شخصی و ابرداده‌ها [۶] هستند.

مطابق با مفاد ماده (۴) آیین‌نامه مذکور، داده‌های شخصی به هرگونه اطلاعاتی اطلاق می‌شود که مبنای شناسایی شخصیت یک فرد است. این اطلاعات می‌تواند اطلاعات هویتی مانند نام و نام خانوادگی، شماره شناسایی کارت ملی، موقعیت مکانی، اطلاعات بیومتریک، ژنتیکی و ... باشند که نقض حریم این‌گونه داده‌ها گاهی می‌تواند خسارات جبران‌ناپذیری داشته باشد [۷]. به‌عنوان مثال در گوشی‌های تلفن همراه نصب نرم‌افزارهای جانبی امکان استخراج شناسه گوشی و ارسال آن به طراح نرم‌افزار را داده و در این صورت تمامی اطلاعات خصوصی دارنده گوشی تلفن همراه قابلیت مشاهده توسط طراح نرم‌افزار را خواهد داشت [۸]. یا در سازوکار عملکرد ابزارهای اینترنت اشیا ارسال اطلاعات جمع‌آوری شده توسط این ابزارها به کنترل‌کننده آنها و از طریق کنترل‌کننده به پردازشگر داده‌ها، امکان دسترسی آسان و کم هزینه سوءاستفاده‌کنندگان از داده‌های خصوصی اشخاص را فراهم می‌آورد.

در حالت عادی دارندگان اطلاعات، هیچ نظارتی بر اینکه چه اطلاعاتی از سوی آنها جمع‌آوری و مورد پردازش قرار می‌گیرد ندارد. مسأله سوءاستفاده از اطلاعات این افراد در مواردی که ابزارهای هوشمند با جمع‌آوری اطلاعات و ارسال آنها در قالب ابرداده مبادرت به انجام وظایف خود می‌نمایند، بیشتر نمود پیدا می‌کند [۹]. ابزارهای هوشمند جهت انجام وظایفی که تولیدکنندگان آنها در قالب دستورالعمل داده شده به پردازنده آنها برایشان تعریف نموده‌اند، در مواردی نیاز به ارسال داده‌های تجمیع شده در قالب ابرداده به پردازندگان خود دارند [۱۰]. ردگیری داده‌های پیام ارسال شده متعدد در مدت زمانی متعارف بسیار آسان‌تر از ردیابی ابرداده متشکل از چندین داده پیام می‌باشد که در زمانی نامشخص از سوی یک دستگاه ارسال می‌شوند. از این رو در صورتی که هر یک از عوامل دخیل در عملکرد ابزارهای هوشمند قصد سوءاستفاده از اطلاعات شخصی افراد را داشته باشد، ارسال این اطلاعات در قالب یک ابرداده می‌تواند مسیری هموار در جهت دستیابی به اهداف تعیین شده باشد. اما پیشگیری از سوءاستفاده از اطلاعات شخصی دارندگان علاوه بر سیاست‌گذاری‌های اجرایی و نظارت حاکمیت بر عملکرد نهادهای دخیل در این پروسه، منوط به سیاست‌گذاری‌های تقنینی صحیح نیز می‌باشد. بر همین رویکرد است که آیین‌نامه مصوب ۲۰۱۶ اتحادیه اروپا در مواد ۱۲ تا ۲۳ دارندگان اطلاعات را

واجد حقوقی تلقی نموده است تا علاوه بر دیگر سازوکارهای نظارتی، سازوکار خودکنترلی دارندگان اطلاعات نیز به‌عنوان روشی در نظارت بر عملکرد کنترل‌کنندگان و پردازندگان اطلاعات خصوصی اشخاص تعیین گردد.

در میان حقوق پیش‌بینی شده، آنچه مبنای بررسی پژوهش حاضر قرار گرفته است، حق بر حمل و تبادل داده موضوع ماده (۲۰) آیین‌نامه مصوب ۲۰۱۶ می‌باشد. سوال اصلی که پژوهش حاضر به‌دنبال پاسخ‌گویی به آن می‌باشد، این است که چالش‌های اجرای حق پیش‌بینی شده در ماده مذکور چه بوده و رویکرد نظامات حقوقی اتحادیه اروپا و ایران در مواجهه با چالش‌های مذکور چه می‌باشد؟ برای پاسخ به سوال فوق، پژوهش حاضر به روش اسنادی و مطالعه تحلیلی نظام حقوقی اتحادیه اروپا و تطبیق مبانی موجود در این اتحادیه با مقررات حاکم بر حقوق ایران، در چهار گفتار ابتدا به بررسی مبناشناسی پژوهش حاضر که متشکل از تحلیل اقتصادی پیاده‌سازی مقررات مرقوم در نظام حقوقی ایران و مفهوم‌شناسی متغیرهای اصلی پژوهش بوده، پرداخته و پس از آن به تبیین مفاد ماده (۲۰) آیین‌نامه مذکور و واکاوی مهم‌ترین چالش‌های حقوقی موجود اقدام نموده است. این پژوهش در گفتار چهارم خود نیز در راستای بهبود به روند به‌کارگیری ابزارهای اینترنت اشیا هم از بعد تقنینی و هم از بعد اجرایی، مبادرت به ارائه توصیه‌های سیاست‌گذارانه نموده است.

۲. مبانی نظری و پیشینه تحقیق

پیش از آغاز مباحث اصلی پژوهش، با توجه به اینکه این حوزه از علم حقوق بردارنده موضوعات و ادبیات جدید و غیر ملموس می‌باشد، ضرورت مبناشناسی پژوهش حاضر، از این حیث ایجاب می‌گردد. این امر در دو محور تحلیل اقتصادی ضرورت به‌کارگیری آیین‌نامه عمومی حفاظت از اطلاعات مصوب ۲۰۱۶ در نظام حقوقی ایران و مفهوم‌شناسی متغیرهای اصلی پژوهش خلاصه می‌گردد.

تحلیل اقتصادی ضرورت به‌کارگیری آیین‌نامه عمومی حفاظت از اطلاعات مصوب ۲۰۱۶ در نظام حقوقی ایران

در دنیای کنونی توسعه فناوری اطلاعات و ابداع ابزارهای نوین دیجیتالی در بهبود تجارت الکترونیکی ملی و فراملی، چالش‌های جدیدی پیش روی سیاست‌گذاران کشورها قرار داده است. حضور ایران در بازارهای جهانی و نقش فعال این کشور در تجارت الکترونیکی نیز ضرورت پذیرش ابزارهای نوین دیجیتالی را ایجاب می‌نماید. این ابزارها در حوزه‌های مختلف تجارت الکترونیکی از جمله ارزهای مجازی در تبادل ارز در بازارهای پولی جهان، ابزارهای واقعیت مجازی در شبیه‌سازی طرح‌های صنعتی در صنایع و ابزارهای اینترنت اشیا در انجام معاملات الکترونیکی یا هر فرایند دیگری که امکان انجام آن به‌وسیله ماشین به‌جای انسان فراهم باشد، به‌کار گرفته می‌شوند.

کشورهای توسعه‌یافته با توجه به چالش‌هایی که نظام حقوقی داخلی خود در مواجهه با این ابزارها با آن مواجه بوده‌اند، برخی سیاست‌گذاری‌های تقنینی را در دستور کار قرار داده‌اند. همان‌طورکه بیان شد، مهم‌ترین چالشی که یک نظام حقوقی در زمینه به‌کارگیری ابزارهای اینترنت اشیا با آن مواجه است، چالش‌های مرتبط با حفظ حریم خصوصی شهروندان می‌باشد. چرا که دسترسی افراد فاقد صلاحیت به اطلاعات خصوصی شهروندان یک کشور، می‌تواند زمینه سوءاستفاده از این اطلاعات از جمله ساخت سلاح‌های بیومتریک، امکان هک حساب‌های بانکی و دیگر اعمال سوء را پدید آورد. این موارد منجر به تحمیل خسارات مالی فراوان نیز به دارنده اطلاعات می‌گردد. از این رو تصویب مقرره‌ای در جهت پیش‌بینی برخی حقوق برای دارندگان اطلاعات، برخی سازوکارهای پیش‌گیرانه در زمینه جهت‌دهی بر عملکرد نهادهای تولید و کنترل‌کننده این ابزارها، برخی مکانیسم‌های نظارتی بر عملکرد نهادهای پردازنده اطلاعات و چگونگی جبران خسارات وارده در این زمینه جزو ضروریات تلقی می‌گردد.

آیین‌نامه عمومی حفاظت از اطلاعات، جدیدترین مصوبه قانونی در سطح جهان می‌باشد، که به‌صورت مفصل قواعد حقوقی حاکم بر این پروسه را مورد طرح و بررسی قرار داده است. این در حالی است که همان‌طور که در بخش‌های آتی نیز تشریح خواهد شد، تنها مقرره موجود در زمینه حفظ امنیت اطلاعات در کشور ایران، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی می‌باشند که نه تنها به‌صورت کاملا مختصر مبادرت به ارائه قواعدی در زمینه چگونگی پردازش اطلاعات نموده و بسیاری از جنبه‌های حقوقی مرتبط با این مبحث را مورد بررسی قرار نداده‌اند، بلکه متن این مواد نیز دارای ابهامات فراوانی می‌باشد که اجرای آنها را نیز با چالش‌های جدی در کشور ایران مواجه می‌گرداند. از این رو توجه به تجربیات نظام حقوقی اتحادیه اروپا و جدیدترین مصوبه این اتحادیه در زمینه حفظ حریم خصوصی اشخاص می‌تواند رافع بسیاری از مشکلات پیش روی نظام حقوقی ایران نیز تلقی گردد.

مفهوم‌شناسی متغیرهای اصلی پژوهش

برای ورود به بحث به جهت تخصصی بودن موضوع ابتدا نیازمند بررسی مفهوم متغیرهای اصلی پژوهش می‌باشیم. از این رو گفتار حاضر در دو بند ذیل به تحلیل مفهوم اینترنت اشیا و کنترل‌کنندگان و پردازندگان اطلاعات می‌پردازد.

اینترنت اشیا

ماده (۲۹) اعلامیه مرکز نظارت بر داده پیام‌های اتحادیه اروپا مصوب ۲۰۱۰ با الحاقات و اصلاحات ۲۰۱۵[۱۱] در تعریف اینترنت اشیا بیان می‌دارد: «اینترنت اشیا زیرساخت‌هایی می‌باشند که در آن میلیاردها حسگر تعبیه شده در دستگاه‌های کاربردی روزمره برای ضبط، پردازش، ذخیره و انتقال داده‌ها طراحی شده و همان‌طور که از قابلیت ارتباط با عامل انسانی برخوردار می‌باشند، با بهره‌مندی از شناسه‌های منحصر به فرد، با دستگاه‌ها یا سیستم‌های دیگر با استفاده از قابلیت‌های شبکه تعامل برقرار می‌کنند»[۱۲]

به‌عبارت دیگر ابزارهای اینترنت اشیا نوعی ابزارهای هوشمند می‌باشند که با تعبیه پروتکل‌های منحصر به فرد به پردازنده آنها، این ابزارها همانند انسان قابلیت دریافت و پردازش داده پیام‌ها جهت انجام وظایف از پیش تعیین شده را پیدا می‌کنند. این ابزارها قابلیت اتصال به بسترهای متمرکز مانند صفحه گسترده جهانی یا نامتمرکز مانند بلاک چین را داشته و از این طریق قابلیت ارتباط از راه دور با انسان یا دیگر سیستم‌ها را کسب می‌کنند. امروزه ابزارهای متعددی از جمله ساعت‌های هوشمند، تلویزیون‌های هوشمند، ترموستات‌های هوشمند و ... طراحی شده‌اند که هر یک با برخورداری از پروتکل‌های خاص نسبت به انجام وظایف تعیین شده اقدام می‌کنند. به‌عنوان مثال ترموستات‌های هوشمند که ساخته شرکت گوگل می‌باشند برای کنترل وضعیت گرما و سرمای منزل، میزان نور موجود در فضا، کنترل آبیاری گیاهان و ... به‌کار گرفته می‌شوند که در هر حال در صورت کمبود نور موجود در فضا یا افزایش یا کاهش دمای محیط یا دیگر شرایط نسبت به برقراری تعادل در فضا اقدام می‌کنند [۱۳]. البته ابزارهای هوشمند تنها در این موارد خلاصه نمی‌شوند. امروزه کاربرد ابزارهای اینترنت اشیا در اقلام مختلفی از جمله ساخت هواپیماهای بدون سرنشین نسل سوم، کنترل و مدیریت امور بازارهای مالی در کشورهای توسعه یافته نیز بر متخصصین این امر مشهود بوده و با توسعه فناوری اینترنت اشیا، سرمایه‌گذاری‌های کلان در زمینه ساخت و توسعه ابزارهای دربردارنده آن در سطح جهان صورت گرفته است.

پردازنده و کنترل‌کننده

بند d از ماده دوم دستورالعمل مصوب ۱۹۹۵ و بند هفتم از ماده چهارم از آیین‌نامه مصوب ۲۰۱۶ اتحادیه اروپا در تعریف کنترل‌کننده بیان می‌دارند: «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» به‌عبارت دیگر ابزارهای اینترنت اشیا دارای سازندگانی می‌باشند که قابلیت دسترسی به اطلاعات این ابزارها را برخوردار بوده و از امکان کنترل آنها نیز بهره‌مند هستند. این اشخاص حقیقی یا حقوقی که کنترل‌کننده نامیده می‌شوند، مطابق با نقش خود در عملکرد یک ابزار می‌توانند شناسایی شوند. به‌عبارت دیگر اگرچه اطلاق عنوان کنترل‌کننده از پردازنده داده پیام جدا می‌باشد، اما در صورتی که پردازش داده پیام توسط ابزار اینترنت اشیا صورت پذیرد، دسترسی کنترل‌کننده به اطلاعات پردازش شده هرچند تحت خط‌مشی تعیین شده توسط وی صورت پذیرد، نمی‌تواند عنوان پردازنده را بر این اشخاص بار نماید. این امر در شماره ۱۱ از بند هشتم از ماده (۲۹) اعلامیه مذکور نیز مورد تأکید سیاست‌گذاران قرار گرفته است [۱۴].

در مقابل به تعبیر بند e از ماده دوم دستورالعمل مصوب ۱۹۹۵ و بند هشتم از ماده چهارم آیین‌نامه مصوب ۲۰۱۶ پردازنده «شخصی حقیقی یا حقوقی، مقامات دولتی، نمایندگی یا هر نهاد دیگری است که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند» بنابراین سازوکار عملکرد پردازشگر تحت خط‌مشی است که توسط کنترل‌کننده تعیین می‌گردد. از این رو در صورتی که خط‌مشی و چگونگی پردازش داده پیام‌ها توسط پردازشگر تعیین گردد، وی دارای عنوان کنترل‌کننده بوده و مسئولیت‌های قانونی موجود در دستورالعمل مصوب ۲۰۱۶ که برای کنترل‌کننده پیش‌بینی شده است، برای وی نیز قابل اعمال خواهد بود. این امر اعم از تعیین فرایند مذکور در قراردادهای فی‌مابین کنترل‌کننده یا پردازنده بوده و در صورتی که بنای طرفین بر این امر استوار باشد یا حتی عرف حاکم حکم بر چنین اعمالی نماید، مسئولیت‌های پیش‌بینی شده برای کنترل‌کننده قابل اعمال بر پردازشگر نیز خواهد بود (بند دهم از ماده ۲۸ آیین‌نامه مصوب ۲۰۱۶). در کنار این موارد اعلامیه مصوب سال ۲۰۱۰ نیز برای تمایز میان پردازنده و کنترل‌کننده دو شرط اساسی تمایز شخصیت و انجام دستورات کنترل‌کننده توسط پردازنده را پیش‌بینی نموده است. از این رو اگر هر دو عنوان پردازنده و کنترل‌کننده در یک شخص وجود داشته باشند، وی در مقام انجام وظایف پردازندگی نیز واجد مسئولیت کنترل‌کنندگی خواهد بود (شماره ۱۱ از بند اول از ماده ۲۹ اعلامیه).

۳. روش تحقیق

روش تحقیق پژوهش حاضر تجویزی می باشد. چرا که به جهت اهمیت موضوع و خلاءهای تقنینی موجود در نظام حقوقی ایران که موضوع حق بر تبادل داده‌های خصوصی، به تفصیل در این پژوهش بیان و راه‌کارهای موجود ارائه داده شده است، نوید برداشتن گام‌هایی موثر در رفع خلاءهای تقنینی و قضایی در این حوزه را ارائه می‌دهد. نوع پژوهش حاضر کیفی بوده و روش جمع‌آوری اطلاعات این پژوهش متناسب با انواع اطلاعات قابل استفاده متفاوت می‌باشد. در این پژوهش مقالات مورد استفاده از بانک‌های نشریات خارجی مانند Heinonline, Springer, Tandfonline, Sience Direct مستخرج و کتب مورد استفاده نیز از سایت Zlibrary که غنی‌ترین سایت انتشار کتب معتبر انگلیسی می‌باشد دانلود شده است. درخصوص منابع مستخرج از سایت‌های اینترنتی نیز اطلاعات با پایش محتوا از سایت‌های معتبر مطالعه و مستخرج گردیده‌اند.

۴. تجزیه و تحلیل داده‌ها و یافته‌ها

تحلیل مفاد ماده ۲۰ آیین‌نامه مصوب ۲۰۱۶

آیین‌نامه مصوب ۲۰۱۶ در راستای حمایت از حقوق دارندگان داده‌های خصوصی واجد مقرراتی است که حقوق دارندگان اطلاعات در مواد ۱۲ تا ۲۳ این آیین‌نامه مورد تبیین قرار گرفته است. تصویب آیین‌نامه مذکور به‌دنبال ابداع فناوری اینترنت اشیا و به وجود آمدن ابزارهای اینترنت اشیا صورت گرفت.

در سازوکار عملکرد این ابزارها کنترل‌کنندگان و پردازندگان نقش اساسی ایفا می‌نمایند. ابزارهای اینترنت اشیا در راستای انجام وظایف از پیش تعیین شده نیاز به جمع‌آوری اطلاعات از محیط پیرامون خود دارند. اطلاعات جمع‌آوری شده توسط این ابزارها بسته به نوع داده پیام‌های تجمیع شده در قالب ابرداده یا به‌صورت داده‌های آزاد به کنترل‌کنندگان ارسال می‌گردند. کنترل‌کنندگان این ابزارها سازمان‌های تولیدکننده آنها می‌باشند که نسبت به عملکرد ابزار کنترل و نظارت لازم را دارند. این سازمان‌ها مطابق با نوع داده‌های ارسال شده از سوی ابزار، داده‌های دریافتی را به سازمان‌های پردازشگر اطلاعات ارسال می‌نمایند. پردازندگان اطلاعات نیز داده‌های دریافتی را مورد پردازش قرار داده و نتیجه پردازش داده‌های دریافتی را به کنترل‌کننده ارسال می‌نمایند.

پردازش داده‌های خصوصی اشخاص باید با رعایت مقررات ماده (۶) آیین‌نامه مصوب ۲۰۱۶ صورت پذیرد. بند اول از ماده مذکور صراحتا بر ضرورت کسب رضایت موردی دارنده در زمینه جمع‌آوری و پردازش داده‌های خصوصی وی اشاره دارد. در این راستا کنترل‌کنندگان هنگام انتقال مالکیت یک ابزار بر اشخاص باید در قالب قراردادی کیفیت و سازوکار عملکرد ابزار را به آنها توضیح داده و به‌صورت موردی رضایت آنها را بر پردازش داده‌های شخصی آنها کسب نمایند [۱۵]. ضمن اینکه پردازش داده‌ها نیز تنها در محدوده عملکرد ابزار، با رعایت مقررات قانونی و در راستای اهداف از پیش تعیین شده برای ابزار مذکور صورت پذیرد (بندهای دوم و سوم و چهارم ماده ۶)[۱۶].

دارندگان اطلاعاتی که اطلاعات آنها در قالب داده پیام‌های تجمیع شده به کنترل‌کنندگان و پردازندگان ارسال شده است، واجد حقوقی در پروسه پردازش این اطلاعات نیز می‌باشند. یکی از حقوق در نظر گرفته شده در آیین‌نامه مصوب ۲۰۱۶، حق بر حمل و تبادل داده توسط دارنده می‌باشد. ماده (۲۰) آیین‌نامه مصوب ۲۰۱۶ واجد مقرراتی در راستای حمایت از حق انتقال داده‌های خصوصی اشخاص توسط دارندگان آنها است. بند اول از ماده مذکور بر حق دارنده بر دریافت اطلاعات پردازش شده وی توسط پردازشگر اشاره دارد [۱۷]. آیین‌نامه مصوب ۲۰۱۶ در زمینه پردازش داده‌های خصوصی اشخاص نیز، اصل رضایت مطلق آنها را مورد توجه قرار داده است. بند اول از ماده (۲۰) این مقررات حق دریافت داده‌های پردازش شده را در قالبی ساختارمند و با فرمتی که برای رایانه‌ها قابل خواندن باشد برای دارنده محفوظ دانسته است [۱۸]. بند ب این ماده نیز بر ضرورت استمرار رضایت دارنده در تبادل و پردازش اطلاعات وی اشاره دارد. این بند بیان می‌دارد که دارنده در هر زمان که تمایل داشته باشد می‌تواند نسبت به انتقال اطلاعات خود از یک کنترل‌کننده به کنترل‌کننده دیگر اقدام نماید [۱۹]. اما این حق نه به‌صورت مطلق بلکه در مواردی که عملکرد کنترل‌کننده در راستای حفظ منافع عمومی باشد مورد تعدیل قرار گرفته است (بند ۳). به‌نظر نگارندگان حفظ منافع عمومی می‌تواند اصطلاحی بسیط باشد که حتی دستور مقامات صلاحیت‌دار را که به هر دلیل قانونی این وظیفه را بر عهده کنترل‌کننده قرار می‌دهند، شامل شود. از این رو در صورتی که تجمیع و پردازش داده‌های شخصی اشخاص مطابق با دستور هر یک از مراجع قضایی، اداری، امنیتی و... نیز باشد، حق تبادل داده‌ها از دارندگان در زمینه‌های مذکور یا مرتبط با آنها سلب می‌گردد.

اجرای حقوق مندرج در ماده (۲۰) آیین‌نامه مصوب ۲۰۱۶، منوط به‌دسترسی و اطلاع مطلق دارنده از سازوکارهای انجام شده در پروسه پردازش می‌باشد. حق دسترسی وی در ماده (۱۵) آیین‌نامه مصوب ۲۰۱۶ مورد تصریح قرار گرفته است. مطابق با مفاد این ماده، کنترل‌کنندگان موظف می‌باشند تا اهداف حاصل از تجمیع و پردازش داده‌ها، نوع و کیفیت دسته‌بندی داده‌های مورد پردازش، پردازندگان و دیگر اشخاصی که اطلاعات پردازش شده در اختیار آنها قرار خواهد گرفت، مدت زمان ذخیره داده‌های مورد پردازش و محل ذخیره

آنها به‌صورت کامل به دارندگان تفهیم نمایند. اما اجرای حق مندرج در ماده (۲۰) آیین‌نامه مصوب ۲۰۱۶، با چالش‌هایی نیز همراه است که در گفتار بعدی به آن اشاره خواهد شد.

چالش‌های اجرای مقررات ماده (۲۰) آیین‌نامه مصوب ۲۰۱۶

اجرای حق حمل و تبادل داده توسط دارنده، در سازوکار پردازش داده‌های خصوصی وی با چالش‌هایی همراه است که به مهم‌ترین آنها اشاره می‌گردد.

محدوده اجرای حق حمل و تبادل داده

سوالی که در مواجهه با چالش مطروحه به ذهن می‌رسد این است که در صورتی که کنترل‌کننده، تولیدکننده انحصاری ابزاری هوشمند باشد که حق انحصاری کنترل این ابزار را به خود اختصاص داده باشد، آیا دارنده حق انتقال تبادل داده‌های خود را از آن کنترل‌کننده به کنترل‌کننده دیگر دارا خواهد بود؟

پاسخ به سوال مذکور نیازمند تحلیل کیفیت حق معنوی کنترل‌کننده‌ای می‌باشد که مالکیت ابزار اینترنت اشیا را به دارنده منتقل نموده است. ابزارهای اینترنت اشیا در انجام وظایف تعیین شده واجد پروتکل‌هایی می‌باشند که تعبیه این پروتکل‌ها به پردازنده آنها، تبیین‌کننده خط‌مشی عملکرد انها محسوب می‌گردد [۲۰]. در صورتی که کنترل‌کننده‌ای با طراحی پروتکلی مشابه با پروتکل کنترل‌کننده ابتدایی، قابلیت نظارت و کنترل بر عملکرد ابزار هوشمند را داشته باشد، در صورتی که پروتکل طراحی شده، به‌منزله نقض حق انحصاری کنترل‌کننده اصلی محسوب نگردد، امکان اجرای حق مقررات ماده (۲۰) و حمل و تبادل داده‌های خصوصی دارنده از کنترل‌کننده اصلی به ثانوی موجود است. اما در صورتی که این امکان وجود نداشته و در هر حال به‌کارگیری پروتکلی مشابه با پروتکل اصلی به‌منزله نقض حق معنوی کنترل‌کننده اصلی باشد، اجرای حق مذکور نیز با چالش‌هایی مواجه خواهد شد.

پروتکل‌های ابزارهای اینترنت اشیا به جهت برخورداری از خصوصیات منحصر به فرد (نوآوری نسبت به گونه‌های مشابه و کاربردهای تکنولوژیکی در بسترهای متمرکز و نامتمرکز) واجد حق معنوی برای طراح خود می‌باشند. از این رو در صورتی که شرکت یا سازمان دیگری نیاز به استفاده از آنها داشته باشد، باید از شرکت سازنده اجازه استفاده را اخذ نماید. اما به‌نظر نگارندگان این امر مانع از تولید پروتکل‌های مشابه توسط دیگر شرکت‌ها یا سازمان‌ها نمی‌گردد. این حق مسلم تولیدکننده در ابداع کالا جهت رفع حاکمیت انحصاری یک شرکت بر بازار می‌باشد و در حوزه پروتکل‌های موجود در بسترهای متمرکز و نامتمرکز نیز چنین امکانی فراهم است. به‌عنوان مثال پروتکل‌های NEM(X-eM) پس از ابداع امکان انجام وظایف پروتکل‌های هایپرلجر با همان کیفیت و کارایی را فراهم آورده‌اند. یا پروتکل‌های NEO و Ethereum به جهت برخورداری از خصوصیاتی مشابه در انعقاد قراردادهای هوشمند نقشی مشابه در بستر بلاک چین ایفا می‌نمایند [۲۱]. اما سوال موجود این است که وجود خصوصیات مشابه در این پروتکل‌ها طراح اولیه را می‌تواند محق بر اقامه دعوی علیه طراح مشابه نماید؟ به‌نظر نگارندگان پاسخ سوال مزبور منفی است. چرا که طراحی یک پروتکل منوط به برنامه‌نویسی دقیق طراح در مدت زمانی طولانی بوده و با کپی‌برداری یا نقشه‌کشی معکوس آن تفاوت ماهیتی دارد. از این رو هنگامی که برنامه‌نویسی، مبادرت به طراحی پروتکلی می‌نماید، اگرچه می‌تواند خصوصیات پروتکل‌های پیش‌تولید را مورد بررسی قرار دهد، اما طراحی آن در یک بستر منوط به برنامه نویسی دقیق خالق آن می‌باشد. از این رو وجوه تشابه میان پروتکل‌های موجود در یک حوزه نمی‌تواند طراح اولیه را محق بر اقامه دعوی کند. به‌عبارت دیگر در حقوق ایران مستفاد از نص ماده (۱) قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری، تولید و طراحی یک پروتکل جدید، نتیجه فکر طراحان آن بوده و در صورتی که واجد خصوصیاتی جدیدتر نسبت به پروتکل

مشابه باشد می‌تواند به‌عنوان پروتکلی معرفی شود که برای اولین بار در ایران ارائه شده و طبیعتا قابلیت رفع مشکلات حوزه فناوری اینترنت اشیا را نیز برخوردار می‌باشد.

اما ایرادی که بر این نظر می‌توان وارد ساخت این است که هدف از شناسایی عنوان طرحی جدید بر یک پروتکل، طراحی نوآورانه آن توسط تولیدکننده است. اگر پروتکلی با الهام‌گیری از پروتکلی دیگر هر چند واجد خصوصیات نوین‌تر نسبت به نسخه پیشین بوده و هر چند تمامی مراحل تولید و طراحی آن توسط برنامه‌نویس صورت گرفته باشد، در حقیقت امر از ایده طراح نشأت نگرفته است. از این رو مطابق با این دیدگاه با بیان ابهام ماده (۱) نمی‌توان پروتکل جدید را مبنای شناسایی طرحی جدید در یک نظام تلقی نمود. از طرفی ماده (۲) قانون فوق‌الذکر اختراعی را قابل ثبت دانسته است که حاوی «ابتکار جدید» در حوزه فناوری موجود باشد. به تعبیر نگارندگان با امعان نظر از عبارات ماده (۲) که پشتبند عبارت ابتکار جدید از آنچه که «در فن وجود نداشته یا برای دارنده مهارت آشکار نباشد» می‌توان برداشت نمود که در طراحی پروتکل‌های نرم‌افزاری، آنچه طرحی نوین تلقی می‌گردد که نمونه پیشینی از آن در جامعه وجود نداشته و از هیچ نمونه دیگری نیز الهام گرفته نشده باشد. البته به‌نظر نگارندگان، تولید چنین پروتکل‌هایی به معنای نقض حق تولیدکننده پروتکل اصلی قلمداد نمی‌شود. چرا که در صورت وجود انحصار در تولید چنین پروتکل‌هایی اولا نوآوری و خلق طرح‌های جدید صنعتی تحت‌الشعاع محدودیت قرار گرفته و ثانیا تولید ابزار به‌دست یک طراح نمی‌تواند به‌منزله قصد وی بر استفاده سوء از طرح دیگری باشد. ضمن اینکه مطابق با مفاد مواد (۶) به بعد قانون ثبت اختراعات... و مواد (۳) به بعد آیین‌نامه قانون مزبور، طراح به‌هیچ وجه ملزم به افشای اسرار تولید طرح خود نبوده و تنها در محدوده مقررات بیان شده باید به کاربردهای صنعتی یا نوآوری‌های اثر خود بپردازد. ضمن اینکه انحصار تولید یک کالا برای یک شرکت به‌منزله منع دیگران از کوشش در راستای تولید کالای مشابه و رفع انحصار طراح نمی‌باشد. چرا که اگر قائل بر انحصار مطلق باشیم، دیگر محلی برای توسعه و پیشرفت صنعت باقی نمی‌ماند. توسعه صنعت در گرو تولید ابزارهای نوآورانه برای رفع انحصار تولیدکنندگان در کشورها می‌باشد. مضافا حمایت از صاحب اثر در گرو سوءاستفاده از کالای تولیدی وی می‌باشد، نه استفاده از کالای دیگری (هرچند مشابه) که به همت شخص دیگری برای رفع انحصار تولیدکننده اولیه تولید شده باشد. علاوه بر آن بر فرض اگر کشورهای در حال توسعه ملحق شده به کنوانسیون‌های بین‌المللی در زمینه حمایت از حق معنوی طراح که از تحریم‌های کشورهای توسعه یافته رنج می‌برند، امکان تولید کالاهای تحریمی کشورهای توسعه یافته که در آن کشورها ثبت شده و کاربردهای تکنولوژیک صنعتی دارد را تنها به استناد اصل موصوف نداشته باشند، محلی برای گذر از تحریم و پیشرفت این کشورها باقی نمی‌ماند. از این رو تلقی بر اطلاق اصل مزبور بر تمامی طرح‌های تولیدی می‌تواند محل تامل قرار گیرد.

استثنائات اصل رضایت از پردازش به‌عنوان مقدمه اجرای حق تبادل

سوال پیش رو در مواجهه چالش حاضر این است که از آنجا که مقررات آیین‌نامه مصوب ۲۰۱۶ اصل رضایت حداکثری را در تبادل داده‌های خصوصی اشخاص مدنظر قرار داده است، آیا در موارد خاص مانند استفاده منصفانه[۲۲] یا وجود اضطرار امکان جمع‌آوری و پردازش داده‌های اشخاص در فضایی خارج از رضایت آنها وجود دارد؟ با عنایت به اینکه آیین‌نامه مصوب ۲۰۱۶ اصل رضایت حداکثری را در زمینه جمع‌آوری و پردازش دادهای خصوصی اشخاص پیش‌بینی نموده است، آیا این اصل محدود به اطلاعات شخصی دارنده می‌باشد یا اعضای خانواده وی را نیز می‌تواند در بر گیرد؟ اگر پاسخ سوال مزبور مثبت است، مسأله کسب رضایت دیگر اشخاص به چه نحو خواهد

بود؟ آیا دارنده می‌تواند در ازای اشخاص بالغ نیز رضایت بر جمع‌آوری و پردازش داده‌ها را ارائه دهد؟ در خصوص دیگر مایملک دارنده مانند محدوده منزل، اسباب و اثاثیه و... آیا ضرورت کسب رضایت دارنده نیز وجود دارد؟ آیا در سازوکار عملکرد ابزارهای اینترنت اشیا، منظور از داده‌های تجمیع شده تنها داده‌هایی می‌باشند که توسط ابزارهای اینترنت اشیا جمع‌آوری شده باشند یا در صورتی که کنترل‌کننده برای بهبود عملکرد ابزار، از طریق دادهای مکانی، کوکی‌ها یا GLPO نسبت به جمع‌آوری اطلاعات اقدام نماید، رضایت اولیه دریافت شده شامل این اطلاعات نیز می‌گردد؟

در پاسخ به سوالات مذکور، مسأله مورد بحث را از دو منظر می‌توان مورد تحلیل قرار داد.

نظر اول اینکه آنچه در زمینه کسب رضایت دارنده در سازوکار عملکرد این ابزارها مطرح می‌گردد، تنها در محدوده داده‌های خصوصی مربوط به وی خلاصه می‌شود [۲۳]. دلیل این امر نیز آن است که در پیشنهاد اولیه کمیسیون اتحادیه اروپا در راستای تصویب آیین‌نامه مصوب ۲۰۱۶، ضرورت کسب رضایت دارنده در پردازش داده‌ها صراحتا بر هر «داده تحت پردازش» تسری داده شده بود [۲۴]. این در حالی است که نسخه نهایی تصویب شده عبارت مذکور به «داده‌های شخصی» تغییر پیدا نموده است. از این رو تغییر صورت گرفته را می‌توان حمل بر تغییر قصد قانون‌گذار تلقی نمود.

اما به‌نظر نگارندگان دیدگاه صحیح‌تر این است که پیش‌بینی ضرورت کسب رضایت در جمع‌آوری داده‌های مورد نیاز در سازوکار عملکرد ابزارهای مذکور رعایت حقوق قانونی دارنده این اطلاعات است. آنچه در محدوده مایملک وی از اموال و دارایی‌های او قرار می‌گیرد نیز در صورتی که واجد اطلاعاتی باشند که دسترسی به آنها برای عموم امکان‌پذیر نباشد نیز دقیقا همانند دسترسی به اطلاعات شخصی خود دارنده تلقی می‌گردد (این نظر از عبارات دیگر مواد آیین‌نامه مذکور همانند ماده (۱۵) که در آن به «کلیه داده‌های جمع اوری شده از موضوع داده» اشاره شده است، نیز مستفاد می‌گردد) و تفاوتی نمی‌نماید این اطلاعات از سوی ابزار به‌صورت مستقیم اخذ گردد یا در پروسه بیان شده توسط فرایندهای دیگر مانند استفاده از کوکی‌ها یا GLPO صورت پذیرد. از این حیث تفاوتی میان مبانی موجود در نظام حقوقی ایران یا اتحادیه اروپا نیز نمی‌باشد. اما همان‌طور که در هر نظام حقوقی حسب مورد استفاده منصفانه از حق دیگری یا استفاده از حق مزبور در موارد ضرورت، می‌تواند نافی مسئولیت استفاده‌کننده باشد، در سازوکار عملکرد ابزارهای اینترنت اشیا نیز اصول بیان شده جاری می‌باشد. اما مسأله اثبات وجود اضطرار یا اثبات شرایط استفاده منصفانه شرطی است که استفاده‌کننده ملزم به اثبات آن است. به‌نظر نگارندگان تهیه یک ابزار از سوی یک سازمان یا حتی یک منزل توسط سرپرست نهاد مذکور یا خانواده و اعلام رضایت مشارالیهم بر جمع‌آوری اطلاعات، موجد حق کنترل‌کننده بر تجمیع و ارسال اطلاعات مذکور به پردازنده بوده و نیازی بر کسب رضایت از تمامی اشخاص حاضر در محل نمی‌باشد. چرا که اولا انعقاد قرارداد تنها با خریدار کالا صورت پذیرفته و تفهیم مفاد آن تنها بر وی صورت می‌پذیرد. ضمن اینکه ضرورت کسب رضایت از اشخاص تنها با این هدف صورت می‌پذیرد که آنها از عملکرد ابزار و پروسه صورت پذیرفته اطلاع یابند، از این رو اعلام رضایت سرپرست در خصوص دیگر کارکنان اداره یا سرپرست خانواده در خصوص اعضا کفایت می‌نماید. البته از آنجا که هر شخص مالک اطلاعات خود می‌باشد، اعلام عدم رضایت وی از جمع‌آوری اطلاعات او می‌تواند ساقط‌کننده رضایت سرپرست باشد.

امکان‌سنجی تبادل بدون بازگشت داده‌های خصوصی از یک کنترل‌کننده به کنترل‌کننده دیگر

همان‌طور که بیان شد، بند سوم از ماده (۲۰) این آیین‌نامه واجد مقرراتی در جهت محدودیت حق حمل‌ونقل داده‌ها از یک کنترل‌کننده به کنترل‌کننده دیگر است. مطابق با مفاد این بند در صورتی که اطلاعات جمع‌آوری شده در راستای

منافع عمومی مورد پردازش قرار گیرد، در پروسه پردازش امکان تغییر کنترل‌کننده توسط دارنده وجود نخواهد داشت. سوال پیش رو این است که آیا دارنده پس از اتمام پردازش قادر به انتقال بدون بازگشت اطلاعات از کنترل‌کننده مذکور به سازمان دیگری خواهد بود؟ از آنجا که استمرار عملکرد هر کنترل‌کننده و به تبع آن پردازنده منوط به رضایت دارنده ابزار می‌باشد، در صورتی که کنترل‌کننده با تخصیص شناسه کاربری به هر داده یا ذخیره اطلاعات در فضای ابری بسترهای متمرکز یا نامتمرکز جهت حفظ انسجام و امنیت داده‌های مذکور، امکان حذف این اطلاعات را از میان برده باشد، وضعیت حقوقی حاکم بر این پروسه چه خواهد بود؟ آیا دارنده حق الزام کنترل‌کننده به حذف داده‌های پردازش شده در راستای منافع عمومی یا ملی را خواهد داشت؟

در پاسخ به چالش‌های بیان شده فوق، در بدایت امر می‌توان بیان داشت، حق دارنده در انتقال داده‌ها منحصر به داده‌های آپلود شده می‌باشد [۲۵]. از این رو در صورتی که داده‌ای در مرحله پردازش توسط پردازنده قرار گیرد، دیگر امکان انتقال ان از سوی کنترل‌کننده به کنترل‌کننده دیگر وجود نخواهد داشت. لذا در صورتی که پس از اتمام پردازش، دارنده قصد بر انتقال داده‌ها از کنترل‌کننده اولیه به ثانویه داشته باشد، از آنجا که در پروسه پردازش این امر امکان‌پذیر نمی‌باشد، به طریق اولی در پروسه پس از پردازش اطلاعات نیز امر مذکور ممکن نخواهد بود. ضمن اینکه پردازش اطلاعات در راستای منافع عمومی از آنجا که به منزله استثنایی بر حق تبادل داده تلقی می‌گردد و یکی از مقدمات انجام پردازش، ضرورت ذخیره اطلاعات پردازش شده می‌باشد، لذا حق حذف اطلاعات مورد پردازش در زمینه حفظ و رعایت منافع عمومی نیز امکان‌پذیر نخواهد بود. درخصوص دیگر داده‌ها نیز چنین است. از آنجا که حق تبادل داده توسط کنترل‌کننده به محض ورود داده به مرحله پردازش از وی سلب می‌گردد، سلب حق مزبور در مراحل بعدی و حتی ذخیره داده‌های پردازش شده توسط کنترل‌کننده ابتدایی نیز محرز خواهد بود.

اقدامات سیاست‌گذاران

محوریت پژوهش حاضر در تحلیل حق بر تبادل اطلاعات در سازوکار عملکرد ابزارهای اینترنت اشیا، در صورتی ماهیتی کاربردی خواهد داشت که امکان به‌کارگیری ابزارهای اینترنت اشیا در کشور ایران فراهم گردد. البته همان‌طور که در مباحث ابتدایی نیز بیان شد، در وضعیت موجود، با توسعه فناوری اطلاعات، سیاست‌گذاری تقنینی و اجرایی در این زمینه نیز جزو ضروریات تلقی می‌گردد. اما اجرای این امر در کشور ایران منوط به طراحی برنامه‌هایی است که اقدامات سیاست‌گذارانه ذیل می‌تواند این روند را بیش از پیش بهبود بخشد:

تصویب قوانین جدید و اصلاح قوانین موجود

اولین چالشی که نظام حقوقی ایران در زمینه ابزارهای اینترنت اشیا با آن مواجه است، خلاء قانونی است. در این نظام تنها در مواد (۵۸) و (۵۹) قانون تجارت الکترونیکی، تنها به‌صورت جزیی به چگونگی پردازش اطلاعات خصوصی اشاره نموده است. این در حالی است که نه تنها این دو مقرره به‌صورت کاملا مبهم این موضوع را بیان کرده‌اند، بلکه خلاء قانونی، روند به کارگیری ابزارهای اینترنت اشیا در ایران را با چالش‌های جدی مواجه می‌گردانند. همان‌طور که بیان شد، ابزارهای اینترنت اشیا، برای انجام وظایف از پیش تعیین شده، نیاز به جمع‌آوری اطلاعات از محیط پیرامون دارند که اطلاعات خصوصی، جزیی از اطلاعات جمع‌آوری شده توسط این ابزارها هستند. اولین بحث در زمینه پردازش اطلاعات خصوصی، شناسایی این اطلاعات است. این در حالی است که تنها مقرره مصوب در نظام حقوقی ایران به‌صورتی کاملا 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 هرعنوان غیرقانونی است.»

در نگاه اول نص ماده قانونی مزبور این امر را به ذهن متبادر 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 نه تنها هیچ مشکلی از نظام حقوقی ایران را حل و فصل نمی‌نماید، بلکه چند پهلو بودن مفاد ماده بر ابهامات موجود در این زمینه و فلسفه تصویب آن بیش از پیش دامن می‌زند. اگر اطلاعات خصوصی اشخاص، داده‌هایی واجد ارزش تلقی می‌شوند که ماده (۵۹) قانون تجارت الکترونیکی [۲۶]، علاوه بر مفاده ماده (۵۸)، شرایط خاص دیگری را 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 غیر قابل شمول ماده (۵۸) را شناسایی نمود. صرف نظر از آنکه حقیقتا قصد سیاست‌گذاران از تصویب این ماده احصا یا بیان مصادیق داده‌های خصوصی بوده و در تالیف 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 اینترنت اشیا 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.

این در حالی است که ماده (۴) آیین‌نامه عمومی حفاظت از اطلاعات خصوصی اتحادیه اروپا مقرر می‌دارد: «اطلاعات خصوصی به هرگونه اطلاعاتی که به‌صورت 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.»[۲۷]

مطابق با مفاد ماده فوق داده‌های شخصی داده‌هایی هستند که در شناسایی مستقیم یا غیر مستقیم یک شخص حقیقی می‌توانند به‌کار گرفته شوند. از این رو اطلاعات مربوط به اشخاص حقوقی در نظام حقوقی اتحادیه اروپا جزء مجموعه داده‌های شخصی محسوب نشده و در ذیل مقررات حاکم بر این عنوان قرار نمی‌گیرند [۲۸]. علاوه بر آن مطابق با پاراگراف ششم از اعلامیه کارگروه ماده (۲۰)۹ این مقررات [۲۹] 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 بسیط 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 [۳۰].

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 صرف نظر 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 تلفن همراه یا خودرو وجود داشته باشد نیز قابلیت قرارگیری در ذیل عنوان داده‌های خصوصی را برخوردار می‌باشند [۳۱].

علاوه بر آنچه بیان شد، نظام حقوقی ایران در زمینه سایر ابعاد حقوقی مرتبط با سازوکار عملکرد ابزارهای اینترنت

اشیا مانند قانون حاکم بر دعاوی، دادگاه صالح در رسیدگی به دعاوی، حقوق قانونی در نظر گرفته شده برای دارندگان اطلاعات، چگونگی اعطای مجوز فعالیت به پردازندگان و کنترل‌کنندگان ابزارهای اینترنت اشیا، چگونگی تبادل داده‌های فراملی، چگونگی نظارت بر عملکرد پردازندگان و کنترل‌کنندگان و چگونگی جبران خسارات، فاقد هرگونه مقرره قانونی می‌باشد که ضرورت تصویب قوانین در این زمینه را نیز ایجاب می‌کند.

پیاده‌سازی زیرساخت‌های به‌کارگیری ابزارهای اینترنت اشیا و آگاهی بخشی به مردم

همان‌طور که بیان شد، ابزارهای اینترنت اشیا برای امکان ارتباط با یکدیگر یا عامل انسانی از طریق اتصال به بسترهای متمرکز یا نامتمرکز را دارند. با توسعه فناوری اطلاعات، امروزه بسترهای نامتمرکز مانند بلاک‌چین [۳۲] به اقصی نقاط جهان گسترده و در آینده نزدیک نوید جایگزینی این بستر با بسترهای متمرکز مانند صفحه گسترده جهانی (شبکه وب) داده می‌شود. این در حالی است که در کشور ایران نه تنها زمینه پیاده‌سازی این بستر نه از نظر تقنینی و نه از نظر اجرایی فراهم نشده است، بلکه عموم مردم نیز آگاهی از ماهیت و چگونگی تبادل اطلاعات در این بستر ندارند. این موضوع می‌تواند به‌کارگیری ابزارهای اینترنت اشیا در ایران را با مشکل مواجه گرداند. ضمن اینکه عملکرد صحیح این ابزارها را نیز تحت‌الشعاع قرار می‌دهد.

موضوع دوم آگاهی بخشی به مردم درخصوص حقوق قانونی خود و چگونگی کار با ابزارهای اینترنت اشیا می‌باشد. حقوق پیش‌بینی شده در قوانین برای دارندگان ابزارهای اینترنت اشیا از جمله حق بر تبادل داده، در صورتی قابلیت اجرایی خواهد داشت، که دارنده اطلاعات از حقوق قانونی خود آگاهی داشته و آنها را به مرحله اجرایی برساند. در کنار این موضوع، نحوه عملکرد ابزارهای اینترنت اشیا و ضرورت جمع‌آوری اطلاعات از محیط پیرامون در سازوکار عملکرد این ابزارها نیز باید به متقاضیان استفاده از آنها آموزش داده شود تا با آگاهی کامل نسبت به استفاده از این ابزارها در محیط پیرامون خود اقدام نمایند.

نظارت دولت بر عملکرد کنترل‌کنندگان و پردازندگان اطلاعات

کنترل‌کنندگان ابزارهای اینترنت اشیا و پردازندگان اطلاعات، نقش اصلی در روند عملکرد این ابزارها بر عهده دارند. این در حالی است که دسترسی آنها به اطلاعات جمع‌آوری شده از سوی این ابزارها، می‌تواند زمینه سوءاستفاده از داده پیام‌ها را ایجاب نماید. خصوصا در مواردی که کنترل‌کننده یا پردازنده در خارج از کشور متبوع دارنده ابزار مستقر بوده و اطلاعات جمع‌آوری شده لزوما باید به نهادی که در کشور بیگانه مستقر می‌باشد، منتقل گردد. این موارد ضرورت نظارت دولت بر عملکرد این نهادها را ایجاب میکند. در این زمینه دولت متبوع باید چند اولویت را مدنظر قرار دهد. اول چگونگی اعطای مجوز فعالیت به این ابزارها می‌باشد. دوم پس از اعطای مجوز فعالیت، چگونگی نظارت بر عملکرد آنها که ضرورتا با تخصیص صلاحیت به یک نهاد نظارتی و تعیین یک نماینده برای بازرسی مکرر از این نهادها باید صورت پذیرد، باید تعیین تکلیف شود. سومین مورد نیز پیش‌بینی ضمانت اجراهای مدنی، کیفری و انظباطی می‌باشد که در موارد مقتضی توسط حاکمیت اجرا شود.

۴. نتیجه‌گیری

اینترنت اشیا یکی از فناوری‌های نوظهور عصر جدید می‌باشد که علی‌رغم کارکردهای فراوان در حوزه‌های صنعت و تجارت، به جهت تقابل مستقیم با اطلاعات خصوصی اشخاص نگرانی‌هایی را برای مجامع قانون‌گذاری کشورهای توسعه یافته پدید آورده است. این امر منجر به تصویب آیین‌نامه مصوب ۲۰۱۶ در اتحادیه اروپا و پیش‌بینی مقررات متعدد در جهت بخشی به نحوه عملکرد ابزارهای بهره‌مند از این فناوری و نهادهای دخیل در پروسه عملکرد ابزارهای

مذکور شده است. تحلیل و ارائه راه‌حل‌های مناسب بر چالش‌های مطرح شده در نظامات حقوقی کشورهای توسعه یافته، می‌تواند یکی از راه‌کارهای پیاده‌سازی این فناوری در کشورهای در حال توسعه مانند ایران نیز تلقی گردد.

حق بر تبادل داده یکی از حقوقی است که در ماده (۲۰) آیین‌نامه مصوب ۲۰۱۶ مورد تصریح سیاست‌گذاران اتحادیه اروپا قرار گرفته است. مطابق با اصل مذکور، دارنده اطلاعات قادر خواهد بود تا ادامه پروسه نظارت و کنترل بر عملکرد ابزار را از کنترل‌کننده اولیه بر ثانویه منتقل نماید. اما این حق تنها تا زمانی پا برجا خواهد بود که داده‌های خصوصی فرد تحت فرایند پردازش توسط کنترل‌کننده اولیه و پردازنده قرار نگرفته باشد. انتقال پروسه پردازش از یک کنترل‌کننده به کنترل‌کننده دیگر حتی درصورتی که ابزار هوشمند محصول انحصاری تولیدکننده اولیه باشد، درصورت طراحی پروتکلی توسط کنترل‌کننده دیگر که قادر بر کنترل ابزار مذکور باشد به‌منزله نقض حق انحصاری او تلقی نمی‌گردد. اما پیاده‌سازی سازوکار عملکرد ابزارهای مذکور در نظام حقوقی ایران علاوه بر سیاست‌گذاری‌های تقنینی بیان شده، نیازمند برخی سیاست‌گذاری‌های اجرایی خواهد بود که پیش‌بینی شرایط و کیفیت عملکرد کنترل‌کننده و پردازندگان اطلاعات مهم‌ترین مسأله پیش روی این نظام می‌باشد. از آنجا که عموم کنترل‌کنندگان ابزارهای مذکور و پردازندگان اطلاعات شرکت‌های خارجی می‌باشند که در صورت نیاز به فعالیت یا مبادرت به تاسیس شعبه در ایران نموده یا در خارج از ایران نسبت به کنترل و پردازش اطلاعات مبادرت می‌کنند، تضمین امنیت داده‌های خصوصی یکی از چالش‌های اساسی حکومت در مواجهه با این ابزارها خواهد بود. چرا که هرگونه سوءاستفاده از اطلاعات شخصی اشخاص می‌تواند عواقب جبران ناپذیری نیز به‌همراه داشته باشد. از این رو جهت بخشی بر نحوه فعالیت این نهادها یکی از الزامات نظام حقوقی ایران تلقی می‌گردد. علاوه بر آن در صورتی که در داخل ایران نیز نهادهایی تمایل بر فعالیت به‌عنوان پردازنده و کنترل‌کننده داشته باشند، نحوه اعطای صلاحیت به این سازمان‌ها و کیفیت نظارت بر عملکرد آنها نیز دیگر مسأله پیش‌روی نهادهای حکومتی می‌باشد که نیازمند سیاست‌گذاری تقنینی است.

پی‌نوشت

1- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

2- 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.

3- Right to Access.

4- Politoa & Etc, 2018, 2.

5- Introna, 1997, 265.

6- big data.

7- ‘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;

8- Gymrek, 2013, 323.

9- Rubinstein, 2013, 78.

10- politoa & Etc, 2018, 4.

11- European Data Protection Supervisory.

12- WP29, Opinion 8/2014 (n 5) 4.

13- Lindqvist, 2019.

14- WP29, Opinion 1/2010 (n 11) 8.

15- De Hert, 2018,196.

16- Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. processing is necessary for compliance with a legal obligation to which the controller is subject;

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1)

17- the processing is carried out by automated means.

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

the processing is carried out by automated means.

In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

18- De Hert, 2018,197.

۱۹- این پروتکل‌ها بسته به ماهیت خود امکان عملکرد ابزار در اتصال به بسترهای متمرکز مانند صفحه گسترده جهانی(World Wide Web) یا بسترهای نامتمرکز مانند بلاک چین را فراهم می‌آورند. به‌عنوان مثال پروتکل‌های 6LOWPAN امکان استفاده بهینه از صفحه گسترده جهانی برای ابزارهای دارای پهنای باند کوتاه را فراهم می‌آورند. (Lunden,2019) همچنین پروتکل‌های Bluetooth Low Energy امکان استفاده بهینه از باتری تلفن همراه یا سایر ابزارهای بهره‌مند از باتری در هنگام تبادل داده پیام را فراهم می‌کنند. (Gottipati,2019) در حوزه بسترهای نامتمرکز نیز می‌توان به پروتکل‌های Graphene اشاره نمود که امکان انجام فرایند اثبات کار(Proof of Work) یا انجام مبادلات الکترونیکی را با سرعت بالاتر فراهم می‌نمایند. همچنین پروتکل‌های هایپرلجر(Hyperledger) امکان ارتباط میان بلاک چین پیاده‌سازی شده در سیستم سازمان‌های مختلف را جهت تبادل داده پیام‌ها در محیطی ایمن فراهم می‌آورند.

Top-10 blockchain protocols changing the world in 2019 http://risingblockchain.com/top10-blockchain-protocols-2019/.

۲۰- برای مشاهده مفهوم‌شناسی و کارکرد قراردادهای هوشمند رک: صادقی، حسین، ناصر، مهدی، (۱۳۹۷)، واکاوی نقش قراردادهای هوشمند در توسعه نظام ثبت الکترونیکی اسناد، فصلنامه دیدگاه‌های حقوق قضایی ، دوره ۲۳، شماره ۸۴.

21- Lunden,2019.

22- Fair Use.

23- De Hert, 2018, 197.

24- GRAEF, 2015, 508.

25- Swire, Lagos, 2013, 347.

۲۶- 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 هنگام جمع‌آوری برای شخص موضوع «داده پیام» شرح داده شده جمع‌آوری گردد و تنها برای اهداف 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 را محو 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.

27- 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.

28- Van der sloot, 2017, 23.

۲۹- پس از لازم‌الاجرا شدن 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 لازم‌الاجرا شدن آن صورت پذیرد.

30- European Commission, 2019.

31- Finck & Pallas, 2020, 16.

۳۲- برای مشاهده ماهیت و چگونگی تبادل اطلاعات در بستر بلاک چین رک: اسلامی تبار، امیر، ناصر، مهدی، (۱۳۹۹)، کارکرد بلاک چین در حمایت از کپی‌رایت، فصلنامه پژوهش حقوق خصوصی، دوره ۸ ، شماره ۳۰، صص ۹-۳۸.

منابع

صادقی، حسین و مهدی ناصر (۱۳۹۷)، «واکاوی نقش قراردادهای هوشمند در توسعه نظام ثبت الکترونیکی اسناد»، فصلنامه دیدگاه‌های حقوق قضایی، دوره ۲۳، شماره ۸۴، صص ۱۰۱-۱۲۴.

اسلامی تبار، امیر و مهدی ناصر (۱۳۹۹)، «کارکرد بلاک چین در حمایت از کپی رایت»، فصلنامه پژوهش حقوق خصوصی، دوره ۸، شماره ۳۰، صص ۹-۳۸.

Eugenia Politou, Efthimios Alepis and Constantinos Patsakis,(2018), Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, Journal of Cybersecurity, 1-20

European Commission, (accessed 13 Nov2019) 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,

Finck Michèle,Pallas Frank,(2020),They who must not be identified—distinguishing personal from non-personal data under the GDPR«,International Data Privacy Law,Volume10,Issue1,February,pp11-36

GRAEF, I, (2015),Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union (22 July 2013).Telecommunications Policy, Vol. 39, No. 6, p. 502-514.

Gymrek M, McGuire AL, Golan D,(2013). Identifying personal genomes by surname inference. Science ;339 :321-4

Hari Gottipati, (Last Visited 22 July 2019) With iBeacon, Apple is going to dump NFC and embrace the Internet of Things, Gigaom, available at https://gigaom.com/2013/09/10/with-ibeacon-apple-is-going-to-dump-on-nfc-andembrace-the-internet-of-things

Ingrid Lunden, (Last Visited 8 July 2019) ARM Acquires Internet of Things Startup Sensinode to Move Beyond Tablets and Phones, Techcrunch ,http://techcrunch.com/2013/08/27/arm-acquires-internet-of-things-startup-sensinodeto-move-beyond-tablets-and-phones

Introna LD.(1997), Privacy and the computer: why we need privacy in the information society. Metaphilosophy; 28:259-75.

Lindqvist Jenna,(2017), New challenges to personal data processingagreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?, International Journal of Law and Information Technology, Downloaded from https://academic.oup.com/ijlit/advance-article-abstract/doi/10.1093/ijlit/eax024/4769343

Nest.com web page(accessed 18 June 2019) <https://nest.com/uk/thermostat/meet-nest-thermostat/

Swire P,.Lagos,Y (2013), Why the Right to Data Portability Likely Reduces ConsumerWelfare: Antitrust and Privacy, Critique Public Law and LegalTheoryWorking,Paper Series No.204,May 31 , 347.

Rubinstein IS. (2013) Big data: the end of privacy or a new beginning? Int Data Privacy L; 3:74-87

Top-10 blockchain protocols changing the world in 2019 http://risingblockchain.com/top10-blockchain-protocols-2019/

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', 31 Computer Law and Security Review, Volume 13, Issue 8, pp 18-34