فصلنامه حقوق اداری (علمی - پژوهشی)
سال هفتم، شماره ۲۳، تابستان ۱۳۹۹

چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا

مسلم آقایی طوق[۱]؛ مهدی ناصر[۲]

تاریخ دریافت: ۱۳۹۸/۰۷/۲۰
تاریخ پذیرش: ۱۳۹۸/۱۰/۱۸

چکیده

اینترنت اشیا، به عنوان یکی از فناوری‌های نوظهور قرن اخیر، به تکنولوژی ایجاد ارتباط میان ابزارهای الکترونیکی با یکدیگر یا عامل انسانی، اطلاق می‌گردد. ابزارهای دربردارنده این فناوری در انجام وظایفی که مطابق با پروتکلهای پیش‌نویس شده به پردازنده آنها داده شده است، نیازمند جمع‌آوری و پردازش اطلاعات به‌دست آمده از محیط پیرامون خود، از جمله اطلاعات خصوصی اشخاص، هستند. چالش‌های مختلفی در ارتباط با اینترنت اشیا وجود دارد؛ مانند امکان افشای اطلاعات خصوصی اشخاص و یا تحدید حقوق مالکانه آنها و یا حتی روابط میان پردازنده و کنترل‌کننده و مسأله مسئولیت مدنی آنها در برابر مصرف کنندگان. مدیریت این چالشها نیازمند برخورداری از یک نظام حقوقی مشخص است که بتواند احکام لازم را در راستای مدیریت مسائل مربوط به اینترنت اشیا، در خود جای دهد. تجربه مقررات‌گذاری اتحادیه اروپا در این‌خصوص می‌تواند مورد توجه قانونگذار ایران قرار گیرد.

واژگان کلیدی: اینترنت اشیا، کنترل‌کننده، پردازنده، قراردادهای پردازش داده‌های خصوصی.

۱. عضو هیأت علمی دانشگاه علوم قضایی و خدمات اداری، (نویسنده مسئول) moslemtog@yahoo.com
۲. دانشجوی دکترای حقوق خصوصی دانشگاه علوم قضایی و خدمات اداری
mn.ujsasac0077@yahoo.com

[DOI: 10.29252/qjal.7.23.33]

مقدمه

امروزه تحت تاثیر تبادل داده پیام‌های الکترونیکی میان نهادهای عمومی یا خصوصی، مسأله حفاظت از اطلاعات، به امری مهم تبدیل شده است. این اطلاعات در دو گروه اطلاعات عمومی و شخصی، طبقه‌بندی می‌شوند. از آنجا که اطلاعات شخصی اتباع کشورها به عنوان سرمایه‌های این کشور تلقی و دسترسی غیرمجاز بیگانگان به این اطلاعات، می‌تواند به نوعی امنیت ملی کشورها را تحت الشعاع قرار دهد؛ کشورهای جهان نیازمند پیش‌بینی سازوکارهای مناسب از بعد سیاست‌گذاری‌های تقنینی و اجرایی هستند. به‌عنوان مثال، دسترسی بیگانگان به اطلاعات بیومتریک اتباع یک کشور، امکان ساخت سلاح‌های کشتار جمعی زیستی را به دشمنان می‌دهد که تنها منجر به نابودی گونه خاصی از افراد با ژنتیک متفاوت می‌شوند؛ یا در اختیار گرفتن اطلاعات مربوط به نظام پرداخت حقوق کارکنان یک کشور توسط بیگانگان، می‌تواند زمینه دستیابی آنها به میزان ارز قابل گردش در بازارهای پولی یک کشور را فراهم آورد. مسائل این چنینی منجر به تصویب دستورالعمل حفاظت از داده پیام‌های الکترونیکی در اتحادیه اروپا در سال ۱۹۹۵ و پیش‌بینی مسئولیت‌های حقوقی برای ناقضان قواعد این دستورالعمل گردید.

در حال حاضر، عملکرد فراملی نهادهای موجود در یک کشور منوط به تبادل داده پیام با بیگانگان است. نهادهای مبدأ که نسبت به ارسال اطلاعات اقدام می‌نمایند، نهادهای کنترل‌کننده و سازمان‌هایی که با دریافت اطلاعات نسبت به پردازش آنها و انجام اعمال مورد نظر نهاد کنترل-کننده اقدام می‌کنند؛ پردازنده داده خطاب می‌شوند. محدوده موضوعی دستورالعمل یادشده، اتحادیه اروپا در حوزه حفاظت از داده‌پیام‌های مربوط به اطلاعات شخصی افراد است. از آنجا که پردازندگان داده‌پیام‌ها می‌توانند در هر نقطه از جهان باشند و عملا دسترسی به آنها جز در موارد وجود قرارداد متقابل میان کشورهای متبوع دو سازمان امکان پذیر نیست؛ محوریت مسئولیت در حفاظت از اطلاعات شخصی افراد بر نهادهای کنترل‌کننده اعمال می‌گردد. البته این نهادها نیز با انعقاد قراردادهای خصوصی با پردازندگان می‌توانند نسبت به پیش‌بینی الزامات حفاظت از اطلاعات مورد تبادل، با استناد به مسئولیت قراردادی، نسبت به اقامه دعوی علیه این سازمان‌ها اقدام نمایند (Grant&Etc, 2019:1).

با توجه به توسعه روزافزون فناوری و ایجاد ابزارهای دیجیتالی جمع‌آوری، پردازش و تبادل‌کننده اطلاعات شخصی؛ مسأله حفاظت از داده‌پیام‌های خصوصی، وجهه‌ای جدید یافته است. درواقع، ابزارهای اینترنت اشیا با برخورداری از پروتکلهای از پیش‌طراحی‌شده، نسبت به جمع‌آوری

[DOI: 10.29252/qjal.7.23.33]

اطلاعات محیط پیرامون خود، پردازش و ارسال اطلاعات به کنترل‌کنندگان یا پردازندگان اقدام می‌نمایند. از آنجا که این فناوری، واجد زوایای گوناگونی است که مدنظر دستورالعمل مصوب ۱۹۹۵ اتحادیه اروپا قرار نگرفته بود، سیاست‌گذاران در این اتحادیه مبادرت به تصویب مقرراتی جدید با عنوان دستورالعمل عمومی حفاظت از اطلاعات اتحادیه اروپا در سال ۲۰۱۶ نمودند که در ماه می سال ۲۰۱۸ لازم‌الاجرا گردیده است (Lindqvist, 2017:2).–از جمله نقاط ضعف دستورالعمل پیشین، عدم وجود حکم خاص در پیش‌بینی مسئولیت قانونی برای پردازندگان، عدم امکان پیش‌بینی میزان مسئولیت پردازندگان یا کنترل‌کنندگان در سازوکار عملکرد ابزارهای اینترنت اشیا، عدم وجود حکمی خاص در نحوه جبران خسارات ناشی از عملکرد ماشینها و... بیان شده است. دستورالعمل جدید با رفع خلاءهای مقررات پیشین و ایجاد تحولات فراوان در میزان مسئولیت ناقضان این مقررات، نحوه جبران خسارات وارده و پیش‌بینی احکام خاص در موارد وجود یا عدم‌وجود قراردادهای خاص میان کنترل‌کننده و پردازنده (ماده ۲۸)، امروزه مبنای عملکرد دادگاه‌های حاکم در اتحادیه اروپاست(Grant&Etc, 2019:3) .

در ادامه، در بخش اول، مفاهیم مربوط به متغیرهای پژوهش همچون اینترنت اشیا بررسی خواهد شد. در بخش دوم، چالش‌هایی که درخصوص حفاظت از داده‌های اشخاص وجود دارد و در بخش سوم، بایسته‌های انعقاد قرارداد میان پردازنده و کنترل‌کننده مورد بحث واقع خواهد شد. روش پژوهش، تحلیلی و در مواردی هنجاری و مبتنی بر رویکرد تطبیقی است.

۱- مفهوم‌شناسی متغیرهای پژوهش

پیش از ورود به تحلیل موضوع، تبیین و ارائه تعریف از مفاهیم بنیادین مرتبط ضروری است؛ از این‌رو، گفتار حاضر در دو بند ذیل، مبادرت به تحلیل مفهوم اینترنت اشیا و کنترل‌کنندگان و پردازندگان اطلاعات می‌نماید.

۱-۱- اینترنت اشیا

ماده ۲۹ اعلامیه مرکز نظارت بر داده‌پیام‌های اتحادیه اروپا مصوب ۲۰۱۰ با الحاقات و اصلاحات ۲۰۱۵،[1] در تعریف اینترنت اشیا بیان می‌دارد: «اینترنت اشیا، زیرساخت‌هایی هستند که در آن، میلیاردها حسگر تعبیه‌شده در دستگاه‌های کاربردی روزمره برای ضبط، پردازش، ذخیره و انتقال داده‌ها طراحی شده است و همان‌طور که از قابلیت ارتباط با عامل انسانی برخوردار

1. European Data Protection Supervisory

[DOI: 10.29252/qjal.7.23.33]

هستند؛ با بهره مندی از شناسه‌های منحصر به فرد، با دستگاهها یا سیستم‌های دیگر با استفاده از قابلیت‌های شبکه، تعامل برقرار می‌کنند.»؛[1] به عبارت دیگر، ابزارهای اینترنت اشیا، نوعی ابزارهای هوشمندند که با تعبیه پروتکل‌های منحصر به فرد به پردازنده آنها، همانند انسان؛ قابلیت دریافت و پردازش داده‌پیام‌ها برای انجام وظایف از پیش‌تعیین شده را کسب می‌کنند. این ابزارها، قابلیت اتصال به بسترهای متمرکز مانند اینترنت یا نامتمرکز مانند بلاک‌چین را دارند و از این طریق، از قابلیت ارتباط از راه دور با انسان یا دیگر سیستم‌ها برخوردار هستند. امروزه، ابزارهای متعددی ازجمله ساعت‌ها و تلویزیون‌های هوشمند طراحی شده‌اند که هر یک با برخورداری از پروتکلهای خاص، نسبت به انجام وظایف تعیین‌شده، اقدام می‌کنند(Nest,2019). علاوه بر آن، کاربرد ابزارهای اینترنت اشیا در اقلام مختلفی از جمله ساخت هواپیماهای بدون سرنشین نسل سوم، کنترل و مدیریت امور بازارهای مالی در کشورهای توسعه‌یافته نیز بر متخصصین این امر مشهود است.

۲-۱- پردازنده و کنترل‌کننده

بند ۷ ماده ۴ دستورالعمل مصوب ۲۰۱۶ اتحادیه اروپا در تعریف کنترل‌کننده بیان می‌دارد: «کنترل‌کننده؛ شخص حقیقی یا حقوقی، مرجع عمومی، نمایندگی یا هر نهاد دیگری است که به تنهایی یا به طور مشترک با دیگران، اهداف و وسایل پردازش داده‌های شخصی را تعیین می‌کند.»؛ به عبارت دیگر، ابزارهای اینترنت اشیا دارای سازندگانی هستند که به اطلاعات این ابزارها دسترسی دارند و از امکان کنترل آنها بهره‌مند هستند. این اشخاص حقیقی یا حقوقی که کنترل‌کننده نامیده می‌شوند؛ مطابق با نقش خود در عملکرد یک ابزار، می‌توانند شناسایی شوند. به عبارتی، اگرچه اطلاق عنوان کنترل‌کننده از پردازنده داده‌پیام جداست؛ اما در صورتی که پردازش داده توسط ابزار اینترنت اشیا صورت پذیرد؛ دسترسی کنترل‌کننده به اطلاعات پردازش شده، هرچند تحت خط‌مشی تعیین‌شده توسط وی صورت پذیرد؛ نمی‌تواند عنوان پردازنده را بر این اشخاص بار نماید. این امر در شماره ۱۱ از بند ۸ ماده ۲۹ اعلامیه مذکور نیز مورد تاکید قرار گرفته است.[2] در مقابل، به تعبیر بند ۸ ماده ۴

1. WP29, Opinion 8/2014 (n 5) 4.
2. WP29, Opinion 1/2010 (n 11) 8.

[DOI: 10.29252/qjal.7.23.33]

دستورالعمل مرقوم، «پردازنده؛ شخصی حقیقی یا حقوقی، مقامات دولتی یا هر نهاد دیگری است که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند.»؛ بنابراین، سازو کار عملکرد پردازشگر، تحت خط‌مشیی است که توسط کنترل‌کننده تعیین می‌گردد؛ از این‌رو، در صورتی که خط‌مشی و چگونگی پردازش داده‌پیام‌ها توسط پردازشگر تعیین گردد؛ وی دارای عنوان کنترل‌کننده است و مسئولیت‌های قانونی پیش‌بینی شده برای کنترل‌کننده، برای وی نیز قابل اعمال خواهد بود. این امر اعم از تصریح یا تبانی بر وجود فرایند مذکور در قراردادهای دوطرف، کنترل‌کننده یا پردازنده و حکم عرف در تعریف مسئولیت حقوقی مذکور، خواهد بود (بند ۱۰ ماده ۲۸). 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 این‌رو، 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).

۲- چالش‌های موجود در راستای حفاظت از داده‌های خصوصی

حفاظت از داده‌های خصوصی، مهم‌ترین مسأله در سازوکار عملکرد ابزارهای اینترنت اشیاست که در زیر در دو بند به مهم‌ترین چالش‌های موجود در این زمینه پرداخته می‌شود.

۲-۱- چالش‌های انعقاد قراردادهای تولید و مصرف‌کننده

هنگام به کارگیری ابزارهای اینترنت اشیا، اطلاعات مصرف‌کنندگان این ابزارها به همراه افرادی که مصرف‌کنندگان با آنها در ارتباط هستند و حتی اطلاعات محیط پیرامون آنها، قابل دریافت توسط این ابزارهاست؛ از این‌رو، در صورتی که در اطلاعات دریافت‌شده، سوءاستفاده‌ای صورت پذیرد؛ می‌تواند اثرهای غیرقابل جبرانی برجای بگذارد. (Wendehorst, 2016: 191) از طرف دیگر، خرید چنین ابزارهایی از تولیدکنندگان آنها در قالب قراردادهای الحاقی صورت می‌پذیرد؛ از این‌رو، مصرف‌کنندگان ملزم خواهند بود، تمام شرایط از پیش‌تعیین‌شده را بدون برخورداری از حق شرط یا قدرت چانه‌زنی قبول و قرارداد را منعقد نمایند. این امر، نه‌تنها اختیار مصرف‌کنندگان در انعقاد قراردادها را تحت‌الشعاع قرار می‌دهد (Walden&Etc,2016:3)؛ بلکه گاه منجر به پیش‌بینی شروطی غیرمنصفانه

[DOI: 10.29252/qjal.7.23.33]

در قرارداد می‌شود (Peppet,2019:686)؛ حتی در مواردی، مفاد قرارداد به نحوی گنجانده می‌شود که به جهت برخورداری عبارات از بار حقوقی، بسیاری از مصرف‌کنندگان از درک مفهوم عبارات نوشته شده عاجز بوده، بدون آگاهی به مفاد آن شروط نسبت به انعقاد قرارداد اقدام می‌کنند.

چالش دیگر، مسأله تحدید مالکیت دارندگان ابزارها توسط تولیدکنندگان آنهاست که به صورت ضمنی یا جداگانه، نسبت به قرارداد فروش صورت می‌پذیرد. در دنیای حاضر، استفاده مالکان از ابزارهای اینترنت اشیا به دلیل مسأله حق انحصاری تولیدکننده از بهره‌برداری از فناوری ابداعی خود، به شکلی بروز نموده است که در صورت خرابی یا نقص ابزار، دارنده از تعمیر شخصی آن محروم بوده و باید طبق قرارداد به نمایندگی‌های تعیین‌شده توسط تولیدکننده مراجعه نماید. این امر در مواردی می‌تواند منجر به ایجاد مشکل گردد. در این خصوص می‌توان به پرونده جان‌دیر، تولیدکننده تراکتورهای هوشمند اشاره کرد هنگامی که تراکتور دارنده با نقص فنی هنگام برداشت محصول مواجه گردید و به جهت ضرورت، دارنده شخصا مبادرت به تعمیر آن کرد؛ شرکت مزبور از طریق فن‌آوری کنترل از راه‌دور[1] مبادرت به از کارانداختن تراکتور نمود که این امر منجر به صدمات مالی بسیار زیادی به دارنده زمین کشاورزی گردید (Coll&Etc,2019:33) .

چالش‌های بیان شده در این بخش، به طور جدی قابلیت طرح در نظام حقوقی ایران را نیز دارد. در نظام حقوقی ایران، تنها اسناد مصوب قانونی در زمینه حفاظت از اطلاعات خصوصی اشخاص، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی هستند که پردازش اطلاعات شخصی اشخاص را منوط به شرایطی نموده‌اند. متاسفانه متن مبهم این مواد، اجرای این مقررات در سازوکار انعقاد قرارداد میان تولید و مصرف‌کننده را با مشکل مواجه می‌کند؛ چرا که متن ماده ۵۸ این قانون تنها مبین مقرراتی در زمینه چگونگی پردازش اطلاعات است؛ در حالی که هیچ حکمی در خصوص کیفیت جمع‌آوری داده‌های مذکور و محدودیت‌های موجود در آن مواد مشاهده نمی‌گردد. ضمن اینکه متن ماده ۵۸ به گونه‌ای تنظیم شده است که پردازشِ داده‌هایِ مبین ریشه‌های قومی، نژادی، عقیدتی، مذهبی، اخلاقی و داده‌هایِ مربوط به وضعیت جسمی، روانی و جنسی اشخاص را منوط به شرایط مقرر در مواد ۵۸ و ۵۹ نموده است و نص ماده، گویای تفکیک میان این گروه

1. Remote Control

[DOI: 10.29252/qjal.7.23.33]

از داده‌ها و دیگر داده‌های شخصی است. اگرچه به نظر نگارندگان، این موضوع ناشی از مسامحه قانونگذار بوده و وی پردازش انواع داده‌های خصوصی را در متن این ماده مدنظر داشته و امکان الغای خصوصیت از مصادیق مذکور را به خواننده اعطا می‌کند؛ اما نص مبهم ماده مذکور و البته نبود مقرره‌ای در زمینه کیفیت جمع‌آوری اطلاعات، ضرورت اصلاح این مقررات را ایجاب می‌کند. در زمینه نظارت بر کیفیت انعقاد قراردادها و پیشگیری از تحدید مالکیت دارندگان نیز دولت نیازمند پیش‌بینی مراجع صلاحیت‌دار نظارتی، ارائه دستورالعمل بر نحوه فعالیت تولیدکنندگان و حتی ارائه نمونه قراردادهای پیش‌نویس‌شده به نهادهای مذکور است تا از انعقاد هرگونه قرارداد دیگری از سوی آنها جلوگیری گردد. در نهایت امر نیز ارائه آگاهی لازم به عموم جامعه از طریق ابزارهای ارتباط جمعی مانند تلویزیون یا شبکه‌های اجتماعی از قبیل تلگرام برای افزایش آگاهی عمومی ضروری است.

۲-۲- چالش‌های تعامل میان پردازنده و کنترل‌کننده

به دلیل آنکه ابزارهای اینترنت اشیا برای انجام وظایف از پیش‌تعیین شده مبادرت به جمع‌آوری انبوهی از اطلاعات می‌نمایند؛ در موارد لزوم، پردازش آنها توسط یک پردازنده باید با سرعت و دقت بالا صورت پذیرد تا خللی در راستای عملکرد این ابزار ایجاد نشود. بند ۲ ماده ۱۷ دستورالعمل ۲۰۱۶، کنترل‌کنندگان را ملزم به انتخاب پردازندگانی نموده است که ضمانت کافی در رابطه با اقدامات فنی خود و حفظ حدود ایمنی ارائه نمایند؛ همچنین، پردازندگان نیز جز در موارد وجود رضایت کنترل‌کننده، نمی‌توانند وظیفه پردازش داده را به پردازندگان دیگر محول نمایند. در کنار این موارد، پردازندگان از همکاری مشترک با چند شرکت کنترل‌کننده نیز، جز در موارد وجود رضایت کنترل‌کننده محرومند (بند دوم ماده ۲۸). اگرچه در هنگام انعقاد قرارداد میان کنترل‌کننده و پردازنده، امروزه چنین مسائلی با پیش‌بینی شروط قراردادی مورد حل و فصل قرار گرفته است؛ اما در صورتی که در قرارداد، چنین امری پیش‌بینی نشود؛ سوال موجود، این است که نوع و میزان مسئولیت هر یک از طرفین قرارداد در موارد سوءاستفاده یک طرف، به چه شکل خواهد بود؟ از آنجا که مسأله حفاظت از داده‌های خصوصی افراد از بعد امنیتی واجد اهمیت بالاست؛ به نظر نگارندگان در شرایط کنونی، عدم اجرای مقررات دستورالعمل ۲۰۱۶ به منزله تقصیر متعاملین است؛ از این‌رو، چه در سیستم‌های مبتنی بر مسئولیت مبتنی بر تقصیر (مانند

[DOI: 10.29252/qjal.7.23.33]

ایران) و چه در سیستم‌های مبتنی بر مسئولیت مبتنی بر خطر در هر حال، سهل‌انگاری در اجرای مقررات دستورالعمل یادشده، مصداق تقصیر است؛ اما نحوه تقسیم مسئولیت میان طرفین قرارداد، چالش پیش‌روست. آیا در صورت تقصیر یک طرف، طرف دیگر نیز مسئول جبران خسارت است؟ آیا جبران خسارات وارده به صورت تضامنی صورت می‌پذیرد یا به صورت نسبی؟ آیا کنترل‌کننده، علاوه بر مسئولیت‌های پیش‌بینی شده در دستورالعمل، واجد مسئولیت اضافی نیز هست؟ درخصوص سوالات مذکور می‌توان بیان داشت از آنجا که در نظام حقوقی اتحادیه اروپا، اصل بر مسئولیت نسبی و شخصی اشخاص بوده و مسئولیت عمل غیر یا مسئولیت اضافی حکمی استثنایی می‌باشد که نیازمند تصریح قانون‌گذار است، می‌توان پاسخ سوالات مذکور را منفی دانست. این نظر در نظام حقوقی ایران نیز می تواند قابلیت استناد داشته باشد.

همان‌طور که بیان شد در نظام حقوقی ایران، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی مصوب ۱۳۸۲، پردازش و ذخیره هرگونه داده پیام شخصی اشخاص را منوط به رضایت صریح و موردی دارنده، در محدوده اهداف مشخص تشریح داده شده به دارنده و به میزان متناسب با اهداف تعیین شده، نموده است؛ از این‌رو، در صورتی که هر یک از شرایط بیان شده توسط کنترل‌کنندگان رعایت نشود، به منزله نقض مقررات قانونی و مسئولیت حقوقی وی تلقی می‌گردد؛ اما در زمینه پردازش داده توسط پردازنده و انتقال این وظیفه به پردازنده فرعی، می‌توان در صورت تصریح در قرارداد میان کنترل‌کننده و مصرف‌کننده؛ رضایت دارنده اطلاعات را در طول رضایت کنترل‌کننده تصور نمود؛ از این‌رو، همانند مفاد مقررات مصوب اتحادیه اروپا، در حقوق ایران نیز تا زمانی که رضایت موردی از کنترل‌کننده در این خصوص اخذ نگردد، پردازنده حق بر انتقال قرارداد را نخواهد داشت. بدیهی است در صورتی که در قرارداد میان تولید و مصرف‌کننده، چنین امری مورد تصریح قرار نگرفته باشد؛ اخذ رضایت دارنده اطلاعات در این زمینه اجتناب‌ناپذیر خواهد بود؛ از طرف دیگر، قید عبارت «رضایت صریح» در ماده ۵۸ قانون مرقوم، ضرورت آگاهی بخشی به دارنده در تمامی مراحل پردازش توسط کنترل‌کننده را القا می‌نماید. اما سوال این است که آیا دارنده، امکان انتقال سازوکار جمع‌آوری و پردازش از یک کنترل‌کننده به کنترل‌کننده دیگر یا از یک

[DOI: 10.29252/qjal.7.23.33]

پردازنده به پردازنده دیگر را خواهد داشت؟ در ماده ۲۰ دستورالعمل مصوب ۲۰۱۶ این امر مورد تصریح سیاست‌گذاران اتحادیه اروپا قرار گرفته است. در نظام حقوقی ایران نیز مستند به عبارت فوق الذکر و با فرض اینکه داده پیام‌های شخصی به منزله ملک اشخاص محسوب گردد و به حکم مقررات عام قانون مدنی از جمله ماده ۳۰ این قانون، آنها حق هرگونه تصرف در این اطلاعات را دارند، می‌توان قائل بر نظر مذکور بود.

سوال دیگری که به ذهن می‌رسد این است که چنانچه کنترل‌کننده، تولیدکننده انحصاری ابزاری هوشمند باشد که حق انحصاری کنترل این ابزار را به خود اختصاص داده باشد؛ آیا دارنده حق انتقال داده‌های خود را از آن کنترل‌کننده به کنترل‌کننده دیگر دارا خواهد بود؟ پاسخ به سوال مذکور نیازمند تحلیل کیفیت حق معنوی کنترل‌کننده‌ای است که مالکیت ابزار اینترنت اشیا را به دارنده منتقل نموده است. ابزارهای اینترنت اشیا در انجام وظایف تعیین شده، واجد پروتکل‌هایی هستند که تبیین‌کننده خط‌مشی عملکرد پردازنده محسوب می‌گردد.[۱] در صورتی که کنترل‌کننده-ای با طراحی پروتکلی مشابه با پروتکل کنترل‌کننده ابتدایی، قابلیت نظارت و کنترل بر عملکرد ابزار هوشمند را داشته باشد؛ چنانچه پروتکل طراحی‌شده، به منزله نقض حق انحصاری کنترل-کننده اصلی محسوب نگردد؛ امکان اجرای حق مقررات ماده ۲۰ و حمل و تبادل داده‌های خصوصی دارنده از کنترل‌کننده اصلی به ثانوی موجود است؛ اما چنانچه این امکان وجود نداشته و در هر حال، به‌کارگیری پروتکلی مشابه با پروتکل اصلی به منزله نقض حق معنوی کنترل‌کننده اصلی باشد؛ اجرای حق مذکور نیز با چالش‌هایی مواجه خواهد شد.

پروتکلهای ابزارهای اینترنت اشیا به دلیل برخورداری از خصوصیات منحصر به فرد، واجد حق معنوی برای طراح خود هستند؛ از این‌رو در صورتی که شرکت یا سازمان دیگری نیاز به استفاده

---

۱. 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 بلاک‌چین را فراهم می‌آورند. به عنوان مثال، پروتکلهای 6LOWPAN ، امکان استفاده بهینه از صفحه گسترده جهانی برای ابزارهای دارای پهنای باند کوتاه را فراهم می‌آورند. همچنین پروتکلهای Bluetooth Low Energy ، امکان استفاده بهینه از باتری تلفن همراه یا سایر ابزارهای بهره‌مند از باتری در هنگام تبادل داده‌پیام را فراهم می‌کنند. 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 برای تبادل داده‌پیام‌ها در محیطی ایمن فراهم می‌آورند. (Gottipati,2019).

[DOI: 10.29252/qjal.7.23.33]

از آنها داشته باشد؛ می‌بایست از شرکت سازنده اجازه استفاده را اخذ کند؛ اما به نظر نگارندگان، این امر مانع از تولید پروتکل‌های مشابه توسط دیگر سازمان‌ها نمی‌گردد. این حق مسلم تولیدکننده در ابداع کالا برای رفع حاکمیت انحصاری یک شرکت بر بازار است و در حوزه پروتکل‌های موجود در بسترهای متمرکز و نامتمرکز نیز چنین امکانی فراهم است. به عنوان مثال، پروتکل‌های NEM(XeM) پس از ابداع، امکان انجام وظایف پروتکل‌های هایپرلجر با همان کیفیت و کارایی را فراهم آورده‌اند یا پروتکل‌های NEO و Ethereum به دلیل برخورداری از خصوصیاتی مشابه در انعقاد قراردادهای هوشمند،[1] نقشی مشابه در بستر بلاک‌چین ایفا می‌نمایند (Lunden,2019)؛ اما سوال موجود این است که وجود خصوصیات مشابه در این پروتکل‌ها، طراح اولیه را می‌تواند محق بر اقامه دعوی علیه طراح مشابه نماید؟ به نظر نگارندگان، پاسخ سوال مزبور منفی است. چرا که طراحی یک پروتکل، منوط به برنامه‌نویسی دقیق طراح در مدت زمانی طولانی است و با کپی‌برداری آن تفاوت ماهیتی دارد. از این‌رو، 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 است. به عبارت 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 به عنوان پروتکلی معرفی شود که برای اولین بار در ایران ارائه شده و طبیعتا از قابلیت رفع مشکلات حوزه فن‌آوری اینترنت اشیا نیز برخوردار است.

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 الهام از پروتکلی دیگر، هرچند با نوآوری‌هایی، طراحی شود؛ در حقیقت ابداعی صورت نگرفته است؛ از این‌رو، 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 یادشده، اختراعی را قابل ثبت دانسته است که حاوی «ابتکار جدید» در حوزه فناوری باشد. با توجه به عبارات ماده ۲ مبنی بر آنچه «در فن وجود نداشته یا برای دارنده مهارت آشکار نباشد»؛ می‌توان برداشت نمود که در طراحی پروتکل‌های نرم‌افزاری،

---

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

[DOI: 10.29252/qjal.7.23.33]

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 تولید چنین پروتکل‌هایی به معنای نقض حق تولیدکننده پروتکل اصلی قلمداد نمی‌شود؛ چرا که در صورت وجود انحصار در تولید چنین پروتکلهایی، اولا خلق طرح‌های جدید صنعتی، تحت‌الشعاع محدودیت قرار گرفته و ثانیا تولید ابزار به دست یک طراح نمی‌تواند به منزله قصد وی بر استفاده سوء از طرح دیگری باشد؛ ضمن اینکه انحصار تولید یک کالا برای یک شرکت به منزله منع دیگران از کوشش در راستای تولید کالای مشابه و رفع انحصار طراح نیست.

چالش دیگر، نحوه شناسایی قانونی پردازنده از کنترل‌کننده است. اگرچه در گفتار پیشین، معیارهای شناسایی پردازنده از کنترل‌کننده مشخص گردید؛ اما در این‌خصوص، ابهاماتی نیز وجود دارد. بند (ب) ماده ۲ دستورالعمل مصوب ۱۹۹۵ و بند ۲ ماده ۴ دستورالعمل مصوب ۲۰۱۶ در تعریف پردازش داده بیان می‌دارند: «پردازش به مجموعه‌ای از عملیات اطلاق می‌گردد که بر روی داده‌های شخصی از طریق اعمالی مانند: جمع‌آوری، ضبط، سازماندهی، ذخیره‌سازی، سازگاری یا تغییر، بازیابی، مشاوره، استفاده، افشای از طریق انتقال، انتشار یا استفاده دیگر، تراز یا ترکیب، مسدود کردن محدودیت، پاک کردن یا تخریب صورت پذیرد.»؛ در تعریف پردازش داده، عبارت «جمع‌آوری داده» ذکر شده است. سوال این است که آیا جمع‌آوری داده جزو وظایف کنترل‌کننده یا ابزار تولید شده توسط وی هست یا این امر توسط پردازنده صورت می‌پذیرد؟ آیا امکان جمع‌آوری داده توسط پردازنده وجود دارد؟ برای رفع چالش بیان‌شده، می‌توان مسأله را از دو منظر بررسی نمود. اگرچه وجود عبارت جمع‌آوری داده در متن مواد یادشده، عبارتی لغو ناشی از مسامحه قانون‌گذار بوده و با تدبر در دیگر مواد مقررات مذکور می‌توان عدم‌کارآیی این عبارت را برداشت نمود؛ اما بر فرض اینکه، وجود چنین عبارتی در تعریف پردازش داده امری صحیح تلقی گردد، به نظر می‌رسد سیاست‌گذاران اتحادیه اروپا در طراحی متن چنین ماده‌ای در دو دستورالعمل مصوب در فواصل سالهای ۲۰۱۶-۱۹۹۵به این موضوع توجه داشته باشند؛ از این‌رو، همان‌طور که بیان گردید، جمع عنوان پردازنده و کنترل‌کننده در یک شرکت نمی‌تواند دور از انتظار باشد (که البته مسئولیت‌های کنترل‌کننده را بر آن شخص اعمال می‌گرداند.)؛ بنابراین، اگر چنین فرایندی صورت پذیرد؛ وجود وظیفه «جمع‌آوری داده» برای

[DOI: 10.29252/qjal.7.23.33]

کنترل‌کننده‌ای که نسبت به پردازش داده اقدام می‌کند، عملا لغو نیست؛ بنابراین، عبارت بیان شده یا عبارات مشابه آن در متن ماده باید در موارد جمع عنوان پردازنده و کنترل‌کننده در یک شخصیت مورد تفسیر واقع گردد.

۳- ملزومات انعقاد قراردادهای میان پردازنده و کنترل‌کننده

پردازش اطلاعات توسط پردازنده، نیازمند انعقاد قراردادهای پردازش میان پردازنده و کنترل‌کننده است. انعقاد این قراردادها نیازمند ملزوماتی به شرح زیر است:

۱-۳- کیفیت انعقاد قرارداد میان پردازنده و کنترل‌کننده

آزادی انعقاد قرارداد جزو اصولی است که در تمامی نظامات حقوقی مورد پذیرش قرار گرفته و جز در موارد استثنایی به طور مطلق بر حق افراد بر انعقاد قرارداد دلالت دارد؛ اما در مواردی، این حق با برخی هنجارهای جامعه یا دیگر حقوق اشخاص، تعارض دارد. در چنین مواردی به جهت ترجیح حق جامعه بر حق شخصی افراد، آزادی قراردادی نیز محدود می‌گردد (Bygrave,2015:104) . یکی از ابزارها، تحدید آزادی قراردادی تصویب قوانین آمره است. از آنجا که حفاظت از اطلاعات شخصی افراد جزو امور مهم تلقی و این امر می‌تواند به امنیت ملی کشورها مرتبط باشد؛ از این‌رو تصویب مقررات مصوب ۲۰۱۶ به منزله تصویب مقرراتی آمره در اتحادیه اروپا تلقی می‌گردد که به تصریح ماده ۱۲ پیمان عملکرد این اتحادیه مصوب ۱۹۹۲ نیز، تمامی کشورهای عضو ملزم به اجرای آنها هستند. ماده ۱۷ دستورالعمل مصوب ۱۹۹۵ در قراردادهای میان پردازنده و کنترل‌کننده نسبت به گنجاندن دو شرط آمره قانونی در قرارداد اقدام نموده است:

الف: پردازنده باید دقیق تحت تعلیمات و مطابق با شرایط تعیین‌شده توسط کنترل‌کننده مبادرت به پردازش داده نماید: در این صورت، اگر در این راه خسارتی نیز وارد گردد؛ کنترل‌کننده، مسئول جبران خسارات وارده می‌شود؛ حتی در موارد ضرورت نیز، پردازنده حق عدول از شرایط تعیین‌شده توسط کنترل‌کننده را نداشته و در صورت انجام چنین عملی، وی مسئول خسارات وارده است.

ب: پردازنده باید تمامی ملاحظات امنیتی در پردازش داده‌ها را رعایت نماید: سهل‌انگاری پردازنده در حفاظت از داده‌ها منجر به مسئولیت مدنی یا کیفری این شخص است. به نظر نمی‌رسد در صورتی که پردازنده از این وظیفه سر باز زند؛ کنترل‌کننده مسئول اعمال وی باشد. ماده ۲۸ دستورالعمل مصوب ۲۰۱۶ ، شرایطی را بر شمرده است تا مطابق با شرایط مذکور که باید در متن

[DOI: 10.29252/qjal.7.23.33]

قرارداد دو طرف گنجانده شود؛ کنترل‌کننده نسبت به انتخاب پردازنده اقدام نماید. این شرایط عبارتند از: «مدت و موضوع پردازش، ماهیت و هدف از پردازش، نوع داده‌های شخصی در حال پردازش، تعهدات و حقوق دو طرف.»؛ از این‌رو، چنانکه در هنگام انتخاب پردازنده، شرایط ماده ۲۸ به ترتیب بیان شده مورد نظر کنترل‌کننده بوده و وی در این خصوص سهل انگاری ننموده باشد، مسئولیتی متوجه وی نخواهد بود.

اما در انعقاد قرارداد، مشکل عملی موجود این است که در حال حاضر، انعقاد قراردادهای میان دو طرف عموما توسط پردازندگان طراحی و توسط کنترل‌کنندگان امضا می‌گردد، (Carey,2015:265)؛ به عبارت دیگر، شرایط پردازش داده‌های خصوصی توسط پردازندگان به شکلی است که در مواردی به جهت انحصار موجود در یک حوزه خاص، کنترل‌کنندگان به ناچار مجبور به انعقاد قرارداد با پردازنده‌ای مشخص می‌شوند. این امر می‌تواند حق آزادی انعقاد قرارداد توسط آنها را تحت‌الشعاع قرار دهد. به عنوان مثال، در حال حاضر شرکت گوگل تنها ارائه‌دهنده خدمات فضای ابری برای شرکت‌های تولیدکننده ابزارهای اینترنت اشیاست. ابزارهای اینترنت اشیا برای انجام وظایف محوله، نیازمند برخورداری از فضای ذخیره اطلاعات با حجم بالا هستند. باالطبع، در صورتی که از هارد دیسک‌های خارجی در این ابزارها استفاده گردد، فرایند مذکور واجد ایراداتی از جمله محدوده فضای هارد و کاهش بازده ابزار به جهت حجم بالای وسیله جانی خواهد بود؛ ضمن اینکه هیچ تضمینی بر ذخیره‌سازی همیشگی اطلاعات در این هاردها نبوده و در هر حال، امکان پاک شدن آنها به دلایل مختلف از جمله سوختگی هارد و... وجود دارد؛ از این‌رو، این ابزارها نیازمند بهره‌مندی از فضایی آنلاین هستند تا اطلاعات خود را در آن ذخیره نمایند. فضای ابری بهترین گزینه برای این امر است؛ اما به دلیل انحصار ارائه آن توسط شرکت گوگل، عملا این شرکت طرف قرارداد با بسیاری از کنترل‌کنندگان بوده و به همین جهت در تعیین شروط قراردادی نیز امکان دخالت را خواهد داشت؛ از این‌رو، مقررات آمره سال ۲۰۱۶ و ۱۹۹۵، این عملکرد را محدود نموده است.

۲-۳-چالش‌های انعقاد قرارداد میان پردازنده و کنترل‌کننده

۱-۲-۳-کیفیت اجرای تعلیمات کنترل‌کننده توسط پردازنده

سوال این است که از آنجا که عموما قراردادهای منعقده میان پردازندگان و کنترل‌کنندگان به صورت الحاقی منعقد می‌گردد؛ چگونگی رعایت تعلیمات کنترل‌کننده توسط پردازنده به چه شکلی

[DOI: 10.29252/qjal.7.23.33]

خواهد بود؟ عملا پاسخ سوال مزبور منفی است و راهی جز پیش‌بینی مسئولیت مطلق برای پردازنده باقی نمی‌ماند؛ اما آیا می‌توان برای کنترل‌کننده نیز مسئولیتی پیش‌بینی نمود؟ از یک طرف، کنترل‌کننده با اراده و اختیار خویش مبادرت به انعقاد قرارداد نموده است و از طرف دیگر، قرارداد منعقده، الحاقی بوده و وی به ناچار نسبت به چنین عملی اقدام نموده است. اگر قائل بر عدم مسئولیت وی در جبران خسارات وارده باشیم؛ عملا وی را از چرخه مسئولیت‌های قانونی و قراردادی که وی مبادرت به انعقاد با مصرف‌کننده نموده‌اند، خارج می‌کنیم و در صورتی که قائل بر مسئولیت وی باشیم؛ این امر می‌تواند عدالت حقوقی را زیر سوال برد؛ چرا که در فضایی که یک شخص به ناچار مجبور به پذیرش شرایطی از پیش‌تعیین شده می‌گردد؛ مسئول نمودن وی بر جبران خسارات وارده، دور از عدالت است؛ از این‌رو، راهی جز سیاست‌گذاری اجرایی در این خصوص باقی نمی‌ماند.

البته در این زمینه، در سال ۲۰۱۳ در پرونده شهرداری شهر سالم در کشور سوئد، با انعقاد قراردادی با شرکت گوگل از فضای ابری این شرکت برای مدیریت اطلاعات ایمیل‌ها و دیگر اطلاعات شهرداری استفاده می‌نمود. از آنجا که این قرارداد به صورت پیش‌نویس از سوی گوگل در اختیار شهرداری قرار گرفته و شهرداری در این زمینه فاقد آزادی قراردادی بود؛ دادگاه، شهرداری را از جبران خسارات وارده ناشی از سوءاستفاده از اطلاعات سکنه شهر مصون دانست (Lindqvist,2017:10). اگرچه مشاهده می‌گردد که در پرونده‌ای‌خاص، دادگاه کشوری با مبنا قراردادن قواعد عام موجود در نظام حقوقی کشور مبتوع خود، مبادرت به صدور چنین حکمی نموده است؛ اما صدور این حکم نمی‌تواند منجر به ایجاد رویه قضایی در دادگاهها گردد؛ چرا که حل چالش‌های بیان شده فوق، نیازمند سیاست‌گذاری تقنینی و اجرایی در نظام حقوقی کشورها بوده و به صرف صدور احکامی خاص در موارد مشابه، نمی‌توان قاعده‌ای آمره از این امر برداشت نمود.

در نظام حقوقی ایران، به نظر می‌رسد مبنای مسئولیت مدنی بر انتساب خسارت بر عامل خسارت استوار است (ره‌پیک، ۱۳۹۵: ۲۰-۱۸) از این‌رو، در این موارد می‌توان فردی را که منجر به تضییع حق دارنده و تحمیل خسارات به وی شده است؛ صرف‌نظر از وجود عمد یا تقصیر یا فقدان هر یک، به جبران تمامی خسارات وارده مستند به اصل جبران کامل خسارت محکوم کرد؛ بنابراین،[1] صرف‌نظر از ماهیت و ساختار قرارداد منعقده میان پردازنده و کنترل‌کننده و شرایط حاکم

---

۱. برای مطالعه بیشتر در خصوص اصل جبران کامل خسارت رک: قسمتی تبریزی، علی، (۱۳۹۴)، اصل جبران کامل زیان، فصلنامه فقه و حقوق اسلامی، سال هفتم، شماره ۱۳

[DOI: 10.29252/qjal.7.23.33]

بر قرارداد، تعداد عوامل دخیل در خسارات وارده مستند به میزان سهم خود در ورود زیان (مستفاد از ماده ۵۲۶ قانون مجازات اسلامی)، مسئول جبران تلقی می‌گردند.

۲-۲-۳- ابهامات موجود در تفسیر قرارداد

بند ۳ ماده ۲۸ دستورالعمل مصوب ۲۰۱۶، پردازنده را در انجام تعهدات قراردادی، تحت قیودی قرار داده است که به جهت عدم وجود صراحت در تفسیر این قیود، می‌تواند زمینه سوءاستفاده آن در اجرای قرارداد را فراهم آورد. مطابق با مفاد بند مذکور، پردازنده موظف است تا «با درنظر گرفتن ماهیت مورد پردازش، با اقدامات فنی و سازمانی مناسب، تا حد امکان» نسبت به اجرای مفاد قرارداد اقدام نماید. وجود چنین کلمات مبهمی می‌تواند در ذهن خواننده، این ابهام را ایجاد کند که در شرایطی، حتی پردازنده می‌تواند از انجام تعهدات قراردادی سرباز زند. از یک طرف، مقررات دستورالعمل، پردازنده را ملزم به انجام مفاد قرارداد تحت تعلیمات کنترل‌کننده نموده و از طرف دیگر، با بیان عباراتی مبهم، امکان سوءاستفاده پردازنده در اجرای قرارداد را پدید آورده است. به نظر نگارندگان، وجود این شرایط در مفاد ماده ۲۸ با توجه به فلسفه تصویب این دستورالعمل باید به گونه‌ای تفسیر گردد که قرارداد را از حالت اجرایی خارج ننماید. اجرای تعهدات قراردادی جزو قواعدی است که از توافق طرفین ناشی می‌گردد؛ از این‌رو، نباید انجام این تعهد را به گونه‌ای در اختیار و اراده یک طرف قرارداد گذاشت و قطعا چنین موضعی، مدنظر سیاست‌گذاران اتحادیه اروپا نیز بوده است. به نظر نگارندگان، وجود بند سوم از ماده ۲۸، اشاره به اجرای صحیح قرارداد دارد. به عبارتی، در صورتی که پردازشگری در حوزه خاصی مبادرت به پردازش داده کند و خدمات وی محدود به اعمال خاصی باشد؛ نسبت به انجام تعهدات قراردادی اقدام نماید؛ از این‌رو اگر قرارداد منعقده خارج از حوزه ارائه خدمات آن شرکت باشد و با توجه به «ماهیت مورد پردازش» از «امکان» انجام صحیح تعهدات قراردادی برخوردار نباشد؛ تنها وضعیت حاکم بر قرارداد، عقیم شدن آن تلقی می‌گردد؛[۱] اما اگر پردازش داده در حوزه ارائه خدمات آن شرکت باشد؛ مطابق با قواعد دستورالعمل مذکور، وی ملزم به اجرای تعهدات قراردادی تحت تدابیر امنیتی لازم است.

---

۱. در نظام حقوقی ایران نیز وجود شرایط مذکور می‌تواند از موارد انفساخ قرارداد شمرده شود. برای مطالعه آثار حاکم بر عقیم شدن عقود و تفاوتهای موجود میان عقد منفسخ در حقوق ایران و عقیم در حقوق اتحادیه اروپا رک:
Stone Richard, Devveney James,(2019), The modern Law of Contract, Taylor and Francis, Twelfth Edition, pp :40-55

[DOI: 10.29252/qjal.7.23.33]

٤- مسئولیت‌پذیری و سازوکار تقسیم مسئولیت میان پردازنده و کنترل‌کننده

پس از بیان چالش‌های مذکور در گفتارهای پیشین، در گفتار حاضر در دو بند به تبیین سازوکار مسئولیت‌پذیری و کیفیت تقسیم مسئولیت میان پردازندگان و کنترل‌کنندگان پرداخته خواهد شد.

٤-١- مسئولیت‌پذیری پردازنده و کنترل‌کننده در اجرای مفاد قراردادهای منعقده

دستورالعمل مصوب ۲۰۱۶ با مبنا قراردادن اصل شفافیت در پردازش داده‌ها، در فراز (هـ) بند ۳ ماده ۲۸، پردازنده را موظف به ارائه گزارشی از اقدامات انجام شده بر روی داده‌پیام‌های مورد پردازش به کنترل‌کننده نموده است؛ از این‌رو، کنترل‌کننده؛ حق اعمال نظارت و حسابرسی بر اعمال پردازنده را خواهد داشت. ماده ۲۹ اعلامیه مصوب ۲۰۱۰ به منظور بهبود نظارت کنترل‌کننده و توسعه حیطه اختیارات وی در زمینه حسابرسی، حقوقی را به شرح زیر برای او در نظر گرفته است:

-حق حسابرسی محل سرورهایی که داده‌ها پردازش و ذخیره می‌شوند.

-حق حسابرسی الگوریتمهایی که در مراحل مختلف پردازش استفاده می‌شوند.

-حق حسابرسی اقدامات امنیتی اعمال شده توسط پردازشگر

اجرای حقوق بیان شده در ماده ۲۹ اعلامیه نیز درعمل با چالش‌هایی مواجه است. همان‌طور که بیان شد، پردازندگان عموما به صورت همزمان، مبادرت به پردازش داده‌های متعلق به چند کنترل‌کننده می‌نمایند؛ از این‌رو، اگر محل ذخیره داده‌پیام‌ها توسط پردازنده، مکان مشخصی باشد که هر کنترل‌کننده امکان دسترسی به آن مکان را داشته باشد؛ عملا امنیت داده‌ای در معرض نقض قرار خواهد گرفت؛ چون در صورتی که یک کنترل‌کننده قصد دسترسی به اطلاعات دیگر کنترل‌کننده‌ها را داشته باشد؛ این امر به‌آسانی برای وی میسر خواهد بود. از سوی دیگر، چنانچه کنترل‌کنندگان متعدد که با پردازشگری واحد طرف قرارداد هستند؛ در بازار رقابت حضور داشته و در حوزه‌ای خاص با یکدیگر به رقابت بپردازند؛ عدم پیش‌بینی تدابیر امنیتی لازم در دسترسی به اطلاعات ذخیره شده می‌تواند توازن موجود در بازار را تحت‌الشعاع قرار دهد. علاوه بر آن، حقوق مندرج در ماده ۲۹ اعلامیه به صورت احکامی اولیه هستند که حکمی ثانویه برای آنها پیش‌بینی نشده است و این امر می‌تواند منجر به ایجاد مشکلاتی گردد. به عبارتی، در صورتی که پردازنده، امکان اعمال حقوق کنترل‌کننده را به وی ندهد، سوال این است که وضعیت قرارداد به چه شکلی

[DOI: 10.29252/qjal.7.23.33]

خواهد بود؟ آیا کنترل‌کننده، ملزم به اقامه دعوی در مراجع قضایی برای الزام پردازنده به انجام تعهدات قانونی بوده یا از امکان اعمال حق فسخ در قرارداد بهره‌مند می‌گردد؟ اگر پاسخ سوال مزبور، امکان اقامه دعوی برای الزام به انجام تعهدات قراردادی باشد؛ چالش آن است که حق مندرج در ماده ۲۹ به شکلی است که کنترل‌کننده، به صورت نامحدود امکان دسترسی به موارد بیان شده را داشته باشد. اگر برای یک بار، دادگاه پس از طی پروسه طولانی اقامه دعوی، مبادرت به صدور حکم بر الزام پردازشگر بر انجام تعهد نماید؛ برای موارد دیگر، ضمانت اجرای قانونی چه خواهد بود؟ آیا به دلیل صرف وقت و هزینه‌های بالای رسیدگی قضایی، امکان اقامه چندباره دعوی در این مراجع وجود دارد؟ به‌یقین پاسخ به سوال مزبور منفی است.

از طرف دیگر، اگر ملاک را بر امکان اعمال حق فسخ برای کنترل‌کننده در نظر بگیریم؛ چالش به‌وجودآمده در جایی خواهد بود که در حوزه‌ای خاص، پردازش داده‌ها و ارائه خدمات توسط پردازنده‌های ویژه‌ای صورت می‌پذیرد. به عنوان مثال، در صورتی که شرکت گوگل در ارائه خدمات فضای ابری و پردازش داده از حقوق قانونی مندرج در ماده ۲۹ جلوگیری نماید؛ فسخ قرارداد توسط کنترل‌کننده عملا موجبی نخواهد داشت؛ چرا که جز شرکت گوگل، شرکت خدمات‌رسانی دیگری وجود ندارد که کنترل‌کننده مبادرت به انعقاد قرارداد با وی نماید. از طرف دیگر، توسل به قواعد عمومی حاکم بر قراردادها و پیش‌بینی ضمانت اجرای عقیم شدن (یا انفساخ) قرارداد (حسب مورد) نیز نمی‌تواند به طورقانونی ضمانت اجرای صحیحی در این خصوص باشد؛ چون عقیم شدن قرارداد در حقوق کامن‌لا در مواردی است که اجرای قرارداد با مانعی قانونی مواجه گردد که امکان انجام تعهدات قراردادی از یک طرف یا طرفین قرارداد سلب گردد؛ در حالی که در قرارداد موصوف، مانع قانونی در این‌خصوص وجود ندارد و اجرای قرارداد توسط پردازنده به طور کامل میسر است؛ از این‌رو، مقررات بیان شده بالا به جهت عدم برخورداری از احکام ثانویه، فاقد قوه اجرایی بوده و راهی جز سیاست‌گذاری تقنینی جدید برای حل چالش‌های بیان شده وجود ندارد.

علاوه بر آن، پردازنده در اجرای تعهدات قراردادی باید تحت دستورات کنترل‌کننده نسبت به پردازش داده اقدام کند. قسمت (هـ) بند ۳ ماده ۲۸ دستورالعمل مصوب ۲۰۱۶، پردازنده را موظف نموده تا در صورتی که دستورات کنترل‌کننده، مغایر با مقررات مصوب اتحادیه اروپا یا کشور متبوع وی باشد؛ با اعلام موارد مغایرت از کنترل‌کننده کسب تکلیف نماید. در این بند نیز سیاست‌گذاران اگرچه با پیش‌بینی حکمی اولیه، سعی در جلوگیری از انجام اعمال مغایر با قوانین آمره داشته‌اند؛ اما در این خصوص نیز حکمی ثانویه بر پیش‌بینی ضمانت اجراهای قانونی، مورد نظر قرار نگرفته

[DOI: 10.29252/qjal.7.23.33]

است. سوال این است که اگر موارد مغایرت از سوی پردازنده به کنترل‌کننده اعلام گردد و کنترل-کننده بر انجام دستورات خود اصرار نماید؛ وظیفه پردازنده چه بوده و چه ضمانت اجرایی در این خصوص وجود خواهد داشت؟ در این خصوص می‌توان مسأله را از دو منظر بررسی نمود:

پردازنده موظف به انجام دستورات کنترل‌کننده است. در این صورت، چالش موجود این است که آیا در صورت انجام اعمال مغایر با قواعد آمره مصوب، پردازنده مسئولیتی خواهد داشت یا خیر؟ اگر وی فاقد مسئولیت باشد و تمامی مسئولیت در ذمه کنترل‌کننده قرار گیرد؛ نکته موجود این است که پردازنده با علم به مغایر بودن اعمال وی، مبادرت به انجام آن نموده است. مقررات دستورالعمل ۲۰۱۶، قواعدی آمره هستند که به جهت سطح امنیتی مقررات حفاظت از داده‌های شخصی، می‌توانند نسبت به دیگر مقررات آمره، قانونی اهم تلقی شوند؛ از این‌رو، انجام هر عمل خلاف این مقررات، به‌ویژه در مواردی که انجام اعمال خلاف، منجر به ضرر جبران‌ناپذیر گردد؛ امری مذموم بوده و انجام دستور آمر قانونی نمی‌تواند رافع مسئولیت پردازنده باشد و اما اگر وی دارای مسئولیت تلقی گردد؛ در این‌صورت، وظیفه وی به انجام دستورات کنترل‌کننده، امری لغو و باطل خواهد بود.

پردازنده موظف به انجام دستورات کنترل‌کننده نیست. اگرچه این نظر می‌تواند مانع از بروز مشکلات ناشی از انجام اعمال مغایر با قانون باشد؛ اما سوال این است که مرجع تشخیص خلاف قانون بودن دستورات کنترل‌کننده، آیا خود کنترل‌کننده هست یا پردازنده نیز حق تشخیص این مورد را دارد؟ اگر پردازنده مبادرت به عدم انجام دستورات کنترل‌کننده نماید و بر فرض، تشخیص وی اشتباه باشد و در این راه، خسارتی نیز از اعمال وی ناشی گردد؛ آیا وی مسئول جبران خسارت است؟ به نظر نگارندگان، مرجع تشخیص خلاف قاعده بودن دستورات کنترل‌کننده، همان مرجع اعلام دستور بوده و پردازنده در این‌خصوص، فاقد صلاحیت است؛ از این‌رو، اگر وی با اعلام این امر به کنترل‌کننده با تاکید وی برای انجام دستور مواجه گردد، به ناچار باید نسبت به انجام دستورات اقدام نماید؛ مگر اینکه دستور صادره به صورت واضح مخالفت صریح با مقررات دستورالعمل نماید که هیچ جای شک و شبهه‌ای در خصوص مغایرت باقی نماند. در این خصوص برای حفظ ضروریات و حفاظت امنیت داده‌ها، می‌توان پردازنده را از انجام دستورات کنترل‌کننده معاف دانست؛ اما در هر حال، سیاست‌گذاری تقنینی در این خصوص نیز برای حل خلاء ایجاد شده ضروری به نظر می‌رسد.

[DOI: 10.29252/qjal.7.23.33]

۲-٤ - سازوکار تقسیم مسئولیت میان پردازنده و کنترل‌کننده

در زمینه جبران خسارت و توزیع مسئولیت میان اشخاص فعال در سازوکار عملکرد ابزارهای اینترنت اشیا، سوالی که در آغاز امر مطرح می‌گردد؛ این است: در مواردی که تولیدکننده ابزار در تولید آن؛ تمامی استانداردهای لازم، قوانین و نکات ایمنی را رعایت نماید؛ چنانچه پس از تولید و عرضه ابزار در بازار، خساراتی از عملکرد آن ناشی گردد؛ آیا می‌توان تولیدکننده را مسئول دانست؟ آیا عنصر زمان می‌تواند در میزان مسئولیت تولیدکننده موثر واقع شود؟ به عبارتی، آیا در میزان یا وجود یا عدم وجود مسئولیت تولیدکننده گذر زمان معقول از لحظه تولید و عرضه کالا به بازار تاثیر دارد؟ در صورتی که میان کنترل‌کننده و پردازنده، قرارداد پردازش داده منعقد شود و پردازنده، به هر دلیل، قرارداد را به پردازنده‌ای دیگر (پردازنده فرعی) منتقل کند و یا حتی پردازنده دیگری را برای انجام وظایف خود در قرارداد به کار گمارد؛ آیا وی مسئول جبران خسارات است؟ از آنجا که ابزارهای اینترنت‌اشیا برای انجام وظایف خود نیازمند پروتکلهایی هستند تا با پیاده‌سازی آنها بر روی پردازنده، دستورات از پیش‌تعیین شده را اجرا کنند؛ در صورت وجود خسارات، آیا امکان مسئول تلقی نمودن برنامه‌نویس مذکور نیز وجود دارد یا تمامی مسئولیت بر ذمه سازنده دستگاه قرار می‌گیرد؟

ماده ۲۳ دستورالعمل مصوب ۱۹۹۵، با پیش‌بینی مسئولیت مطلق برای کنترل‌کننده، وی را مسئول تمامی خساراتی می‌دانست که از اعمال وی یا پردازش صورت گرفته توسط پردازنده ناشی گردد؛ از این‌رو، به علت نقش تبعی پردازنده در سازوکار پردازش داده‌ها و تبعیت وی از دستورات کنترل‌کننده، وی مسئول جبران خساراتی نبود که تحت نظارت و تعلیمات کنترل‌کننده صورت می‌گرفت (Walden,2016:5) . این در حالی است که دستورالعمل مصوب ۲۰۱۶ با ایجاد تحول در نحوه شناسایی مسئولیت میان پردازنده و کنترل‌کننده در ماده ۸۲ ، هر یک را مسئول جبران خسارات ناشی از اعمال غیر قانونی خود قرار داده است؛ البته مطابق با تصریح بند ۲ ماده ۸۲ مقررات فوق‌الذکر، چنانکه تحت تعلیمات و دستورات کنترل‌کننده، پردازنده با انجام اعمالی، مرتکب خسارت گردد؛ اگر ورود خسارت، ناشی از تقصیر پردازنده در نحوه پردازش داده نباشد؛ کنترل‌کننده، مسئول جبران خسارات وارده تلقی می‌گردد. علاوه بر موارد بیان شده، مطابق با نص بند ۴ ماده ۲۸ دستورالعمل اخیرالذکر، چنانچه پردازنده در انجام وظایف خود مبادرت به استفاده از دیگر اشخاص نماید نیز به طور مطلق، مسئول جبران خسارات وارده از ناحیه مشارالیهم نیز خواهد بود. سوال دیگری که به نظر می‌رسد، این است که آیا با انعقاد قرارداد میان کنترل‌کننده و پردازنده، توجها به الزامات امنیتی دستورالعملهای بیان شده، نمی‌توان این مطلب را برداشت نمود که پردازنده

[DOI: 10.29252/qjal.7.23.33]

در انجام تعهدات قراردادی باید به طور مباشرت اقدام کند و از به‌کارگماردن دیگران در این خصوص بپرهیزد؟ مگر نه این است که مقررات بیان شده در انتخاب پردازنده، کنترل‌کننده را موظف به بررسی حیطه تخصصی و انتخاب پردازنده‌ای قابل اعتماد نموده است تا زمینه سوءاستفاده از اطلاعات شخصی افراد رفع گردد؟ پس چطور می‌توان به پردازنده، اجازه همکاری با دیگران در امر پردازش داده‌های خصوصی را داد؟ به نظر می‌رسد سیاست‌گذاران اتحادیه اروپا در تصویب مقررات ماده ۲۸، دچار سهل‌انگاری شده‌اند و بدون توجه به فلسفه تصویب دستورالعمل، تنها با توسل به قواعد عمومی، مبادرت به تصویب مقرره مزبور نموده‌اند؛ اما در پاسخ به سوالات بیان شده در ابتدای این گفتار می‌توان بر اساس اطلاق مقررات دستورالعمل ۲۰۱۶، در صورت ایجاد خسارت ناشی از اعمال پردازنده یا کنترل‌کننده، صرف‌نظر از زمان ورود خسارات، آنها را مسئول جبران زیانهای وارده دانست.

نتیجه‌گیری

فناوری اینترنت اشیا یکی از فناوری‌های نوظهوری است که در حال توسعه در سرتاسر جهان است. پیاده‌سازی این فناوری نیز همانند دیگر فناوری‌های نوظهور، واجد برخی چالش‌های حقوقی خواهد بود که به نمونه‌هایی از آنها در حیطه موضوع این پژوهش پرداخته و راه‌حل‌های موجود مورد تجزیه و تحلیل قرار گرفت؛ اما در راستای پیاده‌سازی این فناوری در نظام حقوقی ایران و پیشگیری از مواجهه سیاست‌گذاران با چالش‌های موجود در نظام حقوقی کشورهای توسعه یافته، توصیه‌های سیاست‌گذارانه زیر برای بهبود روند پیاده‌سازی این فناوری در نظام حقوقی ایران ارائه می‌شود:

۱- لزوم سیاست‌گذاری تقنینی در مدیریت ابزارهای اینترنت اشیا و احتراز از ارجاع این امر بر قواعد کلی موجود در نظام حقوقی ایران: متاسفانه در موارد عدیده‌ای مشاهده می‌گردد که سیاست‌گذاران در کشور ایران پس از شیوع به‌کارگیری ابزار یا فناوری ویژه‌ای در کشور و به‌روز نمودن مشکلات تقنینی و اجرایی حاصل از به‌کارگیری آن، مبادرت به تصویب قوانین در راستای حل آن چالش‌ها می‌کنند. این در حالی است که تصویب قوانین کارآمد در یک نظام توسعه‌یافته باید پیش از بروز مشکل صورت پذیرد تا مشکلات احتمالی ایجاد شده به وسیله آن قوانین حل و فصل گردند؛ از این‌رو، توجه به مصوبات موجود در سطح بین‌الملل، از جمله دستورالعمل مصوب اتحادیه اروپا، می‌تواند راهگشای نظام قانون‌گذاری ایران در مدیریت مسائل مربوط به ابزارهای اینترنت‌اشیا گردد. در ایران، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی تنها به بحث کیفیت پردازش و ذخیره گروهی خاص از داده‌های خصوصی پرداخته و نص مبهم این مواد و البته خلاء قانونی

[DOI: 10.29252/qjal.7.23.33]

در زمینه قانون حاکم بر دعاوی ناشی از این فرایند؛ مفهوم‌شناسی داده‌های خصوصی، کیفیت اعطای مجوز بر فعالیت پردازندگان و کنترل‌کنندگان، سازوکار مسئولیت‌پذیری، دادگاه صالح در رسیدگی به این دعاوی، حقوق دارنده اطلاعات و سازوکار تبادل داده؛ ضرورت تصویب قانون جامع در این زمینه را تحکم می‌بخشد.

۲- سیاست‌گذاری اجرایی در راستای آگاهی بخشی به آحاد جامعه: استفاده گسترده از یک ابزار و بهره‌مندی اقشار جامعه از پتانسیل‌های آن نیازمند آگاهی‌بخشی دولت بر عموم جامعه است. همان‌طور که بیان شد در کشورهای عضو اتحادیه اروپا در موارد عدیده‌ای، انعقاد قراردادهای میان کنترل‌کننده و مصرف‌کننده یا به صورت الحاقی منعقدشده یا مفاد قرارداد به نحوی تنظیم می‌گردد که عموم جامعه از تفسیر مفاد بیان شده عاجز هستند. چنین مسائلی می‌تواند زمینه سوءاستفاده از اطلاعات شخصی افراد را نیز ایجاد کند. پیشگیری از این امر نیازمند آگاهی‌بخشی به عموم جامعه است.

علاوه بر آن، همان‌طور که بیان شد؛ نظارت مستمر دولت بر نحوه انعقاد قراردادهای میان تولید و مصرف‌کننده، نحوه تفسیر قراردادهای منعقده، کیفیت انعقاد قرارداد میان تولید و مصرف-کننده ابزار و ارائه قراردادهای پیش‌نویس به کنترل‌کنندگان نیازمند تفصیل جزئیات این امور به عموم جامعه و افزایش سطح آگاهی عمومی است که ارائه برنامه‌های آموزشی در شبکه‌های اجتماعی و ابزارهای ارتباطی مانند تلویزیون می‌تواند راهگشای بسیاری از مشکلات باشد.

۳- سیاست‌گذاری تقنینی و اجرایی در راستای چگونگی فعالیت کنترل کنترل‌کنندگان و پردازندگان: در حال حاضر، به دلیل عدم فراگیر شدن ابزارهای اینترنت‌اشیا در ایران، شرکت‌های کنترل‌کننده و پردازنده این ابزارها فعالیت خاصی در کشور ندارند؛ اما در سالهای آینده با ورود این فناوری به ایران شاهد حضور فعال شرکت‌های مزبور در بازارهای ایرانی نیز خواهیم بود. مسأله مهم در این خصوص، چگونگی اعطای مجوز فعالیت به شرکتهای مزبور در ایران است که نیازمند سیاست‌گذاری‌های تقنینی و اجرایی است.

در این زمینه، اول آنکه، دولت نیازمند پیش‌بینی مراجع صلاحیتدار در خصوص بررسی سوابق حقوقی و ورشکستگی این سازمان‌ها برای احراز صلاحیت فعالیت در کشور ایران است. دوم اینکه، علاوه بر اعطای مجوز، ضرورت نظارت مستمر بر فعالیت این نهادها و دریافت گزارش‌های منظم از نحوه پردازش اطلاعات و تبادل و ذخیره آنها نیز برای جلوگیری از سوءاستفاده‌های احتمالی، جزو ضروریات نظام حقوقی ایران خواهد بود.

[DOI: 10.29252/qjal.7.23.33]

فهرست منابع

الف. فارسی

۱. رهپیک، حسن (۱۳۹۵)؛ حقوق مسئولیت مدنی و جبران‌ها، تهران: انتشارات خرسندی

۲. صادقی، حسین، ناصر، مهدی(۱۳۹۷)؛ واکاوی نقش قراردادهای هوشمند در توسعه نظام ثبت الکترونیکی اسناد، فصلنامه دیدگاه‌های حقوق قضایی، دوره ۲۳، شماره ۸۴

۳. قسمتی تبریزی، علی (۱۳۹۴)؛ اصل جبران کامل زیان، فصلنامه فقه و حقوق اسلامی، سال هفتم، شماره ۱۳.

ب.لاتین

1. C Wendehorst,(2016), ‘Consumer Contracts and the Internet of Things’ in R Schulze and D Staudenmayer(eds), Digital Revolution: Challenges for Contract Law in Practice (Nomos Verlagsgesellschaft 2016)
2. Gottipati Hari, (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
3. H Grant, A Lambert and K Pickering,(accessed 17 May 2019) ‘Data Protection Day—Data Processors and the GDPR’ (2016)fieldfisher <www.fieldfisher.com/publications/2016/02/data-protection-day-data-processors-and-the-gdpr# sthash.eCrAKFYy.dpbs>
4. Jenna Lindqvist,(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
5. L Coll and R Simpson,(accessed 14 August 2019), ‘Connection and Protection in the Digital Age: The Internet of Things andChallenges for Consumer Protection’ (Consumers International, April 2016) 34 <http://www.consumersinternational.org/media/1292/connection-

[DOI: 10.29252/qjal.7.23.33]

and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

6. Lee A. Bygrave,(2015), Internet Governance by Contract,oxford university press, 1st Edition
7. Lunden Ingrid, (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
8. M. Carey ,Peter LL. ,(2015) Data Protection: A Practical Guide to UK and EU Law,Oxford University Press; 4th edition
9. Nest.com web page(accessed 18 June 2019) <https://nest.com/uk/thermostat/meet-nest-thermostat/
10. Peppet,(accessed 24 March 2019) 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (2012) 59 UCLA L Rev 676, 689. The page numbering used in this article is following University of Colorado Law Legal Studies Research Paper No 11–14 <http://ssrn.com/abstract¼1919013>.
11. Stone Richard, Devveney James,(2019), the modern Law of Contract, Taylor and Francis, Twelfth Edition
12. The Swedish Data Protection Authority,(accessed 18 July 2019) 'Tillsyn enligt personuppgiftslagen (1998:204)—Uppfo¨ljning avbeslut i a¨rende 263-2011' (31 May 2013) www.datainspektionen.se/documents/beslut/2013-05-31-salems-kommun.pdf
13. Walden and Noto La Diega,(2016) Contracting for the 'Internet of Things': Looking into the Nest, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725913.

[DOI: 10.29252/qjal.7.23.33]