فصلنامه سیاستگذاری عمومی، دوره ۶ ، شماره ۳ ، پاییز ۱۳۹۹ ، صفحات ۱۰۳-۸۱

مقاله پژوهشی

ارائه چارچوب حقوقی مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا در بستر دولت الکترونیک؛ تبیین الگوی سیاستگذاری موثر

حسین صادقی[1]

استادیار حقوق کسب و کار دانشگاه تهران

مهدی ناصر

دانشجوی دکتری حقوق خصوصی دانشگاه علوم قضایی

(تاریخ دریافت: ۹۹/۲/۱ - تاریخ پذیرش: ۹۹/۵/۶)

چکیده

اینترنت اشیا فناوری نوظهوری است که دربردارنده چالشهای متعددی از جمله « چارچوب های مسئولیت پذیری» می‌باشد. سوال اصلی پژوهش حاضر این است که ارائه چارچوب حقوقی در زمینه «مسئولیت پذیری» این ابزارها نیازمند اتخاذ چه سیاست هایی می‌باشد؟ برای پاسخگویی به سوال مذکور این پژوهش به روش تحقیق اسنادی و مطالعه تطبیقی میان قواعد حاکم بر نظام حقوقی ایران و اتحادیه اروپا بیان می دارد که ارائه چارچوب حقوقی در تبیین ابعاد مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا نیازمند تبیین چالشها و راهکارهای مناسب در مسئولیت پذیری این ابزارها، سیاست های لازم در بهبود نظارت بر عملکرد این ابزارها و سیاستگذاری عملکرد ابزارهای اینترنت اشیا و کنترل کنندگان آنها در ارتباط با قواعد مسئولیت پذیری می‌باشد. برای عملیاتی نمودن سیاست های اعلام شده در فوق، اجرای برخی سیاستها از جمله ایجاد آگاهی عمومی، برگزاری دوره های آموزشی برای کارکنان شرکت ها، پیش بینی مکانیسم های حمایتی از مالکان اطلاعات، پیش بینی سازوکار اعطای امضائات دیجیتالی و اصلاح قوانین می تواند کارگشا باشد.

واژگان کلیدی: چارچوب حقوقی، ابزارهای اینترنت اشیا، مسئولیت پذیری ، سیاستگذاری.

1- نویسنده مسئول Email: Hosadeghi@ut.ac.ir

مقدمه

امروزه با توسعه فناوری، ابزارهای الکترونیکی از قابلیت ایجاد ارتباط با یکدیگر یا عامل انسانی برخوردار شده اند. فناوری برقراری ارتباط میان ابزارهای الکترونیکی که از آن به عنوان اینترنت اشیا تعبیر می گردد، یکی ازفناوری های نو ظهور عصر دیجیتال می‌باشد که بر مبنای آن ابزارهای الکترونیکی با دریافت داده پیام از سوی عامل انسانی یا دیگر ابزار الکترونیکی و پردازش آن مبادرت به انجام وظایف محول مطابق با پروتکل های داده شده به خود می نمایند. دریافت داده پیام می تواند به هر شکلی از جمله پردازش دستورات داده شده از سوی صدای ابزار یا عامل انسانی متقابل یا برخورداری از انواع هوش مصنوعی مانند یادگیری ماشین و در سطوح پیشرفته تر سیستم های خبره باشد. امروزه شرکت های بزرگی از جمله Cisco، General Electric،Ericsson و Accenture با تولید ابزارهای دیجیتالی برخوردار از فناوری اینترنت اشیا نقش مهمی در انجام مبادلات دیجیتالی مبتنی بر ماشین ها یا توسعه شهرهای هوشمند برخوردار بوده و در سال ۲۰۱۸ رقمی بالغ بر ۲ تریلیون دلار در راستای توسعه این فناوری بر ابزارهای مختلف تجاری، صنعتی و حتی نظامی از سوی اشخاص حقیقی و حقوقی سرمایه گذاری شده است که نشان از اهمیت وافر این حوزه دارد(Gartner,2019) . اما توسعه این ابزارها می تواند چالش هایی نیز در حفظ حریم خصوصی افراد به همراه داشته باشد. به عبارتی برخورداری از ابزارهای اینترنت اشیا از قابلیت پردازش داده های فراگرفته از محیط پیرامون، این امکان را به وجود می آورد تا اطلاعاتی که مربوط به حریم خصوصی اشخاص بوده یا مبین اخلاق، رفتار و سایر خصوصیات خلقی یا زیستی افراد باشد توسط این ابزارها فراگرفته شده و ذخیره این اطلاعات امکان توزیع آنها به افراد سودجو را فراهم آورد. این اطلاعات می تواند علاوه بر خصوصیات خلقی افراد در میزان اموال قیمتی موجود در منزل یا هر اطلاعات دیگری خلاصه گردد که طراحی پروتکل هایی که به قصد انتقال این اطلاعات به اشخاص سودجو طراحی شده اند و یا هک سیستم عامل ابزارهای مذکور توسط هکر ها یا بدافزارها منجر به نقض حریم خصوصی افراد گردد (Brown& Rose,2019) .در راستای حل چالش بیان شده، نظام حقوقی اتحادیه اروپا مبادرت به سیاستگذاری تقنینی در راستای پیش بینی مقرراتی در جهت پیش گیری از مشکلات بیان شده نموده است. اهم این مقررات در دسترسی موردی شرکت های عامل و تولید کننده پروتکل ها یا ابزارهای حوزه اینترنت اشیا در کنترل عملکرد این ابزارها، شفافیت نحوه دریافت، پردازش و جریان داده پیام های الکترونیکی، ایجاد ارتباط میان ماشین ها مبتنی بر رضایت دارنده، تصویب قوانینی در جهت حمایت از حفاظت از داده پیام های ذخیره شده در این ابزارها و پیش بینی محیطی امن در جهت انتقال و ذخیره داده پیام های الکترونیکی خلاصه شده است. در نظام حقوقی اتحادیه اروپا، اولین مقرره ای که در جهت حفاظت از داده پیام های الکترونیکی و اطلاعات شخصی افراد تصویب گردید، دستورالعمل حفاظت از داده پیام های الکترونیکی مصوب ۱۹۹۵ بود. از آنجا که دستور العمل بیان شده از

پتانسیل حمایتی لازم در راستای حفاظت از اطلاعات شخصی افراد که توسط ابزارهای اینترنت اشیا مورد دریافت و تبادل قرار می گرفتند برخوردار نبود، نیاز برای تصویب مقرراتی جدید مطابق با مقتضیات و نیاز های روز جامعه اروپایی در دستور کار قرار گرفت. اهم دلایلی که منجر به تصویب مقرره جدید در این خصوص گردید در عدم وجود مقررات لازم در خصوص مکانیسم حفاظت از داده پیام های الکترونیکی در بسترهای نامتمرکز مانند بلاک چین، عدم وجود مقررات لازم در نحوه حفاظت از داده پیام های دریافت، پردازش و انتقال داده شده توسط ابزارهای اینترنت اشیا و عدم وجود مقررات لازم در راستای پیش بینی مسئولیت های حقوقی برای شرکت ها یا دولت های متبوع شرکت های سازنده ابزارهای الکترونیکی در موارد نقض حقوق دارنده ابزار، خلاصه شده است(Lachlan&Etc,2019,3) . از این رو این اتحادیه با تصویب و اجرایی نمودن مقررات جدیدی با عنوان مقررات عمومی حفاظت از داده پیام‌های الکترونیکی[۲] در سال ۲۰۱۸ لازم الاجرا گردید، مبادرت به تصویب قواعدی جدید در جهت رفع خلاء های قانونی مقررات پیشین نمود. با توسعه فن آوری اینترنت اشیا به اقصی نقاط جهان، کشورهای در حال توسعه نیز نیازمند پیاده سازی این فن آوری در بخش های مختلف تجارت یا صنعت خود خواهند بود. حتی بسیاری از اقشار این جوامع نیز با خرید این ابزارها سعی در انجام بسیاری از امور روزمره یا کاری خود به وسیله ماشین ها را خواهند داشت. از این رو دیر یا زود کشورهای در حال توسعه مانند ایران نیز با چالش های موجود در این حوزه مواجه خواهند شد. از این رو تحلیل تجارب کشورهای توسعه یافته از جمله کشورهای حوزه اتحادیه اروپا در سیاستگذاری های تقنینی یا اجرایی در راستای رفع چالش های موجود می تواند یکی از گام های اساسی در جهت پذیرش هر چه سریعتر این فن آوری باشد. سوال اصلی پژوهش این است که چالش های موجود در راستای حفاظت از حریم خصوصی افراد در برخورد با ابزارهای اینترنت اشیا یا کنترل کنندگان آنها چه بوده و چه راه حل هایی در این خصوص پیش بینی شده است؟ برای پاسخ به سوال فوق، پژوهش حاضر بدلیل عدم وجود هرگونه پیشینه در مقالات و کتب منشره در نشریات علمی کشور ایران به روش اسنادی و با مطالعه تطبیقی جدیدترین مقررات مصوب اتحادیه اروپا و نظریات متخصصین فنی و حقوقی این اتحادیه در پنج گفتار پس از بررسی مبنای انجام پژوهش حاضر و ارائه تعاریفی از متغیر های اصلی پژوهش(گفتار اول)، به تبیین مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا(گفتار دوم)، سیاست های لازم در بهبود مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا (گفتار سوم) اشاره و پس از آن به تحلیل سیاستگذاری های موجود در راستای عملکرد کنترل کنندگان (گفتار چهار) یا ابزارهای اینترنت اشیا(گفتار پنجم) در ارتباط با قواعد مسئولیت پذیری پرداخته است.

2- General Data Protection Regulation

مبنا شناسی پژوهش و مفهوم شناسی متغیر های اصلی

پیش از آغاز مباحث اصلی پژوهش ضرورت بررسی مبنای پژوهش صورت گرفته و بیان تعاریفی از متغیر های اصلی بحث ضرورت دارد. از این رو در این گفتار به تبیین این موارد اقدام می‌شود.

مبنا شناسی پژوهش

محوریت اصلی مقاله حاضر بر ارائه راهکارهای سیاستی در پیاده سازی ابزارهای اینترنت اشیا جهت توسعه دولت الکترونیکی با محوریت مسئولیت پذیری در عملکرد این ابزارها استوار است. دولت الکترونیکی به طور خلاصه به معنای استفاده از فناوری اطلاعات در دولت می‌باشد. وجود این امر منجر شده است تا قانون گذار در ماده ۷۹ قانون تجارت الکترونیکی، وزارت بازرگانی را موظف به پیاده سازی فناوری های نوظهور جهان در کشور ایران نماید. علاوه بر آن توسعه زیرساخت های نهادهای اجرایی در حوزه فناوری اطلاعات مطابق با مقررات حاکم بر آیین نامه اجرایی تحقق دولت الکترونیکی مصوب ۱۳۸۲ منوط به به کارگیری فناوری‌های نوظهور گردیده است. این امر به طور صریح در زمینه تسهیل تبادل اطلاعات در میان دستگاه های دولتی و بخش خصوصی(ماده ۱۸)، ارائه آموزش های لازم به کارکنان در زمینه فناوری های نوین اطلاعاتی (ماده ۱۵) و توسعه زیربنای فناورانه دستگاه های دولتی(ماده ۱۰) در مقررات مرقوم مورد اشعار قرار گرفته است. از طرفی ماده ۲ ضوابط فنی اجرایی توسعه دولت الکترونیکی مصوب شورای عالی فناوری اطلاعات در سال ۱۳۹۳ نیز به طور صریح ضرورت به کارگیری فناوری های نوین در جهت افزایش سرعت، مسئولیت پذیری و اطمینان در دستیابی به اهداف دولت الکترونیکی را متذکر شده است. در سیاستهای کلی نظام اداری ابلاغی سال ۱۳۸۹ مقام معظم رهبری نیز بر تحقق دولت الکترونیک و لزوم استفاده از فناوری های نوین برای ارائه خدمات و مسئولیت پذیری تاکید شده است. در بند ۱۵ سیاستهای مزبور توسعه نظام اداری الکترونیک و فراهم آوردن الزامات آن به منظور ارائه مطلوب خدمات عمومی مورد تاکید قرار گرفته است. بر اساس بند ۱۶ نیز دانش بنیان کردن نظام اداری از طریق بکارگیری اصول مدیریت دانش و یکپارچه سازی اطلاعات، با ابتناء بر ارزشهای اسلامی به عنوان یک سیاست محوری در نظام اداری محسوب است. بند ۲۰ به قانونگرائی و مسئولیت پذیری اداری تاکید شده است که شامل مسئولیت کلیه اشخاص ذیمدخل در فرایند عملکرد ابزارها اینترنت اشیا در بستر دولت الکترونیک می شود. از این رو با عنایت به آنچه در سیاستها، متون قانون فوق مورد ذکر قرار گرفته است، می توان ضرورت انجام پژوهش های کاربردی در زمینه سیاستگذاری پیاده سازی ابزارهای نوین حوزه فناوری اطلاعات از جمله ابزارهای اینترنت اشیا چه در حوزه سیاستگذاری تقنینی و چه در حوزه سیاستگذاری را استنباط نمود. از این رو نگارندگان بر مبنای اهداف بیان شده مبادرت به انجام پژوهش حاضر نموده اند. هرچند در نظام حقوقی ایران، مرز دقیقی بین

قانون گذاری و سیاستگذاری ترسیم نشده است (مرکز مالمیری،۱۳۹۰، ۲۱۵) و در بسیاری از قوانین بویژه قوانین برنامه توسعه (مواد ۶۷ تا ۶۹ قانون برنامه ششم)، سیاستگذاری صورت می‌گیرد، اما بی تردید با توجه با نقش قانون و حاکمیت قانون به عنوان یکی از ویژگی ها و ابعاد حکمرانی خوب، قانونگذاری مطلوب در پاسخ به ضرورت های ناشی از توسعه فناوری های ارتباطی، ضمن اینکه می تواند به عنوان سیاستگذاری به مفهوم عام محسوب شود، در عین حال یک نوع رویکرد سیاستگذاری یعنی سیاستگذاری تقنینی تلقی می شود. ارتباط میان تصویب قوانین کارآمد در مسیر جهت دهی به کیفیت بکارگیری ابزارهای نوین حوزه فناوری اطلاعات و چگونگی اجرایی نمودن استفاده از این نوع ابزارها و نقش توسعه فناوری اطلاعات در شکل گیری سیاست های کلان دولت، امری است که نیازمند بررسی دقیق و انجام پژوهش‌های تفصیلی می‌باشد. از این رو، در مقاله حاضر ضمن تبیین ابعاد حقوقی مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا، توصیه های سیاستی در بهبود کیفیت نوین ترین ابزار فناورانه جهان با عنوان ابزارهای اینترنت اشیا و تبیین سازوکار مسئولیت پذیری نهادهای فعال در این حوزه که عمیقا با شکل گیری سیاست های کلان دولت چه در حوزه های ملی و چه در حوزه های فراملی در ارتباط است، ارائه شده است.

مفهوم شناسی متغیر های اصلی

برای ورود به بحث، به جهت تخصصی بودن موضوع، در ابتدا نیازمند بررسی مفهوم متغیر های اصلی پژوهش می‌باشیم. از این رو گفتار حاضر در دو بند ذیل، مبادرت به تحلیل مفهوم اینترنت اشیا و دارندگان این ابزارها، کنترل کنندگان و پردازندگان اطلاعات می نماید.

اینترنت اشیا

ماده ۲۹ اعلامیه مرکز نظارت بر داده پیام های اتحادیه اروپا مصوب ۲۰۱۰ با الحاقات و اصلاحات ۲۰۱۵،[3] 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 داده ها طراحی شده و همانطور که از قابلیت ارتباط با عامل انسانی برخوردار می‌باشند، با بهره مندی از شناسه های منحصر به فرد، با دستگاه ها یا سیستم های دیگر با استفاده از قابلیت های شبکه تعامل برقرار می‌کنند»[4] به عبارت دیگر ابزارهای اینترنت اشیا نوعی ابزارهای هوشمند می‌باشند که با تعبیه پروتکل های منحصر به فرد به پردازنده آنها، همانند انسان قابلیت دریافت و پردازش داده پیام ها جهت انجام وظایف از پیش تعیین شده را کسب می نمایند. این ابزارها، قابلیت اتصال به بسترهای متمرکز مانند شبکه جهانی وب یا نامتمرکز مانند بلاک چین

3- European Data Protection Supervisory
4- WP29, Opinion 8/2014 (n 5) 4.

را داشته و از این طریق قابلیت ارتباط از راه دور با انسان یا دیگر سیستم ها را برخوردار می‌باشند. امروزه ابزارهای متعددی، ازجمله ساعت ها، تلویزیون ها و ترموستات های هوشمند طراحی شده اند که هر یک با برخورداری از پروتکل های خاص، نسبت به انجام وظایف تعیین شده، 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 توسعه یافته نیز بر متخصصین این امر مشهود می‌باشد. اشخاصی که مبادرت به خرید این نوع ابزارها از تولید کنندگان آنها می نمایند، دارنده ابزار تلقی می شوند. دارنده ابزار می تواند اعم از مالک آن یا شخصی که از طرف مالک، ابزار را در اختیار داشته باشد، شناخته شود.

پردازنده و کنترل کننده

بند هفتم از ماده چهارم از دستورالعمل اجرایی سال ۲۰۱۸ اتحادیه اروپا در تعریف کنترل کننده بیان می‌دارند: «کنترل کننده 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 می‌باشند که قابلیت دسترسی به اطلاعات این ابزارها را برخوردار بوده و از امکان کنترل آنها نیز بهره مند هستند. این اشخاص حقیقی یا حقوقی که کنترل کننده نامیده می‌شوند، مطابق با نقش خود در عملکرد یک ابزار، می‌توانند شناسایی شوند. به عبارتی اگرچه اطلاق عنوان کنترل کننده از پردازنده داده پیام جدا می‌باشد، اما در صورتی که پردازش داده توسط ابزار اینترنت اشیا صورت پذیرد، دسترسی کنترل کننده به اطلاعات پردازش شده، هرچند تحت خط مش 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 مصوب ۲۰۱۰ نیز مورد تاکید قرار گرفته است.[5] در مقابل به تعبیر بند هشتم از ماده چهارم دستورالعمل مرقوم، پردازنده «شخصی حقیقی یا حقوقی، مقامات دولتی یا هر نهاد دیگری است که داده های شخصی را از طرف کنترل کننده پردازش می‌کند.» بنابراین سازو کار عملکرد پردازشگر، تحت خط مشی است که توسط کنترل کننده تعیین می‌گردد. از این رو، در صورتی که خط مش و چگونگی پردازش داده پیام ها توسط پردازشگر تعیین گردد، وی دارای عنوان کنترل کننده بوده و مسئولیت های قانونی پیش بینی شده برای کنترل کننده، برای وی نیز قابل اعمال خواهد بود. این امر اعم از تصریح یا تبانی بر وجود فرایند مذکور در قراردادهای فی مابین کنترل کننده یا پردازنده و حکم عرف در تعریف مسئولیت حقوقی مذکور، خواهد بود (بند دهم از ماده ۲۸). در کنار این موارد اعلامیه مصوب سال ۲۰۱۰ نیز برای تمایز میان پردازنده و کنترل کننده دو شرط اساسی تمایز شخصیت و انجام دستورات کنترل کننده توسط پردازنده را پیش بینی نموده است. از این رو اگر هر دو عنوان پردازنده و کنترل کننده در

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

یک شخص وجود داشته باشند، وی در مقام انجام وظایف پردازندگی نیز واجد مسئولیت کنترل کنندگی خواهد بود (شماره ۱۱ از بند اول از ماده ۲۹ اعلامیه).

تبیین ابعاد سیاستگذاری مناسب در مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا

امروزه به کارگیری ابزارهای اینترنت اشیا در جوامع منجر به ایجاد چالش هایی فنی و حقوقی در مکانیسم عملکرد آنها شده است. سیاستگذاری تقنینی در جهت حل موانع موجود نیازمند شناسایی آنها می‌باشد. ذیلا به تبیین چالشها و ارائه راهکارهای مرتبط با این گفتار اقدام می‌شود.

چالش‌های مرتبط با سیاستگذاری مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا

اخذ رضایت دارنده ابزار در نوع و کیفیت اطلاعات ذخیره و پردازش شده

یکی از مشکلات موجود در عملکرد ابزارهای اینترنت اشیا عدم وجود رضایت دارنده این ابزارها در نوع و کیفیت اطلاعات ذخیره و پردازش شده می‌باشد. بسیاری از ابزارهای اینترنت اشیا در دریافت اطلاعات مورد نیاز خود از روش هایی مانند بازخورد های حسی، صداها یا دستور هایی از راه دور از طریق ابزارهایی الکترونیکی مانند گوشی های تلفن همراه (از طریق آپشن Smart Things) اقدام می نمایند. این فرایند منجر می گردد تا برای عامل انسانی، آگاهی از اینکه چه اطلاعاتی از وی در اختیار ابزار قرار گرفته و به چه شکلی مورد استفاده قرار خواهد گرفت، دشوار باشد. نتیجه این امر می تواند منجر به نقض حقوق معنوی افراد گردد. به عبارت دیگر این حق معنوی هر فرد است که رضایت خود را در دراختیار گرفتن اطلاعات شخصی او یا پردازش آن توسط دیگران ابراز دارد. اطلاعات شخصی افراد جزو حقوق غیر قابل تعرض آنها می باشند که دسترسی به این اطلاعات به صورت موردی، در موارد خاص، به صورت شفاف و با آگاهی آنها باید صورت پذیرد. از این رو دسترسی به هر گونه اطلاعات شخصی از افراد مانند سلامت، جنسیت، اطلاعات بیومتریک و ... با رضایت صریح آنها باید محقق شود. همچنین در بسیاری از موارد مشاهده می گردد که شرکت های فروشنده این ابزارها هنگام انعقاد قرارداد با افراد در قراردادهایی پیش نویس شده مبادرت به پیش بینی شروطی می نمایند که امکان نقض حریم خصوصی آنها را فراهم می آورد. مشکل از آنجا ناشی می گردد که بسیاری از تهیه کنندگان این ابزارها در هنگام خرید آنها نه مفاد قرارداد را مطالعه می کنند نه هنگام خرید کالا حتی در صورت مطالعه مفاد قرارداد از امکان مذاکره به دلایلی همچون عدم آگاهی از شرایط تعیین شده یا الحاقی بودن قرارداد برخوردارند (Luger&Etc,2013,2691).

عدم وجود شفافیت در پردازش اطلاعات

چالش دیگر عدم وجود شفافیت پردازش اطلاعات است. ابزارهای اینترنت اشیا برای انجام وظایف خود نیازمند جمع آوری اطلاعات هستند. چالش موجود این است که اطلاعات جمع آوری شده در کجا و چه مدت نگهداری شده و توسط چه کسانی قابلیت پردازش را خواهد داشت (Tolmie&Etc,2016,457). همچنین در هنگام اتصال دستگاه های مختلف با یکدیگر سوال پیش رو این است که چه اطلاعاتی میان ابزارهای مذکور مورد تبادل قرار گرفته و آیا عامل انسانی بر نحوه تبادل میان ابزارها نظارت دارد. چالش دیگر عدم وجود نظارت در ذخیره یا تبادل داده پیام های الکترونیکی می‌باشد(Urquhart,2017,325) . از آنجا که در محیط شبکه جهانی وب[۶] اطلاعات قابلیت ذخیره در فضای ابری را داشته و سرور های پشتیبانی کننده این بستر خارج از کشور های اتحادیه اروپا قرار دارد، نظارت بر نحوه ذخیره سازی و حفاظت از حریم خصوصی افراد دیگر چالشی است که در این نظام مورد نظر قرار گرفته است. همچنین به جهت عدم امکان کنترل در محل های ذخیره این اطلاعات در شبکه جهانی وب همواره امکان انتقال اطلاعات شخصی اتباع کشورها به کشورهای معاند و سوءاستفاده از آنها وجود دارد.

راهکار های حل چالش های سیاستگذاری مسئولیت پذیری در عملکرد ابزار های اینترنت اشیا

راهکار مبتنی بر حساب مجازی

علی رغم وجود چالش های بیان شده، مقررات سال ۲۰۱۸ اتحادیه اروپا واجد قواعدی آمره در راستای پیش بینی راه حلی از سوی کشور ها در راستای رفع چالش های موجود می‌باشد. مطابق با مفاد مقررات مذکور، اخذ رضایت اشخاص در دسترسی به اطلاعات شخصی آنها و پردازش اطلاعات مذکور، تحت عنوان «حق دسترسی و پردازش اطلاعات» جزو حقوق غیر قابل نقض آنها قلمداد شده(مواد ۱۵و۲۱) و افراد در هر زمان از حق ایجاد محدودیت در دسترسی کنترل کنندگان ابزارها به اطلاعات آنها(ماده ۱۸)، پاک کردن اطلاعات در اختیار گرفته شده از سوی کنترل کنندگان(ماده ۱۷) و تعیین شرایط انتقال یا ایجاد محدودیت در انتقال اطلاعات خود(ماده ۲۰) برخوردار شده اند. راه حلی که در این خصوص مورد تصریح ماده پنجم مقررات مذکور قرار گرفته است، ایجاد حساب مجازی برای دارندگان این ابزار ها می‌باشد. از این رو اطلاعات دریافتی این ابزارها تنها به شکلی قابلیت دریافت و پردازش یا انتقال توسط خود آنها

6- World Wide Web

یا کنترل کنندگان آنها را خواهند داشت که مطابق با تصریح مفاد بند دوم از ماده سوم مقررات ۲۰۱۸، جزئیات این دسترسی در حسابی کاربری به اطلاع دارنده رسیده و وی وقوع تراکنش‌های مذکور را مورد تایید موردی قرار دهد(Lachlan&Etc,2019,6-7) .

ارائه گزارش عملکرد توسط کنترل کنندگان

مطابق با مفاد ماده ۲۹ مقررات مذکور شرکت ها موظف می باشند تا در مواعد معینی از زمان، گزارشی از نحوه عملکرد خود و اطلاعات به دست آمده از کاربران را به دولت متبوع خود ارائه نمایند. فرایند پیش بینی شده واجد اثرات مثبتی می‌باشد. مطابق با مفاد ماده ۵ مقررات مذکور، شرکت های تولید و کنترل کننده ابزارهای اینترنت اشیا مسئولیت مطلق در راستای حفاظت از اطلاعات شخصی افراد دارند. در این صورت هرگونه سوءاستفاده از اطلاعات اشخاص چه با عمد یا تقصیر شرکت کنترل کننده ابزار صورت گرفته یا این سوء استفاده استنادی به آن شرکت نداشته باشد، منجر به مسئولیت مدنی شرکت مذکور خواهد بود. تصویب چنین مقرراتی که مفاد آنها با اصول و قواعد کلی حقوق داخلی کشور ها در تعارض می‌باشد، نشان از توجه حداکثری نظام حقوقی اتحادیه اروپا به لزوم تدوین سیاستها و راهبرهای مناسب برای حقاظت از اطلاعات شخصی افراد و پاسخگو نمودن نظام مدیریت عملکرد ابزارهای اینتنت اشیا می‌باشد. در نظام حقوقی کشورهای توسعه یافته یا در حال توسعه مانند ایران، شناسایی مسئولیت مطلق برای اشخاص حقیقی یا حقوقی خلاف اصول حقوقی بوده و این امر نیاز به تصریح قانونی دارد. از این رو تا زمانی که این مقررات در نظام حقوقی کشوری مورد تصویب قرار نگیرد، نمی توان با وحدت ملاک گیری از این مقررات، در مسئولیت پذیری شرکت های تولید کننده این ابزار ها در کشورهای متبوع، قائل به مسئولیت تضمینی بود. از این رو در حال حاضر در کشوری مانند ایران، در صورتی می توان این شرکت ها را مسئول شناخت که اولا سوءاستفاده از اطلاعات افراد مستند به عملکرد آنها بوده یا در این خصوص تقصیر نموده باشند. از این رو اگر رایی در دادگاه های کشورهای عضو اتحادیه اروپا در این خصوص صادر گردد که نشان از مسئولیت تضمینی شرکتی در ایران باشد و این رای برای اجرا به دادگاه ایرانی احاله گردد، سوال پیش رو این است که آیا رای مزبور قابلیت اجرا در نظام حقوقی ایران را خواهد داشت؟ آیا این قواعد می تواند قواعد آمره موجود در نظام حقوقی ایران را که با نظم عمومی در ارتباط هستند، نقض نماید(ماده ۱۶۹ قانون اجرای احکام مدنی مصوب ۱۳۵۶)؟ چالش موجود از آنجا ناشی می گردد که ممکن است در هنگام انعقاد قرارداد، متعاملین؛ قانون حاکم بر قرارداد را قانون کشوری خاص از جمله ایران در نظر گرفته باشند که قواعد حقوقی ناظر بر آن با قواعد مقررات مصوب ۲۰۱۸ در شناسایی مسئولیت مطلق در تعارض است. از این رو از یک طرف دادگاه های کشورهای اتحادیه اروپا ملزم به رعایت مقررات آمره مصوب ۲۰۱۸ می باشند که به جهت ملاحظات امنیتی که در تصویب آنها لحاظ شده است شدیدا با نظم عمومی این

اتحادیه دارای تلازم می‌باشد و از طرفی دیگر چنین مقرراتی قابلیت اجرا در نظام حقوقی ایران را ندارند. از این رو اگر حکمی بر خلاف این مقررات صادر شود قابلیت اجرا نداشته و اگر مطابق با مقررات مصوب صادر گردد، منجر به نقض اصل حاکمیت اراده طرفین در انعقاد قراردادها می‌باشد که صراحتا در بند اول از ماده ۳ مقررات رم یک مورد تصریح قرار گرفته است (Marshall&Etc,2012,28). از این رو چالش بیان شده یکی از خلاء های این مقررات در راستای اعمال آن در نظام حقوقی کشور های اتحادیه اروپا تلقی می گردد. در نظام حقوقی ایران اصل حاکمیت اراده در تعیین قانون حاکم بر قرارداد به حکم ماده ۹۶۸ قانون مدنی در خصوص اتباع خارجی مورد شناسایی و در خصوص اتباع ایرانی یا ایرانی و خارجی مطلقا تابع قانون محل وقوع عقد قرار گرفته است. صرف نظر از اختلاف نظراتی که حقوق دانان در راستای تفسیر مقررات این ماده ارائه نموده اند، به نظر نگارندگان به جهت آمره بودن مقررات این ماده و گنجاندن آن در قانونی ماهوی و آمره، مطابق با نص قانون باید مفاد آن به صورت الزامی مورد توجه مراجع قضایی قرار گیرد. از این رو اگر متعاملین خارجی قانون حاکم بر قرارداد را مقررات مصوب اتحادیه اروپا قرار دهند بر طبق همان مقررات عمل و اگر متعاملین ایرانی یا خارجی و ایرانی باشند، باید قواعد موجود در نظام حقوقی ایران بر توافقات آنها اعمال گردد. البته به نظر می رسد در حالت اخیر اگر حکمی مطابق با قواعد موجود در نظام حقوقی ایران از دادگاه ایرانی صادر گردد، به جهت مخالف با مقتضیات مقررات مصوب ۲۰۱۸ در کشورهای اروپایی قابلیت اجرا نداشته باشد. نکته ای که خاطر نشان می گردد این است که اگر مقررات مصوب ۲۰۱۸ در نظام حقوقی ایران به عنوان قانون ماهوی مورد تصویب قرار گیرد، به نظر نگارندگان مفاد مقررات مزبور در خصوص متعاملین خارجی که مطابق با قواعد آمره ماده ۹۶۸ قانون مدنی قانون حاکم بر قرارداد را قانون کشوری ثالث قرار دهند، به جهت ارتباط آن با نظم عمومی بر قراردادهای آنها حاکم خواهد بود. به عبارتی تصویب مقررات مصوب ۲۰۱۸ می تواند مخصص مفاد ماده ۹۶۸ قانون مدنی در خصوص اتباع خارجی باشد.

تبیین سیاست‌های لازم در بهبود روند نظارت بر مسئولیت‌پذیری در عملکرد ابزارهای اینترنت اشیا

مطابق با مفاد بند اول از ماده ۲۴ مقررات سال ۲۰۱۸، دولت ها موظفند تا در راستای عملکرد صحیح شرکتهای تولید کننده ابزارهای اینترنت اشیا و تحقق هر چه بهتر اهداف مقرر در این مقررات، مبادرت به سیاستگذاری های صحیح در این خصوص نمایند. مطابق با مفاد ماده ۳۵ مقررات سال ۲۰۱۸ اطلاعاتی دارای ریسک بالا[7] تلقی می گردند که واجد خطراتی از جمله زیان

7- High Risk

مالی[۸] یا سرقت اطلاعات هویتی[۹] افراد باشند. از آنجا که عملکرد صحیح ابزارهای اینترنت اشیا می تواند به نوعی دربردارنده جمع آوری اطلاعات بیومتریک افراد باشد، این امر موجب می گردد تا دولت ها در نحوه عملکرد شرکت های تولید ابزارهای اینترنت اشیا دخالت نموده و با وضع سیاست های کلی مبادرت به نظارت بیشتر در نحوه فعالیت آنها نمایند. اهم سیاست های تصریح شده در این مقررات به قرار ذیل است:

سیاست‌های صدور گواهینامه فعالیت

فعالیت شرکت هایی که مستقیما با اطلاعات بیومتریک و حریم خصوصی افراد در تولیدات خود در ارتباط می باشند، به حکم ماده ۳۰ مقررات ۲۰۱۸ اتحادیه اروپا منوط به تشخیص صلاحیت آنها از سوی کشور متبوع می‌باشد. از این رو کشورها نیازمند سیاستگذاری های اجرایی و تقنینی در جهت پیش بینی تشریفات تخصیص مجوز فعالیت برای شرکت های متبوع هستند. این مجوز ها پس از شناسایی شخصیت، هویت و صلاحیت های اخلاقی کارکنان شرکت ها، سوابق حقوقی و کیفری مشارالیهم، نوع و کیفیت فعالیت آنها و بررسی تولیدات آنها از حیث رعایت ملاحظات امنیتی باشد. این امر می تواند سوء استفاده شرکت ها از اطلاعات در دسترس را به حداقل ممکن برساند. در کشورهای توسعه یافته اتحادیه اروپا، تخصیص مجوز استفاده از امضائات دیجیتالی یا تبادل ارزهای رمزنگاری شده دیجیتالی مطابق با مفاد ماده ۲ کنوانسیون یکنواخت سازی معاملات مبتنی بر ارزهای مجازی منوط به شناسایی هویت و مایملک اشخاص از سوی مراجع صلاحیت دار دولت متبوع آنها می‌باشد. این مقررات به نوعی می توانند نیازهای جامعه اروپایی در بررسی موشکافانه مدارک هویتی کارکنان شرکت ها (موضوع ماده ۳۰ مقررات ۲۰۱۸) را نیز شامل شوند. پیاده سازی این تشریفات در راستای تخصیص گواهینامه های فعالیت مطابق با تشریفات ماده ۲ کنوانسیون مذکور می تواند سیاستگذاری صحیحی در اعطای مجوز تلقی گردد. از این رو در صورتی که افراد دارای مجوز های بیان شده باشند، نیازی به صرف هزینه برای بررسی صلاحیت مجدد آنها نیز وجود نخواهد داشت. این تشریفات در حال حاضر در نظام حقوقی ایران قابلیت پیاده سازی ندارند. چرا که به جهت عدم سیاستگذاری های تقنینی و اجرایی صحیح از سوی حاکمیت، بسیاری از اراضی موجود در ایران فاقد سابقه ثبتی می باشند. از این رو شناسایی مایملک افراد به عنوان یکی از مشکلات جاری در نظام حقوقی ایران قلمداد می گردد. توجه به تجربیات کشورهای توسعه یافته در این زمینه می تواند به عنوان راه حلی مناسب از سوی نگارندگان پیشنهاد گردد. از آنجا که مهمترین مشکلات نظام ثبتی کشورها در جهت انجام عملیات مقدماتی، ثبت املاک هزینه بالا و وقت گیر بودن این تشریفات می‌باشد کشورهای توسعه یافته مانند انگلستان و اسکاتلند در راستای اجرایی نمودن اهداف تصویب

8- Financial Loss
9- Identity Theft

قوانین ثبت سال های ۲۰۰۲ و ۲۰۱۲ خود، برای مشارکت بیشتر شهروندان در این خصوص اقداماتی مانند تخفیف و معافیت های مالیاتی برای افرادی که در مواعد تعیین شده از سوی دولت اقدام به ارائه اظهارنامه ثبتی نمایند پیش بینی نموده اند. همچنین از آنجا که کاهش هزینه‌های ثبتی یکی از مهمترین عوامل علاقه مندی افراد به ارائه اظهارنامه های ثبتی می‌باشد، دولت‌های این کشور ها موظف گردیده اند تا مقدار یا در برخی شرایط تمامی هزینه های ثبتی اراضی فاقد سابقه ثبتی را نیز بر عهده بگیرند(camba,2015,2) .

ایجاد شفافیت در عملکرد نهادها

شفافیت در عملکرد نهادهای تولید کننده ابزارهای اینترنت اشیا یکی از مبانی حفاظت از داده پیام های الکترونیکی برای دولت های متبوع آنهاست(Singh&Etc,2019,4-5) . این امر در ماده ۱۲ مقررات مذکور نیز مورد تاکید قرار گرفته است. مطابق با مفاد این مقررات، شرکت های بیان شده تنها در صورتی قابلیت پردازش داده پیام های شخصی افراد را خواهند داشت که برای اهداف مشخصی با جلب رضایت مالک این ابزارها، این پردازش صورت گیرد. از این رو پردازش داده پیام های مذکور جز در مواردی که این اهداف از ضرورت کافی برخوردار نباشد می تواند منجر به مسئولیت مدنی شرکت مزبور گردد. این فرایند باید در پروتکل های طراحی شده برای تعیین خط مش عملکرد ابزارهای اینترنت اشیا نیز پیش بینی گردد، ثمره این امر می تواند جلوگیری از سوءاستفاده های احتمالی از اطلاعات شخصی افراد به دلایل واهی باشد. همچنین مطابق با مفاد ماده ۱۲ شرکت های مذکور موظف می باشند تا میزان اطلاعات جمع آوری شده، پردازش شده و ذخیره شده را طی گزارش های موردی به اطلاع مراجع صلاحیت دار برسانند (Abrams,2019). مفاد ماده ۱۲ مقررات ۲۰۱۸ در هیچ کدام از قوانین مصوب کشور ایران مورد تصریح قرار نگرفته است. از این رو اگر این مقررات به عنوان قانون آمره در کشور ایران تصویب نشده یا مقررات آنها در قوانین مصوب گنجانده نشود، نمی توان این تشریفات را به صرف صدور آیین نامه ها یا بخشنامه های دولتی برای اشخاص حقیقی یا حقوقی خارج از دولت حاکم دانست و برای آنها ایجاد مسئولیت نمود. از این رو عدم وجود این مقررات به عنوان یکی از خلاء های قانونی در نظام حقوقی ایران شناخته می شود که حل آن نیازمند سیاستگذاری های صحیح تقنینی می باشند.

سیاستگذاری عملکرد نهادهای کنترل کننده در ارتباط با قواعد مسئولیت پذیری

آنچه در حوزه مقررات حفاظت از داده ها در سال ۲۰۱۸ گنجانده شده است در دو مقوله عملکرد ابزارهای اینترنت اشیا و عملکرد کنترل کنندگان آنها مورد تحلیل قرار می گیرد. از این رو گفتار حاضر با اختصاص دو بند به نحوه عملکرد کنترل کنندگان ابزارهای اینترنت اشیا در جمع آوری، پردازش و تبادل این داده پیام ها و مکانیسم های حمایتی در ارتباط با انجام وظایف

قانونی این نهاد ها در مقررات ۲۰۱۸ پیش بینی شده است، به تبیین سیاستگذاری های تقنینی موجود می پردازد.

ایجاد محدودیت در جمع آوری داده های اولیه، پردازش و تبادل آن‌ها

دسترسی بدون محدودیت به داده پیام ها و پردازش و تبادل آنها همواره می تواند موجبات سوءاستفاده از آنها را پدید آورد. از این رو باید محدودیت هایی در تمامی مراحل جمع آوری، پردازش و حتی تبادل داده پیام ها پیش بینی گردد تا روند دسترسی و به کارگیری این اطلاعات تحت قیود قانونی انجام پذیرد. در این خصوص مقررات حاکم بر اتحادیه اروپا واجد احکامی کاربردی می باشند که توجه به آنها می تواند زمینه هرچه بهتر سیاستگذاری تقنینی در این خصوص در کشورهای در حال توسعه مانند ایران را فراهم آورد. مطابق با مفاد بند دوم از بخش اول از ماده پنجم مقررات ۲۰۱۸ داده های شخصی تنها در صورتی قابلیت جمع آوری را خواهند داشت که برای اهداف مشخص و روشنی این امر صورت گرفته باشد. از این رو دریافت این داده ها بر خلاف اهداف تعیین شده واجد مسئولیت مدنی خواهد بود. از طرفی مطابق با بند سوم از بخش اول ماده پنج مقررات مذکور در مرحله پردازش نیز تنها آن میزان از داده پیام های جمع آوری شده قابلیت پردازش را می یابند که به صورت لازم و کافی برای انجام وظایف ابزار اینترنت اشیا یا کنترل کننده آن ضروری باشند. در مرحله تبادل این اطلاعات به کشورهای خارج از اتحادیه اروپا نیز مقررات مواد ۴۶ و ۴۷ تبادل کنندگان این اطلاعات را ملزم به ارائه گزارش دقیق از میزان و نحوه انتقال اطلاعات به کشور متبوع شخص تحت استانداردهای کمیسیون اتحادیه اروپا نموده است. از جمله این استاندارد ها می توان به انعقاد قراردادهای حفاظت از داده ها[10] اشاره نمود که طی این قراردادها تحت وجود قرارداد متقابل میان کشور انتقال گیرنده با کشور انتقال دهنده یا اتحادیه اروپا اطلاعات مورد نظر برای موارد به خصوصی که در قرارداد کاملا مشخص باشد مورد انتقال قرار می گیرند. در کنار تمامی موارد فوق این اطلاعات در صورتی قابلیت جمع آوری، پردازش یا تبادل را خواهند داشت که با اجازه موردی مالک آنها صورت پذیرند. حقوق مندرج در مقررات ۲۰۱۸ اتحادیه اروپا در مواد ۱۵،۲۸ و ۲۱ به مالک این اطلاعات حق جلوگیری، مشخص نمودن میزان و کیفیت انتقال اطلاعات، اعتراض به فرایند جمع آوری، پردازش و انتقال اطلاعات را اعطا نموده و برای انتقال دهنده مسئولیت تضمینی در صورت وقوع هرگونه سوءاستفاده از این اطلاعات ازجمله لغو گواهینامه عملکرد و جبران خسارات وارده را در نظر گرفته است.

چالش پیش رو این است که در موارد نقض قرارداد های منعقده میان کنترل کننده خارج از اتحادیه اروپا و کشور انتقال دهنده اطلاعات، ملاحظات سیاسی بین المللی همواره می تواند صحت اجرای این مقررات را تحت الشعاع قرار دهد. به عنوان مثال به کرات مشاهده شده است

10- Data Protection Contracts

که کشور هایی نظیر آمریکا در راستای صیانت از منافع خود مبادرت به جاسوسی از کشورهای دیگر دول اتحادیه اروپا نموده اند. اگر سازمانی در ارتباط با مراجع امنیتی کشور آمریکا، این اطلاعات را به صورت غیر قانونی در اختیار آن مراجع قرار داده و با محکومیت در دادگاه‌های اتحادیه اروپا شناخته شود، اولا اجرای چنین احکامی در کشور متبوع این سازمان می تواند محل چالش باشد و ثانیا آیا انعقاد قرارداد می تواند تضمین کننده عدم سوءاستفاده کشوری ثالث از مهمترین اطلاعات بیومتریک شهروندان کشورهای انتقال دهنده اطلاعات باشد به گونه ای که دسترسی غیر مجاز به این اطلاعات حتی می تواند زمینه ساخت سلاح های بیومتریک و کشتار جمعی را نیز برای دول متخاصم پدید آورد؟ اگرچه منطق حقوق مبتنی بر اعتماد متقابل است اما در بسیاری از موارد مشاهده شده است که ملاحظات سیاسی یا امنیتی شدیدا این منطق را تحت الشعاع نقض قرار داده اند. این چالش در پیاده سازی مقررات مذکور در نظام حقوقی ایران نیز می تواند مطرح گردد. از یک طرف انجام وظایف ابزارهای اینترنت اشیا ملازمه با انتقال برخی اطلاعات به کنترل کنندگان آنها دارد و از طرف دیگر انتقال اطلاعات مذکور می تواند نگرانی های بیان شده را دربرداشته باشد. از این رو جامعه بین المللی نیازمند سیاستگذاری اجرایی صحیح در تحلیل ابعاد مسئله است.

سازوکار های حمایتی

دسترسی کنترل کنندگان به اطلاعات مالکان، همواره نگرانی های حاصل از سوءاستفاده از اطلاعات را در نظر مالکان تقویت می نماید. این موضوع نیازمند پیش بینی برخی سازوکارهای حمایتی می‌باشد تا منجر به ایجاد آگاهی کامل از نحوه دسترسی و پردازش اطلاعات توسط مالکان داده پیام ها شود. ضمن اینکه کسب رضایت مالک در تمامی مراحل انجام جمع‌آوری و پردازش داده جزو مهمترین شرایطی می‌باشد که باید توسط کنترل کنندگان مورد اتخاذ واقع شود. نظام حقوقی اتحادیه اروپا در خصوص این مسئله نیز واجد راه حل هایی دقیق می‌باشد که تبیین آنها می تواند در بهبود سیاستگذاری تقنینی در ایران نیز موثر واقع شود. در راستای محقق نمودن جلب رضایت مالک اطلاعات شخصی بر کیفیت جمع آوری یا پردازش اطلاعات ماده ۱۲ مقررات مذکور کنترل کنندگان را ملزم به ارائه گزارشی مختصر، شفاف و قابل فهم برای مالک در خصوص فرایند در حال وقوع نموده است. به عبارت دیگر هر اطلاعاتی که از انسان در اختیار ماشین یا کنترل کننده آن قرار می گیرد باید با زبانی قابل فهم برای وی تفهیم شده و اثرات این امر به وی ابراز گردد(Edwards,2017,27) . همچنین مطابق با مفاد ماده ۱۳ شرکت های کنترل کننده این ابزارها ملزم می باشند تا نسبت به نگهداری رکورد هایی از فرایند های صورت گرفته در مدت زمانی معقول اقدام نمایند تا در صورتی که مالک یا دولت متبوع وی مبادرت به دریافت و بررسی فرایند های انجام گرفته نماید، این امر به آسانی ممکن باشد (ماده ۱۳). علاوه بر این موارد، در راستای حمایت از حقوق مالکان، مکانیسم های دیگری از

جمله ضرورت پردازش داده پیام ها یا کیفیت جمع آوری اطلاعات برای موارد مشخص از سوی ابزار یا کنترل کننده آن در مقررات مختلفی از جمله ماده ۶ این مقررات پیش بینی شده است که به‌طور مشروح در بند پیشین مورد تحلیل قرار گرفت. در کنار این موارد مواد ۳۲ الی ۳۴ مقررات مذکور مبادرت به پیش بینی برخی شرایط در نحوه نگهداری اطلاعات جمع آوری شده و ارائه آن به مراجع صلاحیت دار حکومتی نموده است. ماده ۳۲ این مقررات شرکت های فعال در این حوزه را ملزم به ذخیره اطلاعات تحت فرایند های رمزنگاری داده ای در محیط های ایمن و به دور از تعرض بدافزارها یا هکرها نموده است. با عنایت به تاریخ تصویب این مقررات که همزمان با پیدایش بسترهای نامتمرکز[۱۱] و بهره مندی این بسترها از فن آوری رمزنگاری داده ای می‌باشد، به نظر می رسد، منظور سیاستگذاران از نگهداری داده های جمع آوری شده، ذخیره این اطلاعات در بسترهای نامتمرکز می‌باشد که از سطح امنیت بالاتر نسبت به نوع متمرکز خود برخوردار هستند. مشخص ترین نوع این بسترها بلاک چین[۱۲] نام دارد که داده پیام های الکترونیکی پس از رمزنگاری داده ای در بلوک های این زنجیره ذخیره می شوند. ماهیت نامتمرکز این بستر منجر می گردد تا اطلاعات ذخیره شده در آن از هرگونه حمله سایبری یا خرابکاری بدافزاری در امان باشند (اسلامی تبار، ۱۳۹۹، ۱۴-۱۵). البته به جهت وجود مسئولیت تضمینی در حفاظت از این داده پیام ها، شرکت های فعال در این حوزه قابلیت ذخیره آنها در بسترهای متمرکز یا هر هارد درایو دیگری را نیز دارند. اما آنچه در متن این ماده مورد تاکید قرار گرفته و عدم رعایت آن می تواند منجر به مسئولیت مدنی شرکت گردد، رمزنگاری داده پیام های الکترونیکی است. به عبارت دیگر در صورتی که شرکت به هر طریقی از ذخیره داده پیام در بسترنامتمرکز خودداری نماید، رمزنگاری داده پیام ها در هر مکانی که مورد ذخیره واقع شوند،

۱۱- محبط اینترنت از دو نوع بستر متمرکز و نامتمرکز تشکیل شده است. بسترهای متمرکز بسترهایی هستند که در آنها مرکزیت داده ای وجود دارد. به عبارتی عملکرد این بسترها تحت نظارت سرور مرکزی انجام شده و در صورتی که در عملکرد سرور مرکزی خللی پیش آید، عملکرد تمامی بستر تحت الشعاع خلل پیش آمده قرار می گیرد. مشخص ترین این بسترها، شبکه جهانی وب نام دارد که امروزه به بستر تبادل بسیاری از داده پیام های الکترونیکی یا ذخیره آنها تبدیل شده است. بسترهای نامتمرکز بسترهایی هستند که در آنها مرکزیت داده ای وجود ندارد. در این بسترها داده پیام های الکترونیکی تحت فن آوری رمزنگاری داده ای ذخیره و عدم وجود سرور مرکزی در این بسترها، آنها را از بسیاری از حملات سایبری مصون می نماید. مشخص ترین این بسترها بلاک چین نام دارد (آقایی طوق، ۱۳۹۸، ۱۱-۱۲).

12- Blockchain

بلاک چین بستری نامتمرکز است که از سه جزء بلاک، هش بلاک و پیش هش بلاک تشکیل شده است. بلاک به هر بلوک از این زنجیر گفته می شود که داده پیام های الکترونیکی پس از رمزنگاری داده ای در آنها ذخیره می شوند. هش بلاک به جزئی از این بستر بیان می گردد که مشخص کننده تعداد و نوع داده پیام های ذخیره شده در هر بلاک می باشد. به عبارت دیگر داده پیام های ذخیره شده در هر بلاک، از طریق هش بلاک آن بلاک قابلیت شناسایی و بازخوانی را پیدا می نمایند. این جزء برای هر بلاک منحصر به فرد بوده و به منزله اثر انگشت برای انسان می باشد. پیش هش بلاک نیز به عنوان رابط بلاک های این زنجیره شناخته می شود. این جزء می تواند در مواردی که هر کدام از بلاک های این زنجیره تحت حملات هکر ها یا بدافزارها آسیب دیده یا اطلاعات آنها به سرقت رفته باشد، برای شناسایی بلاک معیوب به کارگرفته شود. به عبارت دیگر در صورت تغییر هر هش بلاک، تغییر تقارن میان پیش هش بلاک ها می تواند در شناسایی بلاک معیوب موثر واقع شود. بلاک چین به دو نوع عمومی و خصوصی تقسیم می شود. بلاک چین عمومی بلاک چینی است که تمامی افراد با استفاده از کلیدهای عمومی خود (که در فرایند تخصیص امضائات دیجیتالی دریافت می دارند) با ورود به سیستم مبادرت به مشاهده اطلاعات ذخیره شده در آن را نمایند. بلاک چین خصوصی نیز بلاک چینی است که عموما در سیستم نهادها یا سازمان های دولتی یا غیر دولتی پیاده سازی شده و افراد با برخورداری از پین کد های منحصر به فرد قابلیت ورود به آن را دارند. (صادقی و زرعی، ۱۳۹۸، ۸۱)

امری ضروری می‌باشد. همچنین در صورتی که نهادهای صلاحیت دار حکومتی مبادرت به درخواست ارائه گزارش از نحوه عملکرد این شرکت ها نمایند، طبق مقررات ماده ۳۳ شرکت ها موظف به ارائه اطلاعات لازم ظرف مدت ۷۲ ساعت می باشند، در غیر این صورت به جریمه‌های مقرر در ماده ۳۴ محکوم خواهند شد(Lachlan &Etc,2019,15) .

سیاستگذاری عملکرد ابزارهای اینترنت اشیا در ارتباط با قواعد مسئولیت پذیری

همانطور که در گفتار پیشین نیز اشاره گردید، پیاده سازی قواعد مسئولیت پذیری موجود در مقررات ۲۰۱۸ اتحادیه اروپا در دو مقوله عملکرد ابزارهای اینترنت اشیا و کنترل کنندگان آنها خلاصه می گردد. کیفیت عملکرد و ایفای نقش این ابزار ها بسته به پروتکل های طراحی شده برای آنها یا نرم افزاری هایی دارد که در پردازنده آنها بارگزاری شده و خط مش عملکرد این ابزارها را تعیین می کنند. عملکرد این ابزارها در ارتباط با داده پیام های شخصی که از دارندگان آنها به دست می آورند، الزاما باید تحت قواعدی که در مقررات مصوب ۲۰۱۸ پیش بینی شده است صورت گیرد. از این رو در این گفتار به تبیین سیاستگذاری های تقنینی اتحادیه اروپا در عملکرد ابزارهای اینترنت اشیا پرداخته می شود.

ایجاد محدودیت در راستای جمع آوری و پردازش داده های اولیه

جمع آوری گسترده اطلاعات از محیط پیرامون به جهت الزاماتی که ابزارهای اینترنت اشیا در انجام وظایف خود دارند یکی از چالش های این حوزه در ایجاد محدودیت عملکرد آنها تلقی می گردد. پردازنده ابزارهای اینترنت اشیا به صورت پیش فرض هر اطلاعاتی که برای پیشبرد خط مش پیش بینی شده برای آنها طراحی شده باشد را بدون در نظر گرفتن ماهیت این اطلاعات جمع آوری و پردازش می کنند. در صورتی که این پردازنده از نوع پیشرفته هوش مصنوعی مانند سیستم های خبره باشد، این سیستم ها می توانند در دریافت اطلاعات از محیط پیرامون، با تشخیص اطلاعات زیستی یا شخصیتی افراد، محدودیت های پیش بینی شده قانونی را در خصوص آنها اعمال و از دریافت یا پردازش این اطلاعات خودداری نمایند (ناصر، ۱۳۹۷، ۶۸-۶۹). این در حالی است که در پردازنده هایی که فاقد برخورداری از هوش مصنوعی بوده و به صرف برخورداری از پروتکل یا نرم افزارهای یک یا دو بعدی مبادرت به اجرای وظایف تعیین شده می نمایند، تشخیص نوع اطلاعات دریافت یا پردازش شده با چالش های فنی مواجه است.(صادقی و ناصر، ۱۳۹۷، ۱۴۶) از این رو ابزارهای اینترنت اشیا در هر حال ملزم به دریافت اطلاعاتی می باشند که برای انجام پروتکل های داده شده به آنها ضروری باشد. لذا در ایجاد محدودیت در عملکرد این ابزارها سیاستگذاران اجرایی ناچار به طراحی پروتکل هایی هستند که در حوزه های مشخصی به تعیین خط مش عملکرد این ابزارها اقدام نمایند. دیگر چالشی که طراحان پروتکل ها یا نرم افزارهای ابزارهای اینترنت اشیا در عملکرد این

ابزارها با آن مواجه هستند، کسب رضایت دارنده ابزار در کیفیت داده پیام های دریافت و پردازش شده توسط ابزارهای تولیدی می‌باشد. در حالت عادی، یک ماشین مانند انسان قابلیت تعامل با عامل انسانی را ندارد. از این رو اجرای مفاد ماده ۱۲ مقررات مصوب ۲۰۱۸ با چالش های فنی مواجه می‌باشد. چرا که یک ماشین در حالت عادی قابلیت فهماندن اطلاعات به انسان یا پاسخگویی به تمام سوالات وی (جز موارد پیش فرض تعبیه شده در پردازنده آن ابزار) را ندارد. از این رو راه حلی که سیاستگذاران اجرایی در راستای تحقق اهداف تقنینی مقررات ۲۰۱۸ پیش بینی نموده اند پیش بینی دیتا باکس هایی می‌باشد که عامل انسانی با در اختیار گرفتن حساب مجازی و ورود به این دیتا باکس از کیفیت اطلاعات ذخیره و پردازش شده توسط ابزار اینترنت اشیا خبردار می گردد(Crabtree,2017,14) . این دیتا باکس ها نیازمند ایجاد در محیط های ایمن می باشند تا اطلاعات ذخیره شده در آنها از حملات سایبری هکر ها یا بدافزارها در امان بماند و در هر حال شرکت عامل عملکرد ابزار اینترنت اشیا مسئولیت تضمینی در جبران خسارات احتمالی پیش آمده در این خصوص را خواهد داشت. ایرادی که دیتاباکس های طراحی شده دارند این است که اگرچه وجود آنها می تواند اهداف شفاف سازی در راستای جمع آوری یا پردازش اطلاعات کاربران را محقق سازد، اما اطلاعات ذخیره شده در این دیتا باکس ها ابتدائا توسط ابزار جمع آوری و پس از آن در دیتاباکس تعیین شده ذخیره می شوند. از این رو وجود این عملکرد می تواند خلاف مفاد مقررات مصوب ۲۰۱۸ در کسب رضایت کاربر در جمع آوری اطلاعات یا پردازش آنها باشد. به عبارت دیگر همانطور که پیشتر بیان گردید، جمع آوری یا پردازش اطلاعات باید با کسب رضایت دارنده صورت پذیرد. این در حالی است که دارنده با ورود به دیتا باکس خود قابلیت مشاهده داده پیام های ذخیره شده ای را خواهد داشت که دریافت یا پردازش آنها با رضایت اولیه وی نبوده است. از این رو راه حل بیان شده اگرچه در جهت ایجاد شفافیت می تواند مفید باشد، اما تضمین کننده اجرای دقیق مفاد مقررات مصوب تلقی نمی گردد. راه حلی که برای رفع چالش های بیان شده ارائه گردیده است، پیش بینی آیتم های مختلف در دیتاباکس های طراحی شده می‌باشد. این آیتم ها به پنج بخش کاربر[۱۳]، منبع داده پیام[۱۴]، محل ذخیره داده پیام[۱۵]، داشبورد[۱۶] و پردازنده داده پیام[۱۷] تقسیم می گردد.

13- User
کاربر به دارنده ابزار اینترنت اشیا بیان می گردد که اطلاعات شخصی وی توسط ابزار جمع آوری، پردازش یا مورد انتقال واقع می گردد. این اطلاعات در محل ذخیره داده پیام در دیتاباکس مربوط به کاربر ذخیره می شوند.

14- Data Source
مبنع داده پیام به ابزار خارج از دیتاباکس اطلاق می گردد که مبادرت به جمع آوری داده پیام از محیط پیرامون کاربر یا خود او نموده و این اطلاعات را در دیتاباکس ذخیره می‌کند. ابزارهای اینترنت اشیا نمونه از منبع داده تلقی می گردند.

15- Data Store
محل ذخیره داده پیام، محلی ا ست که داده پیام های اولیه یا پردازش شده تو سط ابزارهای اینترنت ا شیا در آن ذخیره شده و توسط کاربر قابلیت مشاهده را خواهند داشت.

16- Dashboard
آیتمی اســت که به وســیله آن، کاربر امکان تبادل داده پیام های خود را با اشــخاص ثالث داشــته یا از این طریق می تواند به اشخاص ثالث امکان دسترسی به اطلاعات شخصی خود را اعطا نماید.

17- Data Processors

(McAuley&Etc,2018) نحوه استفاده از این آیتم ها برای کاربران به وسیله برنامه های راهنما[۱۸] که توسط شرکت های تولید کننده ابزارهای اینترنت اشیا طراحی شده اند به صورت کاملا ملموس به زبان ساده به اطلاع کاربران می رسد. تمامی اطلاعات ذخیره شده در دیتاباکس کاربر با اعلامیه ای[۱۹] به پست الکترونیکی یا شماره تلفن همراه وی به اطلاع او رسیده و کاربر از تمامی فرایند های صورت گرفته بر اطلاعات خود آگاهی می یابد. دسترسی کاربر به محل ذخیره داده پیام و عدم ایجاد محدویت در دریافت یا پردازش داده پیام های ذخیره شده در دیتاباکس به منزله اعلام رضایت کاربر در عملکرد ابزار اینترنت اشیا تلقی می شود. از این رو الزامات مقرر در مقررات مصوب ۲۰۱۸ در آگاهی بخشیدن به کاربران و کسب رضایت آنها در نحوه دریافت یا پردازش اطلاعات آنها می تواند به نوعی مورد حل و فصل قرار گیرد.

ایجاد محدودیت در تبادل داده های اولیه

یکی از مهمترین چالش هایی که اتحادیه اروپا در حوزه حفاظت از اطلاعات با آن مواجه است، ابزارهایی هستند که توسط کشورهای خارج از این اتحادیه تولید و به عنوان کالای وارداتی، وارد کشورهای این اتحادیه می شوند. اگرچه مطابق با آنچه که بیان گردید، دیتاباکس هایی در این ابزارها وجود دارد که امکان مشاهده اطلاعات ذخیره شده را برای کاربر فراهم می‌کند، اما این امر مانع از انتقال اطلاعات ابزارهای وارداتی از طرقی غیر قانونی برای کشور صادر کننده نخواهد بود. به عبارت دیگر هیچ تضمینی وجود ندارد که شرکت تولید کننده این ابزارها برای کسب اطلاعات محرمانه شهروندان یک کشور از طریق این ابزارها، اطلاعات شخصی آنها را به صورت محرمانه نگهداری و انتقال ننماید. این امر به یکی از چالش های لاینحل اتحادیه اروپا در راستای وارد نمودن چنین ابزارهایی به کشورهای عضو این اتحادیه قلمداد شده است. البته عواملی مانند بازبینی فنی ابزارهای وارداتی و انجام آزمایش های لازم بر روی این ابزارها می تواند تا حدودی نسبت به شناسایی ابزارهای مخرب کمک کند اما راه حلی تضمینی در این خصوص تلقی نمی گردد. چرا که در هر حال امکان پشتیبان گیری مجازی[۲۰] از داده پیام های ذخیره شده در دیتاباکس فرد و انتقال آن به هر طریق الکترونیکی فراهم می‌باشد (Christidis &Etc,2016,2297-8).

راه حلی که متخصصین برای حل این مسئله بیان نموده اند اتصال سیستم عامل ابزارهای اینترنت اشیا به بستر بلاک چین است. در این صورت داده پیام های ذخیره شده در این بستر

ماشـین های خارج از دیتاباکس می باشـند که توسـط کنترل کنندگان ابزارهای اینترنت اشـیا طراحی و به دیتا باکس هر ابزار متصل می گردند. این ماشین ها قابلیت دریافت اطلاعات ذخیره شده توسط ابزار اینترنت اشیا و ارسال آنها به کنترل کننده را دارند.

18- Bespoke Software
19- Manifest
20- Virtual Backup

برای تمامی افرادی که دارای کلید های عمومی[۲۱] باشند، قابلیت مشاهده را خواهد داشت (Urquhart&Etc,2019,23). از این رو امکان انتقال محرمانه داده پیام ها برای ابزار مزبور منتفی است. به نظر نگارندگان این راه حل نمی تواند به صورت قطعی موجبات رفع نگرانی های موجود را فراهم نماید. چرا که اولا در صورتی منظور از بلاک چین، نوع عمومی آن باشد، آنچه مورد بحث است، اطلاعات محرمانه اشخاص می‌باشد که از دید دیگران باید محفوظ بماند. اگر قرار بر توزیع این اطلاعات در بستری شفاف باشد که همگان قابلیت مشاهده آنها را داشته باشند، عملا سخن از محرمانگی آن اطلاعات بیهوده خواهد بود. ثانیا در صورتی که منظور از بلاک چین نوع خصوصی آن باشد، اتصال سیستم عامل این ابزارها به بلاک چین هیچ محدودیتی از پشتیبان گیری از اطلاعات و ارسال آنها به طرق دیگر الکترومغناطیسی به شرکت تولید کننده ابزار ندارد. از این رو راه حل بیان شده چندان نمی تواند مورد قبول تلقی گردد. لذا حل این مسئله منوط به سیاستگذاری اجرایی و تحلیل دقیق ابعاد فنی این موضوع است.

افزایش امنیت داده‌ای

همانطور که بیان گردید انجام وظایفی که در قالب پروتکل های داده شده به ابزارهای اینترنت اشیا پیش بینی گردیده است، منوط به دریافت اطلاعات و پردازش آنها می‌باشد. این اطلاعات پس از ذخیره در محل های ذخیره داده پیام ها در دیتاباکس های مربوط به هر کاربر قابلیت مشاهده توسط وی را خواهند داشت. از آنجا که این اطلاعات یکبار توسط این ابزارها دریافت می گردد تا زمانی که کاربر نسبت به حذف آن اطلاعات اقدام نکند و ابزار را از جمع آوری مجدد آنها ممنوع ننماید، ابزار در انجام دستورات داده شده به آن، اطلاعات اولیه را مورد پردازش قرار می‌دهد. چالش پیش رو این است که اگر این اطلاعات در دیتاباکس مورد حملات سایبری بدافزار ها یا هکر ها واقع شده و در نوع اطلاعات تغییر ایجاد شود، عملکرد ابزار اینترنت اشیا نیز متناسب با آن دچار تغییر خواهد شد (Ibid). از این رو باید مکانیسمی طراحی گردد که از وقوع چنین فرایندی تا حد امکان پیش گیری شود. اگرچه فلسفه ضرورت رمزنگاری داده پیام های ذخیره شده توسط کنترل کنندگان ایجاب می نماید که در ذخیره این داده پیام ها در دیتا باکس نیز چنین فرایندی صورت پذیرد، اما فقدان رمزنگاری داده ای یکی از خلاء های مقررات مصوب ۲۰۱۸ در ارتباط با این مبحث تلقی می گردد. مگر اینکه با وحدت ملاک گیری از مفاد مواد این مقررات، ضرورت رمزنگاری داده پیام های ذخیره شده در دیتا باکس نیز به مورد پیشین اضافه گردد. علی ایحال به جهت فقدان این عملکرد، یکی از راه حل های موجود در راستای رفع چالش بیان شده پیش بینی محل های متعدد ذخیره داده ها در فرمت های مختلف قلمداد شده است. به عنوان مثال داده پیام هایی که نشان دهنده میزان رطوبت هوا، دما و وضعیت هوا بوده و هر یک با عنوان مخصوص به خود در محل ذخیره دیتا باکس قابل بازخوانی باشند، تحت

21- Public Key

ابرداده ای با عنوان «شرایط محیطی» نیز با فرمت دیگری در دیتا باکس ذخیره شوند تا در صورت تغییر داده پیام های اولیه ، امکان شناسایی آنها برای ابزار از طریق بازخوانی داده پیام های مشابه با آنها فراهم باشد. ضمن اینکه سیاستگذاری اجرایی بر ذخیره اطلاعات در بلاک چین خصوصی تحت فن آوری رمزنگاری داده ای می تواند تا حدود زیادی این مشکل را مرتفع نماید.

نتیجه گیری

همانطور که در متن پژوهش مورد تصریح قرار گرفت، تبیین سازوکار مسئولیت پذیری نهادهای فعال در سازوکار عملکرد ابزارهای اینترنت اشیا با چالشهای متعددی مواجه می‌باشد. از جمله این چالش‌ها می توان به عدم وجود شفافیت، کیفیت جمع آوری و پردازش اطلاعات، نگرانی های حاصل از نقض حریم خصوصی اشخاص، نوع مسئولیت نهادهای فعال در عملکرد ابزارهای مذکور و ... را نام برد که برای رفع چالشهای مذکور سیاست های صدور گواهینامه فعالیت، ایجاد حساب مجازی، شفافیت در عملکرد نهادها، ایجاد محدودیت در دسترسی، پردازش و تبادل داده ها، ایجاد سازوکار های حمایتی و تخصیص دیتاباکس ها از جمله راه حل هایی بوده است که در نظام حقوقی اتحادیه اروپا در مواجهه با چالشهای مذکور در پیش گرفته شده است. اما اجرای مکانیسم های پیش بینی شده در این پژوهش منوط به سیاستگذاری های تقنینی و اجرایی از سوی کشورهای دربردارنده آنها می‌باشد. از جمله مهمترین سیاستگذاری های لازم می توان به موارد ذیل اشاره نمود:

۱- ایجاد آگاهی عمومی در کیفیت تایید دسترسی ابزارهای اینترنت اشیا یا کنترل کنندگان آن‌ها به اطلاعات شخصی آنها: همانطور که در متن پژوهش مفصلا بیان گردید، رویکرد اتحادیه اروپا در حفاظت از داده پیام های الکترونیکی مبتنی بر رضایت دارنده در جمع آوری، پردازش و انتقال این اطلاعات می‌باشد. دارندگان ابزارهای اینترنت اشیا هنگامی خواهند توانست که رضایت یا عدم رضایت خود در انجام فرایند های مذکور را اعمال نمایند که آگاهی لازم از نحوه عملکرد این ابزارها پیدا نموده و با حقوق قانونی خود به طور کامل آشنا شوند. این امر جز با برگزاری دوره های آموزشی از طریق وسائل ارتباط جمعی مانند تلویزیون یا تدارک کلیپ‌های آموزشی از طریق شبکه های اجتماعی مانند واتس آپ و... به آسانی ممکن نمی گردد. از این رو دول متبوع شهروندان ملزم به اختصاص بودجه لازم در تهیه برنامه های آموزشی به زبان ساده می باشند تا اطلاعات لازم را در اختیار شهروندان آن کشور قرار دهد.

۲- برگزاری دوره های آموزشی برای کارکنان شرکت ها یا کارمندان دولتی در راستای یادگیری مفاد مقررات مصوب ۲۰۱۶، نحوه تعامل با اطلاعات شخصی افراد و مسئولیت مدنی نهادها و کارکنان ذی ربط در تخطی از وظایف مقرره در این مقررات: همانطور که بیان گردید، مقررات ۲۰۱۸ اتحادیه اروپا در راستای حفاظت از حریم خصوصی اشخاص مبادرت به پیش بینی مسئولیت مطلق برای شرکت های تولید کننده ابزارهای اینترنت اشیا نموده است. از این رو حتی

به صرف کوچکترین اشتباه صورت گرفته از سوی هر یک از کارکنان این شرکت ها، شرکت مزبور واجد مسئولیت مدنی خواهد بود. لذا برگزاری دوره های آموزشی تخصصی برای کارکنان شرکت ها در آگاهی بخشی بر نحوه انجام وظایف قانونی خود یکی از ضروریات تلقی می گردد. ضمن اینکه مطابق با قواعد کلی حقوق، در صورتی که شرکت مزبور با برخورداری از مسئولیت مدنی ملزم به جبران خسارات وارده یا پرداخت جرایم موصوف در مقررات ۲۰۱۸ گردد، برای جبران زیان پرداختی به عامل زیان رجوع خواهد نمود. دسترسی افراد فاقد صلاحیت به اطلاعات خصوصی اشخاص گاها می تواند خسارات جبران ناپذیری را نیز فراهم آورد. در بدترین شرایط ممکن دسترسی کشور های معاند به اطلاعات بیومتریک اتباع کشور ها می تواند آنها به ساخت سلاح های بیومتریکی قادر سازد که بدون هرگونه خسارت مالی، گونه خاصی از موجودات جهان را به طور کامل نابود گرداند. اهمیت وافر این موضوع به شکلی است که کشورهای جهان در راستای پیشگیری از مشکلات بیان شده نیازمند آگاهی بخشی به افرادی هستند که در معرض دسترسی به این اطلاعات می باشند. این امر با سیاستگذاری‌های صحیح قابلیت تحقق را دارد.

۳- پیش بینی مکانیسم های حمایتی از مالکان اطلاعات مذکور در احقاق حقوق قانونی خود از جمله رسیدگی‌های خارج از نوبت در محاکم قضایی یا پیش بینی مراجع صلاحیت دار قانونی در راستای رسیدگی اختصاصی به شکایات مردمی در ارتباط با عملکرد ابزارهای اینترنت اشیا: حفاظت از حریم خصوصی اشخاص امری حیاتی بوده و این امر به خوبی در مقررات اتحادیه اروپا مورد تحلیل قرار گرفته است. همانطور که بیان گردید، اشخاص در موارد نقض حریم خصوصی یا عدم کسب رضایت در جمع آوری ، پردازش یا تبادل اطلاعات خود محق بر اقامه دعوی می باشند. اگرچه دادگستری مرجع عام تظلم خواهی افراد می‌باشد، اما به جهت وجود مشکلات بیان شده در نحوه اجرای احکام دادگاه ها، جامعه بین الملل نیازمند پیش بینی مکانیسم های خاص در راستای تحقق بهتر اهداف تظلم خواهی افراد می‌باشد. این امر نیازمند سیاستگذاری تقنینی است. به عبارت دیگر در صورتی که مجامعی صلاحیت دار در عرصه بین الملل پیش بینی شوند که صلاحیت انحصاری بر رسیدگی به اعتراضات افراد در این خصوص را داشته باشند، هم مسئله اجرای احکام آنها مورد حل و فصل قرار می گیرد و هم زمینه رسیدگی هر چه سریعتر به اعتراضات افراد فراهم می گردد. این امر می تواند واجد اثرات مثبتی همچون قضا زدایی و جلوگیری از صرف هزینه و وقت در اقامه دعوی در دادگستری نیز گردد. اما این موضوع نیازمند تصویب قوانینی در جهت رفع موانع صلاحیتی این مراجع و همچنین اعطای قدرت حاکمیتی بر حل اختلافات باشد.

۴- پیش بینی مکانیسم تخصیص امضائات دیجیتالی به اتباع کشورهای در حال توسعه: تخصیص امضائات دیجیتالی به اتباع کشور ها واجد اثرات مثبتی در ملازمه با حوزه مورد بحث در پژوهش حاضر است. همانطور که در متن پژوهش تصریح گردید، پیش بینی تشریفات اعطای گواهینامه

فعالیت به شرکت ها منوط به بررسی موشکافانه صلاحیت کارکنان آنها در حفاظت از حریم خصوصی اشخاص است. اعطای این گواهینامه در مواردی که افراد واجد امضائات دیجیتالی باشند می تواند به آسانی میسر گردد. چرا که مراجع صلاحیت دار در موارد اعطای این مجوز، صلاحیت حقوقی و سوابق افراد را به صورت کامل مورد بررسی قرار داده و پس از احراز این امر، مجوز برخورداری از امضائات دیجیتالی را تقدیم آنها می نمایند. ضمن اینکه بازخوانی اطلاعات ذخیره شده در بلاک چین نیز منوط به برخورداری از افراد از امضائات دیجیتالی می‌باشد. در کشور ایران به جهت پیش بینی امضائات الکترونیکی مطمئن در قانون تجارت الکترونیکی مصوب ۱۳۸۲ مسئله تخصیص امضائات دیجیتالی نیازمند سیاستگذاری قانونی است. چرا اولا تشریفات خاصی برای اعطای امضائات الکترونیکی مطمئن در قانون مزبور پیش بینی نشده است. از این رو مجامع قانون گذاری نیازمند پیش بینی تشریفات اعطای این نوع امضائات همانند آنچه در نظام حقوقی غرب وجود دارد می باشند. ضمن اینکه ورود این امضائات می تواند محدوده عملکرد امضائات الکترونیکی مطمئن را نیز تحت الشعاع قرار دهد. به عبارتی با ورود این نوع امضا به نظام حقوقی ایران، دیگر موجبی برای به کارگیری نوع الکترونیکی مطمئن آن وجود نداشته و به ناچار باید قوانین تجاری ایران دگرگون اصلاح قرار گیرد.

۵- اصلاح قوانین مصوب: آنچه از بررسی قوانین مصوب فعلی در کشور ایران مشاهده می‌گردد این است که تنها دو ماده ۵۸ و ۵۹ قانون تجارت الکترونیکی ایران واجد مقرراتی در زمینه کیفیت حفاظت از داده پیام های الکترونیکی می باشند. تنها حکمی که در این دو ماده مورد تصریح قانون گذار قرار گرفته است، ضرورت کسب رضایت مالک داده پیام در پردازش اطلاعات و انجام این پروسه در حیطه اهداف تعیین شده می‌باشد. در حالی که هیچ حکمی در زمینه تعیین دقیق حقوق دارنده اطلاعات، کیفیت جمع آوری داده ها،، نحوه عملکرد کنترل کننده و پردازندگان اطلاعات، چگونگی اعطای مجوز فعالیت به این نهادها، نحوه نظارت بر عملکرد آنها، سازوکار مسئولیت پذیری، تعیین قانون حاکم و دادگاه صالح در رسیدگی به دعاوی و.. در این قانون ذکر نشده است. وجود تمامی خلاء های موجود می تواند ضرورت اصلاح قانون تجارت الکترونیکی در این زمینه را بهبود بخشد.

منابع

۱- آقایی طوق، مسلم،(۱۳۹۸) ، سازوکار و چالشهای پیاده سازی بستر بلاک چین در توسعه دولت الکترونیکی و آثار آن بر نظام مالیاتی، فصلنامه حقوق اداری، سال ششم، شماره ۱۹

۲- اسلامی تبار، امیر،(۱۳۹۹)، کارکرد بلاک چین در حمایت از کپی رایت، فصلنامه پژوهش حقوق خصوصی، سال هشتم، شماره ۳۰

۳- صادقی، محسن، ناصر، مهدی،(۱۳۹۷)، ملاحظاتی برای سیاستگذاری حقوقی قراردادهای هوشمند، فصلنامه سیاستگذاری عمومی، دوره چهارم، شماره۲

۴- صادقی، حسین، زرعی، حمیده،(۱۳۹۸)، چالشهای اعطای وام های فاین تک:سیاستگذاری و راهکارهای بانک جهانی، صندوق بین المللی پول و نظام حقوقی اتحادیه اروپا، فصلنامه مطالعات بین المللی، سال شانزدهم، شماره ۶۴
۵- مرکزمالمیری، احمد(۱۳۹۰)،تاملی در مرزهای سیا ستگذاری و قانونگذاری (مطالعه موردی: مفاد قانون برنامه پنجم تو سعه در حوزه فرهنگی)، فصلنامه مجلس و راهبرد، دوره ۱۸، شماره ۶۷
۶- ناصر، مهدی،(۱۳۹۷)، قراردادهای هوشمند: مطالعه تطبیقی حقوق ایران و آمریکا، چاپ اول، تهران، انتشارات مجد

7- Crabtree,(2017), Accountable Internet of Things? Outline of the IoT databox model, https://ieeexplore.ieee.org/abstract/document/7974335, online edition
8- Ewa Luger, Stuart Moran, and Tom Rodden,(2013), 'Consent for all' Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Social Sciences and Administrative Services
9- Gartner Newsroom(Last visited 12 Aug2019), Gartner, 'Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016', https://www.gartner.com/newsroom/id/3598917
10- Ian Brown, (Last Visited 8Aug 2019), Regulation and the Internet of Things(International Telecommunications Union 2015), https://www.itu.int/en/ITUD/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf
11- Jatinder Singh, Christopher Millard, Chris Reed, Jennifer Cobbe, Jon Crowcroft,(2019), Accountability in the Internet of Things (IoT): Systems, law & ways forward, Social Science Research Network
12- Karen Rose, (Last Visited 28 May 2019), Internet of Things:An Overview(Internet Society 2015),https://www.sfbayisoc.org/wp-content/uploads/2015/12/ISOC-IOT-FEB-2016-Rose.pdf
13- Konstantinos Christidis and Michael Devetsikiotis,(2016) 'Blockchains and Smart Contracts for the Internet of Things', IEEE Access, vol. 4
14- Lachlan Urquhart, Neelima Sailaja, and Derek McAuley, (2017) Realising the right to data portability for the domestic internet of things' Personal and Ubiquitous Computing, vol. 22
15- Lachlan Urquhart, Tom Lodge, Andy Crabtree,(2019), Demonstrably doing accountability in the Internet of Things, International Journal of Law and Information Technology,Vol27
16- Lilian Edwards and Michael Veale,(2017), 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for' Duke Law and Technology Review, vol. 16
17- Marshall, Brooke Adele,(2012) «Reconsidering The Proper Law of The Contract», Melbourne Journal of International Law, Vol 13
18- Martin Abrams(Last Visited 13Aug2019), Data Protection Accountability: The Essential Element, (Centre for Information Policy Leadership, Brussels 2009) https://www.hunton.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf
19- McAuley&Etc,(2018), Building accountability into the Internet of Things: the IoT Databox model,online Edition: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6560684/
20- Peter Tolmie, Peter, Andy Crabtree, Tom Rodden, James Colley and Ewa Luger ,(2016) 'This has to be the cats' - personal data legibility in networked sensing systems.' Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, Social Sciences and Administrative Services
21- Stephen camba ,(2015)Sasines registration abrief guide the land registration act 2012 https://www.ros.gov.uk/services/registration/land-register/faqs/essential-guide-to-the-2012-act.