چهارچوب‌های حقوقی حفظ امنیت پردازش داده‌های خصوصی
(مطالعه تطبیقی در حقوق ایران و اتحادیه اروپا)

تاریخ دریافت: ۱۳۹۸/۸/۲۵ تاریخ تأیید: ۱۳۹۹/۵/۶

محبوب افراسیاب* مهدی ناصر**

چکیده

ابداع ابزارهای اینترنت اشیا، به‌رغم برخورداری از کاربردهای فراوان در صنعت و تجارت، چالش‌هایی را نیز پیش روی نظامات حقوقی قرار داده است. یکی از مهم‌ترین این چالش‌ها، حفظ امنیت پردازش داده‌های خصوصی می‌باشد. سؤال اصلی پژوهش حاضر این است که چه چهارچوب‌های حقوقی در جهت حفاظت از اطلاعات خصوصی اشخاص در پردازش داده‌های خصوصی توسط شرکت‌های فراملی در حقوق ایران و اتحادیه اروپا موجود بوده و حقوق ایران در برابر خلاءهای موجود باید چه سیاست‌گذاری‌های تقنینی و اجرایی را در پیش گیرد؟ مهم‌ترین چهارچوب‌های حقوقی موجود اعطای مجوز فعالیت به کنترل‌کنندگان ابزارهای اینترنت اشیا و پردازندگان این اطلاعات، تعیین حدود و کیفیت عملکرد این نهادها در مواجهه با اطلاعات خصوصی اشخاص، نظارت بر عملکرد نهادهای مذکور و پیاده‌سازی سازوکار انعقاد قراردادهای پردازش در بسترهای نامتمرکز می‌باشد. البته دراین‌باره حقوق ایران نیازمند تصویب قوانین کارآمد درخصوص مکانیسم پردازش داده‌های خصوصی، تخصیص مجوز به‌کارگیری امضائات دیجیتالی، اعتبارسنجی و سازوکار تبادل ارزهای مجازی و پیش‌بینی مراجع صلاحیت‌دار نظارتی می‌باشد.

واژگان کلیدی: حفاظت از اطلاعات، ابزارهای اینترنت اشیا، پردازش داده‌های خصوصی، حقوق اتحادیه اروپا.

* دکترای حقوق خصوصی دانشگاه علامه طباطبائی / نویسنده مسئول (mahboobafrasyab@yahoo.com).
** دانشجوی دکتری حقوق خصوصی دانشگاه علوم قضایی (mn.ujsasac0077@yahoo.com).

مقدمه

فناوری ارتباط میان ابزارهای الکترونیکی که از آن بـه اینترنـت اشـیا تعبیـر مـی‌گـردد، یکـی از فناوری‌های نوظهور قرن بیست و یکم می‌باشد که ابداع و به‌کارگیری آن صنعت و تجارت منجر بـه تحولات فراوانی شده است. ابزارهای اینترنت اشـیا، ابزارهـایی هسـتند کـه بـا اتصـال سنسـورهای مختلف به بدنه و تعبیه پروتکل‌های لازم به پردازنده آنها، قادر به انجام وظایف از پیش تعیین شـده مـی‌باشـند (Bello & ETC, 2014, 30) ابزارهـای مـذکور بـرای انجـام وظـایف خـود، نیازمنـد جمع‌آوری اطلاعات از محیط پیرامون، طبقه بندی و پردازش آنها می‌باشند. عملکـرد ایـن ابزارهـا توسط تولیدکنندگان آنها که اصـطلاحا کنترل‌کننـده نامیـده مـی‌شـوند نظـارت و کنترل‌کننـدگان بـا دریافت اطلاعات جمع‌آوری شده توسـط ایـن ابزارهـا، مبـادرت بـه ارسـال آنهـا بـه پردازشـگران می‌نمایند. پردازشگران اطلاعات نیز با پردازش داده‌های خام ارسال شده از سوی کنترل‌کننده، داده محتوای پس از پردازش را مجددا برای کنترل‌کننده ارسال مـی‌نماینـد. درصـورتی کـه پردازنـدگان، دارای تابعیت کشور متبوع کنترل‌کننده باشند، عملا مشکلی از حیث رعایت مسائل امنیتی حفاظت از اطلاعات پیش نخواهد آمد. اما درصورتی که شرکت‌های مـذکور شـرکت‌های فراملـی یـا ملـی باشند که اقامتگاه آنها در کشور ثالثی غیر از کشور متبوع تولیدکننده یا دارنـده ابـزار باشـد، چـالش پیش رو چگونگی تضمین امنیت داده‌های قابل پردازش خواهد بود. اطلاعات جمـع‌آوری شـده از سوی ابزارهای اینترنت اشیا، شـامل انـواع داده پیام‌هـای الکترونیکـی مـی‌گـردد. دسـته‌ای از ایـن اطلاعات، داده پیام‌های شخصی اشخاص از جمله اطلاعات بیومتریـک آنهـا مـی‌باشنددسترسـی اشخاص فاقد صلاحیت به این اطلاعات مـی‌توانـد واجـدآثار جبـران ناپـذیری از جملـه سـاخت سـلاح‌های بیومتریـک و نقـض امنیـت ملـی یـک کشـور باشـد. چنـین مسـائلی ضـرورت سیاست‌گذاری‌های تقنینی و اجرایی صحیح را در زمینه حفاظـت از ایـن اطلاعـات بـیش از پـیش تقویت می‌نماید.

تاریخچه تبادل داده‌های الکترونیکی به سال ۱۹۷۳ میلادی باز می‌گـردد. سـوئد اولـین کشـور اتحادیه اروپا می‌باشد که با تصویب قانون یکنواخت‌سازی صادرات داده به کشـورهای ثالـث ایـن امر را به صورت قانونی در نظام حقوقی خـود پذیرفتـه اسـت (Kuner, 2011, p.14) پـس از آن در سال ۱۹۷۸ میلادی اتریش ارسال داده پیام‌های مرتبط با اطلاعات شهروندان خـود بـه کشـورهای ثالث درصورت ارائه تضامنی در جهت حفظ امنیت این داده‌ها مـورد پـذیرش قـرار داد. بعـدها در

سال ۱۹۹۵ دستورالعمل حفاظت از اطلاعات اروپاییان توسط کمیسیون اتحادیه اروپا با هدف هماهنگ‌سازی قوانین موجود در کشورهای عضو اتحادیه به عنوان اولین قانون جامع در جهت حفاظت از حریم خصوصی اشخاص تصویب شد (Wanger, 2019, p.2) به جهت مشکلات اجرایی که دستورالعمل مذکور در پذیرش فناوری‌های نوین از جمله ابزارهای اینترنت اشیا با آن مواجه بود، در سال ۲۰۱٦ مقرراتی با عنوان دستورالعمل عمومی حفاظت از اطلاعات (General Data Protection Regulations) که در ماه می‌سال ۲۰۱۸ به مرحله اجرایی در آمده است، مورد تصویب کمیسیون اتحادیه اروپا قرار گرفت.

آنچه در پژوهش حاضر مورد تحلیل نظری از سوی نگارندگان قرار گرفته است، چهارچوب‌های حقوقی حفظ امنیت پردازش‌های خصوصی اشخاص در مواردی که پردازندگان اطلاعات شرکت‌های فراملی دارای تابعیت کشوری غیر از کشور متبوع کنترل‌کننده و دارنده ابزار بوده می‌باشد. این پژوهش به روش اسنادی و با مطالعه تحلیلی راهکارهای موجود در نظام حقوقی اتحادیه اروپا و تطبیق این راهکارها با مقررات حاکم بر نظام حقوقی ایران، در قالب یک پژوهش تجویزی سعی در ارائه راه حل‌های کاربردی در جهت رفع چالش‌های حقوقی و بهبود سیاست‌گذاری تقنینی در راستای به‌کارگیری این فناوری در کشور ایران دارد.

۱. ضرورت اخذ مجوز فعالیت از سازمان‌های صلاحیت‌دار

فعالیت نهادهای فراملی در یک کشور نیازمند نظارت مستمر مراجع صلاحیت‌دار قانونی آن کشور بر نحوه عملکرد نهادهای مزبور است. این امر زمانی که نهادهای فعال در کشورهای خارجی یا شرکت‌های فراملی با دسترسی به اطلاعات اتباع یک کشور از امکان نقض امنیت ملی آن کشور برخوردار می‌شوند، جلوه بیشتری می‌نماید. در مسئله پردازش اطلاعات خصوصی اتباع کشورها نیز حکم مذکور صادق است. ازآنجاکه پردازش اطلاعات از سوی شرکت‌های پردازنده می‌تواند زمینه دستیابی بیگانگان به اطلاعات خصوصی اروپاییان را فراهم نماید، نظام حقوقی اتحادیه اروپا در جهت پیشگیری از وقوع این مشکل، مبادرت به تنظیم سازوکارهای اعطای مجوز فعالیت به شرکت‌های پردازنده در مواد ٤٥ و ٤٦ دستورالعمل مصوب ۲۰۱٦ نموده است.

مطابق با مفاد بند اول از مادّه ٤٥، انتقال اطلاعات به کشور ثالث یا یک سازمان فراملی تنها درصورت تأیید صلاحیت کشور مذکور در امکان حفاظت از اطلاعات خصوصی اروپاییان توسط

کمیسون اتحادیه اروپا امکـان پـذیر مـی‌باشـد. عـلاوه بـر آن، مـادّه ٤٦، شـرکت‌های تبادل‌کننـده اطلاعات را ملزم به سپردن تضـامن مـالی بـه نهادهـای صـلاحیت‌دار در راسـتای تضـمین جبـران خسارات وارده به دارندگان اطلاعات نموده است (EuropeanCommision, 2019, E.2).

علاوه بر آنچه بیان شد، مقررات مصوب ۲۰۱٦ واجد شرایطی بـرای کشـورهای غیـر اروپـایی میزبان اطلاعات خصوصی اروپاییان نیز می‌باشد. این شرایط کـه از آن بـه شـرط «کفایـت» تعبیـر می‌گردد، در پروتکل الحاقی به مادّه ٤٥ دستورالعمل مورد تصریح قرار گرفتـه اسـت (European Commission, 2017, pp.8-9) مطابق با بخش اول از بند دوم پروتکل مزبـور، کشـورهای میزبـان اطلاعات خصوصی اروپاییان که خارج از اتحادیه اروپا می‌باشند، در دریافت این اطلاعـات بایـد واجد سطح امنیتی لازم برای حفظ امنیت داده‌های مذکور و شفافیت کافی برای امکان نظـارت بـر عملکرد نهادهای فعال در صلاحیت سرزمینی خود باشند. این امر درصورتی محقق خواهد شد که معاهدات یا دیگر مقررات مصوب اتحادیه اروپـا از جملـه مفـاد دسـتورالعمل حمایـت از حقـوق جمعـی مصـرف‌کنندگان مصـوب ۲۰۱۸ (EU Consumer Protection Directive 2018) ایـن اتحادیه در پیش مسئولیت تضامنی دولت در موارد نقض قواعد امنیتی پردازش داده‌های خصوصـی توسط شرکت‌های تبعه این کشور، مورد پذیرش کشور ثالث قرار گیرد.

اما اجرای سازوکارهای بیان شده در مادّه ٤٥ با محدودیت‌هایی نیز مواجه می‌باشد. چرا که اولا ممکن است اعمال سلیقه در تصمیمات کمیسیون منجر به تضییع حق برخی سـازمان‌های فراملـی یا ایجاد زمینه تبانی میان اعضای کمیسیون و برخی سازمان‌ها گردد. دوما عدم وجـود شـفافیت در کیفیت اعطای مجوز و تصمیم گیری در وقوع این مهم، منجر به سردرگمی سازمان‌ها یا کشـورهای پذیرنده اطلاعات در تشخیص معیارهای کمیسیون در تطبیق اسـتانداردهای خـود بـا ایـن معیارهـا می‌باشد. به عبارت دیگر درصورتی که شرایط خاصی از سوی کمیسیون به شـرکت‌ها و کشـورهای پذیرنده اطلاعات ارائه گردد تا با تطبیق استانداردهای خود نسبت به جذب صـلاحیت از کمیسـیون مربوطه اقدام نمایند، امکان هر چه بهتر اجرای مقررات مادّه ٤٥ نیز فراهم خواهد شـد (Wanger, 2019, p.4).

علاوه بر آن چـالش دیگـری کـه در زمینـه اجـرای مقـررات مـذکور متصـور اسـت، ضـرورت سیاسـت‌گذاری تقنینـی در پیاده‌سـازی ایـن سـازوکار در نظـام داخلـی کشـورهای عضـو اتحادیـه می‌باشد. به عبارت دیگر درصورتی کـه کشـوری از مقـررات مـواد ٤٦ و ٤٥ دسـتورالعمل پیـروی

ننماید، ضمانت اجرای این امر در نظام حقوقی اتحادیه اروپا چه می‌باشد؟ آیا امکان محکوم نمودن دولت مذکور در دادگاه‌های اتحادیه اروپا با سازوکاری معین وجود دارد؟ در این خصوص به نظر نگارندگان با اخذ وحدت ملاک از مادّه ١٦ دستورالعمل مصوب ٢٠١٨ که در راستای مقررات مادّه ٨٠ دستورالعمل مصوب ٢٠١٦ در حوزه اقامه دعاوی جمعی برای جبران خسارات ناشی از نقض قواعد امنیتی تصویب شده است، امکان پیش‌بینی مسئولیت تضامنی دولت‌های عضو اتحادیه و سازمان‌های فعال در محدوده صلاحیت سرزمینی آنها در جبران خسارات وارده ناشی از نقض قواعد تعیین شده در مقررات مذکور موجود است. چرا که عدم اجرای مقررات اولیه مواد ٤٦ و ٤٥ از حیث قواعد عام حقوقی به منزله تقصیری تلقی می‌گردد که خسارات وارده را منتسب دولت متبوع سازمان واردکننده زیان می‌گرداند. از طرف دیگر مبانی تصویب مقررات مادّه ١٦ حمایت از حقوق دارندگان اطلاعات است و تسری این مقررات به موارد مشابهی که ضرورت حفاظت از حقوق دارندگان اطلاعات در اتحادیه اروپا احساس می‌گردد خالی از هرگونه ایراد خواهد بود.

مضاف بر آنچه بیان شد درخصوص مفاد پروتکل الحاقی مادّه ٤٥ نیز می‌توان بیان داشت، وجود چنین سازوکاری اگرچه در جهت حفظ امنیت اطلاعات اروپاییان می‌تواند مفید باشد، اما برای کشورهای خارج از اتحادیه اروپا واجد چالش‌هایی است. اولا حاکمیت و استقلال هیچ کشوری نخواهد پذیرفت که الزامات امنیتی کشور یا اتحادیه دیگری در نظام قانون گذاری داخلی آن کشور وارد گردد. ضمن اینکه سؤال پیش رو این است که معیار تعیین سطح امنیتی لازم که در بند دوم از پروتکل الحاقی مورد تصریح قرار گرفته است چه می‌باشد؟ به جهت آنکه در هر حال امکان تفاسیر متعدد از کیفیت تعیین امنیت لازم برای حفاظت از داده‌ها وجود دارد، به نظر نمی‌رسد معیار مشخصی نیز پیش روی اتحادیه اروپا در همکاری مبادلاتی با کشورهای دیگر جهان وجود داشته باشد. ثمره این امر ایجاد رویکردهای متعدد در مواجه با این حکم خواهد بود. از طرف دیگر، برخی از کشورهای در حال توسعه مانند ایران، حتی فاقد قوانین اولیه در زمینه حفاظت از داده‌های الکترونیکی مورد تبادل در مبادلات فرامرزی می‌باشند که پذیرش شرایط اتحادیه اروپا در نظام داخلی این کشورها جزو دیگر مشکلات اجرایی پیش روی اتحادیه خواهد بود.

در نظام حقوقی ایران، سازوکاری مبنی بر تبادل اطلاعات خصوصی میان شرکت‌های تابعه و

دیگر شرکت‌های فراملی یا موجود در کشوری دیگر وجود ندارد. پیاده‌سازی فناوری ابزارهای اینترنت اشیا در نظام حقوقی ایران، ضرورت چنین تبادلاتی را خصوصا در مواردی که پردازندگان این اطلاعات به صورت انحصاری تنها در چند کشور خاص وجود داشته باشند، احساس خواهد شد. از این حیث مقوله‌های مورد بحث در پیاده‌سازی فناوری اینترنت اشیا در این نظام، چگونگی اعطای مجوز فعالیت به شرکت‌های کنترل‌کننده و پردازنده اطلاعات، نحوه وقوع فرایند ارسال و تبادل اطلاعات ایرانیان به کشورهای خارجی و ضمانت اجرای نقض مقررات امنیتی تعیین شده از سوی دولت ایران می‌باشد. دراین‌باره نکته قابل توجه عدم قابلیت قیاس قدرت حاکمیتی اتحادیه اروپا که متشکل از چندین کشور بوده و از ابزارهای اعمال فشاری از جمله تحریم‌های اقتصادی در وارد نمودن فشار بر ناقض مقررات یا دولت متبوع آن، با کشور ایران می‌باشد. از این رو برای انجام فعالیت کنترل‌کنندگان و پردازندگان اطلاعات در کشور ایران اولا دریافت تضمین‌های مالی کافی از آن سازمان و ثانیا انعقاد قراردادهای متقابل میان کشور متبوع سازمان و کشور ایران برای پیش‌بینی مسئولیت بین‌المللی آن کشور الزامی می‌باشد. از سوی دیگر تا زمانی که شعبه‌ای از یک شرکت کنترل‌کننده در کشور ایران دایر نبوده و امکان صدور و اجرای حکم بر علیه این سازمان وجود نداشته باشد، هرگونه فعالیت این سازمان‌ها در خارج از مرزهای ایران واجد ایراد است. علاوه بر آن دولت نیازمند اخذ تضمین‌های کافی مبنی بر ضمانت صحت پروسه پردازش داده توسط شرکت‌های پردازشگری که در خارج از مرزهای ایران مبادرت به پردازش داده می‌نمایند، از سوی کنترل‌کننده می‌باشد.

سازوکارهای بیان شده نیازمند تصویب مقررات قانونی خواهد بود. چرا که اولا حقوق ایران، مسئولیت ناشی از فعل غیر را تنها در موارد استثنایی پذیرفته و اصل و قاعده‌ای خلاف در این خصوص وجود ندارد. لذا اجرایی نمودن پیشنهاد بیان شده نیازمند تصویب قانونی مستقل در این باب است. از طرف دیگر در حقوق ایران، مستفاد از مواد ۱و ۲و ۳ قانون مسئولیت مدنی، مطابق با صحیح‌ترین نظر از میان نظرات موجود، دولت درصورتی ملزم به جبران خسارات ناشی از اعمال اتباع خود می‌باشد که این عمل قابلیت انتساب به وی را نیز داشته باشد (رهپیک، ۱۳۹۵، ص۱۸) ضمن اینکه حتی بر فرض انتساب عمل بر دولت، مبنای ارائه شده در مادّه ۵۲۶ قانون مجازات اسلامی، تنها محکومیت دولت بر اساس میزان تقصیر وی را لازم شمرده و درصورتی که تعیین میزان مسئولیت وی از سوی دادگاه ایرانی امکان پذیر نباشد، صدور حکم بر مسئولیت مساوی

تمامی مسببین ضرورت خواهد یافت. اما مشکل موجود ایـن اسـت کـه اگـر دولـت بـه هـر دلیـل مسئولیت جبران تمامی خسارات وارده به اتباع ایرانی یا دولت ایران را عهده‌دار نشود ممکن است از یک طرف امکان دسترسی به عامل دیگر زیان فراهم نبوده و از طرف دیگر حتی بر فـرض دسترسـی توانایی جبران خسارت وارده را نداشته باشد. ضمن اینکه ضرورت حفظ امنیت ملی یک کشـور در گرو اعمال ضمانت اجراهای حداکثری می‌باشد تا زمینه نقض امنیت ملی کاهش یابد. اگـر کشـور ثالثی در جبران خسارات وارده از ناحیه اتباع خود مسئولیت مطلـق داشـته باشـد، حتـی بـا اعمـال نظارت داخلی نیز از وقوع هرگونه سوءاستفاده پیشگیری می‌نماید. از ایـن رو در زمینـه حفاظـت از اطلاعات خصوصی، کشور ایران نیازمند تصویب قانون جدید در زمینه اعطای حداکثری مسـئولت به دولت کشوری که سازمان کنترل‌کننده تبعه آن کشور بوده می‌باشد و از طرف دیگر انعقاد قـرارداد متقابل برای تعیین مسئولیت بین‌المللی دولت مذکور دیگر الزام پیش روی دولت ایران خواهد بود.

۲. تعیین کیفیت تبادل و پردازش داده‌های خصوصی

پس از لازم الاجرا شدن دستورالعمل مصوب ۲۰۱٦، کارگروهی تحت عنوان کارگروه مـادّه ۲۹ این دستورالعمل متشکل از نمایندگان کشورهای عضو اتحادیه در ۲۵ می۲۰۱۸ تشکیل گردید تا با بررسی مقررات موجود در دیگر کشـورها مبـادرت بـه ارائـه پیشـنهاداتی در زمینـه کیفیـت اجـرای مقررات دستورالعمل مذکور به کمیسیون اتحادیه اروپـا نمایـد. تعیـین کیفیـت پـردازش داده‌هـای خصوصی اروپاییان نیز یکی از الزامات این اتحادیه می‌باشد که کارگروه مذکور با ارائه گزارشـی بـه کمیسیون اتحادیه که درسپتامبر سال ۲۰۱۸ از سوی این کمیسیون مورد تصویب قرار گرفتـه اسـت، مبادرت به سیاست‌گذاری اجرایی نموده اسـت (European Commission, 2019, E.3) الزامـات بیان شده در گزارش کارگروه مادّه ۲۹ در شش بند به شرح ذیل است:

داده‌های شخصی تنها باید به اهداف خاصی مورد پردازش قرار گیرند.

پردارش داده‌های شخصی برای اهداف دیگری ممکن نبوده مگر شرایط خاصـی ماننـد شـرایط موجود در مادّه ۱۳ دستورالعمل پارلمان اروپا در حفاظـت از افـراد در پـردازش و تبـادل داده‌هـای خصوصی آنها مصوب ۱۹۹۵ موجود باشد.

اطلاعات جمع‌آوری شده باید دقیقا در حوزه عملکرد ابزار صورت گرفته و بـه طـور مرتـب بـه روزآوری شوند.

داده‌های جمع‌آوری شده امکان ذخیره و نگهداری به صورت نامحدود را نداشته و تنها در مدت زمان متعارف قابلیت نگهداری توسط پردازشگر را خواهند داشت.

دارنده (مالک) اطلاعات باید از حق آگاهی از میزان و کیفیت داده‌های جمع‌آوری و پردازش شده وی برخوردار بوده و در هر زمان از امکان اصلاح اطلاعات نادرست به دست آمده از وی یا ارائه دستور حذف اطلاعات جمع‌آوری شده از سامانه پردازنده را برخوردار باشد.

تبادل اطلاعات میان پردازنده اصلی و فرعی به هر دلیل علاوه بر تأیید کنترل‌کننده باید به تأیید دارنده اطلاعات نیز رسیده و رضایت موردی وی در این خصوص کسب گردد (Raul, 2017, pp.11, 22).

همان‌گونه که از بندهای پیشنهادی کارگروه مذکور هویداست، مسئله جمع‌آوری و پردازش موردی داده‌ها مطابق با سازوکار عملکرد ابزار اینترنت اشیا جزو ارکان اساسی عرضه ابزارهای مذکور در بازارهای کشورهایی اروپایی تلقی می‌گردد. بند اول از الزامات مذکور جمع‌آوری و پردازش داده‌ها را تنها در حیطه خاصی که ابزار اینترنت اشیا مورد استفاده دارنده قرار گرفته باشد پذیرفته است. هنگام فروش ابزار توسط کنترل‌کننده به دارنده، قراردادی پیرامون کیفیت عملکرد ابزار و جمع‌آوری و پردازش داده‌های مورد نیاز این ابزار میان متعاملین منعقد و مطابق با مفاد بند اول و پنجم از الزامات مذکور، این مورد باید به آگاهی دارنده رسیده و رضایت موردی وی در این فرایند اخذ گردد (Lachlan&Etc, 2019, pp.6-7).

پردازش داده‌های شخصی اشخاص جز در موارد خاص که مشابه آن در مادّه ۱۳ دستورالعمل مصوب ۱۹۹۵ ذکر شده است، امکان پذیر نیست. موارد مندرج در مادّه ۱۳ دستورالعمل فوق الذکر نیز در شش بند به موارد (حفظ امنیت ملی، نظم عمومی، کشف جرایم، سیاست‌گذاری تقنینی، مسائل مهم اقتصادی و شناسایی حقوق اساسی اروپاییان) خلاصه شده است. از مجموع موارد بیان شده می‌تواند به ضرورت حفظ نظم و امنیت داخلی یا خارجی کشور در پردازش داده‌های خصوصی اشخاص رسید که مواردی از این قبیل نیز امکان ورود به الزامات مذکور در اعلامیه کارگروه مادّه ۲۹ را خواهند داشت. سؤال پیش رو این است که آیا مرجعی صالح جهت تشخیص موارد بیان شده در مادّه ۱۳ دستورالعمل مصوب ۱۹۹۵ یا موارد مشابه با آن وجود دارد یا صلاحیت تشخیص موارد بیان شده بر عهده نهاد مزبور است؟ در این خصوص مرجع صالحی در مقررات مصوب اتحادیه اروپا پیش‌بینی نشده است، اما به حکم مادّه ۱۲ پیمان عملکرد اتحادیه

اروپـا و مـادّه ٤٤ دسـتورالعمل مصـوب ٢٠١٦ کـه کشـورهای عضـو اتحادیـه را ملـزم بـه سیاست‌گذاری‌های تقنینی در اجرای هر چه بهتـر مقـررات اتحادیـه نمـوده اسـت، درصـورتی کـه کشوری خاص مرجعی را برای تشخیص موارد بیان شده پیش‌بینی نموده باشد، کنترل‌کننده ملزم بـه رعایت شرایط نهاد ناظر دراین‌باره خواهد بود. اما درصـورت عـدم وجـود چنـین مرجعـی بـه نظـر نگارندگان وجود صلاحیت تشخیص موارد بیان شده توسط نهاد کنترل‌کننده خالی از اشکال است. چرا که الزامات بیان شده از سوی کارگروه مطلقا مـوارد اسـتثنا از اهـداف تعیـین شـده را مشـخص نموده و اصولا مرجع عامل سیاست‌های مذکور از صلاحیت تشخیص ایـن مـوارد جـز درصـورت تصریح سیاست‌گذار برخوردار خواهد بود.

نکته دیگر «حق دسترسی» دارنـده در آگـاهی از اطلاعـات جمـع‌آوری شـده از وی و «اصـل شـفافیت» درچگـونگی عملکـرد کنترل‌کننـده و پردازنـده اطلاعـات جمـع‌آوری شـده مـی‌باشـد (Finance Latvia, 2018, p.47) همان‌طور که بیان گردید، به حکم بند پنجم از الزامـات مـذکور، دارنده از حق آگاهی از کمیت و کیفیت اطلاعات بـه دسـت آمـده و صـحت یـا عـدم صـحت آن اطلاعات برخوردار است. همچنین به حکم اصل شفافیت که در بند ششم از الزامات مـذکور ذکـر شده است درصورتی که اطلاعاتی غیر آنچه که مورد توافـق و رضـایت میـان دارنـده و کنترل‌کننـده باشد، میان کنترل‌کننده و پردازنده مورد تبادل واقع گردد، این امر بایـد بـا رضـایت دارنـده صـورت پذیرد. از این رو اگر سوءاستفاده‌ای از سوی پردازنده یا کنترل‌کننده انجام شـود هـر یـک مطـابق بـا قواعد عام مسئولیت مدنی مسئول جبران خسارات وارده و دولت متبوع مشارالیهم نیز مستند به مادّه ١٦ دستورالعمل مصوب ٢٠١٨ مسئول خواهد بود.

کیفیت پردازش داده‌های خصوصی در نظام حقوقی ایران نیز مطابق با مقـررات مـواد ۵۸ و ۵۹ قانون تجارت الکترونیکی تعیین می‌گردد. مادّه ۵۸ قانون مذکور، انجام هرگونه عملیات پردازش یـا هر عملیاتی که مقدمه پرداش داده‌هـای خصوصـی اشـخاص از جملـه داده‌هـای مبـین ریشـه‌های قومی، خصوصیات اخلاقی، روانی، جنسی و... را منوط به «رضایت صریح» دارنـدگان اطلاعـات نموده است. مشروطیت اخذ رضایت صریح دارندگان در سازوکار پردازش اطلاعات آنها می‌توانـد آثاری را در برداشته باشـد. اولـین اثـر ایـن امـر شناسـایی حـق مالکیـت دارنـده بـر داده پیام‌هـای جمع‌آوری شده از سوی وی خواهد بود. از این رو انجام هر عمل مغایر به منزله نقض حق معنـوی فرد بر داده‌های خود و وقوع جرایم حوزه مالکیت فکـری مـی‌گـردد. از طـرف دیگـر امعـان نظـر از

عبارت «رضایت صریح» این نکته را به ذهن متبادر می‌نماید که دارنده اطلاعات در هـر مرحلـه از پردازش داده‌های خود امکان جلوگیری از وقـوع پروسـه مـذکور و حتـی منـع کنترل‌کننـده از ارائـه اطلاعات خود به پردازنده مشخصی را دارا می‌باشد. اما سؤال پیش رو این است که در مکان‌هـایی مانند ادارات یا منزل که اشخاص متعدد علاوه بر خریدار ابزار، حضور دارند، طبیعتا انجام صـحیح وظایف ابزار منوط به جمع‌آوری انواع اطلاعات از جمله اطلاعات شخصی دیگران نیز مـی‌باشـد. چگونگی تفسیر این مادّه جهت حل و فصل مسئله کسب رضایت صریح تمامی دارنـدگان بـه چـه شکلی خواهند بود؟ آیا کنترل‌کننده در زمینه پردازش داده‌ها ملزم به اخذ رضایت تمـامی دارنـدگان است یا این امر را می‌تواند به نمایندگی از سوی خریدار انجام دهد؟

به نظر نگارندگان به‌رغم تصریح مادّه ۵۸ بر ضرورت کسب رضایت صـریح تمـامی اشـخاص موجود در محیط، هدف از تنظیم این مادّه اطـلاع و آگـاهی دارنـده از وقـوع پروسـه پـردازش داده می‌باشد تا هم هدف وقوع شفافیت عملکرد پردازنده تامین گـردد و هـم درصـورت نقـض قـوانین، امکان اقامه دعوا توسط دارندگان اطلاعات از فرد خـاطی فـراهم شـود. از ایـن رو در مـواردی کـه ابزاری برای جلب منافع عموم تهیه می‌گردد، مانند موردی که ابزار برای انجام اعمال در درون یـک اداره یا خانواده تهیه شده باشد، ارائـه رضـایت از سـوی رئـیس اداره یـا سرپرسـت خـانوار در ایـن خصوص کفایت می‌کند. مضافا اینکه اگر بنا بر ضرورت کسب رضایت از تک تک افراد حاضـر در محل باشد، در این صورت حتی این رضایت موردی باید از میهمانان منزل یـا مراجعه‌کننـدگان بـه اداره نیز کسب گردد که عملا امکان پذیر نمی‌باشد.

علاوه بر مادّه ۵۸، مادّه ۵۹ قانون تجارت الکترونیکـی درصـورت وجـود شـرایط مـادّه ۵۸ در کسب رضایت صریح دارنده، انجام هرگونه عملیات پردازش داده‌های خصوصی را منوط به شـرایط ذیل نموده است:

اهداف پردازش داده مشخص و واضح باشند.

داده پیام تنها به اندازه ضرورت و متناسب با اهداف تعیین شده مورد پردازش واقع شود.

داده پیام باید صحیح و روزآمد باشد.

امکان دسترسی دارنده اطلاعات به پروسه پردازش فراهم بوده و امکان محو یا اصلاح داده‌های نادرست یا ناقص یا محو کلیه داده‌های منتسب به وی برای او فراهم باشد.

به نظر نگارندگان، تحقق اهداف تصویب بند اول مادّه ۵۹ قانون مرقوم به جهت برخورداری از

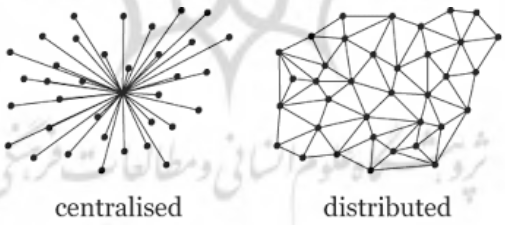
الزامات امنیتی که نقض آنها می‌تواند امنیت ملی یک کشور را تحت الشعاع قرار دهد، نیازمند دریافت مجوز از مراجع صلاحیت‌دار حکومتی، نظارت بر عملکرد نهادهای پردازشگر و ارائه گزارش عملکرد نهادهای مذکور به این مراجع صلاحیت‌دار می‌باشد. اما در مادّه مذکور نه شرایطی بر نحوه دریافت مجوز از نهادهای صلاحیت‌دار پیش‌بینی شده است و نه در زمینه نظارت بر عملکرد پردازشگران و چگونگی تشخیص اهداف پردازش داده‌های خصوصی اشخاص از سوی آنها حکمی ذکر شده است. اگر بنا بر ارائه گزارش عملکرد و بیان اهداف پردازش تنها بر دارنده اطلاعات باشد، عملا اهداف تصویب قانون مذکور به وقوع نخواهد پیوست. چرا که اولا مرجع تشخیص صحت و سقم موارد بیان شده از سوی پردازنده مشخص نمی‌باشد و ثانیا به جهت تخصصی بودن بسیاری از مراحل پردازش داده و عدم آگاهی عموم جامعه از نحوه وقوع این پروسه، درصورتی که نهادی واجد تخصص کافی بر عملکرد پردازشگران نظارت نداشته باشد، قطعا زمینه سوء استفاده از ناآگاهی جامعه برای آنها فراهم خواهد بود. علاوه بر آن مقدمه لازم در تحقق اهداف حاصل از پیش‌بینی حق دسترسی بیان شده در بندهای چهارم و پنجم از این مادّه (که در این پژوهش در بند چهارم تجمیع شده اند) آگاهی بخشی از سوی حاکمیت به عموم جامعه می‌باشد. اگر پردازنده اطلاعات حق مذکور در بندهای چهارم و پنجم را محترم شمرده و در این خصوص امکانات لازم برای دارنده را فراهم آورد، درخصوص مواردی که تخصص لازم در شناسایی داده‌های خام ناقص دریافت شده از سوی دارنده لازم بوده و یا حتی در راستای تحقق امکان محو و جلوگیری از پردازش داده‌های صحیح دریافت شده از وی، آگاهی دارنده از وقوع پروسه مذکور امری ضروری می‌باشد. ازآنجاکه امکان محول نمودن سازوکار آگاهی بخشی به مردم به پردازشگران به جهت ذی نفع بودن آنها در تداوم ناآگاهی جامعه، امری عبث می‌باشد، این وظیفه بر عهده نهادهای حکومتی کشور خواهد بود.

۳. به‌کارگیری بسترهای نامتمرکز در سازوکار انعقاد قراردادهای پردازش

انتقال مالکیت از کنترل‌کننده ابزار به دارنده و تبادل داده‌های خام مورد پردازش میان کنترل‌کننده و پردازنده منوط به انعقاد قراردادهای فروش و پردازش میان آنها می‌باشد. مسئله موجود ضرورت حفظ شفافیت در انعقاد معامله، حفظ امنیت مبادلاتی در پیشگیری از کلاهبرداری یا

دیگر جرایم مالی و تضمین صحت اجرای قرارداد توسط طرفین می‌باشد. امروزه به‌کارگیری بسترهای نامتمرکز در انعقاد قراردادهای پردازش راه حلی فناورانه در حل و فصل مشکلات بیان شده پیش روی نظام حقوقی اتحادیه اروپا قرار داده است.

محیط اینترنت از دو بستر متمرکز و نامتمرکز[1] تشکیل شده است. در بسترهای متمرکز (Centralised Ledgers) که شاخص‌ترین نوع آنها صفحه گسترده جهانی (World Wide Web) می‌باشد، ذخیره و تبادل داده‌ها تحت نظارت کنترل‌کننده‌ای مرکزی رخ می‌دهد که هرگونه خلل در عملکرد آن منجر به اخلال در کل سیستم می‌گردد. در مقابل، بسترهای نامتمرکز (Distributed Ledgers) که شاخص‌ترین نوع آنها بلاک چین می‌باشد فاقد هرگونه کنترل‌کننده مرکزی هستند. بلاک چین (Blockchain) زنجیره‌ای متشکل از تعداد زیادی بلاک می‌باشد. بلاک‌ها مکان‌هایی جهت ذخیره داده پیام‌هایی هستند که تحت توابع هش (Hash)[2] به صفر و یک تبدیل و قابلیت ذخیره‌سازی در بلاک‌ها را پیدا می‌نمایند. اجزای تشکیل دهنده هر بلاک، هش بلاک و پیش هش بلاک هستند. هش بلاک به منزله شناسنامه هر بلاک بوده و نشان دهنده کمیت و کیفیت داده‌های ذخیره شده در آن است. از این رو بازخوانی داده‌های ذخیره شده در بلاک به وسیله مشاهده نوع آنها از هش بلاک رخ می‌دهد. پیش هش بلاک نیز ابزاری جهت ارتباط و اتصال هر بلاک به بلاک



۱.

۲. تابع هش تایعی ریاضی می‌باشد که مقدار ورودی را به مقداری دیگر تبدیل می‌کند. کارکرد این تابع در فرایند رمزنگاری داده‌ای می‌تواند منجر به تولید داده پیام‌های رمزنگاری شده گردد. استفاده از این توابع در رمزنگاری داده پیام‌های حاصل از انعقاد قراردادهای هوشمند و ذخیره آنها در بستر بلاک چین منجر به ایجاد امنیت داده‌ای در این بستر می‌گردد. مکانیسم عملکرد این تابع به شکلی است که داده پیام اولیه با ورود به آن به شکل داده پیامی ثانویه رمزنگاری می‌گردد. بازخوانی داده پیام ثانویه و تبدیل آن به داده پیام اولیه نیز با طی مراحل پیشرفته به صورت عکس انجام می‌گیرد. درصورتی که داده پیام ثانویه مورد تخریب یا دست کاری قرار گیرد، در تبدیل آن به داده پیام اولیه نیز داده پیام حاصل، با داده پیام نخستین تفاوت خواهد داشت. این فرایند موجب می‌گردد تا داده پیام‌هایی که در حملات سایبری دچار تغییر شده باشند به آسانی شناسایی شوند (برای مطالعه بیشتر، ر. ک:
Hingley Tom, Asmartnewworld: blockchainandsmartcontracts, https: //www. freshfields. com /en-gb/our-thinking/campaigns/digital/fintech/blockchain-and-smart-contracts/2017.

قبلی می‌باشد که هرگونه اخلال در یک بلاک منجر به تغییر هش بلاک آن می‌شود (Sean, 2019) وجود این خصیصه در هش بلاک در شناسایی بلاک‌های معیوب توسط کاربران سیستم موثر خواهد بود. بلاک چین به دو نوع بلاک چین عمومی و بلاک چین خصوصی تقسیم می‌گردد. بلاک چین عمومی بستری است که تمامی اطلاعات ذخیره شده در آن قابلیت مشاهده توسط عموم جامعه را داشته و اشخاص به وسیله امضائات دیجیتالی خود قادر به مشاهده و تهیه رونوشت از اطلاعات ذخیره شده در بلاک چین عمومی هستند. اما بلاک چین خصوصی بستری است که عموما در سیستم نهادها و موسسات یا شرکت‌ها تعبیه می‌گردد و ورود و دسترسی به اطلاعات ذخیره شده در آن نیازمند برخورداری کاربر از پین کدهای منحصر به فرد خواهد بود (Lopez & Etc, 2018, p.6).

سازوکار انعقاد قراردادهای مبتنی بر بلاک چین که اصطلاحا قراردادهای هوشمند نامیده می‌شوند، به شکلی است که می‌تواند اهداف بیان شده در ابتدای این گفتار را به خوبی تامین نماید. قراردادهای هوشمند قراردادهایی هستند که پس از انعقاد در بلاک چین، مفاد آنها به صورت شفاف در بلاک‌های این زنجیره ذخیره و توسط عموم جامعه قابل مشاهده می‌باشند (Karen E.C. Levy, 2017, p.2) سازوکار انعقاد و امضای این قراردادها در بلاک چین منوط به برخورداری اطراف معامله از امضائات دیجیتالی می‌باشد. همچنین آنچه به عنوان وجه در این نوع قراردادها مورد تبادل قرار می‌گیرد ارزهای رمزنگاری شده دیجیتالی می‌باشند (Silverberg, French, Ferenzy, Van Den Berg, 2016, p.5) در نظام حقوقی اتحادیه اروپا، تخصیص مجوز بهره مندی از امضائات دیجیتالی منوط به شناسایی هویت و مایملک اشخاص، وضعیت حقوقی و سوابق ورشکستگی یا کیفری فرد و به طور کلی تأیید صلاحیت متقاضی دریافت مجوز از نهادهای صلاحیت‌دار کشور متبوع خود می‌باشد. به جهت سازوکار طولانی که در اعطای این مجوز در اتحادیه اروپا وجود دارد، کشورهای اعطاکننده مجوز به اتباع خود، ضامن صحت اجرای تعهدات موجود در قراردادهای منعقده به وسیله امضائات دیجیتالی می‌باشند (Stephen E. Blythe, 2007, pp.47 & 49) علاوه بر آن سازوکار تخصیص مجوز تملک ارزهای مجازی در اتحادیه اروپا مطابق با مفاد مواد ۲و ۳ کنوانسیون یکنواخت‌سازی معاملات مبتنی بر ارزهای مجازی مصوب ۲۰۱۷[1]

1. Uniform Regulation Virtual Currency Business Act, July 2017 (URVCBA).

سازوکاری مشابه با سـازوکار تخصـیص مجـوز بهـره منـدی از امضـائات دیجیتـالی درخصـوص شناسایی هویت و مایملک اشخاص پیش‌بینی نموده است.

آنچه در زمینه به‌کارگیری این سازوکار در حقوق ایران می‌تواند محل تامـل قـرار گیـرد، کیفیـت به‌کارگیری امضائات دیجیتالی و اعتبار سنجی ارزهای مجازی می‌باشد. ازآنجاکه مطابق با مواد ۲و ۱۰ قانون تجارت الکترونیکی، امضائات الکترونیکی مطمئن در این نظام مورد تصریح قـرار گرفتـه است، سؤال موجود این است که آیا امضائات الکترونیکی مطمئن قادر بـه بهـره منـدی از پتانسـیل به‌کارگیری در قراردادهای هوشمند خواهنـد بـود؟ امضـائات الکترونیکـی مطمـئن نـوعی امضـای دیجیتالی می‌باشند. امضائات دیجیتالی از دو کلیـد خصوصـی و عمـومی تشـکیل شـده‌اند. کلیـد خصوصی جهت امضا قراردادهای هوشمند و کلیـد عمـومی جهـت بـازخوانی مفـاد قراردادهـای هوشمند به کارگرفته می‌شوند. تفاوت موجود میان امضائات دیجیتالی به معنای اخص و امضـائات الکترونیکی مطمئن در گواهی امضای الکترونیکی مطمئن به وسیله دفاتر گـواهی امضـا در کشـور ایران می‌باشد (برای مطالعه بیشتر درمـورد امضـای الکترونیکـی مطمـئن، ر.ک: لینـان دبلفـون، ۱۳۹۰، ص۲۰۳). به‌کارگیری نوع اخیر از امضا در قراردادهای هوشـمند مـی‌توانـد در بردارنـده مشـکلات حاصل از گواهی امضای تبعه ایران از سوی دفاتر مذکور باشد. به عبارت دیگر تفـاوت اساسـی در نحوه به‌کارگیری امضائات دیجیتالی به معناص خاص در اتحادیـه اروپـا و امضـائات الکترونیکـی مطمئن در ایران در این است که در اتحادیـه اروپـا پـس از درج امضـا در قـرارداد، نیـاز بـه وجـود مرجعی دیگر جهت تأیید هویت امضاکننده موجود نمی‌باشد. در حـالی کـه پـس از درج امضـای الکترونیکی مطمئن در ایران، تحقق معامله منوط به شناسایی هویت امضاکننده توسط دفاتر گواهی امضا و تأیید این امر است.

مکانیسم موجود در کشور ایران اگرچه از جهت امنیتی می‌تواند مزایایی دربرداشـته باشـد، امـا مشکل اساسی آن این است که در قراردادهـای الکترونیکـی کـه طـرف دیگـر قـرارداد در کشـوری خارجی قرار دارد، تأیید هویت طرف دیگر به چه شکلی امکان پذیر خواهد بود؟ اگر انعقاد قـرارداد منوط به تأیید هویت طرف ایرانی به وسیله دفاتر گواهی امضای الکترونیکی باشد، آیا نظام حقـوقی کشور دیگر مبادرت به پذیرش این سازوکار خواهد بود؟ از طرف دیگر اگر پس از امضای قـرارداد، مدت زمان مدیدی میان امضا و تأیید آن توسط دفاتر بیان شده سپری گردد، سـازوکار ذخیـره مفـاد قراردادهای منعقد شده میان طرف ایرانی و خارجی در بلاک چین به چه شکلی خواهد بود؟ علاوه

بر چالش‌های مذکور مشکل دیگری کـه در زمینـه انعقـاد قـرارداد بوسـیله امضـائات الکترونیکـی مطمئن وجود دارد، ابهام در چگونگی تخصیص این مجوز به متقاضیان است. به عبـارتی تـدبر در مقررات موجود در قانون تجارت الکترونیکی ایران نشان می‌دهد که قانون گذار ایران بدون هرگونـه پیش‌بینی در کیفیت اعطای این مجوز به متقاضی، تنها با بیان خصوصیات این نوع امضـا (در مـادّه ۱۰ قانون مرقوم) سعی در معرفی آن در حقوق ایران داشته است. در حالی که مسـئله اساسـی نحـوه به‌کارگیری این امضا توسط متقاضیان است که اعطای آن در ایران را با ابهـام مواجـه نمـوده اسـت. علاوه بر آن عدم ضمانت صحت قراردادهای منعقده به وسیله ایـن امضـائات توسـط دولـت ایـران دیگر تفاوت میان نظام حقوقی ایران و اتحادیه اروپا است. اگر قـراردادی میـان یـک ایرانـی و یـک اروپایی منعقد و دولت متبوع طرف اروپـایی بـا درج امضـای دیجیتـالی صـحت انجـام تعهـدات قراردادی به وسیله تبعه خود را تضمین نماید، انتظار انجام عمل متقابل از سوی دولت ایـران را نیـز دارد. این در حالی است که در کشور ایران قانونی مبنی بر تضمین صحت انجام تعهدات قـراردادی صورت گرفته به وسیله امضائات الکترونیکی مطمئن موجود نمی‌باشد. از ایـن حیـث قـانون گـذار ایران یا نیازمند تصویب قانون در جهت پیش‌بینی سازوکار تخصیص امضائات دیجیتالی در کشـور ایران می‌باشد و یا باید به نحوی شایسته با در نظر گـرفتن چالش‌هـای بیـان شـده در ایـن پـژوهش مبادرت به اصلاح قوانین مصوب از جمله قانون تجارت الکترونیکی نماید.

سوال دیگری که دراین‌باره می‌تواند محل توجه قرار گیرد، مسئله اعتبار سنجی ارزهـای مجـازی است. در نظام حقوقی ایران، از بعد حقوقی تنها سند قانونی که مبادرت به تعریف ارز نموده است، مادّه ۱ قانون مبارزه با قاچاق کالا و ارز میباشد. این مادّه ارز را «پول رایج کشورهای خـارجی، اعـم از اسکناس، مسکوکات، حوالجات ارزی و سایر اسـناد مکتـوب یـا الکترونیکـی کـه در مبـادلات کاربرد داشته باشد» تعریف نموده است. از بعد اقتصاد پولی نیز ارز به «پول رایج کشور کـه توسـط حاکمیت آن کشور تولید و در قالب اسکناس یا سکه در بازارهای پولی عرضـه مـی‌گـردد»، اطـلاق می‌شود. وجه شباهت تعاریف بیان شده تولید و عرضه ارز توسط حاکمیت یک کشور می‌باشد. لذا ارزهای مجازی که توسط ماینرها از بسترهای نامتمرکز استخراج می‌شوند، به جهـت عـدم تولیـد و عرضه توسط حاکمیـت کشـور قابلیـت اطـلاق عنـوان ارز در نظـام حقـوقی ایـران را ندارنـد. امـا درخصوص ارزهای تولید شده توسط حاکمیت کشورها میتوان از دو حیث قائل به تفصیل شد.

اول اینکه مطابق با مفاد مادّه ۱ قانون مبارزه با قاچاق کالا و ارز با امعـان نظـر از عبـارت «اعـم

از» موجود در صدر مادّه توجها به اعتبار سنجی اسناد الکترونیکی مورد تبادل توسط قانون گذار در مادّه مرقوم، ازآنجاکه این ارزها نیز توسط حاکمیت کشور به وجود آمده و توسط افراد نیز مورد مبادله قرار می‌گیرند، بتوان عنوان ارز را بر این ابزارها پیاده نمود.

دوم اطلاق عنوان ارز بر این نوع ابزارها واجد ایراد می‌باشد. چرا که اولا آنچه که قانونگذار در این قانون از عبارت ارز تعریف نموده است، منحصرا اختصاص به مقررات این قانون داشته و نمی‌توان از این عبارت تعریف کلی از عنوان ارز برداشت نمود. چرا که مادّه ۲ قانون پولی و بانکی کشور نیز که به عنوان قانون مبنا در حوزه عملکرد نهادهای فعال در بازارهای پولی شناخته می‌شود، پول رایج کشور را تنها در قالب اسکناس و سکه تعبیر و تعهد به پرداخت دین را تنها به این طرق شناسایی نموده است و اگر نیاز به بازشناسی عنوان ارز در تعاریف قانونی باشد، سیاست‌گذاران باید نسبت به اصلاح قوانین پولی و بانکی اقدام نمایند.

اما تدبر در شرایط حاکم بر جامعه و مقتضیات روز، تسری تعریف مقرر در مادّه ۱ قانون مبارزه با قاچاق کالا و ارز را در شناسایی ارز در بازارهای پولی ایران ایجاب می‌نماید. از طرف دیگر این نظر با تدبر در مواد ۵ و ۷ قانون پولی و بانکی کشور ایران نیز قابل برداشت می‌باشد. چرا که مادّه ۵، یکی از دارایی‌های «ارزی» بانک مرکزی در برابر اسکناس‌های منتشره در بازار را ارز طبق مادّه ۷ برشمرده است. بند ح مادّه ۷ نیز یکی از دارایی‌های ارزی بانک مرکزی را اسناد بهادار خارجی قابل تبدیل به ارز مورد قبول آن بانک قرار داده است. از این رو توجها به تولید ابزارهای مذکور توسط حاکمیت کشورهای خارجی و بهادار بودن آنها در بازارهای جهانی که امکان تبدیل به ارزهای مورد قبول بانک مرکزی از جمله یورو را به آنها اعطا مینماید، میتوان ارز بودن این ابزارها را استنباط نمود.

در نظام حقوقی اتحادیه اروپا ارز به هر آنچه که توسط عرف جامعه در بازار به عنوان وسیله مبادله کالا یا دریافت خدمات تلقی گردد (Rouse, 2020) و در بازارهای پولی در حال گردش باشد (Debitoor, 2020) بیان می‌شود. آنچه از ماهیت ارزهای مجازی و سازو کار تبادل این ارزها بیان گردید، نشان از اطلاق عنوان ارز بر هر دو گونه ارزهای مجازی در اتحادیه اروپا می‌باشد. چرا که هر دو گونه ارز توسط عرف تجار در بازار مورد تبادل قرار گرفته و مطابق با مفاد تعریف مذکور در حال گردش در بازارهای پولی این اتحادیه می‌باشد. همچنین با توجه گزارش مورخ ۲۰۱۸ پارلمان اروپا توجها به تعریفی که در سال ۲۰۱۳ بانک مرکزی اتحادیه اروپا (The European

Central Bank) از ارز نموده است، ارز، هر برگه بهاداری می‌باشد که قابلیت تبادل در بازارهای پولی را داشته باشد (Houben & Etc, 2018, p.22) به نظر نگارندگان عبارت برگه بهادار ناشی از مسامحه مقام ارائه دهنده گزارش بوده و بر تأکید آن سازمان بر ارزهای کاغذی اشاره دارد که در اطلاق تعریف مزبور بر دیگر انواع ابزارهای دیجیتالی یا غیر دیجیتالی می‌توان از این عبارت الغای خصوصیت نمود، اما خاطر نشان می‌گردد که ارزهای مجازی قابلیت ذخیره در ابزارهای مختلفی را دارند. یکی از این ابزارها برگه‌هایی موسوم به Paper Walletها می‌باشند. این برگه‌ها با برخورداری از کدهای QR می‌توانند در بردارنده انواع مشخصی داده پیام از جمله ارز مجازی باشند که میزان ارزش مورد تبادل این برگه‌ها در بازارهای پولی بر اساس ارزش داده پیام‌های ذخیره شده در آنها تعیین می‌گردد (Alkadri, 2019, p.79) لذا به جهت بهادار بودن این برگه‌ها در بازار و قابلیت تبادل کالا یا خدمات بر آنها اطلاق عنوان ارز بر این گونه برگه‌ها مطابق با تعریف بیان شده خالی از اشکال است.

نتیجه

در عصر حاضر تضمین امنیت حفاظت از اطلاعات به عنوان یکی از چالش‌های نظامات حقوقی مورد طرح قرار گرفته است. ابزارهای اینترنت اشیا نیز ابزارهایی الکترونیکی می‌باشند که جهت انجام وظایف خود، مبادرت به جمع‌آوری اطلاعات از محیط پیرامون، ارسال آنها به کنترل‌کننده و دریافت داده‌های پردازش شده توسط پردازنده از سوی کنترل‌کننده می‌نمایند. اما چالش موجود سازوکار حفظ امنیت اطلاعات خصوصی جمع‌آوری شده از اشخاص در فرآیند پردازش توسط پردازندگانی می‌باشد که یا دارای تابعیت کشوری غیر از کشور متبوع کنترل‌کننده یا دارنده ابزار هستند، یا شرکت‌های فراملی می‌باشند که حقوق و تعهدات آنها بر اساس مقررات بین‌المللی مورد توجه قرار می‌گیرد.

امروزه در نظام حقوقی اتحادیه اروپا، با تصویب دستورالعمل عمومی حفاظت از اطلاعات خصوصی اروپاییان مصوب ۲۰۱۶ در زمینه اعطای مجوز پردازش داده و کیفیت وقوع پروسه مذکور مقررات جامعی در این اتحادیه در دستور کار کشورهای عضو قرار گرفته است. از طرف دیگر به‌کارگیری سازوکار انعقاد قراردادهای پردازش در بسترهای نامتمرکز به عنوان راه حلی در جهت تضمین شفافیت و تضمین اجرای تعهدات قراردادی در این نظام پیشنهاد شده است. اما

کشور ایران به عنوان یکی از کشورهای در حال توسعه که در آینده نزدیک نیازمند پیاده‌سازی فناوری ابزارهای اینترنت اشیا در نظام داخلی خود می‌باشد، باید با مطالعه چالش‌هایی که نظام حقوقی اتحادیه اروپا در زمینه سازوکار عملکرد این ابزارها با آن مواجه بوده و راه حل‌های ارائه شده در این نظام، امکان هر چه بهتر به‌کارگیری این فناوری در بخش‌های مختلف صنعت و تجارت را فراهم نماید. از این رو پیشنهادات ذیل برای تحقق این مهم ضرورت دارد:

تصویب قانون جامع در زمینه کیفیت پردازش داده‌های خصوصی: همان‌طور که بیان شد در حال حاضر چهارچوب قانونی موجود در نظام حقوقی ایران در زمینه پردازش داده‌های خصوصی تنها به دو مادّه ۵۸ و ۵۹ قانون تجارت الکترونیکی محدود می‌باشد. این در حالی است که هیچ مقرره دیگری در زمینه کیفیت اعطای مجوز به نهادهای فعال در زمینه پردازش داده، سازوکار پردازش داده و ضمانت اجراهای حقوقی و کیفری نقض قواعد امنیتی حاکم بر این مسئله، مکانیسم موجود در زمینه تبادل داده‌های خصوصی میان شرکت‌های داخلی با بین‌المللی یا ارسال داده به کشورهای خارجی، سازوکارهای امنیتی لازم در زمینه فرایند انعقاد قراردادهای پردازش و نقش دولت دراین‌باره مشخص نمی‌باشد. از این رو مجلس قانون گذاری ایران با بهره مندی از تجربیات نظام بین‌الملل از جمله دستورالعمل مصوب ۲۰۱۶ اتحادیه اروپا نیازمند تصویب قانونی جامع در جهت پیش‌بینی تفصیلی ابعاد حقوقی حاکم بر حفاظت از داده‌های خصوصی می‌باشد.

پیش‌بینی کیفیت به‌کارگیری بلاک چین در نظام حقوقی ایران و سازوکار اعطای مجوز بهره مندی از امضائات دیجیتالی: همان‌طور که بیان شد، پیاده‌سازی بسترهای نامتمرکز به عنوان یکی از راه‌های ایجاد شفافیت و توسعه امنیت مبادلاتی می‌باشد. کشور ایران نیز در آینده نزدیک برای حضور فعال در عرصه تجارت بین‌الملل نیازمند پیاده‌سازی ابزارهای نوین در نظام حقوقی خود می‌باشد. در این میان مسئله به‌کارگیری امضائات دیجیتالی و سازوکار اعطای آنها به افراد یکی از چالش‌های نظام حقوقی ایران می‌باشد. همان‌طور که بیان شد در این نظام نه سازوکار مناسبی در جهت پیش‌بینی چگونگی اعطای این امضا به اشخاص موجود است و نه مکانیسم عملکرد امضائات الکترونیکی مطمئن می‌تواند به نوعی پاسخگوی این نظام در مواجهه با قراردادهای منعقده در عرصه بین‌الملل باشد. رفع این مسئله نیز جز با تصویب قانونی جامع امکان پذیر نخواهد بود.

تصویب قانون جامع در جهت اعتبارسنجی و جهت بخشی به روند تبادل ارزهای مجازی در

بازارهای پولی ایران: یکی دیگر از چالش‌های اساسی نظام حقوقی ایران در عرصه تجارت الکترونیکی مسئله اعتبارسنجی ارزهای مجازی می‌باشد. روند رو به رشد به‌کارگیری این ارزها در مبادلات بین‌المللی از یک طرف و عدم قابلیت اطلاق عنوان ارز بر ارزهای مستخرج از بسترهای نامتمرکز و امکان ارائه استدلالات مختلف درخصوص ارزهای تولید شده توسط حاکمیت کشورها، ضرورت تصویب قانونی جامع در جهت اعتبارسنجی این ارزها را دوچندان می‌نماید. از طرف دیگر ازآنجاکه استخراج ارزهای رمزنگاری شده از بلاک چین و عرضه آنها در بازارهای پولی درصورتی که بدون پشتوانه صورت پذیرد، واجد اثرات منفی بر شاخص اقتصادی کشور می‌شود، ضرورت ورود حاکمیت بر پیش‌بینی مجوز تملک و تبادل ارزهای مجازی توسط اشخاص ضروری می‌باشد. امروزه با تصویب کنوانسیون یکنواخت‌سازی معاملات مبتنی بر ارزهای مجازی، سازوکارهای نسبتا مفیدی در جهت سامان بخشی بر چگونگی نظارت بر عملکرد استخراج‌کنندگان ارزهای مجازی و تبادل‌کنندگان آنها پیش‌بینی شده است که توجه به آنها می‌تواند کمک شایانی به سیاست‌گذاری تقنینی این امر در نظام حقوقی ایران نماید.

پیش‌بینی نهادهای صلاحیت‌دار در جهت روند نظارت بر عملکرد نهادهای فعال در سازوکار عملکرد ابزارهای اینترنت اشیا: همان‌طور که بیان شد نظام حقوقی ایران در پیاده‌سازی این فناوری نیازمند تصویب قانون جامع در جهت تعیین کیفیت پردازش داده‌های خصوصی و چگونگی اعطای مجوز به نهادهای فعال در این پروسه می‌باشد. اما محقق نمودن اهداف موجود در حفاظت از اطلاعات، علاوه بر تصویب قوانین کارآمد، نیازمند پیش‌بینی نهادهای صلاحیت‌دار ناظر می‌باشد. در حال حاضر به‌رغم وجود مقررات مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی در زمینه کیفیت پردازش داده ها، هیچ مقرره قانونی در جهت بیان چگونگی نظارت بر تبادل و پردازش داده‌ها و نحوه عملکرد پردازندگان در ایران یا ارسال و دریافت داده‌ها به خارج از ایران وجود ندارد. البته مطابق با مفاد مواد ٦٦و ۷۲ قانون آیین دادرسی کیفری سازمان‌های مردم نهاد و مقامات و اشخاص رسمی که از وقوع هر یک از جرایم غیر قابل گذشت مطلع شوند از امکان ارائه گزارش به نهادهای صلاحیت‌دار برخوردارند. اما نهادهای مذکور صلاحیت نظارت بر عملکرد دیگر سازمان‌ها را ندارند. این در حالی است که مادّه ۱۰ کنوانسیون حمایت از افراد درخصوص پردازش خودکار داده‌های شخصی که از آن به معاهده شماره ۱۰۸ اتحادیه اروپا یاد می‌گردد، با پیش‌بینی سازمان‌های صلاحیت‌دار نظارتی که امکان ارائه گزارشات رسمی به مقامات قضایی در موارد وقوع

هرگونه سوءاستفاده که زمینه تحقق جرایم مرتبط با داده‌ها را فراهم آورد، به نـوعی نسـبت بـه حفـظ امنیت داده در فضای عمومی مبادرت نموده است. این سـازمان‌ها کـه الزامـا بایـد جـزو نهادهـای حکومتی باشند، از حق دسترسی به تمامی اطلاعات دریافتی و مورد پردازش از سوی پردازشـگران و نظارت همه جانبه بر فعالیت آنها برخوردار بوده و در هر زمان درصورت مشاهده هرگونـه تخلـف از سوی آنان الزاما باید نسبت به درجریان گذاشتن مقامات قضایی و انتظـامی جهـت پیگـرد نهـاد متخلف اقدام نمایند. وجود این سازوکار منجر می‌گردد تا درصورتی که نهاد مذکور نسبت به ارائـه گزارش به هر نحو به سازمان‌های صلاحیت‌دار اقدام نکند، مسئولیت جبران خسـارات وارده ناشـی از عمل خود را پذیرا باشد. دراین‌باره توجه مجلس قانون گذاری ایران به مقررات مصوب بین‌المللی از جمله معاهده مذکور می‌تواند کمک شایانی در پیش‌بینی مراجع صلاحیت‌دار نظـارتی و حـدود صلاحیت، اختیارات و تکالیف آنها در کشور ایران نماید.

منابع

۱. رهپیک، سیامک؛ **حقوق مسئولیت مدنی و جبران‌ها**؛ تهران: خرسندی، ۱۳۹۵.

۲. لینان دبلفون، زویه؛ **حقوق تجارت الکترونیک**؛ ترجمه ستار زرکلام (همراه با تحلیل قانون تجارت الکترونیکی ایران)؛ چ۲، تهران: انتشارات شهر دانش، ۱۳۹۰.

3. Alan Charles Raul; Privacy; **Data Protection and Cybersecurity Law Review**; Law Business Research Ltd; Fourth Edition; Gideon Roberton Publisher; 2017

4. Alkardi Susan; "Defining and Regulating Cryptocurrency: Fake Internet Money or Legitimate Medium of Exchange?"; **Duke University School of Law**; J. D. expected May, 2019; B. S. in Psychology; University of California, Davis; 2019

5. Christopher Kuner; Regulation of Transborder Data Flows under Data Protection and Privacy Law; Past, Present and Future, OECD Digital Economy Papers; No. 187; OECD Publishing; **http: //dx. doi. org/10. 1787/5kg0s2fk315f-en, 2011 (Last Visited Online Edition 13 Nov2019).**

6. Council of Europe; Details of Treaty No. 108; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; online Edition: **https: //www. coe. int/en/web/conventions/full-list/-/conventions/treaty/108 (Last Visited 13 Nov2019).**

7. Debitoor; Currency - What is currency?; **https: //debitoor. com/dictionary/currency, (Last Visited 13 April 2020).**

8. EuropeanCommision; Data protection in the EU**; https: //ec.**

europa. eu/info/law/law-topic/data-protection/data-protection-eu_en/E1, (Last Visited 13 Nov2019).

9. European Commision; Justice and Consumers; Article 29 Working Party**; https: //ec. europa. eu/newsroom/article29/news. cfm?item_type=1358/E2, (Last Visited 13 Nov2019).**

10. European Commission; The Article 29 Working PartyCeased to Exist as of 25 May 2018; **https: //ec. europa. eu/newsroom/article29/item-detail. cfm?item_id=629492, (Last Visited 13 Nov2019).**

11. European Commission; Communication from the Commission to the European Parliament and the Council; Exchanging and Protecting Personal Data in a GlobalisedWorld; online Edition: **https: //ec. europa. eu › newsroom › document, 2017**

12. Finance Latvia Association; Guidelines For implementation of the General Data Protection; Online Edition: **https: //www. financelatvia. eu/wp-content/uploads/2018/09/Guidelines-For-implementation-of-the-General-Data-Protection-Regulation-. pdf, 2018**

13. HingleyTom; A smart new world: blockchain and smart contracts; Online Edition: **https: //www. freshfields. com/en-gb /our-thinking/campaigns/digital/fintech/blockchain-and-smart-contracts/2017 (Last Visited 13 Nov2019).**

14. Houben Robby; Alexander Snyers; **Cryptocurrencies and blockchain , Legal context and implications for financial crime, money laundering and tax evasion;** Policy Department

for Economic, Scientific and Quality of Life Policies; 2018

15. Julian Wagner; "The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?"; **International Data Privacy Law**; online Edition: https: //academic. oup. com › advance-article-pdf › doi › idpl › ipy008 › ipy008, 2019
16. Karen E. C. Levy; "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law"; **social science and research network, www. ssrn. com, 2017**
17. Lachlan Urquhart, Tom Lodge, Andy Crabtree; "Demonstrably doing accountability in the Internet of Things"; **International Journal of Law and Information Technology**; Vol27; 2019
18. Lopez Aurelio, Martinez Tarruella; "Smart Contracts from a Legal. Perspective"; **Facultat de Dret Facultad de Derecho, Universiad de Alicante**; downloaded from www.ssrn.com; 2018
19. OECD; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; online Edition: **https: //www. oecd. org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata. htm#part1, (Last Visited 10 Nov2019).**
20. Oladayo Bello &SheraliZeadally; "Intelligent Device-to-Device Communication in the Internet of Things"; IEEE Systems Journal, available at **http: //syslog. co. in/files/eciot/Intelligent%20Device-**

toDevice%20Communication. pdf, 2014 (Last Visited online Edition 13 Nov2019).

21. Rouse Margaret; currency; **https: //whatis. techtarget. com/definition/currency, (Last Visited 13 April 2020).**

22. Sean; If you understand Hash Functions, you'll understand Blockchains, **https: //decentralize. today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d, (Last Visited 29 Nov 2019).**

23. Silverberg Kristen, French Conan, Ferenzy Dennis, Van Den Berg Stephanie; "Getting Smart: Contracts on the Blockchain"; **Institute Of International Finance**; Available at: www.ssrn.com; 2016

24. Stephen E. Blythe; **Hungary's, Electronic Signature Act: Enhancing Economic Development with Secure Electronic Commerce Transactions;** School of Management; New York Institute of Technology; USA; 2007.