Reforms Raised by Internet of Things in Administrative Law and Smart Governance

FarKhondeh Kyayi

Assistant Professor, Department of Electrical Engineering, Technical and Vocational University, Tehran, Iran, f.kiaee@tvu.ac.ir

Date Received: 2023/08/19
Date of Release:2023/11/07

Abstract

Recent smart city strategies are directly or indirectly related to Internet of Things (IoT) applications. Administrative and constitutional norms can impose motivations to introduce applications of the IoT in the public administration. The results of this paper introduce the IoT design necessities for a closer exchange between citizens and the state, namely ensuring the legal conformity of automated administrative procedures and not existing any margin of appreciation. Processing personal data in IoT applications requires that public and private institutions comply with the principles of data protection laws, namely the principle of privacy of personally identifiable information and the principle of necessity and purpose limitation. Moreover, the results show the potential of the IoT to change administration and administrative law i.e., transition of roles for humans and the public administration, opportunity creation of cooperative legislator, construction information symmetries and equity, changes in administrative procedures and structures, and redirection of human resources where they are really needed. Achieving these advantages requires a legal system that can take into account the necessary rules during the implementation of an IoT application. Germany's regulatory experience in this regard can be taken into consideration by Iranian legislators.

Key words: Internet of Things (IoT), Smart governance, Administrative law, Privacy, Margin of appreciation.

فصلنامه حقوق اداری
سال دهم، پاییز ۱۴۰۲، شماره ۳۶
مقاله علمی پژوهشی

تحولات برخاسته از اینترنت اشیا در حقوق اداری و تحقق حکمرانی هوشمند

فرخنده کیائی[۱]

تاریخ دریافت: ۱۴۰۲/۰۵/۲۸
تاریخ پذیرش: ۱۴۰۲/۰۸/۱۶

چکیده

استراتژی‌های اخیر حکمرانی هوشمند به‌طور مستقیم یا غیرمستقیم با برنامه‌های اینترنت اشیا مرتبط هستند. هنجارهای اداری و قانون اساسی می‌توانند انگیزه‌هایی را برای معرفی کاربردهای اینترنت اشیاء در حقوق اداری ایجاد کنند. نتایج این پژوهش الزامات ارائه طرح‌های اینترنت اشیا در تحقق تعامل نزدیکتر بین شهروندان و دولت، شامل الزام انطباق رویه‌های اداری خودکار با قانون و عدم وجود حاشیه مجاز تفسیر در فرآیند اداری را معرفی می‌کند. علاوه بر این، نهادهای عمومی و خصوصی هنگام پردازش داده‌های شخصی در کاربردهای اینترنت اشیا باید اصول قوانین حفاظت از داده‌ها را رعایت کنند که شامل اصل رعایت حریم خصوصی در پردازش اطلاعات قابل شناسایی شخصی و اصل ضرورت و محدودیت هدف است. همچنین امکان ایجاد تغییرات بالقوه در قوانین اداری و نحوه حکمرانی با بکارگیری اینترنت اشیا مانند تغییر نقش‌ها برای انسان‌ها و ادارات عمومی، فرصت قانونگذاری مشارکتی، تغییرات در روند و ساختار اداری و هدایت منابع انسانی به جهات مورد نیاز مورد بررسی قرار می‌گیرند. تحقق این ویژگی‌ها نیازمند برخورداری از یک نظام حقوقی مشخص است که بتواند احکام لازم را در راستای بکارگیری اینترنت اشیا، در خود جای دهد. تجربه مقررات‌گذاری آلمان در این خصوص می‌تواند مورد توجه قانونگذار ایران قرار گیرد.

واژگان کلیدی: اینترنت اشیا، حکمرانی هوشمند، حقوق اداری، حریم خصوصی، حاشیه مجاز تفسیر.

۱. استادیار، گروه مهندسی برق، دانشگاه فنی و حرفه‌ای، تهران، ایران، f.kiaee@tvu.ac.ir

مقدمه

در چند سال اخیر، مفهوم نوینی به نام اینترنت اشیا[1] ذهن بشر را به خود معطوف کرده است. تحقیقات علمی در مورد این تحول جدید در حکمرانی به طور فزاینده‌ای تحت کلمات کلیدی «دولت الکترونیک»، «اینترنت اشیا عمومی» یا «دولت هوشمند» ارائه می‌شود. با این حال، این فناوری هنوز در بسیاری از کشورها از منظر خط‌مشی‌گذاری عمومی و حقوق اداری به ندرت مورد ارزیابی قرار گرفته است. (شهریاری، ۱۳۹۷: ۱۱-۲) از این رو این پژوهش سعی دارد تا تحولات برخاسته از اینترنت اشیا در حقوق اداری، در راستای تحقق حکمرانی هوشمند را برجسته کند.

تأثیر تغییر و توسعه علم و فن‌آوری مدرن بر قانون و نظام حقوقی همه جانبه است. حقوق اداری حوزه‌های بسیار گسترده‌ای را شامل می‌شود و از نظر محتوایی بسیار غنی و متفاوت از سایر زیرشاخه‌ها در علم حقوق است. بنابراین، واکاوی ویژگی‌ها و تحولات برخاسته از اینترنت اشیا در حقوق اداری، اهمیتی روزافزون می‌یابد. از این رو، پژوهش درخصوص نوآوری در فرآیندهای اداری، به عنوان یکی از اولویت‌های اساسی در نظام حقوقی ایران مطرح است. ضرورت دیگر انجام پژوهش حاضر، فقدان ادبیات حقوقی کافی در این زمینه است. با بررسی موضوعات حقوقی مرتبط با اینترنت اشیا، می‌توان دریافت که مطالعه اینترنت اشیا در قانون مدنی و کیفری شامل مسئولیت‌پذیری عملکرد ابزارهای اینترنت اشیا و همچنین در حفاظت از داده‌ها و حریم خصوصی متمرکز شده است. (صادقی و ناصر، ۱۳۹۹: ۱۰۳-۸۱) در مقایسه، پژوهش کافی در مورد تحولات حقوق اداری مبتنی بر اینترنت اشیا انجام نشده است. (طاهری و خاکپور، ۱۳۹۹: ۱۶۴-۱۴۵)

از این رو دانش و تجربه کمی در زمینه نواندیشی فرآیندهای اداری در دست است که استمرار این روند می‌تواند تأخیر در استقرار یک نظام کارآمد و مؤثر را افزایش و زمینه از دست رفتن فرصت‌های پیش رو را فراهم سازد. بر این اساس، پژوهش حاضر در پی پاسخ به این سؤال اصلی است که چالش‌های حقوقی و راهکارهای آنها برای بکارگیری اینترنت اشیا در فرآیندهای اداری چگونه است؟ سؤال‌های فرعی پژوهش عبارتند از: ۱. الزامات طراحی عینی و غیرانتزاعی فرآیندهای نوین اداری مبتنی بر فناوری اینترنت اشیا چیست؟ ۲. چه زمینه‌های بالقوه‌ای درخصوص بکارگیری اینترنت اشیا برای تغییر قوانین اداری و دستیابی به حکمرانی مطلوب یا به زمامداری وجود دارد؟ فرض این است که فرآیندهای سنتی اداری با تأخیر در بروزرسانی و عدم انعطاف‌پذیری خاصی در زمینه خودکارسازی برپایه اینترنتت اشیا، همراه بوده است. بدین ترتیب به نظر می‌رسد با گذشت زمان و تجارب عملی، بازنگری فرآیندهای اداری نه تنها ضروری بلکه نوآورانه است.

---

1. Internet of Things (IoT)

از میان کشورهای اروپایی که تجربه بکارگیری فناوری اینترنت اشیا در حکمرانی هوشمند را دارند، آلمان رتبه نخست را در اتحادیه اروپا دارد، پیش‌بینی‌ها نشان می‌دهد، گردش مالی فناوری اینترنت اشیا در حوزه حکمرانی در این کشور تا سال ۲۰۲۴ به حدود ۳ میلیارد یورو می‌رسد. در آلمان، علاوه بر «مقررات عمومی حفاظت داده‌ها» (GDPR)[1] که برای همه کشورهای اتحادیه اروپا اعمال می‌شود، قانون جداگانه‌ای تحت عنوان «قانون فدرال حفاظت از داده‌ها» (BDSG)[2] نیز وجود دارد که بر اساس آنها به‌گونه موفقی نمونه‌های عملی از بکارگیری این فناری در حکمرانی هوشمند پیاده سازی شده است. بدین‌ترتیب پژوهش حاضر که کاربردی و آینده‌نگرانه است با روش تحقیق توصیفی و با الگوگیری از کشور آلمان ارائه شده است. در ابتدا مطالعات مورد نیاز برای این پژوهش با استناد به منابع کتابخانه‌ای و با تحلیل و بررسی معتبرترین اسناد در این حوزه، گردآوری شده و با توصیف مفهوم اینترنت اشیا به بیان نمونه‌های عملی بکارگیری این فناوری در حکمرانی هوشمند می‌پردازیم (گفتار نخست). آن‌گاه، با نگاهی به قوانین کشور آلمان، انگیزه‌ها و محدودیت‌هایی که قوانین و سیاستگذاری‌های این کشور بر بکارگیری اینترنت‌اشیاء در حقوق اداری ایجاد می‌کنند را مورد مداقه قرار می‌دهیم (گفتار دوم). سپس به بیان چالش‌های حقوقی سیاستگذاری و بکارگیری اینترنت اشیا در ایران می‌پردازیم (گفتار سوم). در ادامه الزامات ارائه طرح‌های عینی در بکارگیری اینترنت اشیا در فرآیندهای ادرای خودکار را با استفاده از قوانین کشور آلمان ارائه می‌کنیم (گفتار چهارم). سرانجام امکان بالقوه بکارگیری اینترنت‌اشیا برای تغییر قوانین اداری و نحوه حکمرانی را مطرح می‌کنیم (گفتار پنجم). در قسمت نتیجه گیری نیز برآنیم تا به ارائه پیشنهاداتی برای تحقق این تغییر و تحولات نوین نائل شویم.

۱. نمونه‌های عملی بکارگیری اینترنت اشیا

در علوم کامپیوتر و سایر حوزه‌های علمی تلاش‌های زیادی برای شناسایی مفهوم اینترت اشیا ارائه شده است. به طور کلی اینترنت که در این اصطلاح یک مفهوم تقلیل یافته است به این معنی است که اشیاء محیطی به سیستم‌های فناوری اطلاعات به گونه‌ای مجهز می‌شوند که شبکه‌ای، قابل شناسایی و آدرس‌دهی را تشکیل می‌دهند و می‌توانند مشاهدات خاصی را از طریق حسگرها انجام دهند، به گونه‌ای که سیستم شبکه‌ای حاصل می‌تواند به این مشاهدات واکنش نشان دهد.

اصطلاح «شهر هوشمند» [3] به یک روند برنامه‌ریزی اداره شهری اشاره دارد که از مدتی پیش مطرح شده است و بر اساس آن استفاده از فناوری اطلاعات و ارتباطات برای بهبود زندگی در شهرها و پایدارتر

1. General Data Protection Requlation (GDPR)
2. German Federal Data Protection Act (Bundesdatenschutzgesetz-BDSG)
3. Smart City

کردن آن‌ها در نظر گرفته شده است. استراتژی‌های اخیر شهر هوشمند به طور مستقیم یا غیرمستقیم با برنامه‌های اینترنت‌اشیا مرتبط هستند. (Chatfeild and Christopher, 2019: 346-357)

کارکرد اصلی اینترنت اشیا، کاهش دخالت انسان است که می‌تواند موجب افزایش بهره‌وری، افزایش دقت در عین سرعت و کاهش هزینه‌ها انجام فعالیت‌ها طبق برنامه زمان‌بندی شود. به‌عنوان یک نمونه عملی گویا از بکارگیری اینترنت اشیا، «سیستم‌های کنترل ترافیک هوشمند» در بزرگراه‌ها را می‌توان عنوان کرد. در این خیابان‌ها، سنسورها حجم ترافیک، شرایط آب‌وهوایی و سایر شرایط مرتبط با ایمنی را اندازه‌گیری می‌کنند. این داده‌ها به مراکز داده ارسال می‌شوند، که می‌توانند با تنظیم محدودیت‌های سرعت، ممنوعیت سبقت یا تغییر مسیر ترافیک، ترافیک را از طریق علائم دیجیتال ترافیکی کنترل کنند.

نمونه‌ای دیگر «سیستم‌های تماس اضطراری خودکار» است که سازندگان خودرو و همچنین خدمات امداد و نجات موظف به پیاده‌سازی آن هستند. در این سیستم، در صورت بروز سوانح و تصادفات، سنسورهای موجود در وسایل نقلیه به طور خودکار ارتباط تلفنی را با مرکز امداد و نجات برقرار می‌کنند و پیامک حاوی مهمترین اطلاعات برای امدادگران ارسال می‌شود.

برنامه‌های اینترنت اشیا امکان طراحی تجهیزات با واکنش‌های خودکار را فراهم می‌کنند. به عنوان مثال، روبات‌های آتش‌نشان و پهپادهایی که می‌توانند با سطحی از خودمختاری تصمیم‌گیری عمل کنند در حال حاضر در حال توسعه هستند. پهپادها می‌توانند سریع‌تر به سمت منبع آتش حرکت کنند، در حالی که از ربات‌ها می‌توان در آتش سوزی‌های بسیار خطرناک بدون به خطر انداختن انسان استفاده کرد.

نظارت تصویری هوشمند نمونه عملی دیگری از بکارگیری فناوری اینترنت اشیا است. یک دوربین نظارتی هوشمند می‌تواند اطلاعات تصویری را در زمان واقعی ارائه دهد که می‌توان از راه دور از هر جایی آن را مشاهده کرد. این دوربین می‌تواند با دستگاه‌های دیگر ارتباط برقرار کند تا به طور بالقوه سیستم هشدار صوتی را تنظیم کند یا به پرسنل امنیتی در مورد تهدیدات احتمالی هشدار دهد. برخی از دوربین‌های امنیتی اینترنت اشیا حتی ویژگی‌های تشخیص چهره و بینایی رایانه‌ای پیشرفته دارند یعنی می‌توانند اطلاعات معنی‌داری از تصاویر برای شناسایی متجاوزان یا افراد مشکوک ارائه کنند.

بدین ترتیب، بکارگیری فناوری اینترنت اشیا فرصت‌ها و همچنین تهدیداتی را با خود به همراه دارد. فرصت‌های بزرگ اینترنت‌اشیا در مزایای فناوری حسگر و امکانات ارائه شده توسط تجزیه و تحلیل داده‌ها و اقدامات خودکار دیده می‌شود. در زمینه فناوری حسگر، جمع‌آوری داده‌ها به‌طور خودکار به صورت محلی در همه‌جا و در همه زمان‌ها امکان‌پذیر است. اهمیت این امر به‌ویژه در پوشش مشاهده مناطق بزرگ یا مکان‌های دورافتاده، آشکار می‌شود. یکی دیگر از مزایای فناوری حسگر جامع این است که داده‌ها را می‌توان با دقت و جزئیات بسیار بیشتری نسبت به ابزارهای معمولی جمع‌آوری کرد.

با اینحال تهدیدات مختلفی در ارتباط با اینترنت‌اشیاء وجود دارد. فناوری اینترنت اشیا خطرات خاصی را کاهش می‌دهد، اما می‌تواند آسیب‌پذیری‌های جدیدی را ایجاد کند و عواقب جدی برای طرف‌های درگیر داشته باشد. (Caruso, 2019: 157-188) عملکرد ثبت اطلاعات توسط حسگرها همچنین می‌تواند برای حریم خصوصی افرادی که داده‌هایشان ثبت می‌شود مشکل‌ساز باشد. تا آنجا که به تهدیدات خارجی مربوط می‌شود، این تهدیدات به‌ویژه بر یکپارچگی سیستم‌ها و امنیت داده‌های ذخیره‌شده در آن‌ها تأثیر می‌گذارد و حتی حملات خارجی می‌تواند سیستم را از راه دور کنترل کند. از آنجا که سیستم‌های اینترنت اشیا می‌توانند برای فعالیت‌های خاصی در اینترنت استفاده شوند، به دلیل امنیت ناکافی فناوری اطلاعات، برنامه‌های اینترنت اشیا که به اینترنت متصل هستند، می‌توانند مشابه رایانه کنترل شوند به طوری که حملات امنیتی توزیع شده می‌تواند با استفاده از سیستم‌های ناامن اینترنت‌اشیا، سایت‌ها و سرویس‌های اینترنتی خاصی را غیرقابل دسترس کنند. لذا نیاز است با تدوین قوانین و سیاست‌گذاری‌های مناسب در بکارگیری فناوری اینترنت اشیا، به تعادلی بین مزایای توسعه این فناوری جدید و خطرات متصور و مسائل بالقوه آن دست یافت.

۲. قوانین سیاستگذاری برای بکارگیری اینترنت اشیا در آلمان

اگر اداره دولتی بخواهد برنامه‌ای از اینترنت اشیا و سایر فناوری‌ها را در راستای حکمرانی هوشمند پیاده‌سازی کند، قانون می‌تواند نقش‌های نظارتی متفاوتی ایفا کند و راهنمایی‌هایی را در رابطه با رویه‌های آینده ارائه دهد. این نظارت قانون می‌تواند انگیزه‌ای برای خرید و بکارگیری محصولات اینترنت اشیا باشد، اما در عین حال محدودیت‌هایی نیز ایجاد می‌کند. (پورعزت و همکاران، ۱۳۹۸: ۱۸–۸)

از بسیاری از الزامات قانونی که می‌توان در طول اجرای برنامه اینترنت اشیا در نظر گرفت، به عنوان قوانین حفاظت از داده‌ها و امنیت فناوری اطلاعات یاد می‌شود، این موارد قانونی اغلب به بیان محدودیت‌ها در زمینه بکارگیری اینترنت اشیا می‌پردازند. در آلمان، علاوه بر «مقررات عمومی حفاظت داده‌ها» (GDPR)[1] که برای همه کشورهای اتحادیه اروپا اعمال می‌شود. قانون جداگانه‌ای در آلمان تحت عنوان "قانون فدرال حفاظت از داده‌ها" (BDSG)[2] نیز وجود دارد. هم نهادهای عمومی (مانند دفاتر، مقامات) و هم نهادهای غیر دولتی (مانند افراد خصوصی، شرکت‌ها) هنگام پردازش داده‌های شخصی باید قوانین حفاظت از داده‌ها را رعایت کنند.

1. General Data Protection Regulation (GDPR)
2. German Federal Data Protection Act (Bundesdatenschutzgesetz–BDSG)

۱-۲. مقررات عمومی حفاظت داده‌ها

اینترنت اشیا به دلیل امکان جمع آوری داده‌ها به صورت خودکار، در همه مکان‌ها و زمان‌ها، بسیاری از مسائل مربوط به حفاظت داده‌ها را مطرح می‌کند. به طور خاص، مفهوم اطلاعات قابل شناسایی شخصی، اصل ضرورت محدودیت هدف باید مورد بررسی قرار گیرد.

۱-۱-۲. اصل رعایت حریم خصوصی در پردازش اطلاعات قابل شناسایی شخصی

معیار تعیین‌کننده برای قابل اجرا بودن قانون حفاظت داده‌ها، آن است که آیا اطلاعات قابل شناسایی شخصی[1] در حال پردازش است یا خیر. اطلاعات قابل شناسایی شخصی شامل هرگونه داده‌ای می‌شود که بتوان از آن به تشخیص هویت فرد یا افرادی خاص رسید. به معنای دیگر هرگونه اطلاعاتی که به صورت مستقیم یا غیرمستقیم به شخصی مربوط باشد، اطلاعات قابل شناسایی شخصی محسوب می‌گردد. نام، آدرس ایمیل، شماره تماس، اطلاعات بانکی و کدملی از نمونه‌های آن هستند. علاوه بر اطلاعات شخصی ساده، به اصطلاح «دسته‌های خاص اطلاعات شخصی» نیز وجود دارد. این به ویژه داده‌های حساس افرادی است که تحت حمایت ویژه قرار دارند و قانون با آنها سختگیرانه تر رفتار می‌کند. دسته‌های ویژه داده‌های شخصی شامل منشأ نژادی و قومیتی، عقیده سیاسی، اعتقاد مذهبی/ایدئولوژیک، داده‌های ژنتیکی، داده‌های بیومتریک و داده‌های سلامت می‌شود.

امروزه در بستر کاربردهای گسترده اینترنت اشیا بسیاری از اطلاعات قابل شناسایی شخصی جمع‌آوری، ذخیره و پردازش می‌شوند. در این شرایط این امکان وجود دارد که با رخنه این اطلاعات به بیرون، افراد زیادی قربانی انواع حملات، کلاهبرداری‌ها و یا آسیب‌های دیگر شوند. حتی در صورت عدم بروز موارد فوق این موضوع ممکن است منجر به خدشه‌دار شدن حریم خصوصی اشخاص گردد. (اقدسی و محقق داماد، ۱۴۰۰: ۶۷-۵۰) به همین دلیل حفاظت و کنترل اطلاعات قابل شناسایی شخصی و نحوه جمع‌آوری آن از اهمیت ویژه‌ای برخوردار است و از مسائل بسیار بحث برانگیز است.

با توجه به قانون فدرال حفاظت داده‌های آلمان (BDSG) که مبتنی بر دستورالعمل حفاظت داده‌ها است، «همه منابع اطلاعاتی که به طور محتمل و مستدل توسط شخص مسئول پردازش یا توسط شخص ثالث برای شناسایی افراد قابل استفاده باشد» باید در تعیین قابل شناسایی بودن یک فرد در نظر گرفته شود. دیوان دادگستری اتحادیه اروپا (ECJ) پس از آن در این خصوص حکم داد که «اگر

1. Personally identifiable information

اطلاعات به صورت ناشناس عرضه شده باشد یا شناسایی فرد عملاً غیرقابل اجرا باشد» نیازی به اعمال قانون حفاظت داده‌ها نیست[1].

۲-۱-۲. اصل ضرورت و محدودیت هدف

ویژگی‌های اینترنت اشیا در جمع‌آوری داده‌ها (خودکار بودن، فراگیر بودن، ماندگاری) نیز در زمینه توجیه هدف جمع‌آوری و استفاده از داده‌ها تأثیر دارد. با توجه به بند اول از ماده ۱۳ قانون فدرال حفاظت داده‌ها (BDSG) در آلمان، معیار اصلی برای جمع‌آوری داده‌های شخصی برای انجام وظیفه توسط مقام مسئول، اصل ضرورت است. داده‌هایی ضروری است که «مقام عمومی نتواند تکلیف مورد نظر را به طور کامل، قانونی یا در زمان مناسب انجام دهد». باید در نظر داشت که این اقدام باید با هدف جمع‌آوری اطلاعات نیز متناسب باشد.

دادگاه قانون اساسی فدرال همچنین تصریح کرده است که شرط لازم برای قابل پذیرش بودن یک اقدام، تعریف قانونی واضح از هدف جمع‌آوری داده‌ها است. این هدف همچنین امکان پردازش داده‌ها را همانطور که در ماده ۱۴ قانون فدرال حفاظت داده‌ها (BDSG) بیان شده است، محدود می‌کند. طبق قانون قضایی دادگاه قانون اساسی فدرال، هدف از استفاده از داده‌ها باید «محدوده خاص» و «دقیق» باشد.

این موضوع در پژوهش‌ها بحث برانگیز است که آیا این محدودیت باید برای دولت الکترونیک و کلان داده نیز صادق باشد. در حالی که از یک سو ترس از فرسایش حفاظ‌های امن قانونی وجود دارد، از سوی دیگر، اصل محدودیت هدف و ساختار قانونی پشت آن به عنوان رویکرد نظارتی اشتباه مورد انتقاد قرار می‌گیرد. قانونگذار اروپایی سازش جالبی را در رابطه با سیستم‌های تماس الکترونیکی و نوآوری‌های آینده پیشنهاد کرده است. همانطور که در ماده ۶ پاراگراف ۲ مقررات تماس الکترونیکی ذکر شده است، خود سیستم تماس اضطراری الکترونیکی به هدف ارتباط خودکار با مراکز تماس اضطراری محدود می‌شود. علاوه بر این، الزامات سختگیرانه ناشناس‌سازی اطلاعات وجود دارد. با این حال، سازندگان می‌توانند خدماتی با مزایای اضافی در سیستم حسگر ارائه دهند، بدون اینکه هدف سختگیرانه مقررات تماس الکترونیکی برای آن‌ها اعمال شود. (Mulder and Nynke, 2021: 11)

۲-۲. مقررات اختصاصی امنیت فناوری اطلاعات

اگر دولت‌ها بخواهند از محصولات و برنامه‌های کاربردی اینترنت اشیا استفاده کنند، باید تابع قوانین و مقررات حاکم بر این فناوری و اقدامات احتیاطی امنیتی مربوط به آن باشند. (وکیل و نوروزپور، ۱۳۹۹: ۱۰۷-۱۴۰)

1. Case C-582/14: Judgment of the Court (Second Chamber) of 19 October 2016 (request for a preliminary ruling from the Bundesgerichtshof — Germany)

وظیفه عمومی برای ایمن‌سازی سیستم‌های فناوری اطلاعات به طور غیرمستقیم از بند اول اصل 91C قانون اساسی آلمان[1] قابل استخراج است. الزامات امنیتی در ماده ۲۳ قانون دولت الکترونیک برلین یا ماده ۸ قانون دولت الکترونیک باواریا بر دولت آلمان تحمیل شده است. (Srinivas, 2019: 178-188) مقررات مختلفی انگیزه کلی برای نصب حفاظ‌های امن فنی و سازمانی را نتیجه می‌دهد[2]. طبق تمام مقررات مذکور، اقدامات باید متناسب با کاربرد باشند و به طور مشخص براساس قانون از راه دور آلمان (TMG)[3]، قانون ارتباطات راه دور آلمان (TKG)[4] و مقررات عمومی حفاظت داده‌ها (GDPR)، باید از آخرین و جدیدترین نتایج علمی استفاده شود. اینکه چه اقداماتی باید اتخاذ شود باید به طور موقت تعیین شود یا از استانداردهای موجود گرفته شود. چنین استانداردهایی ممکن است توسط خود ادارات تهیه شوند یا ممکن است حاصل از انجمن‌های صنعتی و سازمان‌های مشابه باشند.

در آلمان، آسیب‌پذیری‌های شناسایی شده در سیستم امنیتی اینترنت اشیا توسعه داده شده توسط سازمان‌ها، توسط اداره فدرال امنیت اطلاعات آلمان (BSI)[5] مورد بررسی قرار داده می‌شود. اطلاعات مربوط به پیشینه فنی و اقدامات بالقوه به طور منظم توسط این سازمان به روز شده و در دسترس قرار می‌گیرد.

سازمان‌هایی که (بالقوه) تحت حمله امنیتی قرار می‌گیرند، طبق قانون آلمان ملزم به شناسایی سیستم‌ها و اجزای مرتبط و انجام اقدامات مناسب در سریع‌ترین زمان ممکن هستند. برای مثال ماده ۳۲ مقررات عمومی حفاظت داده‌ها (GDPR)، بند اول از بخش‌های a۸ و 8c قانون آلمان در مورد اداره فدرال امنیت اطلاعات (BSI-Gesetz)[6] موید این موضوع هستند. اگر در طول بررسی‌های فنی مشخص شود که مهاجمان واقعاً موفق شده‌اند از آسیب‌پذیری سیستم‌های اینترنت اشیا استفاده کنند، ممکن است تعهدات اعلان زیر اعمال شود:

کنترل‌کننده‌ها و پردازشگرها همانطور که در مقررات عمومی حفاظت از داده‌ها (GDRP) تعریف شده‌اند (آقایی طوق و ناصر، ۱۳۹۹: ۵۵-۳۳): نقض داده‌های مرتبط با آسیب‌پذیری‌های امنیتی می‌تواند نیازمند اطلاع‌رسانی سریع به مقامات نظارتی حفاظت از داده‌ها و موضوع‌های داده باشد (ماده‌های ۳۳ و ۳۴). پردازنده‌ها باید نقض داده‌ها را به کنترل کننده‌ها گزارش کنند.

---

1. Grundgesetz

۲. مانند ماده ۹ قانون فدرال حفاظت داده‌ها (BDSG) یا ماده ۳۲ مقررات عمومی حفاظت داده‌ها (GDPR)، و همچنین بند ۷ ماده ۱۳

3. Telemediengesetz
4. Telekommunikationsgesetz
5. Bundesamt für Sicherheit in der Informationstechnik
6. Esetz über das Bundesamt für Sicherheit in der Informationstechnik

اپراتورهای زیرساخت‌های حیاتی: اپراتورهای زیرساخت‌های حیاتی باید اداره فدرال امنیت اطلاعات آلمان (BSI) را از حوادث در موارد ذکر شده در بند ۴ از بخش 8b قانون آلمان در مورد اداره فدرال امنیت اطلاعات (BSI-Gesetz) مطلع کنند. این مورد در حال حاضر تنها اگر حوادث مهم بتواند منجر به خرابی یا آسیب زیرساخت‌های حیاتی شود اعمال می‌شود.

ارائه‌دهندگان خدمات دیجیتال (به ویژه بازارهای آنلاین، موتورهای جستجوی آنلاین، و خدمات رایانش ابری): ارائه دهندگان خدمات دیجیتال همچنین ممکن است ملزم شوند اداره فدرال امنیت اطلاعات آلمان را در صورتی که یک حادثه امنیتی تأثیر قابل توجهی داشته باشد، مطلع کنند (بند ۳ از بخش 8c قانون آلمان در مورد اداره فدرال امنیت اطلاعات (BSI-Gesetz). هنگام تعیین اینکه آیا یک حادثه تأثیر قابل توجهی دارد یا خیر، آیین‌نامه اجرایی کمیسیون مربوطه باید در نظر گرفته شود.

شرکت‌های دارای منافع عمومی خاص نیز ملزم به اطلاع اداره فدرال امنیت اطلاعات آلمان (BSI) هستند- بند ۷ و ۸ از بخش 8f قانون آلمان در مورد اداره فدرال امنیت اطلاعات (BSI-Gesetz).

اپراتورهای شبکه‌های مخابراتی عمومی و ارائه دهندگان خدمات مخابراتی در دسترس عموم: در نهایت، این اپراتورها و ارائه دهندگان نیز موظفند در صورت وجود مشکل امنیتی، به آژانس شبکه فدرال آلمان برای برق، گاز، مخابرات، پست و راه آهن[1] طبق بخش ۱۶۸ قانون مخابرات آلمان (TKG) اطلاع دهند.

برخی از برنامه‌ها نیز با توجه به امنیت فناوری اطلاعات استاندارد شده‌اند. در زمینه معرفی سیستم‌های تماس اضطراری الکترونیکی، استانداردهای مختلفی برای ایمنی سیستم‌ها ایجاد شد. اگر یک سازمان دولتی بخواهد برنامه خاصی را پیاده‌سازی کند، می‌تواند یک مدل امنیتی ایجاد کند یا مدل امنیتی خود را فراتر از تعهدات قانونی خاص گسترش دهد. چنین شرایطی، علاوه بر این، می‌تواند در کسب تجربه برای تنظیم کلی سیستم‌های اینترنت‌اشیا مفید باشد. این روند می‌تواند با ایجاد تبادل دانش بین مقامات مختلف در سطوح مختلف موفقیت‌آمیز باشد. چنین تبادل دانشی برای رفع شکاف‌های امنیتی نیز از اهمیت بالایی برخوردار است.

۳. چالش‌های و راهکارهای حقوقی سیاستگذاری و بکارگیری اینترنت اشیا در ایران

از نظر حقوقی عدم نقض حریم خصوصی افراد، یکی از چالش‌های بکارگیری فناوری اینترنت اشیا است. در حقوق ایران، دایره حریم خصوصی و اطلاعات قابل شناسایی شخصی مفهوم تعریف نشده‌ای به حساب می‌آید. علاوه براین تعریف استانداردهای حریم خصوصی برای ایجاد اعتماد و امنیت روانی در افراد جامعه در سطح بالایی موردنیاز است. حفظ محرمانگی داده‌ها نگرانی دیگری در بکارگیری این فناوری

1.Bundesnetzagentur

است. در اینترنت اشیا حجم بزرگی از داده‌ها تولید و مخابره می‌شود. بسا داده‌هایی که از طریق سیستم‌های اینترنت اشیا جمع آوری می‌شود از طریق نفوذگرها یا کارخانه‌های سازنده اشیای درگیر در شبکه اینترنت اشیا یا دستگاه‌هایی که برای هماهنگی اشیا داخل یک شبکه اینترنت اشیا به کار می‌روند، در اختیار دیگران قرار گیرد. البته فناوری بلاک چین می‌تواند یکسری از نگرانی‌ها و خطرات احتمالی را از بین ببرد، اما قطعاً تمامی نگرانی‌ها را نمی‌تواند به صفر برساند.

در نظام حقوقی ایران، ماده ۵۸ قانون تجارت الکترونیکی بیان می‌کند: «ذخیره، پردازش و یا توزیع داده پیامهای شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیامهای راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیر قانونی است». علاوه براین، مواد ۵۸ قانون تجارت الکترونیکی مصوب ۱۳۸۲، پردازش و ذخیره هرگونه داده پیام شخصی اشخاص را منوط به رضایت صریح و موردی دارنده، در محدوده اهداف مشخص تشریح داده شده به دارنده و به میزان متناسب با اهداف تعیین شده، نموده است. (عبداله زاده و حاجی پور کندرود، ۱۴۰۱: ۱۹۰-۱۶۸)

با اینحال، در حوزه حفاظت از داده‌های کاربر باید مشابه مقررات عمومی حفاظت داده‌ها در اروپا، قانونگذاری انجام شود. وزارت ارتباطات و فناوری اطلاعات در ایران باید لایحه حفاظت از داده‌های کاربران را تنظیم کند تا با تصویب دولت، به مجلس ارائه شود. البته باید به این نکته توجه داشت که لایحه مذکور باید با ادغام حفاظت از داده‌ها و آزادی اطلاعات، از عدم تقارن اطلاعاتی نامطلوب میان دولت و سایر افراد جلوگیری کند. معرفی سیستم‌های اینترنت‌اشیا یک پایگاه اطلاعاتی بی‌سابقه‌ای ایجاد می‌کند که اگرچه نوید تأثیر مثبت بر اثربخشی تصمیمات اداری را می‌دهد ولی قدرت اطلاعاتی جدید دولت، بر درک مردم از حکومت و قانون اساسی در عصر دیجیتال مؤثر است. این روند به معنای ایجاد عدم تقارن اطلاعاتی قابل توجه به نفع دولت است و افزایش امکانات اجرایی دولت از طریق پایگاه اطلاعاتی گسترده‌تر نیز می‌تواند تأثیرات شدیدی بر هنجارهای قانونی موجود داشته باشد. تحت این شرایط، باید توجه جدیدی به تساوی حقوق و تقارن اطلاعاتی در قانون‌گذاری داده شود. (قهرمانی و همکاران، ۱۴۰۱: ۲۱۳-۱۸۳)

این موضوع در قوانین دیگر مورد توجه قرار گرفته است. بر اساس قانون انتشار و دسترسی آزاد به اطلاعات مصوب بهمن ۱۳۸۷ «مؤسسات عمومی مکلفند اطلاعات موضوع این قانون را در حداقل زمان ممکن و بدون تبعیض در دسترسی مردم قرار دهند». در مقابل این تکلیف چنین حقی نیز برای شهروندان تدارک دیده شده است که «هر شخص ایرانی حق دسترسی به اطلاعات عمومی را دارد، مگر آن که قانون منع کرده باشد». در ماده ۵۹ قانون تجارت الکترونیک تاکید شده است که در ذخیره، پردازش و توزیع داده پیام‌های شخصی در بستر مبادلات الکترونیکی باید شخص موضوع داده پیام به

پرونده‌های رایانه‌ای حاوی داده پیامهای شخصی مربوط به خود دسترسی داشته و بتواند داده پیام‌هایی ناقص و یا نادرست را محو یا اصلاح کند.

یکی دیگر از چالش‌های جدی اینترنت اشیا، چالش‌های امنیت فناوری اطلاعات به دلیل نفوذ غیرمجاز در سیستم‌ها یا اشیا در ارتباط با هم و دادن دستوری خلاف واقع به آن‌ها یا عدم عملکرد صحیح آنهاست، که می‌تواند حتی گاهی خسارات غیرقابل جبرانی به بار آورد. اسناد مرجع در حوزه امنیت فناوری اطلاعات در ایران شامل سند تبیین الزامات[1] مصوب سال ۹۶ و سندی اجرایی تحت عنوان معماری و طرح کلان شبکه ملی اطلاعات مصوب سال ۹۹ است. در سند طرح کلان و معماری شبکه ملی اطلاعات که ۵۳ اقدام کلان تعریف شده است که حدود ۲۰ اقدام کاملاً امنیتی است و ۳۳ اقدام باقی مانده نیز که کاملاً امنیتی نیستند نیازمند طراحی امنیتی هستند به این معنی که تمام پروژه‌ها باید طراحی امنیتی داشته باشد.

به نظر می‌رسد که حوزه امنیت در فناوری اطلاعات در ایران حوزه‌ای واگرا است. حداقل ۶ معاونت و اداره‌کل مختلف در وزارت ارتباطات و فناوری اطلاعات به نوعی مرتبط با حوزه امنیت هستند که هر کدام از این بخش‌ها برای خود پروژه مستقل انجام می‌دهند. این حوزه شامل معاونت امنیت سازمان فناوری اطلاعات، مرکز امنیت سامانه‌های صیانتی زیرساخت، اداره کل امنیت سیستم‌های ارتباطی سازمان تنظیم مقررات و ارتباطات رادیویی، کمیته پدافند غیرعامل، پژوهشکده امنیت پژوهشگاه ارتباطات و دستگاه‌های زیرمجموعه وزارت ارتباطات و فناوری اطلاعات، می‌شود که لازم است هماهنگی لازم صورت گیرد که در اقدامات خود با یکدیگر همگرا شوند.

٤. الزامات طراحی در بکارگیری اینترنت اشیا با نگاهی به حقوق آلمان

قانون نه تنها انگیزه‌ها و محدودیت‌هایی را برای بکارگیری اینترنت‌اشیاء در حکمرانی فراهم می‌کند، بلکه می‌تواند الزامی برای طراحی باشد. چنین طراحی ممکن است ضروری باشد زیرا خودکارسازی فرآیندهای اداری از لحاظ کیفی آنقدر جدید است که نیازمند مقررات جدید است. این الزام فقط در مورد طراحی قانونی فن‌آوری نیست، بلکه در مورد درک تأثیرات هدایت‌کننده قانون بر فناوری و استفاده از آن‌ها برای دستیابی به اهداف دولت است. (Schulz and Kevin 2016: 14) امکانات و نیازهای طراحی ناشی از این الزامات را می‌توان با نگاهی به ماده 35a قانون فرآیند اداری فدرال آلمان (VwVfG)[2] توضیح داد. (Djeffal 2017: 12)

---

۱. از سند تبیین الزامات به عنوان «قانون اساسی شبکه ملی اطلاعات» تعبیر می‌شود.

2. Verwaltungsverfahrensgesetz (VwVfG)

۱-٤. هدف تبادل نزدیکتر بین شهروندان و دولت

در ماده ۳۵ قانون فرآیند اداری فدرال (VwVfG)، که در ۱ ژانویه ۲۰۱۷ لازم الاجرا شد، برای اولین بار امکان صدور قوانین اداری را کاملاً به صورت خودکار تحت شرایطی ارائه می‌کند. پیش از آن، فقط مقرراتی برای کمک گرفتن از دستگاه‌های خودکار در اتخاذ تصمیمات اداری، وجود داشت[۱]. بدین ترتیب نه تنها قانون مالیات‌های عمومی[۲]، بلکه رویه اداری عمومی و قانون آیین دادرسی اداره اجتماعی نیز در آلمان با تغییراتی مواجه شد.

بخش 35a از قانون فرآیند اداری فدرال (VwVfG) به عنوان یک قاعده کلی نیاز به تفسیر بیشتری دارد و هدف از این ماده به ویژه با توجه به تاریخچه پیدایش آن مشخص می‌شود. با توجه به توسعه موازی رویه‌ها، از اهداف خودکارسازی فرآیندهای اداره مالیات در آن استفاده شده است و علاوه بر مزایایی مانند کارایی و سرعت رویه، بر هدف دیگری نیز تأکید شده است. براساس این هدف، رویه خودکارسازی نباید به «کیفیت کمتر تصمیم‌گیری» منجر شود و منابع انسانی باید بر مواردی که واقعاً ضروری هستند متمرکز شود. بنابراین خطر ذاتی خودکارسازی، یعنی از دست دادن رابطه شخصی بین مرجع و مخاطب، نه تنها حذف بلکه حتی معکوس می‌شود.

خودکارسازی می‌تواند وعده شهروندمداری را که با دیجیتالی شدن دولت در قانون مدیریت خدمات کشوری ایران مرتبط شده است، جبران کند. (کاظمی و هداوند، ۱۳۹۲: ۹۳-۶۳) خودکارسازی می‌تواند به تماس انسانی با معنای بیشتر منجر شود؛ زیرا یک تصمیم انسانی تنها زمانی بهتر است که فرد تصمیم‌گیرنده زمان کافی و منابع حرفه‌ای را در اختیار داشته باشد. خودکارسازی از یک سو و شهروند مداری و انسانیت از سوی دیگر در تضاد با یکدیگر نیستند. این جنبه از هدف قانون در اینجا به عنوان انسانی‌سازی فرآیند توسط خودکارسازی نامیده می‌شود. بنابراین، این دیدگاه بخشی از طرز تفکری است که استفاده از فناوری را تشویق می‌کند که امکان تبادل نزدیکتر بین شهروندان و دولت را فراهم می‌کند. نه تنها اینترنت، بلکه اینترنت‌اشیا نیز به‌عنوان چشم‌اندازی برای افزایش خودکارسازی، می‌تواند در این دیدگاه از اهمیت اساسی برخوردار باشد، زیرا می‌توان از منابع جدید موجود برای جدی‌تر گرفتن نگرانی‌های شهروندان استفاده کرد.

---

۱. به‌عنوان مثال به مورد ۴ از بند ۲ ماده ۲۸، بند ۴ از ماده ۳۷ و مورد ۳ از بند ۲ ماده ۳۹ قانون فرآیند اداری فدرال و همچنین مقررات خاصی مانند بخش 6a قانون فدرال حفاظت از داده‌ها و ماده ۲۲ مقررات عمومی حفاظت از داده‌ها مراجعه شود.

2. Abgabenordnung

۲-٤. الزام انطباق رویه‌های اداری خودکار با قانون

براساس بخش 35a از قانون فرآیند اداری فدرال (VwVfG) اولین شرط برای مجاز دانستن انجام اقدام اداری توسط یک فرآیند کاملاً خودکار، وجود یک ماده قانونی در آن خصوص است. الزام وجود ماده قانونی مستلزم برنامه‌ریزی اولیه برای اطمینان از انطباق رویه‌های اداری خودکار با قانون است. مفهوم قانونگذاری هم قوانین و هم سایر مقررات حقوقی را در بر می‌گیرد. بنا به انواع دلایل حقوقی در سطوح مختلف، فرض بر این است که بر اساس ارزیابی فناوری، قانونگذار باید رویه را به گونه‌ای طراحی کند که حقوق رویه‌ای مخاطب رعایت شود. (Harlow and Richard, 2019: 10) این امر از آثار رویه‌ای حقوق بنیادی ناشی می‌شود که براساس آن حقوق بنیادی بر سازمان و رویه‌ها، به‌ویژه بر رویه‌های اداری تأثیر می‌گذارد. از این مفهوم در آلمان، یک «الزام قانون اساسی» نتیجه شده است که براساس آن «یک رویه یا شکل سازمانی خاص» می‌تواند توسط اشخاص مورد تقاضا قرار گیرد. در خصوص نحوه تغییر رویه، می‌توان بند ۴ ماده ۱۵۵ قانون عمومی مالیات[1] در آلمان را مثال زد. احکام مالیاتی مشخص تا آنجا که «دلیلی برای رسیدگی به پرونده فردی توسط مقامات انسانی وجود ندارد» می‌تواند به طور خودکار صادر شود. موارد ممکن دیگر از تغییر رویه و خودکارسازی را می‌توان از مفاد مقررات عمومی حفاظت از داده‌ها (GDRP) استخراج کرد که به عنوان مثال، ادعای مداخله مستقیم توسط یک شخص یا اعتراض به یک تصمیم در آن ذکر شده است. این بدان معناست که هم رویه فردی و هم جنبه‌های نهادی و سازمانی باید در نظر گرفته شود.

امکان بازگرداندن مسئولیت تصمیم گیری به مدیر انسانی (به جای تصمیمات خودکار)، اگر شخص مربوطه چنین درخواستی داشته باشد، از طریق مقررات رویه‌ای وجود دارد. (Nagtegaal, 2021: 14) با این حال، انتقال رویه به تصمیم انسانی ممکن است به دلیل تنظیمات فنی سیستم‌های خودکار یا به جهت رسیدگی به اعتراض، مانند مورد بند ۴ ماده ۱۵۵ قانون عمومی مالیات آلمان آغاز شود. از نقطه نظر نهادی و سازمانی، در اختیار داشتن متخصصین مناسب در مراجع مختلف از اهمیت بالایی برخوردار است. به ویژه، زمانی که الگوریتم‌های پیچیده تصمیم‌گیری می‌کنند، تضمین شفافیت و قابلیت ردیابی این تصمیمات بسیار دشوار و از اهمیت ویژه‌ای برخوردار است.

۳-٤. عدم وجود رویه حاشیه مجاز تفسیر

شرط دوم بخش 35a از قانون فرآیند اداری فدرال (VwVfG) برای مجاز دانستن انجام اقدام اداری توسط یک فرآیند کاملاً خودکار، این است که هیچ حاشیه‌ی مجاز تفسیری[2] در رویه آن وجود نداشته

1. Abgabenordnung
2. Margin of appreciation

باشد. بدین ترتیب موارد محدودی که حاشیه‌های مجاز تفسیر در هر صورت در آنها وجود دارند، از تصمیم‌گیری خودکار باید حذف شوند. در رویه حاشیه‌ی مجاز تفسیر، هدف آن است که تفاوتهای میان اشخاص ناگزیر پذیرفته شود و به ابزارهای مناسب برای مهار تمایلات به سوی همگونی شدید و همسانی مطلق تصمیمات اداری دست یافت. پیش فرض عدم وجود حاشیه مجاز تفسیر در قانون فرآیند اداری فدرال آلمان را می‌توان به صورت انتزاعی یا غیرانتزاعی تفسیر کرد.

اگر این ماده به صورت انتزاعی تفسیر شود، در صورتی که مبنای حقوقی یک فرآیند اداری، حاشیه مجاز تفسیر را اعطا کند، نمی‌توان تصمیم کاملاً خودکار بدون عامل انسانی را در نظر گرفت. به طور مشخص می‌توان بررسی کرد که آیا جایی برای حاشیه مجاز تفسیر در فرآیند اداری موردنظر وجود دارد یا خیر. اگر قبلاً در این فرآیند از آن استفاده شده بود، تصمیم خودکار منتفی است و اعمال حاشیه مجاز تفسیر در این شرایط موردنظر است. استدلال قوی برای دیدگاه انتزاعی این است که قانونگذار بر لزوم تصمیم‌گیری انسانی تأکید کرده است. این با دیدگاهی که از گذشته تثبیت شده است، مطابقت دارد که اصولاً در صورتی که مبنای حقوقی فرآیند اداری، حاشیه مجاز تفسیر را داشته باشد، مانع از پذیرش اقدامات اداری توسط دستگاه‌های خودکار می‌شود. بااینحال، به صورت استثناء، قانون 31a از کتاب نهم قانون تأمین اجتماعی[1] در آلمان نشان می‌دهد که سیستم حقوقی در حالت کلی تصمیمات خودکار را رد نمی‌کند. در این قانون فرض بر این است که لازم نیست هر تصمیمی بر اساس مفهوم حاشیه مجاز تفسیر، توسط شخص اتخاذ شود. زیرا منطق این قانون نشان می‌دهد که خودکارسازی دقیقاً انسانی کردن فرآیند است و در صورت تخصیص بهتر منابع می‌تواند منجر به عدالت بیشتر شود. این مورد در واقع یکی از دلایل اصلی نوسازی و خودکارسازی رویه‌های مالیاتی در آلمان است. اگرچه یک سازمان باید مجاز باشد که فقط اقدامات خاصی را بدون استفاده از حاشیه مجاز تفسیر، از پیش برنامه ریزی و تحریر کند. بااینحال باید توجه داشت، اعمال حاشیه مجاز تفسیر به صورت از پیش برنامه‌ریزی‌شده، اساساً غیرقانونی نیست، یک مرجع می‌تواند با اعمال حاشیه مجاز تفسیر توسط دستورالعمل‌های تحریرشده، در خصوص برخی اقدامات تصمیم گیری کند.

تفسیر غیرانتزاعی فوق از بخش 35a از قانون فرآیند اداری فدرال (VwVfG) مانع از این می‌شود که برنامه‌های خودکار کاربردی قبلاً اجرا شده، غیرقانونی یا بر اساس یک مبنای قانونی متفاوت قلمداد شوند و یا از پیشرفت‌های آینده منع شوند. این دیدگاه را می‌توان به ویژه با سیستم‌های کنترل ترافیک که قبلاً ذکر شد نشان داد. این موارد ممکن است به عنوان احکام عمومی صادر شوند که طبق ماده قانون ترافیک جاده‌ای[2] تصمیمات اختیاری بر اساس ابزار خودکار از پیش برنامه‌ریزی شده هستند.

1. Sozialgesetzbuch IX
2. Straßenverkehrsordnung

امکان اعمال خودکار حاشیه مجاز تفسیر، توسعه و نوآوری در قانون رویه اداری آلمان و به عنوان مثال بهره‌مندی از مزایای تجزیه و تحلیل خودکار کلان داده را میسر می‌کند. در مواجهه با نوآوری‌های فنی، مانند یادگیری ماشین و الگوریتم‌های خودآموز، مفاهیم سنتی خودکارسازی ممکن است به زودی منسوخ شوند. به خصوص در مورد تصمیمات پیچیده اداری با پارامترهای مختلف، اهداف موردنظر از اعمال حاشیه مجاز تفسیر می‌توانند با استفاده از روش خودکار بهتر از تصمیم انسانی به دست آیند. به دلایل فوق، به طور کلی پیشنهاد شده است که اعمال حاشیه مجاز تفسیر خودکار ممنوع نشود، بلکه آن در محدوده حاکمیت قانون رها شود. بدین ترتیب، اداره ممکن است حاشیه مجاز تفسیر خود را از طریق ابزار خودکار و طراحی برنامه‌های کاربردی اینترنت‌اشیا اعمال کند.

۵. ایجاد تغییرات بالقوه در قوانین اداری و حکمرانی جدید با اینترنت اشیا

معرفی رویه‌های خودکار از طریق اینترنت اشیا به صورت بالقوه می‌تواند تغییرات اساسی در قوانین اداری ایجاد کند. در ادامه، پنج نظریه در این خصوص براساس آنچه قبلاً گفته شد، ارائه می‌شود.

۵-۱. تغییر نقش‌ها برای انسان‌ها و ادارات عمومی

استفاده گسترده از اینترنت‌اشیا توسط دولت به معنای تغییر اساسی است، زیرا اطلاعات به صورت خودکار جمع‌آوری می‌شود، تصمیمات می‌توانند به طور خودکار اتخاذ شوند و اقدامات می‌توانند به طور خودکار انجام شوند. بدین ترتیب، اقدامات اداری در هر سه سطح در حال تغییر هستند. بنابراین، اینترنت‌اشیا این پتانسیل را دارد که یک تغییر ساختاری در فرایند اداری را ایجاد کند. اجرای امور اداری دیگر موضوع بوروکراسی‌ای نخواهد بود که بر مردم تحمیل شود و اعمال انسانی بر برنامه‌ریزی از قبل و پیگیری تصمیمات حیاتی متمرکز است. اگر قبلاً به اشیا مأموریت نسبت داده می‌شد، این مأموریت نه تنها از طریق اینترنت‌اشیا بدیهی و قابل درک است، بلکه پشت چنین ماموریتی اقتدار حکمرانی وجود دارد. خودکار شدن اجرای قانون روز به روز امکان‌پذیرتر می‌شود و همه این‌ها عملکرد و معنای اداره را تغییر می‌دهد.

۵-۲. فرصت قانونگذاری مشارکتی

اگر با بهره‌مندی از فناوری اینترنت اشیا، اقدامات تا حد زیادی از پیش تعیین شده باشند، در موقعیت‌های عملی غیرانتزاعی و عینی، تصمیم‌گیری دیگر بر عهده یک مأمور انسانی نیست. مشارکت انسانی به ویژه بر فرآیند مقدماتی برنامه‌ریزی و پیاده سازی سیستم، یعنی «تصمیم اولیه» متمرکز می‌شود. این تصمیم اولیه در واقع قانون را اجرا می‌کند، اما علاوه بر آن یک مؤلفه قانونگذاری را نیز در بر می‌گیرد. بدین ترتیب، در روند پیاده سازی مؤلفه‌های خود، فرصت‌ها و همچنین ضرورت‌هایی برای مشارکت سایر عاملان در قانون‌گذاری وجود دارد.

۳-۵. تغییرات در روند و ساختار اداری

خودکارسازی همچنین تقاضاهای خاصی را برای فرآیند اداری ایجاد می‌کند. بخش 35a از قانون فرآیند اداری فدرال آلمان (VwVfG) به مقررات خاصی اشاره دارد که باید توسط قانونگذار وضع شود. این مورد، در خصوص معرفی گسترده برنامه‌های کاربردی اینترنت‌اشیا، می‌تواند منجر به رشد مقررات شود. قانونگذار باید در مورد انطباق رویه اداری و به ویژه تعمیم نهادها و اصول تأمل کند. علاوه بر این، سؤالاتی در مورد چگونگی سازگاری ساختارهای رشد یافته، از نقش مقامات رسمی تا ساختار دولت‌ها (در کشورهای بکارگیرنده فناوری اینترنت اشیا)، مطرح خواهد شد. (Corvalán, 2018: 55-87) ایجاد دانش تخصصی برای دولت‌ها و همچنین در دسترس قرار دادن آن برای عموم چالش برانگیز خواهد بود و در این صورت باید یک مرجع مستقل صالح برای این منظور در نظر گرفته شود.

٤-۵. هدایت منابع انسانی به جهات موردنیاز

چشم‌انداز اینترنت‌اشیا چشم‌اندازی از خودکارسازی است که در آن رایانه‌ها در همه جا حضور دارند و به محیط شبکه متصل می‌شوند. چنین سیستم‌هایی فرصت‌هایی را ایجاد می‌کنند، اما موارد استفاده از آن‌ها را مشخص نمی‌کنند. در یک سیستم خودکار که عمدتاً اشیا در آن عمل می‌کنند، ممکن است به نظر رسد که این امر منجر به افزایش فاصله بین دولت و شهروند می‌شود. با این حال، خودکارسازی قوانین در زمینه رویه‌های مالیاتی نشان می‌دهد که نه تنها اینطور نیست، بلکه خودکارسازی می‌تواند منجر به آزادسازی منابع انسانی و هدایت آن‌ها به جایی که واقعاً مورد نیاز است شود. وقتی برنامه‌های اینترنت‌اشیا با این هدف پیاده‌سازی می‌شوند، دیگر تنها موضوع انتقال از اینترنت رایانه‌ها به اینترنت‌اشیا نیست، بلکه انتقال از یک ماشین اداری مبتنی بر افراد به یک اداره انسانی مبتنی بر ماشین‌ها است. بدین ترتیب ترکیب انسان و ماشین عمل کارآمد و فراتر از اقدام انسانی را تضمین می‌کند. وعده‌های اثربخشی و کارایی، در این زمینه، از پتانسیل‌های پیشرفت فناوری برای تأثیرگذاری مثبت بر روابط بین شهروندان و دولتشان با ایجاد کیفیت جدیدی در ارتباطات استفاده می‌کنند. بدین ترتیب، این هدف انسانی را باید با شکل دادن فعالانه به خودکارسازی ادارات دولتی جستجو کرد.

نتیجه گیری و پیشنهادات

اینترنت اشیا فناوری نوظهوری است که در آینده نزدیک به سرعت، سازمان‌ها و سیستم‌های ارتباطی را احاطه خواهد کرد. این فناوری با برقراری ارتباط بین اشیا متفاوت، بدون دخالت انسان به انجام فعالیت می‌پردازد. این اشیا اطلاعات خود را به اشتراک خواهند گذاشت و در پی این تعامل، شبکه‌ای از اشیا متصل به هم به وجود خواهد آمد. خدمات و اپلیکیشن‌های اینترنت اشیا می‌تواند با کارآمدتر کردن، امن‌تر کردن و هوشمندتر کردن جامعه مزایای اجتماعی زیادی داشته باشد؛ اما این مزایا هنوز هم در برخی از کشورهای جهان غالباً با چارچوب‌های حقوقی و مقررات گذاری مسدود شده است. بدین ترتیب نیاز است که یک نگاه تعادلی بین مزایای توسعه این فناوری جدید و خطرات متصور و مسائل بالقوه آن حاصل شود.

الزامات طراحی سامانه‌های عینی مبتنی بر اینترنت اشیا در راستای حکمرانی هوشمند باید شامل تحقق هدف تعامل نزدیکتر بین شهروندان و دولت، الزام انطباق با قانون در رویه‌های اداری که خودکارسازی با استفاده از اینترنت اشیا را در بردارند و برقراری شرط عدم وجود حاشیه مجاز تفسیر در رویه اداری باشند. از سوی دیگر حفاظت از داده‌ها، حریم خصوصی و امنیت از ابعاد مهم بکارگیری اینترنت اشیا به حساب می‌آیند که باید تضمین شوند تا پذیرش حداکثری آن در جامعه حاصل شود.

در حوزه حفاظت از داده‌های کاربر باید مشابه مقررات عمومی حفاظت داده‌ها در اروپا، قانونگذاری انجام شود. وزارت ارتباطات و فناوری اطلاعات در ایران باید بر لایحه حفاظت از داده‌های کاربران، پیشنهادات و اصلاحات لازم را اعمال کند تا با تصویب دولت، به مجلس ارائه شود. با اینحال در تدوین لایحه باید دقت شود که با ادغام حفاظت از داده‌ها و آزادی اطلاعات، از عدم تقارن اطلاعاتی نامطلوب میان دولت و سایرین جلوگیری شود.

عدم نقض حریم خصوصی افراد، یکی از چالش‌های بکارگیری فناور اطلاعات است که در این راستا ابتدا باید دایره حریم خصوصی و اطلاعات قابل شناسایی شخصی که در حقوق ایران، مفهوم تعریف نشده‌ای به حساب می‌آید، به خوبی تعریف شود. سپس برای ایجاد اعتماد و امنیت روانی در افراد جامعه، استانداردهای حریم خصوصی تعریف و در سطح بالایی مدنظر بقرار گیرد. در مورد انتشار اطلاعات خصوصی کاربران، کسب و کارها، و یا سازمان‌ها و شرکت‌ها که با افزایش شدت حملات سایبری روی می‌دهد، سازمان‌های متولی در زمان وقوع رخداد باید مسئولیت را برعهده بگیرند. زیرا مطابق با سند تقسیم کار مقابله با حوادث فضای مجازی (مصوب شورای عالی فضای مجازی)، مسئول نشت اطلاعات در هر سازمان و دستگاهی، بالاترین مقام همان سازمان است.

حوزه امنیت از سوی دیگر نیازمند صرف هزینه از سوی سازمان‌ها و مراکز برای ایمنی در برابر حملات سایبری است. باید توجه داشت صرفاً با خرید تجهیزات و نیروی انسانی و صدور دستور العمل، امنیت در یک سازمان تأمین نمی‌شود و باید فرهنگ امنیت در مجموعه و یا سازمان نهادینه شود. از سوی دیگر بودجه دولتی برای حوزه امنیت کم است و باید مدل کسب و کار حوزه امنیت در کشور اصلاح شود. با اینحال در کشور مرجعی وجود ندارد که محصولات حوزه امنیت را از نظر عملکرد ارزیابی کند. به همین دلیل، هر یک از سازمان‌ها، متفاوت از سازمان دیگر تضمین امنیت محصولات و تجهیزات حوزه امنیت را تأیید می‌کند.

در این راستا آئین نامه‌ای با کمک چندین نهاد از جمله وزارت ارتباطات و فناوری اطلاعات، سازمان ملی استاندارد و سازمان نظام صنفی رایانه‌ای به عنوان بخش خصوصی باید تدوین گردد تا امکان ارزیابی عملکرد محصولات و تجهیزات حوزه امنیت فراهم شود و رویه‌ای را نتیجه دهد که همه سازمان‌ها مطابق آن عمل کنند. بدین ترتیب با تدوین این آئین نامه تمامی گواهینامه‌های حوزه امنیت در سازمان‌ها یکپارچه خواهد شد.

فهرست منابع

الف. فارسی

آقایی طوق، مسلم، ناصر، مهدی (۱۳۹۹). «چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا»، فصلنامه علمی پژوهشی حقوق اداری، شماره ۲۳، ص ۳۳-۵۵

اقدسی، فاطمه، محقق داماد، مریم السادات (۱۴۰۰). «ابعاد حقوقی حریم خصوصی در اینترنت اشیا»، نشریه پژوهش‌های حقوقی میان رشته‌ای، شماره ۶، ص ۵۰-۶۷

پورعزت، علی‌اصغر، رفیعی، سیاوش، مومن‌زاده، پریا، کوکلان، نیلوفر (۱۳۹۸). «بازگشت عقلانیت؛ کاربست هوش مصنوعی در حکمرانی و خط‌مشی‌گذاری عمومی». مطالعات و پژوهش‌های اداری، شماره ۳، ص ۸-۱۸.

شهریاری، حمید (۱۳۹۷). «اینترنت اشیا؛ چیستی و کارکردها در حوزه حاکمیت»، نشریه ره‌آورد نور، شماره ۶۴، ص ۲-۱۱

صادقی، حسین، ناصر، مهدی (۱۳۹۹). «ارائه چارچوب حقوقی مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا در بستر دولت الکترونیک، تبیین الگوی سیاستگذاری مؤثر»، فصلنامه سیاستگذاری عمومی، شماره ۵، ص ۸۱-۱۰۳

طاهری، علی، خاکپور، سارا (۱۳۹۹). «تأملی بر چیستی و چرایی ظهور حقوق اداری نوین»، پژوهش‌های نوین حقوق اداری، شماره ۳، ۱۴۵-۱۶۴

عبداله زاده، انس، حاجی پور کندرود، علی (۱۴۰۱). «تحلیل چالش‌های دولت الکترونیک با حریم خصوصی اطلاعاتی شهروندان». فصلنامه علمی پژوهشی حقوق اداری، دوره ۹، شماره ۳۱، ص ۱۶۸-۱۹۰

قهرمانی، غفور، شریف شاهی، محمد، احمدی، سید محمد صادق (۱۴۰۱). «اعلام، طبقه‌بندی و خروج از محرمانگی اسناد اداری در پرتو حق دسترسی به اطلاعات در نظام حقوقی ایران و ایالات متحده امریکا». پژوهش حقوق عمومی، شماره ۷۶، ص ۱۸۳-۲۱۳

کاظمی، داود، هداوند، مهدی (۱۳۹۲). «تأملی بر اصول مدرن حقوق اداری در قانون مدیریت خدمات کشوری (تحلیل ماده ۹۰ قانون مدیریت خدمات کشوری». راهبرد، شماره ۶۷، ص ۶۳-۹۳

وکیل، امیرساعد، نوروزپور، حسام (۱۳۹۹). «حکمرانی چند ذینفعی اینترنت و حقوق بین الملل: مفاهیم رایج یا رویکردی نوین؟». پژوهش حقوق عمومی، شماره ۶۶، ص ۱۰۷-۱۴۰

ب. انگلیسی

Caruso, David, Michael Legg, and Jordan Phoustanis (2019). "The automation paradox in litigation: The inadequacy of procedure and evidence law to manage electronic evidence generated by the'internet of things' in civil disputes." Macquarie Law Journal 19, 157-188.

Chatfield, Akemi Takeoka, and Christopher G. Reddick (2019). "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government." Government Information Quarterly 36, no. 2, 346-357.

Corvalán, Juan Gustavo (2018). "Digital and intelligent public administration: transformations in the era of artificial intelligence." A&C-Revista de Direito Administrativo & Constitucional, 55-87.

Djeffal, Christian (2017). "Smart Government: Updating eGovernment with the IoT." AoIR Selected Papers of Internet Research.

Harlow, Carol, and Richard Rawlings (2019). "Proceduralism and automation: challenges to the values of administrative law." The Foundations and Future of Public Law (LSE Legal Studies Working Paper), 3.

Mulder, Trix, and Nynke E. Vellinga (2021). "Exploring data protection challenges of automated driving." Computer Law & Security Review 40, 105530.

Nagtegaal, Rosanna (2021). "The impact of using algorithms for managerial decisions on public employees' procedural justice." Government Information Quarterly 38, no. 1, 101536.

Schulz, Wolfgang, and Kevin Dankert (2016). "'Governance by things' as a challenge to regulation by law." Internet Policy Review 5, no. 2, 2017-01.

Srinivas, Jangirala, Ashok Kumar Das, and Neeraj Kumar (2019). "Government regulations in cyber security: Framework, standards and recommendations." Future generation computer systems 92, 178-188.