اینترنت اشیاء (۳): چارچوب مقرراتگذاری، امنیت سایبری و مقرراتگذاری داده در اینترنت اشیاء برای ایران

کد موضوعی: ۳۱۰
شماره مسلسل: ۱۷۰۱۲
اردیبهشت‌ماه ۱۳۹۹

معاونت پژوهش‌های زیربنایی و امور تولیدی
دفتر: مطالعات انرژی، صنعت و معدن

به‌نام خدا

فهرست مطالب

اینترنت اشیاء (۳): چارچوب مقرراتگذاری، امنیت سایبری و مقرراتگذاری داده در اینترنت اشیاء برای ایران

چکیده

یک موضوع کلیدی در مقررات اینترنت اشیا، بحث مقرراتگذاری درباره داده در اینترنت اشیاست. هدف از این گزارش ارائه چارچوب مقررات‌گذاری، امنیت سایبری و مقررات‌گذاری داده در اینترنت اشیا برای ایران است. براساس گزارش اتحادیه اروپا پیرامون قانون GDPR و اینترنت اشیا پنج موضوع مهم وجود دارد که سیاستگذاران باید بدان‌ها توجه داشته باشند: نقض امنیت، رضایت، حریم خصوصی توسط طراحی و حریم خصوصی به‌صورت پیش‌فرض، حقوق ارتقایافته درخصوص موضوع داده و پردازش داده‌های شخصی مربوط به کودکان. موضوع مهم دیگر درخصوص اینترنت اشیا، ملاحظات امنیت سایبری در اینترنت اشیاست. از مرور قوانین و مقررات در آسیا، اروپا و آمریکا، نتیجه گرفته می‌شود که چارچوب مقرراتگذاری در اینترنت اشیا برای ایران حداقل باید چهار بخش را پوشش دهد: نخست، نحوه اعمال قوانین به اینترنت اشیا. دوم، امنیت و حفاظت از داده و مصرف‌کننده برای حوزه‌هایی ازقبیل آزاد بودن جریان داده‌های غیرشخصی، امنیت سایبری، حفاظت از داده، امنیت شبکه و سیستم‌های اطلاعاتی، حقوق مصرف‌کننده، مسئولیت محصول. سوم، بی‌طرفانه بودن فناوری و اجتناب از برخی سیاست‌های بخش صنعت که طرفدار فناوری‌های غیرسلولی هستند و چهارم، مسئولیت و اتخاذ بهترین شیوه‌ها در رابطه با اشتراک داوطلبانه از داده‌های غیرشخصی تولید شده توسط دستگاه و تأکید قراردادی بر حل مسائل بالقوه پیرامون مسئولیت اینترنت اشیا که می‌تواند سبب تقویت رقابت‌پذیری در کشور و اعتماد کاربر نهایی در اینترنت اشیا شود.

مقدمه

امروزه با ظهور تحول دیجیتالی، جوامع و کسب‌وکارها با فرصت‌های عظیمی در جهت افزایش رفاه و بهبود اقتصاد مواجه شده‌اند. علت اصلی این امر پیدایش فناوری اینترنت اشیا به‌عنوان انقلاب صنعتی چهارم است. فناوری اینترنت اشیا با متصل کردن اشیا و اشخاص به شبکه سبب جمع‌آوری داده‌های آنها و سپس پردازش آنها می‌شود، به‌طوری‌که نتایج می‌توانند در جهت افزایش رفاه مردم و بهبود وضعیت

کسب‌وکارها به خدمت گرفته شوند. البته در پردازش داده‌های اینترنت اشیا فناوری‌های رایانش ابری و کلان داده بسیار حائز اهمیت هستند.

به‌کارگیری فناوری اینترنت اشیا می‌تواند سبب هوشمندسازی بخش‌های مختلف صنعت ازجمله: حمل‌ونقل، کشاورزی، بندر و گمرک، سلامت، نفت و گاز، برق، خرده‌فروشی، زنجیره تأمین، خودرو، محیط زیست، ساختمان هوشمند، کنتورهای هوشمند، شهر هوشمند و بسیاری از حوزه‌های دیگر شود. این هوشمندسازی می‌تواند از یک‌سو به کاهش هزینه‌ها به‌ویژه هزینه‌های لجستیکی منجر شود و ازسوی‌دیگر سبب افزایش بهره‌وری خواهد شد. علاوه‌براین، مجمع اقتصاد جهانی در تجزیه و تحلیل خود نشان داد که حدود ۸۴٪ از توسعه‌های اینترنت اشیا در حال حاضر مرتبط با اهداف توسعه پایدار سازمان ملل هستند یا به‌طور بالقوه به تحقق این اهداف در آینده منجرخواهند شد. درنتیجه این فناوری می‌تواند مزایای خوبی را در بخش‌های مختلف صنعت و اقتصاد فراهم کند.

ازاین‌رو، فناوری اینترنت اشیا را سیاستگذاران کشورهای مختلف مورد توجه قرار داده‌اند. سیاستگذاران در کشورهای متعدد در تلاش هستند تا با تدوین سیاست‌ها و مقررات بین‌بخشی در این حوزه فرصت‌هایی را برای کسب‌وکارها در جهت توسعه اقتصاد در محیطی رقابت‌پذیر فراهم آورند. سیاست‌ها و مقررات موجود جهانی به اندازه کافی با داده‌ها و ارتباطات اینترنت اشیا سازگار نیستند. بنابراین، سیاستگذاران در کشورهای مختلف نیاز دارند تا یک چارچوب مقرراتی مناسب برای اینترنت اشیا طراحی کنند تا علاوه بر کمک به رفاه شهروندان، فرصت‌های جدیدی برای افراد و کسب‌وکار ایجاد کنند تا به توسعه کشور منجر شود. این گزارش یک چارچوب مقرراتگذاری اینترنت اشیا را پیشنهاد می‌کند که می‌تواند در فرایندهای مقرراتگذاری اینترنت اشیا در کشور مفید واقع شود. بدین‌منظور ابتدا ملاحظات مقرراتگذاری پیرامون داده در اینترنت اشیا در آسیا، اروپا و آمریکا بررسی می‌شود. سپس موارد مهم در چارچوب مقرراتگذاری اینترنت اشیا در کشور توضیح داده می‌شود و در ادامه ملاحظات امنیت سایبری در اینترنت اشیا براساس استانداردهای اروپایی و تطبیق ملاحظات مربوط به اینترنت اشیا با قانون GDPR بحث خواهد شد. این گزارش با ارائه چارچوب پیشنهادی برای مقرراتگذاری اینترنت اشیا در کشور و جمع‌بندی یافته‌ها به پایان می‌رسد.

فصل اول ـ ملاحظات مقرراتگذاری پیرامون داده در اینترنت اشیا

۱-۱. مسائل مربوط به مقررات عمومی پیرامون داده

امروزه نه‌تنها اینترنت اشیا داده‌ها را جمع‌آوری می‌کنند بلکه بسیاری از پلتفرم‌های دیگر (مانند شبکه‌های اجتماعی) نیز داده‌ها را جمع‌آوری می‌کنند. در برخی مواقع داده‌های جمع‌آوری شده بدون اطلاع کاربران (یا کاربر به‌طور ساده‌لوحانه اجازه این کار را داده است تا بتواند در یک سرویس مشخص عضو شود) به

اشتراک گذاشته می‌شوند. داده‌ها ممکن است از این پلتفرم‌ها به سرقت بروند. ازاین‌رو، بسیاری از کشورهای جهان سعی دارند تا مقرراتی را برای حفاظت از داده‌های کاربران ایجاد کنند. البته بسیاری از کشورها هنوز درک دقیقی از این موضوع ندارند و هیچ مقررات مشخصی ندارند یا در برخی موارد از مقررات قدیمی برخوردارند که بسیار محدودکننده است. برخی از اصولی که در هنگامی‌که مقررات به قانون تبدیل می‌شوند و آنها منتشر می‌شوند باید رعایت شوند، عبارتند از: [۱]

- حفاظت داده در برابر داده‌های باز،
- نهاد مسئول برای حفاظت داده،
- چه‌کسی می‌تواند به داده‌های جمع‌آوری شده دسترسی داشته باشد؟،
- طبقه‌بندی و پردازش داده‌ها،
- رضایت صاحب داده وجود دارد یا خیر؟،
- جمع‌آوری و اشتراک‌گذاری داده ملی در مقابل بین‌المللی،
- محافظت از مصرف‌کننده.

ازاین‌رو، درخصوص اقدامات بالقوه رگولاتوری می‌توان به موارد زیر اشاره کرد: [۲]

- تشویق شرکت‌ها برای توسعه سازوکارهای جدید برای کسب رضایت آگاهانه از افراد مربوطه هنگام جمع‌آوری یا استنتاج از داده‌های حساس،
- استفاده بیشتر از ارزیابی اثرات حریم خصوصی توسط سازمان‌های تخصصی،
- تدوین و توسعه رهنمودها و دستورالعمل‌های بیشتر از رگولاتورهای حریم خصوصی جهانی در مورد استفاده از اصول حداقل رساندن داده،
- همکاری و تعامل بیشتر بین رگولاتورهای تلکام و رگولاتورهای دیگر ازقبیل نهادهای حفاظت از داده و حفظ حریم خصوصی.

درخصوص مقررات عمومی مربوط به داده لازم است تا مسائل مهمی مورد توجه قرار گرفته شود. مناطق مختلف و حتی کشورهای مختلف در همان منطقه به‌طور متفاوتی با مسائل مربوط به داده سروکار دارند. مشکل اصلی ناشی از این واقعیت است که بیشتر رگولاتورهای حوزه ارتباطات و فناوری اطلاعات از رگولاتوری بخش ارتباطات تکامل یافته‌اند. سرویس‌های ارتباطی، سرویس‌های دارای مجوز بوده و هستند؛ و رگولاتورها ازطریق شرایط مجوز مورد استفاده، محدودیت‌هایی را بر استفاده از داده مصرف‌کننده تحمیل می‌کنند. داده‌های اصلی مورد استفاده شامل ضبط جزئیات تماس (CDR[1]) و سوابق مشترکان بودند. شرکت‌های مخابراتی داده‌ها را در اختیار داشتند و تصور می‌شد که آن را ایمن

---

[1] Call Detail Record

نگه دارند. اگرچه، با افزایش دسترسی موبایل پهن‌باند، تلفن‌های هوشمند مجهز به یک گیرنده GPS[۱] شده‌اند و کاربردهای مختلف بسیاری از شرکت‌ها راه‌اندازی شدند که انواع مختلفی از خدمات را ارائه می‌دهند. این خدمات معمولاً خدمات OTT[۲] نامیده می‌شوند. این خدمات OTT میزان زیادی از داده‌های کاربران را جمع‌آوری می‌کنند که به نقض داده منجر می‌شود. برخی از کشورها یک نهاد جداگانه برای حفاظت از داده تأسیس کرده‌اند. رگولاتور فناوری اطلاعات و ارتباطات هنوز کنترل خود بر نحوه اشتراک‌گذاری داده‌ها را حفظ کرده است. ازاین‌رو، عمده‌ترین مسائل پیش‌رو به شرح زیر هستند:[۱]

○داده‌ها لازم است با چه کسی و چگونه (به‌عنوان نمونه: ناشناس ماندن) به اشتراک گذاشته شوند.

○چه نوع از داده‌ای باید در مرزهای جغرافیایی باقی بماند و چه داده‌ای می‌تواند در خارج از کشور ساکن شود.

امروزه، تولید داده توسط کاربران به‌شدت افزایش یافته است. این داده‌ها می‌توانند در فرایندهای تصمیم‌گیری پیرامون بسیاری از برنامه‌ها در هر دو بخش خصوصی و دولتی استفاده شوند. فناوری‌های جدید مانند اینترنت اشیا از این قابلیت برخوردارند که می‌توانند داده‌های بیشتری را در مقایسه با افراد تولید کنند. [۱]

فناوری‌هایی مانند رایانش ابری[۳]، نیاز به قرار دادن داده‌ها در نقاط مختلفی دارند که ممکن است خارج از مرزهای جغرافیایی یک کشور باشند. مقدار زیادی از داده‌ها تنها می‌توانند با تجزیه و تحلیل کلان داده[۴] به‌کار گرفته شوند که مجدداً نیازمند استفاده از رایانش ابری هستند. این تجزیه و تحلیل‌ها در هوش مصنوعی[۵] به‌شدت مورد استفاده قرار می‌گیرند. بنابراین، درخصوص اشتراک‌گذاری داده نیاز به مقررات محدودکننده حداقلی وجود دارد. [۱]

۲-۱. مقررات مربوط به داده در آسیا

مقررات مربوط به داده در آسیا به‌شرح زیر هستند: [۱]

- همان‌طورکه قبلاً نیز بدان اشاره شد، مقررات داده در یک منطقه نیز در مراحل مختلفی قرار دارد.
- به‌طور کلی، در کشورهایی که عملکرد خوبی در بخش فناوری اطلاعات و ارتباطات دارند، مقررات پیشرفته‌تر است. برای نمونه در سنگاپور، قانون اصلی مرتبط، قانون حفاظت از داده‌های شخصی وجود دارد که در سال ۲۰۱۲ صادر شده است و کاملاً جامع است و جنبه‌های مختلفی را پوشش می‌دهد. ازسوی‌دیگر، در کشور ویتنام هیچ قانونی برای مقرراتگذاری داده‌های حریم خصوصی مشخص نشده است.

---

2. Global Positioning System

۲. Over The Top

۳. Cloud Computing

۴. Big Data

۵. Artificial Intelligence

۳-۱. مقررات مربوط به داده در آمریکا

مقررات مربوط به داده‌ها در آمریکا به‌شرح زیر است: [۳]

- در ایالات متحده، حریم خصوصی و امنیت از داده‌های شخصی توسط طیف گسترده‌ای از قوانین فدرال و ایالتی اداره می‌شود.
- در بالاترین سطح، اصلاحیه چهارم قانون اساسی ایالات متحده، از حق افراد برای امنیت داشتن در خانه‌ها، اوراق، افراد و اثرات آنها در برابر جستجوهای غیرمنطقی و تصرفات حمایت می‌کند.
- در بخش رگولاتوری، چندین آژانس فدرال قوانین مختلف مربوط به حریم خصوصی متناسب با صنایع مشخص، یا استفاده از اطلاعات اعمال کرده‌اند.
- این قوانین شامل اطلاعات سلامت، اطلاعات مالی، سوابق آموزشی، اطلاعات کودکان و استفاده دولت از داده‌های شخصی می‌شود (اما به این موارد محدود نمی‌شوند).
- سازمان‌های رگولاتوری که وظیفه اجرای این موارد را دارند عبارتند از:
  - کمیسیون تجارت فدرال،
  - وزارت بهداشت و خدمات انسانی ایالات متحده،
  - دفتر حمایت مالی مصرف‌کنندگان،
  - کمیسیون ارتباطات فدرال.

همچنین در سطح ایالتی نیز دادستان‌های عمومی ایالتی وجود دارند که قوانین حریم خصوصی ایالتی را اعمال می‌کنند.

۴-۱. مقررات مربوط به داده در اروپا

یکی از مهم‌ترین ویژگی‌های اینترنت اشیا این است که این فناوری به‌طور ذاتی چندبخشی است. ازاین‌رو، طیف وسیعی از مقررات و ابتکارات سیاستگذاری متفاوت مرتبط با توسعه اینترنت اشیا در اتحادیه اروپا وجود دارد. این ابتکارات کلیدی را می‌توان به سه دسته گسترده تقسیم‌بندی کرد: قوانین مربوط به مقررات سرویس‌ها و شبکه‌های ارتباطات الکترونیکی، قوانین حفاظت از مصرف‌کننده و قوانین مخصوص صنعت. در ادامه هریک از این سه مورد بیان خواهند شد.[۴]

- مقررات مربوط به سرویس‌ها و شبکه‌های ارتباطات الکترونیکی:

مقررات مربوط به سرویس‌ها و شبکه‌های ارتباطات الکترونیکی در اروپا عبارتند از:[۴] کد ارتباطات الکترونیکی اروپا (EECC)[۱] (ادغام دستورالعمل دسترسی، دستورالعمل مجوزدهی، دستورالعمل چارچوب و دستورالعمل سرویس جهانی)، بی‌طرفی شبکه (بخشی از بسته قانونی قاره متصل)، مقررات

---

[۱] European Electronic Communications Code

رومینگ و دستورالعمل حریم خصوصی الکترونیکی.

- مقررات مخصوص صنعت:

درباره مقررات مخصوص صنایع مختلف می‌توان به موارد زیر اشاره کرد:[۴]

خودرو (به‌عنوان نمونه دستورالعمل سیستم‌های حمل‌ونقل هوشمند، مقررات تأیید نمونه، مقررات تماس الکترونیکی)، کشاورزی (سیاست کشاورزی مشترک)، انرژی (به‌عنوان نمونه دستورالعمل عملکرد انرژی ساختمان‌ها)، حمل‌ونقل هوایی (مقررات اساسی اتحادیه اروپا برای هواپیماهای بدون سرنشین) و سلامت (دستورالعمل دستگاه‌های پزشکی).

کمیسیون اروپا اقدامات فعال مختلفی را برای تسریع در جذب اینترنت اشیا و رونق بخشیدن به پتانسیل‌های آن در اروپا به نفع شهروندان و کسب‌وکارهای خود انجام داده است. یک تمرکز ویژه برای اطمینان از یک اکوسیستم پررونق اینترنت اشیا، یک نگرش اینترنت اشیا انسان‌محور و ایجاد یک بازار واحد برای اینترنت اشیا بوده است، مانند مسئولیت برای فناوری‌های دیجیتال درحال ظهور و اشتراک‌گذاری داده، قابلیت همکاری، استفاده و دسترسی به داده.[۴]

به‌عنوان نمونه، سند هیئت کاری کمیسیون اروپا در مورد مسئولیت، بر چالش‌های ناشی از اکوسیستم پیچیده از اپراتورهای بازار تأکید می‌کند که امکان ایجاد و عملکرد فناوری‌های دیجیتالی نوظهور را فراهم می‌آورد.[۵] همچنین، بر این موضوع تأکید شده است که موانع قراردادی با موضوع‌هایی که برای «کاربران داده» مهم‌تر از «تولیدکنندگان داده» است مانع اشتراک‌گذاری، دسترسی و استفاده از داده در اتحادیه اروپا می‌شود.[۶] علاوه‌براین، رهنمودی در مورد اشتراک‌گذاری داده بخش خصوصی در اقتصاد داده اروپا صادر شده است.[۷] گروه متخصص روی اشتراک‌گذاری داده‌های B2G[۱]، داده‌های غیرشخصی که می‌تواند شامل دستگاه‌های اینترنت اشیا باشند را نیز بررسی می‌کند.

- قانون و مقررات حفاظت از مصرف‌کننده:

قانون و مقررات مربوط به حفاظت از مصرف‌کننده در اروپا را می‌توان به‌صورت زیر برشمرد: مقررات آزاد بودن جریان داده‌های غیرشخصی، قانون امنیت سایبری، قانون GDPR، دستورالعمل کالاهای ملموس[۲]، دستورالعمل امنیت شبکه و سیستم‌های اطلاعاتی، دستورالعمل حقوق مصرف‌کننده، دستورالعمل مسئولیت محصول و دستورالعمل شیوه‌های تجاری ناعادلانه.[۴]

قانون GDPR انتظار دارد که:[۱]

- ○ از حقوق افراد به‌طور مؤثرتر در سراسر قاره محافظت شود.
- ○ ثبات تفسیر از قوانین جدید تضمین شود.

---

[۱] Business-to-Government

[۲] Tangible Goods Directive

○ در موارد بین‌کشوری که چندین اداره حفاظت از داده ملی درگیر می‌شوند، یک تصمیم نظارتی واحد اتخاذ شود.

در رابطه با نگرش کفایت در قانون GDPR باید بدین موضوع اشاره کرد که نگرش «کفایت» (که گاهی اوقات به‌عنوان یک نگرش لیست سفید شناخته می‌شود) تشخیص می‌دهد که آیا کل قلمرو هدف یک میزان کافی از حفاظت برای انتقال داده‌های شخصی را فراهم می‌کند یا خیر. این نگرش توسط کشورهای مختلف ازجمله اعضای اتحادیه اروپا، ژاپن و سوئیس استفاده می‌شود.[۱]

درخصوص بحث داده بین اتحادیه اروپا و ایالات متحده چندین موضوع حائز اهمیت است:[۸] اتحادیه اروپا و ایالات متحده در رابطه با یک توافق حفاظت از داده بین‌مرزی دیرینه مجدداً مذاکره کرده‌اند. این توافقنامه که پیش از این، چارچوب بندرگاه ایمن اتحادیه اروپا-آمریکا نامیده می‌شد، اکنون به‌عنوان سپر حریم خصوصی اتحادیه اروپا-آمریکا شناخته می‌شود. چارچوب سپر حریم خصوصی اتحادیه اروپا-ایالات متحده توسط وزارت بازرگانی و تجارت آمریکا و کمیسیون اروپا طراحی شده است. با این هدف که سازوکاری برای موافقت با الزامات محافظت از داده برای شرکت‌های دو طرف اقیانوس اطلس در هنگام انتقال داده‌های شخصی از اتحادیه اروپا به ایالات متحده برای پشتیبانی از تجارت فراتر از اقیانوس اطلس فراهم شود.[۸]

۵-۱. قانون GDPR و اینترنت اشیا

قوانین حفاظت از داده و مقررات داده به‌طور ویژه به اینترنت اشیا مربوط می‌شوند. به‌طورکلی، همه مقررات عمومی حفاظت از داده همچنین به اینترنت اشیا نیز اعمال می‌شوند. البته ممکن است الزامات اضافی برای اینترنت اشیا وجود داشته باشد. مسائل مربوط به حفاظت از داده‌های ناشی از اینترنت اشیا به‌صورت یک نظریه از بند ۲۹ کارگروه حفاظت از داده که در سال ۲۰۱۴ صادر شده است، درنظر گرفته شده است. این حفاظت از داده‌های مربوط به اینترنت اشیا به‌دلیل پتانسیل بسیار زیاد آن و این حقیقت که این می‌تواند داده‌های زیادی را تولید کند، درنظر گرفته شده بود. این موضوع، نگرانی ایجاد کرده است که گسترش اینترنت اشیا می‌تواند حفاظت از داده‌های قابل توجه و خطرات و چالش‌های حریم خصوصی شخصی را ایجاد کند.[۹]

ازاین‌رو، براساس گزارش اتحادیه اروپا پیرامون قانون GDPR و اینترنت اشیا پنج موضوع مهم که باید بدان‌ها توجه داشت عبارتند از:[۹]

۱-۵-۱. نقض امنیت

یکی از اصلی‌ترین نگرانی‌های مربوط به حریم خصوصی که در دستگاه‌های اینترنت اشیا بیان شده است، این است که آنها اهدافی را برای هکرها فراهم می‌کنند و مستعد نقض امنیت هستند.

قانون GDPR درصورت نقض داده‌های شخصی، یک روش اطلاع‌دهی اجباری را معرفی می‌کند.

کنترل‌کنندگان داده موظفند تا نقض داده شخصی را به مرجع نظارتی خود حداکثر ۷۲ ساعت پس از آگاهی از این تخلف گزارش دهند. در برخی موارد، از آنها خواسته می‌شود تا این تخلفات را به افراد تحت تأثیر گزارش دهند. کنترل‌کننده‌های داده برای استفاده از اینترنت اشیا باید اطمینان حاصل کنند که آنها در موقعیتی هستند که بتوانند نقض امنیت را شناسایی کنند و واکنش نشان دهند، به‌طوری‌که مطابق با الزامات GDPR باشد.

۲-۵-۱. رضایت

تردیدهایی در مورد توانایی دستگاه‌های اینترنت اشیا، حتی تحت رژیم موجود حفاظت از داده اتحادیه اروپا برای فراهم کردن رضایت با کیفیت کافی از کاربران چنین دستگاه‌هایی در رابطه با فعالیت‌های پردازش داده ابراز شده است.

قانون GDPR از الزاماتی در خصوص موضوع رضایت داده برخوردار است، بنابراین نیاز دارد تا کنترل‌کنندگان داده نشان دهند که در روشی به‌صورت شفاف، آزادانه، مشخص، آگاهانه و بدون ابهام رضایت گرفته شده است، به‌طوری‌که این رضایت، توافق موضوع داده برای پردازش داده شخصی کاربر را نشان می‌دهد.

۳-۵-۱. حریم خصوصی توسط طراحی و حریم خصوصی به‌صورت پیش‌فرض

حریم خصوصی توسط طراحی و حریم خصوصی به‌صورت پیش‌فرض مفاهیمی هستند که در قوانین فعلی حفاظت از داده در GDPR وجود دارند. این امر تعهداتی را به کنترل‌کنندگان داده تحمیل می‌کند تا اقدامات فنی و سازمانی قابل توجه جدیدی را اتخاذ کنند تا انطباق خود با الزامات GDPR را نشان دهند. این موارد ممکن است شامل انجام ارزیابی تأثیر حفاظت از داده‌ها در شرایط خاص باشد، به‌طوری‌که احتمالاً درخصوص سیستم‌های اینترنت اشیا به‌وجود می‌آیند.

۴-۵-۱. حقوق ارتقا یافته درخصوص موضوع داده

قانون GDPR حقوق ذاتی جدیدی به موضوع‌های داده در رابطه با داده‌های شخصی آنها می‌دهد. این حقوق ذاتی شامل یک حق صریح برای فراموشی، حقوق قابلیت حمل داده و حق اعتراض به تصمیم‌گیری خودکار است.

در طراحی دستگاه‌ها، برنامه‌های کاربردی و سیستم‌های اینترنت اشیا باید بررسی شود که آیا قابلیت‌های لازم برای تسهیل استفاده از حقوق موضوع داده به‌ویژه درخصوص قابلیت حمل داده، مطابق با GDPR ساخته شده است یا خیر.

۵-۵-۱. پردازش داده‌های شخصی مربوط به کودکان

مطابق با قانون GDPR، برای کودکان زیر ۱۳ سال امکان‌پذیر نیست تا آنها خودشان به پردازش داده‌های شخصی درخصوص سرویس‌های آنلاین رضایت دهند. برای کودکان بین سن‌های ۱۳ تا ۱۵ سال، این وضعیت به قانونگذاری در هریک از کشورهای عضو بستگی دارد. البته وضعیت پیش‌فرض این است که کودکان درون این سن نتوانند از طرف خود، به خود رضایت دهند.

این مقررات چالش‌هایی را برای کسانی ایجاد می‌کند که قصد دارند تا دستگاه‌های اینترنت اشیا مورد استفاده برای کودکان را وارد بازار کنند، هم درخصوص امکان معرفی سازوکارهای رضایت والدین به دستگاه‌ها، و هم توانایی برای بازار چنین دستگاه‌هایی در سطح اتحادیه اروپا، بر این اساس قانون مرتبط با کودکان بین ۱۳ تا ۱۵ سال ممکن است در سراسر تمام کشورهای عضو یکنواخت نباشد.

فصل دوم ـ موارد مهم در چارچوب مقرراتگذاری اینترنت اشیا در کشور

۲-۱. مقدمه

اگرچه تحول دیجیتالی[1] سبب پیشرفت سریع جوامع و اقتصادها شده است، همچنین دریچه‌ای از فرصت‌ها را برای کشورها گشوده است تا بتوانند در این حوزه در جهان پیشتاز شوند و حرفی برای گفتن داشته باشند. علت اصلی این فرصت‌ها رشد فناوری اینترنت اشیا است که یک پیوند اساسی بین اقتصاد داده و اقتصاد فیزیکی فراهم می‌آورد. فناوری اینترنت اشیا با متصل کردن هر شیء و هر شخص به شبکه، بنیان جوامع دیجیتالی و همچنین رقابت‌های آتی برای کشورهای مختلف محسوب می‌شود.[۴]

اینترنت اشیا با توجه به نقش تعیین‌کننده‌ای که می‌تواند در پرداختن به چالش‌های اجتماعی و اقتصادی داشته باشد، به‌سرعت در دستور کار سیاستگذاران کشورهای مختلف در سراسر جهان قرار گرفته است. به‌عنوان نمونه، فناوری اینترنت اشیا می‌تواند شرایط محیط زیست را بهبود بخشد و از تبدیل انرژی پشتیبانی کند. همچنین این فناوری می‌تواند مراقبت پیشگیرانه از سلامت افراد را ایجاد کند، محصولات کشاورزی را افزایش دهد درحالی‌که مصرف آب را کاهش می‌دهد و استفاده هوشمندانه از کودها را فراهم آورد. علاوه‌براین، فناوری اینترنت اشیا می‌تواند به برنامه‌ریزی مؤثر در حمل‌ونقل عمومی کمک شایانی کند، و با ارائه راهکارهای هوشمند، ترافیک را بهبود بخشد و منجر به کاهش آلودگی هوا شود. درحقیقت، یک تجزیه و تحلیل توسط مجمع اقتصاد جهانی[2] نشان داده است که حدود ۸۴٪ از توسعه‌های اینترنت اشیا درحال حاضر مرتبط با اهداف توسعه پایدار سازمان ملل هستند یا به‌طور بالقوه منجر به تحقق این اهداف در آینده خواهند شد.[۴]

---

[1] Digital Transformation

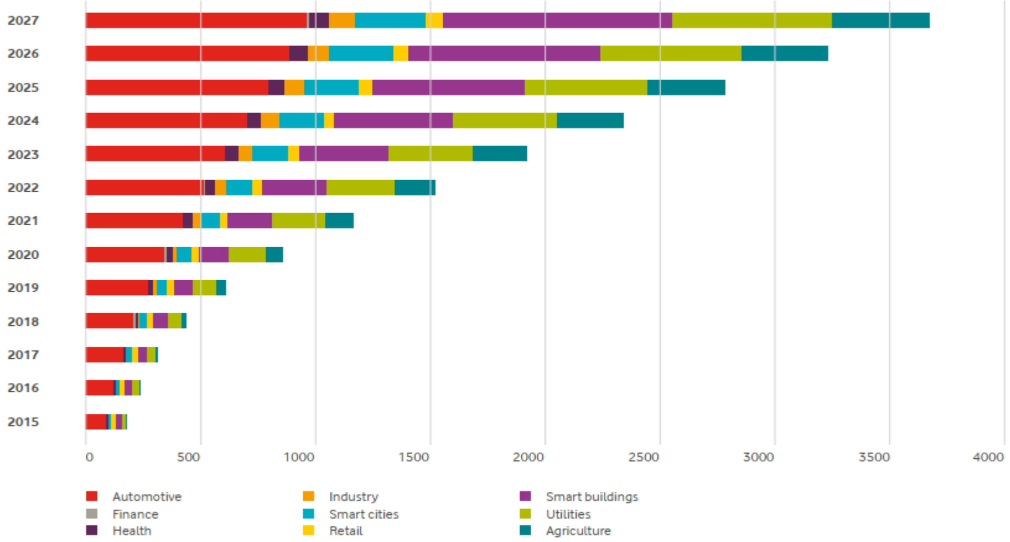
[2] World Economic Forum

کشورهای مختلف در توسعه کاربردها و خدمات اینترنت اشیا با فرصت‌های عظیمی مواجه خواهند شد. سیاستگذاران کشورها باید اطلاع داشته باشند که اگر سیاست و مقررات درست برای اینترنت اشیا را درنظر نگیرند، پیشرفت کشورهایشان در این حوزه را با چالش مواجه خواهند کرد. سیاست‌ها و مقررات موجود جهانی به اندازه کافی با داده‌های اینترنت اشیا و ارتباطات دستگاه –به–دستگاه (M2M[۱]) سازگار نیستند. درنتیجه سیاستگذاران در کشورهای مختلف نیازمند آن هستند تا یک چارچوب مقرراتی مناسب برای اینترنت اشیا طراحی کنند تا به رفاه شهروندان کمک کند و همچنین فرصت‌های جدیدی برای افراد و کسب‌وکار ایجاد نماید تا سبب توسعه کشور شود.

۲-۲. گستردگی بازار اینترنت اشیا و نیاز به نگرش مقرراتگذاری بین بخشی

اینترنت اشیا از بازار گسترده‌ای برخوردار است. همان‌طورکه در شکل ۱ نیز نشان داده شده است، اینترنت اشیا دارای بازار بسیار متنوعی با توزیع گسترده‌ای از اتصالات به شبکه در میان بسیاری از بخش‌های مختلف اقتصاد است. اگرچه باید خاطر نشان کرد که خارج از محدوده شکل ۱، اینترنت اشیا مصرف‌کننده نیز یکی از بخش‌های مهم بازار است، به‌طوری‌که براساس برآورد IDC که هزینه‌های صرف شده این بخش با تمرکز بر خانه هوشمند، سلامت شخصی و ارتباط با وسایل نقلیه متصل به شبکه را محاسبه کرده است، این بازار در سال ۲۰۱۹ در سراسر جهان بالغ بر ۱۰۸ میلیارد دلار (۹۶ میلیارد یورو) بوده است.[۱۰]

شکل ۱. اتصالات اینترنت اشیا در سراسر جهان براساس بخش‌های مختلف[۱۱]



---

۱. Machine-to-Machine

مطالعه OECD در مورد اندازه‌گیری و کاربردهای اینترنت اشیا، ذات متنوع بازار اینترنت اشیا و نیاز برای یک رویکرد سیاستگذاری مشترک را تأیید می‌کند. در این مطالعه [۱۲] که در اکتبر سال ۲۰۱۸ انجام شد، OECD تعاریف متنوعی را مشخص کرد که می‌تواند در سراسر ادارات رگولاتوری ملی و منطقه‌ای و بازیگران زنجیره ارزش مشاهده شود. OECD یک طبقه‌بندی با تفکیک اینترنت اشیا به دسته‌بندی‌هایی براساس رویکرد مورد-به-مورد را پیشنهاد می‌کند، به‌طوری‌که بسیاری از دستگاه‌های متصل، الزامات مختلفی از کیفیت سرویس و شبکه دارند (به‌عنوان نمونه، کاربردهای اینترنت اشیا بحرانی مانند جراحی از راه دور و وسایل نقلیه خودکار به قابلیت اطمینان بالا و اتصال به شبکه با تأخیر بسیار کم نیاز دارند). این مطالعه همچنین به این نتیجه رسید که ممکن است سیاست‌های جدید و چالش‌های مقرراتی در برخی حوزه‌ها پدیدار شود. ازاین‌رو، ایجاد شاخص‌هایی برای آگاهی از سیاست‌گذاری در این زمینه‌ها یک اولویت محسوب می‌شود.

۳-۲. آنالیز الزامات رگولاتوری اینترنت اشیا

شناسایی موانع مقررات موجود بر سر راه اینترنت اشیا به طراحی چارچوب مقرراتی اینترنت اشیا کمک شایانی می‌کند. کاربرد قوانین قابل اعمال به اینترنت اشیا مبهم یا نامشخص است. برخی قوانین اعمال به اینترنت اشیا سبب اعوجاج بازار ازطریق کاربرد ناهمگون فناوری‌های سلولی و غیرسلولی می‌شود. در برخی موارد، لازم است قوانین برای تأمین یک نتیجه وجود داشته باشند، اما قوانین تنها به کاربردهای سلولی اعمال می‌شوند، بنابراین یک شکاف در سرویس اینترنت اشیا ازطریق اتصال غیرسلولی ایجاد می‌شود. در موارد دیگر، نیازی به قوانین موجود نیست یا آنها متناسب نیستند، بنابراین وجود آنها باعث ایجاد فشار غیرضروری برای ارائه‌دهندگان فناوری‌های سلولی می‌شود و برای ارائه‌دهندگان اتصال غیر سلولی این‌طور نیست.[۴] ازاین‌رو، مقررات موجود نیازمند انواع تغییرات زیر هستند:

- ممکن است قوانینی حذف شوند. قوانینی وجود دارد که مورد نیاز نیست و درحال حاضر فقط به موارد کاربردی که ازطریق اینترنت اشیا سلولی متصل هستند اعمال می‌شوند. این قوانین باید کاهش یابند. به‌عنوان نمونه، تعهد نگهداری داده‌ها برای یک مورد استفاده اینترنت اشیای کشاورزی توسط ارائه‌دهندگان اتصال شبکه سلولی.

- ممکن است قوانینی دستخوش تغییر شوند. بسیاری از قوانین مربوط به ارتباطات بین افراد هستند و در این قوانین ارتباطات بین اشیا درنظر گرفته نشده است. روشی که یک قانون کلی اعمال شود برای موارد کاربرد اینترنت اشیا باید تغییر یابد. به‌عنوان مثال هیچ کاربردی از مقررات رومینگ برای یک مورد استفاده اینترنت اشیا B2B2C[۱] که هزینه مبتنی‌بر استفاده به کاربر نهایی وجود ندارد.

---

[1] Business-to-Business-to-Costumer

- ممکن است برخی قوانین ارتقا یابند. قوانینی وجود دارند که برای موارد کاربردی اعمال می‌شود که تنها ازطریق اینترنت اشیای سلولی متصل هستند. این قوانین به‌منظور پوشش تمام راهکارهای اتصال (اعم از سلولی و غیرسلولی) نیاز دارند تا ارتقا یابند. به‌عنوان نمونه الزامات مرتبط با امنیت برای دستگاه‌های اینترنت اشیا که مصرف‌کننده با آنها سروکار دارد.
- ممکن است برخی قوانین براساس ارزیابی عملکرد اینترنت اشیا اعمال شوند. قوانینی وجود دارند که کاربرد آن باید به‌گونه‌ای اصلاح شوند که براساس خطر آسیب مربوط به عملکرد دستگاه اینترنت اشیا اعمال شوند. به‌عنوان نمونه هیچ الزامی برای نگهداری داده در یک دستگاه اینترنت اشیای کشاورزی وجود ندارد، برخلاف یک دستگاه اینترنت اشیا که مصرف‌کنندگان با آن سروکار دارند.

بخش‌های مختلف در موارد کاربرد اینترنت اشیا را بسته به اینکه آیا رابطه قراردادی ایجاد شده بین بازیگران درگیر در زنجیره ارزش فقط B2B[1] یا بین کسب‌وکارهاست یا شامل یک مصرف‌کننده (B2C[2] یا B2B2C) می‌شود، می‌توان به دو گروه تقسیم کرد:[۴]

- بخش‌های B2B: کشاورزی و محیط زیست، ساخت‌وساز، تولید و عرضه، مدیریت هوشمند کسب‌وکارهای گسترده.
- بخش‌های B2C و B2B2C: خودرو، لوازم الکترونیکی مصرف‌کنندگان، سرویس‌های اورژانسی و امنیت ملی، سلامت، ساختمان‌های هوشمند، خرده‌فروشی، شهرهای هوشمند و حمل‌ونقل هوشمند، شرکت‌های توزیع آب و برق و کنتورهای هوشمند.

۴-۲. پیشنهاد چارچوب مقرراتگذاری اینترنت اشیا

در این قسمت یک چارچوب جدید برای مقرراتگذاری اینترنت اشیا پیشنهاد شده است تا موانع توسعه و اتخاذ اینترنت اشیا در ایران را حذف کند.

اصول نوآوری، قابلیت اطمینان و آینده‌نگاری و بی‌طرفانه بودن فناوری باید در مقررات درنظر گرفته شوند. علاوه‌براین موارد، هزینه‌های انطباق پایین، اطمینان و وضوح نظارتی، و هماهنگی نیز به افزایش تحقیق و نوآوری و افزایش رقابت‌پذیری در کشور کمک می‌کند. اساس یک چارچوب جدید تنظیم مقررات اینترنت اشیا به چهار حوزه وسیع و مهم طبقه‌بندی می‌شود. ازاین‌رو، یک چارچوب جدید برای اینترنت اشیا به‌صورت زیر پیشنهاد می‌شود:

---

2. Business-to-Business
3. Business-to-Costumer

۱. نحوه اعمال قوانین به اینترنت اشیا

نحوه اعمال قوانین اینترنت اشیا بدین‌معناست که اگر قوانینی که برای ارتباطات بین‌فردی طراحی شده‌اند به کاربردهای اینترنت اشیا و دستگاه-به-دستگاه اعمال شوند، هزینه انجام کسب‌وکار را افزایش داده و تأخیر در پیاده‌سازی این فناوری را بالا می‌برند.

فشارهای مقرراتی روی بازیگران اینترنت اشیا در اکوسیستم اینترنت اشیا در مواردی که آنها برای دستیابی به هدف مقرراتی که در ابتدا طراحی شده بودند دیگر ضروری نیستد، لازم است تا کاهش یابند یا حذف شوند.

نهادهای مقرراتگذاری باید امکان مدیریت شبکه مؤثر برای سرویس‌های اینترنت اشیا و توسعه سرویس‌های نوآورانه با الزامات کیفیت مشخصی را ترغیب کنند. یک اپراتور باید امکان آن را داشته باشد تا به‌صورت پویا منابع را در بین برش‌های شبکه با کارآمدترین روش به اشتراک بگذارد تا بهترین کیفیت را برای کاربران انتهایی به ارمغان آورد.

ارائه‌دهندگان اتصال باید اجازه داشته باشند تا ابَرداده‌های[1] ارتباطی را به‌منظور بررسی ابعاد لازم برای ارائه خدمات توافق شده پردازش کنند. این شامل پردازش برای مدیریت ارتباط با مشتری و صورتحساب، اطمینان از امنیت خدمات، جلوگیری و بررسی کلاهبرداری، توسعه خدمات و همچنین ایجاد اطلاعات آماری جمع‌آوری شده از ابَرداده‌های ارتباطی می‌شود.

رضایت نباید تنها راهکار برای اجازه پردازش بیشتر ابَرداده‌های ارتباطی باشد. در وضعیت اشخاص حقیقی رضایت یک رویکرد قابل قبول است، اما برای اشخاص حقوقی، توافق‌های قراردادی باید استفاده شود.

۲. امنیت و حفاظت از داده

- امنیت:

تعهدات امنیتی مناسب مربوط به خطرات باید در سراسر کشور و در کل زنجیره ارزش اینترنت اشیا قابل اعمال باشند.

آسیب‌پذیری‌ها غالباً از اجرای نرم‌افزارهایی که در آنها ملاحظات امنیتی لحاظ نشده است ناشی می‌شود. ازاین‌رو، برنامه‌های نرم‌افزاری در دستگاه‌های اینترنت اشیا مصرف‌کنندگان باید به‌طور امن و در زمان به‌موقع قابل به‌روزرسانی باشد. البته دستگاه‌های اینترنت اشیا باید بتوانند در زمان به‌روزرسانی، فعالیت خود را نیز انجام دهند و اگر چنین نباشد کاربران با مشکلات امنیتی بزرگی مواجه خواهند شد.

برقراری هر ارتباط و انتقال داده‌ها باید به‌صورت امن و با رمزگذاری باشد تا در مقابل حملات نیز مقاوم باشند. همچنین باید سطوح در معرض حمله به حداقل رسانده شود. تولیدکنندگان دستگاه‌ها و ارائه‌دهندگان سرویس در رابطه با اینکه اطلاعات شخصی مصرف‌کنندگان، توسط چه فردی و با چه

---

[1] Metadata

هدفی استفاده می‌شوند به آنها اطلاعات صریح و روشنی ارائه کنند و اطمینان ایجاد کنند که اطلاعات شخصی آنها محافظت می‌شود. امکان پاک کردن اطلاعات شخصی به روشی ساده نیز باید برای مصرف‌کننده وجود داشته باشد.

- حفاظت از داده:

درنظر گرفتن قوانینی برای حفاظت از داده‌های اینترنت اشیا سبب ایجاد امنیت و حفظ حریم خصوصی افراد خواهد شد. ازاین‌رو باید یک روش اطلاع‌دهی اجباری وجود داشته باشد. دستگاه‌های اینترنت اشیا برای فعالیت‌های پردازش داده رضایت کافی پیرامون داده را به‌صورت صریح و بدون ابهام از کاربران کسب کنند. پردازش داده‌های شخصی و رضایت مربوط به آن برای کودکان نیز باید توسط قانونگذار به‌صورت صریح مشخص شود.

۳. مقررات بی‌طرفانه نسبت به فناوری

از دیدگاه شبکه اتصال، اینترنت اشیا بسیار متنوع است. تنوع راهکارهای اتصال، شامل شبکه‌های تلفن همراه، ماهواره و شبکه‌های خصوصی، امکان آن را فراهم می‌کند تا ارائه‌دهندگان بتوانند الزامات متنوع و درحال تحقق مشتریان را در سراسر طیف وسیعی از موارد کاربرد در بخش‌های مختلف برآورده کنند. همان‌طورکه در جدول ۱ نیز نشان داده شده است، تخمین‌ها در سال ۲۰۱۸ نشان می‌دهد که تقریباً ۱۲٪ از مجموع دستگاه‌های اینترنت اشیا از طریق شبکه‌های تلفن همراه (اینترنت اشیای سلولی) متصل شده بودند، درحالی‌که مابقی آنها ازطریق پروتکل‌های ارتباطی برد کوتاه، اتصال ماهواره‌ای یا شبکه‌های خصوصی برد بلند توان پایین بوده‌اند.

جدول ۱. تعداد دستگاه‌های متصل در فناوری‌های مختلف در سراسر جهان

(برحسب میلیارد)

اینترنت اشیا	۲۰۱۸	۲۰۲۴
اینترنت اشیا برد بلند (شامل اینترنت اشیا سلولی)	۱/۴	۴/۴
اینترنت اشیا سلولی	۱	۱/۴
اینترنت اشیا برد کوتاه	۹/۳	۱۷/۸
مجموع	۱۰/۷	۲۲/۲

مأخذ: [۱۳]

گزارش BEREC در مورد شاخص‌های اینترنت اشیا، چالش‌های نگاشت اکوسیستم اینترنت اشیا را تأیید می‌کند. در گزارش ماه مارس ۲۰۱۹ [۱۴]، BEREC چالش‌های نگاشت اکوسیستم را تأیید کرد و پیشنهاد داد که یک مطالعه ثانویه در نیمه دوم ۲۰۲۰ انجام شود. در این سند، BEREC لزوم اتخاذ یک نقش پیشگیرانه برای اطمینان از بی‌طرفانه بودن فناوری و آموزش ذی‌نفعان را تشخیص داد.

علاوه‌براین، BEREC الزاماتی را تنظیم کرده است تا روی طبقه‌بندی اولیه خود از اینترنت اشیا مبتنی‌بر تعداد محدودی از موارد کاربرد، به‌وسیله طبقه‌بندی سرویس‌های اینترنت اشیا براساس فناوری‌های اتصال (به‌عنوان نمونه، اتصال شبکه سلولی در مقابل اتصال شبکه غیرسلولی)، استفاده از طیف‌های مختلف (طیف‌های دارای مجوز و طیف‌های آزاد)، یا الزامات عملکردی شبکه، اعمال کند.

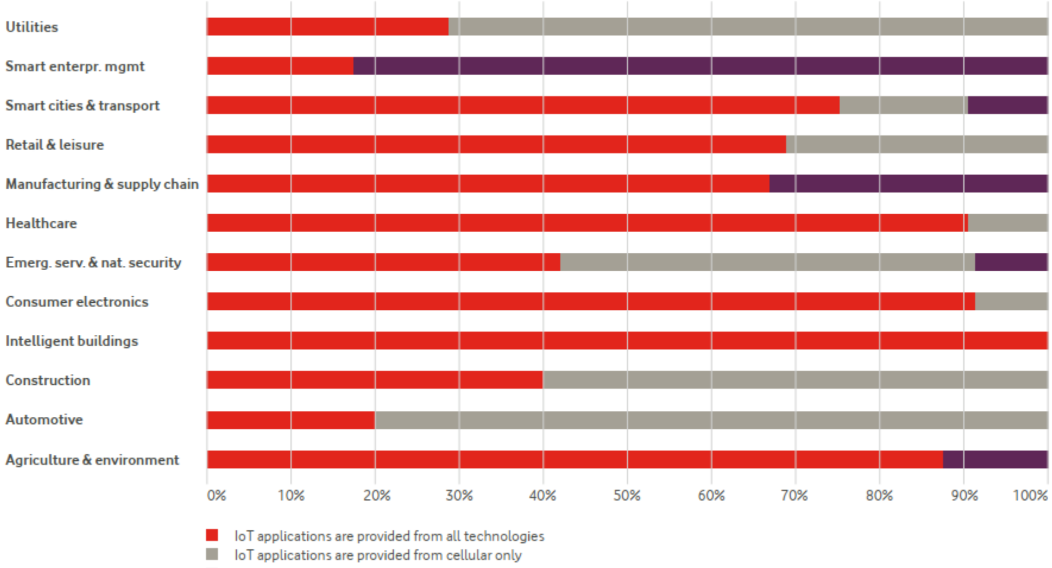
- رقابت‌پذیری:

مقررات باید یک زمین بازی بین بازیگران در اکوسیستم اینترنت اشیا و همچنین بین بازیگران اینترنت اشیا که راهکارهای فناورانه مختلفی به‌کار می‌گیرند را تقویت کند.

- بی‌طرفانه بودن فناوری:

در شکل ۲، درصد اتصال فراهم شده ازطریق فناوری سلولی، فناوری غیرسلولی یا هردو صورت از فناوری برای موارد کاربرد از بخش‌های مختلف اینترنت اشیا را نشان می‌دهد. تجزیه و تحلیل نشان می‌دهد که در بسیاری از بخش‌ها، اکثر موارد استفاده اینترنت اشیا را می‌توان به‌طور موازی با استفاده از طیف وسیعی از فناوری‌های اتصال ارائه داد.[۴]

شکل ۲. درصد موارد کاربرد اینترنت اشیا در هر بخش به‌طوری‌که تا چه میزان ازطریق فناوری سلولی و یا غیرسلولی فراهم می‌شود



مأخذ: [۴]

بااین‌حال، به‌رغم وجود فناوری‌های اتصال رقیب برای اینترنت اشیا، تجزیه و تحلیل‌ها نشان می‌دهد که تقریباً ۳۰٪ از نیازهای بررسی شده فقط مربوط به ارائه‌دهندگان کاربردهای اتصال اینترنت اشیا ازطریق شبکه‌های سلولی با استفاده از سیم کارت و شماره‌های عمومی هستند[۴]. تعهدات مقرراتی باید بدون درنظر گرفتن فناوری‌های مورد استفاده به‌صورت مساوی اعمال شوند و از به‌نفع بودن یا به ضرر بودن مقررات برای یک راهکار فناوری خاص جلوگیری شود. کاربردهای ردیابی مصرف‌کننده (به‌عنوان نمونه برای دوچرخه‌ها، حیوانات خانگی، کیف‌ها و تناسب اندام) می‌توانند ازطریق فناوری سلولی یا غیرسلولی متصل شوند، اگرچه، درحال حاضر الزامات مقرراتی مانند قابلیت حمل، رومینگ، ثبت سیم کارت، رهگیری قانونی تنها به اینترنت اشیا سلولی اعمال می‌شوند که لازم است این موارد برای همه راهکارهای اتصال اعمال شود.

۴. مسئولیت و اتخاذ بهترین شیوه‌ها درخصوص اینترنت اشیا

اتخاذ محدود از بهترین شیوه‌ها در رابطه با اینترنت اشیا، شامل اشتراک داوطلبانه از داده‌های تولید شده توسط دستگاه‌ها بدون دخالت انسان، گواهینامه امنیتی اینترنت اشیا و اقدامات قراردادی در مورد مسئولیت اینترنت اشیا هستند.

- نوآوری و اثبات فناوری:

تفسیر و کاربرد قوانین برای خدمات اینترنت اشیا باید نوآوری را ازطریق به‌کارگیری انعطاف‌پذیری مقررات و آزمایش تسهیل بخشد. برای ارتقای نوآوری، شرکت‌کنندگان در زنجیره ارزش اینترنت اشیا باید به‌طور منطقی تلاش کنند تا داده غیرشخصی و تولید شده توسط دستگاه‌ها را به‌صورت عادلانه، معقول و غیرتبعیض‌آمیز با درنظر گرفتن همه قوانین مربوط به امنیت، حریم خصوصی و رقابت یا ملاحظات محرمانگی به اشتراک گذارند.

برای رسیدگی به مسائل احتمالی پیرامون مسئولیت، شرکت‌کنندگان در زنجیره ارزش و اکوسیستم اینترنت اشیا باید اطمینان حاصل کنند که توافقات قراردادی بین آنها درخصوص اینکه کدام بازیگر مسئول در رویدادی که یک محصول مبتنی‌بر اینترنت اشیا باعث خسارت شده است، به‌طور صریح بیان شده است. برای نمونه، مسئولیت احتمالی درخصوص پیدایش موارد کاربرد ازقبیل هواپیماهای بدون‌سرنشین یا خودروهای خودران باید به‌طور روشن در قوانین مشخص شود.

فصل سوم ـ ملاحظات امنیت سایبری در اینترنت اشیا

۱-۳. امنیت سایبری برای اینترنت اشیا براساس استانداردهای ارتباطاتی اروپا

نهاد انجمن استانداردهای ارتباطاتی اروپا (ETSI[۱])، یک سازمان استانداردسازی غیرانتفاعی و مستقل اروپایی در صنعت مخابرات است که با شرکت‌های تخصصی و بنگاه‌های اقتصادی در سراسر جهان همکاری می‌کند. این نهاد در ابتدای سال ۲۰۱۹ سندی با عنوان «امنیت سایبری برای مصرف‌کننده اینترنت اشیا» منتشر کرده است [۱۵] که هدف آن حمایت از همه سازمان‌ها و شرکت‌های درگیر در تولید و توسعه شبکه اینترنت اشیا با راهنمایی درخصوص محفوظ نگه داشتن محصولاتشان است. تمرکز این سند روی برطرف کردن تمامی چالش‌های امنیتی مصرف‌کنندگان اینترنت اشیا نیست، بلکه بیشتر بر ارائه سیاست‌های سازمانی و کنترل فنی که بیشترین اهمیت را در کاستی‌های گسترده امنیتی دارند، تمرکز دارد. ازآنجایی‌که خدمات و دستگاه‌های اینترنت اشیا داده‌های شخصی را ذخیره و پردازش می‌کنند، سند مذکور کمک می‌کند تا این اطمینان حاصل شود که مطابق با قوانین GDPR[۲] است. [۱۵]

۲-۳. مقررات امنیت سایبری برای مصرف‌کنندگان اینترنت اشیا

در این قسمت به‌طورکلی به بررسی قوانینی که در سند فوق‌الذکر بیان شده است، پرداخته می‌شود. این سند ۱۳ موضوع مهم را بررسی و قوانینی را پیشنهاد می‌کند که در ادامه بیان خواهند شد.

۱-۲-۳. عدم گذرواژه پیش‌فرض و عمومی

قانون ـ گذرواژه تمامی دستگاه‌های اینترنت اشیا باید به‌صورت منحصربه‌فرد باشد و قابل تنظیم مجدد به هیچ یک از مقادیر پیش‌فرض کارخانه نباشد. [۱۵]

بسیاری از دستگاه‌های اینترنت اشیا برای واسط‌های کاربری از طریق پروتکل‌های شبکه، با نام کاربری و گذرواژه پیش‌فرض و عمومی فروخته می‌شوند. این امر منبع بسیاری از مشکلات امنیتی در اینترنت اشیاست و بنابراین باید این مورد برطرف شود.

۲-۲-۳. پیاده‌سازی شیوه‌ای به‌منظور مدیریت گزارش‌های آسیب‌پذیری‌ها

قانون- کلیه شرکت‌هایی که خدمات و دستگاه‌های متصل به اینترنت را ارائه می‌دهند باید نقطه تماس عمومی به‌عنوان بخشی از سیاست افشای آسیب‌پذیری ارائه دهند تا محققان امنیتی و سایرین بتوانند تا مشکلات را گزارش دهند. [۱۵]

قانون- در خصوص آسیب‌پذیری‌های افشا شده باید به موقع وارد عمل شد. [۱۵]

---

[۱] European Telecommunications Standards Institute

[۲] General Data Protection Regulation

قانون- همچنین شرکت‌ها به عنوان بخشی از چرخه امنیتی محصول، لازم است به طور پیوسته به نظارت، شناسایی و اصلاح آسیب‌پذیری‌های امنیتی خدمات خود و محصولاتی که می‌فروشند و یا در حال تولید آن هستند، بپردازند. [۱۵]

دانستن در مورد آسیب‌پذیری‌های امنیتی شرکت‌ها را قادر می‌سازد تا واکنش لازم را نشان دهند. انتظار می‌رود در مرحله نخست، آسیب‌پذیری‌ها مستقیماً به ذی‌نفعان گزارش شود. اگر امکان برطرف نمودن آسیب‌پذیری‌ها توسط آنها وجود نداشت، آنگاه به دستگاه‌ها و نهادهای کشوری گزارش داده شود. همچنین می‌توان شرکت‌ها را به اشتراک‌گذاری اطلاعات خود با سایر دستگاه‌های ذی‌صلاح صنعت ترغیب کرد.

۳-۲-۳. به‌روزرسانی نرم‌افزار

قانون- لازم است کلیه اجزای نرم‌افزاری در دستگاه‌های اینترنت اشیا مصرف‌کنندگان، به‌طور امن قابل به‌روزرسانی باشد. [۱۵]

قانون- لازم است مصرف‌کننده از طریق یک نهاد مناسب همچون تولیدکننده و یا ارائه‌دهنده خدمات از نیاز به به‌روزرسانی مطلع شود. [۱۵]

قانون- هنگامی که اجزای نرم‌افزار قابل به‌روزرسانی هستند، به‌روزرسانی‌ها باید به‌موقع باشند. [۱۵]

قانون- هنگامی که اجزای نرم‌افزار قابل به‌روزرسانی هستند، لازم است سیاستی برای پایان عمر دستگاه‌ها تعیین شود که در آن، حداقل طول دوره زمانی که به‌روزرسانی‌های نرم‌افزار دریافت می‌شود و دلایل پشتیبانی برای این مدت زمان نیز منتشر شود. [۱۵]

قانون- هنگامی که اجزای نرم‌افزار قابل به‌روزرسانی هستند، لازم است نیاز به به‌روزرسانی به مصرف‌کننده به‌طور واضح اعلام شود و همچنین لازم است تا به‌روزرسانی به‌راحتی اجرایی شود. [۱۵]

توسعه و استقرار به‌موقع به‌روزرسانی‌های امنیتی نرم‌افزار یکی از مهم‌ترین اقدامات یک شرکت است که می‌تواند به محافظت مشتریان و اکوسیستم گسترده فنی خود بپردازد. آسیب‌پذیری‌ها غالباً از اجرای نرم‌افزاری ناشی می‌شود که به آن از دیده امنیتی نگاه نشده است. بهترین اقدام این است که همه نرم‌افزار به‌روز شده به‌خوبی نگهداری شود.

«به‌موقع»[۱] در زمینه به‌روزرسانی نرم‌افزار می‌تواند متناسب با مشکلات خاص و رفع آنها و سایر عوامل چون امکان دسترسی به دستگاه و یا ملاحظات تحمیل شده دستگاه متغیر باشد. درخصوص یک باگ غیرحیاتی، ارائه به‌روزرسانی نرم‌افزار در یک دوره معین قابل قبول است. اما برای یک نقض اجرایی حاد در کد، می‌توان ارائه به‌روزرسانی سریع‌تری را انتظار داشت.

به‌روزرسانی‌های امنیتی نرم‌افزار دستگاه‌ها می‌تواند با روشی پیشگیرانه، به‌عنوان بخشی از به‌روزرسانی‌های خودکار ارائه شود که بتواند آسیب‌پذیری‌های امنیتی را قبل از سوءاستفاده از آن رفع کند.

---

[۱] Timely

در بسیاری از موارد، انتشار به‌روزرسانی نرم‌افزار وابستگی‌های مختلفی به سایر نهادها همچون تولیدکنندگان زیرمجموعه دارد؛ بااین‌حال دلیلی برای جلوگیری از به‌روزرسانی نیست. ضروری است که تمام زنجیره تأمین نرم‌افزار در توسعه و استقرار به‌روزرسانی امنیتی در نظر گرفته شود.

انتظار می‌رود به‌روزرسانی‌های نرم‌افزار بعد از فروش نرم‌افزار ارائه شود و در دوره‌های مناسب برای دستگاه فرستاده شود. مشتری انتظار دارد در هنگام خرید محصول، این دوره به‌روزرسانی نرم‌افزار مشخص شده باشد.

نرم‌افزار دستگاه اینترنت اشیا مصرف‌کننده را می‌توان به یک یا چند دسته تقسیم‌بندی کرد:[۱] Firmware، نرم‌افزار پلتفرم[۲] از قبیل سیستم عامل، خدمات و اپلیکیشن‌ها. فرایند به‌روزرسانی می‌تواند برای دسته‌بندی‌های متعدد نرم‌افزاری، متفاوت باشد. [۱۵]

قانون- هنگامی که اجزای نرم‌افزار قابل به‌روزرسانی هستند، لازم است در صورت امکان عملکرد اصلی دستگاه حین به‌روزرسانی حفظ شود، چون ممکن است در دسترس بودن در طول به‌روزرسانی حیاتی باشد. [۱۵]

برای مصرف‌کنندگان مهم است که یک دستگاه بتواند در حین به‌روزرسانی به‌کار خود ادامه دهد. به همین دلیل است که قانون فوق «حفظ عملکرد اصلی دستگاه» در جایی که ممکن است را پیشنهاد می‌دهد. به‌ویژه انتظار می‌رود دستگاه‌هایی که عملکرد مرتبط با ایمنی دارند، در صورت به‌روزرسانی کاملاً خاموش نشوند و برخی از حداقل قابلیت‌های عملکردی سیستم به‌کار خود ادامه دهند. برای مثال در طول به‌روزرسانی، انتظار می‌رود یک ساعت وظیفه اصلی خود یعنی زمان را اعلام کند، یک ترموستات خانگی به عملیاتی بودن خود ادامه دهد و تنظیمات گرمایشی توسط کاربر قابل تغییر باشد، یک قفل هوشمند به جهت قفل و باز کردن درب قابل استفاده باشد. در صورتی‌که این موضوع به‌درستی مدیریت نشود، می‌تواند باعث مشکلات امنیتی جدی در برخی از انواع دستگاه‌ها شود.

قانون- هنگامی که اجزای نرم‌افزار قابل به‌روزرسانی هستند، لازم است از منبع به‌روزرسانی‌های نرم‌افزار اطمینان حاصل شود و پیچ‌های امنیتی روی یک کانال امن تحویل داده شوند. [۱۵]

۴-۲-۳. ذخیره‌سازی اعتبارها[۳] و اطلاعات امنیتی حساس به‌صورت امن

قانون- لازم است اعتبارها و داده‌های حساس امنیتی به‌صورت امن در خدمات و دستگاه‌ها ذخیره شوند. مناسب است از اعتبارهای کد سخت[۴] در نرم‌افزار دستگاه استفاده نشود. [۱۵]

با مهندسی معکوس دستگاه‌ها و اپلیکیشن‌ها، به‌راحتی می‌توان اعتبارها از قبیل نام کاربری و گذرواژه‌های کد سخت شده را در نرم‌افزار شناسایی کرد. همچنین از روش‌های ساده انسداد[۵] به‌منظور

---

[۱] این موارد جامع نیستند.

[۲] Platform

[۳] Credentials

[۴] Hard-coded

[۵] Obfuscation

پنهان‌کردن و رمزگذاری این اطلاعات کد سخت استفاده می‌شود که به‌راحتی شکسته می‌شوند. روش‌های ذخیره‌سازی مطمئن و ایمن می‌تواند برای تأمین امنیت داده‌های با حساسیت امنیتی بالا از قبیل مواردی که یک محیط اجرای مطمئن (TEE)[۱] و ذخیره‌سازی امن و مرتبط با آن ارائه می‌دهد یا قابلیت‌های پردازش و ذخیره‌سازی امن نرم‌افزاری که روی UICC[۲] و eUICC[۳]ها اجرا می‌شوند، استفاده شوند.

۵-۲-۳. برقراری ارتباط به‌صورت ایمن

قانون- لازم است هر کنترل و مدیریت از راه دور داده‌ها با حساسیت امنیتی، در هنگام انتقال رمزگذاری شود که این قبیل رمزگذاری‌ها متناسب با کاربرد و فناوری خواهد بود. [۱۵]

قانون- تمامی کلیدها باید به‌صورت امن مدیریت شوند. [۱۵]

انتظار می‌رود محصولاتی پاسخگوی نیاز کاربران هستند که در مقابل حملات روی رمزگذاری‌ها نیز مقاوم باشند. با این وجود، اقتضای کنترل‌های امنیتی و استفاده از رمزگذاری به عوامل بسیاری به‌ویژه زمینه مورد استفاده بستگی دارد.

۶-۲-۳. به حداقل رساندن سطوح در معرض حمله

اصل حداقل امنیت[۴] سنگ بنایی از مهندس امنیتی صحیح است که تاحدامکان در هر زمینه کاربردی در حوزه اینترنت اشیا قابل استفاده خواهد بود.

قانون- لازم است پورت‌های بدون استفاده نرم‌افزار و شبکه بسته شود. [۱۵]

قانون- سخت‌افزار نباید دسترسی به حمله را باز بگذارد (به عنوان مثال نقاط تست، پورت‌ها و دسترسی سریال باز)[۱۵]

قانون- خدمات نرم‌افزاری که استفاده نمی‌شوند نباید در دسترس باشند. [۱۵]

قانون- لازم است برای اجرای عملکرد ضروری در دستگاه و یا خدمات، کد به حداقل برسد. [۱۵]

قانون- لازم است نرم‌افزار با حداقل امنیت لازم با درنظر گرفتن هر دو موضوع عملکرد و امنیت اجرا شود. [۱۵]

۷-۲-۳. حصول اطمینان از یکپارچگی نرم‌افزار

قانون- لازم است نرم‌افزار دستگاه اینترنت اشیا با استفاده از مکانیزم‌های بوت[۵] امن که به روت[۶] سخت‌افزاری مطمئن نیاز دارد، تأیید گردد. [۱۵]

---

[۱] Trusted Execution Environmen یا TEE.

ناحیه‌ای امن در پردازنده اصلی است و تضمین می‌کند که داده‌ها و کدهای بارگذاری شده در آن با توجه به محرمانگی و یکپارچگی محافظت شوند.

[۲] Universal Integrated Circuit Card

[۳] embedded Universal Integrated Circuit Card

[۴] Principle of Least Privilege

[۵] Boot

[۶] Root

قانون- اگر تغییر غیرمجاز در نرم‌افزار شناسایی شد، لازم است دستگاه مشکل را به مصرف‌کننده و یا متولی[۱] هشدار دهد و برای انجام اعلام هشدار نباید نیاز به اتصال به شبکه‌های گسترده‌تر مانند اینترنت باشد. [۱۵]

۳-۲-۸. حصول اطمینان از حفاظت از اطلاعات شخصی

قانون- لازم است تولیدکنندگان دستگاه و ارائه‌دهندگان سرویس به مصرف‌کنندگان درباره این نکته که برای هر دستگاه چگونه از اطلاعات شخصی آنها، توسط چه فردی و با چه هدفی استفاده می‌شوند، اطلاعات روشن و شفافی ارائه کنند. [۱۵]

قانون- درصورتی‌که اطلاعات شخصی برمبنای رضایت مشتری پردازش می‌شود، لازم است این رضایت به روشی معتبر کسب شود. [۱۵]

قانون- لازم است برای مشتریانی که جهت پردازش اطلاعات شخصی خود رضایت داده‌اند، این فرصت وجود داشته باشد که هر زمان خواستند بتوانند رضایت خود را پس بگیرند. [۱۵]

انتظار می‌رود نهادهای مناسب ازجمله ارائه‌دهندگان سرویس یا تولیدکنندگان دستگاه از پردازش اطلاعات شخصی مطابق با قوانین حفاظت از داده (به‌عنوان مثال GDPR) و همچنین مطابق با قانونگذاری درخصوص موضوعات رگولاتوری و امنیتی اطمینان حاصل کنند.

۳-۲-۹. انعطاف‌پذیری سیستم‌ها در مقابل خاموشی

قانون- با در نظرگرفتن امکان قطع شبکه و یا برق، لازم است در دستگاه‌ها و خدمات اینترنت اشیا درصورتی‌که برای استفاده خود و یا سایر سیستم‌های متکی نیاز شود، انعطاف‌پذیری وجود داشته باشد.[۱۵]

قانون- تا جایی که به‌صورت منطقی امکان‌پذیر است، لازم است دستگاه‌های اینترنت اشیا در موارد قطع شبکه عملیاتی و محلی باقی بمانند و در حالت احیا قطعی برق به‌صورت کامل بازیابی شوند. [۱۵]

قانون- دستگاه‌ها باید بتوانند در وضعیتی پیش‌بینی شده، پایدار و عملیاتی و با روشی منظم نسبت به ارتباط مجدد در مقیاس گسترده به شبکه بازگردند. [۱۵]

۳-۲-۱۰. نظارت بر داده‌های سیستم مکان‌یابی

قانون- اگر داده‌های مکان‌یابی مانند داده‌های اندازه‌گیری، از دستگاه‌ها و خدمات اینترنت اشیا گردآوری می‌شوند، لازم است درخصوص ناهنجاری‌های امنیتی ارزیابی صورت گیرد. [۱۵]

قانون- اگر داده‌های مکان‌یابی از دستگاه‌ها و خدمات اینترنت اشیا جمع‌آوری می‌گردند، لازم است پردازش داده‌های شخصی به حداقل برسند و چنین داده‌هایی ناشناس بمانند. [۱۵]

قانون- اگر داده‌های مکان‌یابی از دستگاه‌ها و خدمات اینترنت اشیا گردآوری می‌گردند، لازم است به مصرف‌کننده اطلاعات مربوطه به اینکه چه داده‌های مکان‌یابی جمع‌آوری می‌گردد و دلایل آن ارائه شود.

---

[۱] Administrator

بررسی مکان‌یابی شامل لاگ[1] داده‌ها، برای ارزیابی‌های امنیتی مفید است و برای موقعیت‌های نامعمول، شناسایی سریع و مقابله برای به حداقل رساندن ریسک امنیتی مشکلات را کاهش می‌دهد. [۱۵]

۱۱-۲-۳. امکان پاک کردن ساده اطلاعات شخصی برای مصرف‌کننده

قانون- دستگاه‌ها و خدمات باید به‌گونه‌ای تنظیم شوند که در زمانی که مالکیت منتقل می‌شود، زمانی که مصرف‌کننده مایل به حذف یک سرویس از یک دستگاه است و یا زمانی که مایل به دور انداختن دستگاه است، داده‌های شخصی بتواند به‌راحتی از آنها حذف شود. [۱۵]

قانون- لازم است به مصرف‌کننده دستورالعمل روشنی درخصوص چگونگی پاک نمودن اطلاعات شخصی خود داده شود. [۱۵]

قانون- لازم است به مصرف‌کننده تأیید شفافی جهت اینکه اطلاعات شخصی او از خدمات، دستگاه‌ها و اپلیکیشن‌ها حذف گردیده است، ارائه شود. [۱۵]

اغلب دستگاه‌های اینترنت اشیا تغییر مالکیت می‌دهند و نهایتاً بازیافت و یا دور ریخته می‌شوند. مکانیزم‌هایی می‌توانند فراهم شوند تا این امکان را به مشتری ارائه دهند که بتواند آنها را کنترل کند و اطلاعات شخصی را از خدمات، دستگاه‌ها و اپلیکیشن حذف کند. هنگامی که یک مصرف‌کننده می‌خواهد داده‌های شخصی خود را به‌طور کامل حذف نماید، پیش‌بینی می‌کند که آنها نسخه‌های پشتیبان[2] را دربردارند که ممکن است ارائه‌دهنده سرویس آنها را نگهداری کرده باشد.

حذف اطلاعات شخصی از یک دستگاه و یا سرویس به‌سادگی با بازگرداندن تنظیمات آن به حالت کارخانه حاصل نمی‌شود. نمونه‌های بسیاری وجود دارد که در آن مصرف‌کننده مالک دستگاه نیست اما می‌خواهد اطلاعات شخصی خود را از دستگاه و تمامی سرویس‌های مرتبط چون سرویس‌های ابری و یا اپلیکیشن‌های موبایل حذف نماید. به‌عنوان نمونه، کاربری را در نظر بگیرید که به‌طور موقت از دستگاه‌های اینترنت اشیا مصرف‌کننده در یک خانه اجاره‌ای استفاده می‌کند. با اجرای بازگشت به حالت کارخانه محصول، می‌توان تنظیمات پیکربندی را حذف کرده و یا دستگاه را غیرفعال نمود که این به‌ضرر مالک آپارتمان و یا کاربر آینده است. پاک کردن تمامی داده‌های شخصی در این خصوص، مکانیزم فنی نامناسبی خواهد بود.

۱۲-۲-۳. آسان کردن نصب و نگه‌داری دستگاه‌ها

قانون- لازم است به‌منظور نصب و نگه‌داری دستگاه‌های اینترنت اشیا، حداقل مراحل ممکن در نظر گرفته شود و بهترین عمل امنیتی درخصوص قابلیت استفاده دنبال شود. همچنین لازم است به مصرف‌کننده یک راهنما درخصوص چگونگی تنظیمات ایمن دستگاه خود نیز ارائه گردد. [۱۵]

مسائل امنیتی با سردرگمی مصرف‌کننده یا تنظیمات نادرست ایجاد می‌شوند که می‌توانند با

---

[1] Log

[2] Backup

پرداختن صحیح به پیچیدگی و طراحی مناسب رابط کاربری آنها را کاهش داد و یا در بعضی مواقع آنها را برطرف کرد. راهنمایی شفاف کاربران درخصوص چگونگی تنظیم دستگاه‌ها به‌صورت امن همچنین می‌تواند در معرض خطر قرار گرفتن آنها را کاهش دهد.

۱۳-۲-۳. اعتبارسنجی داده‌های ورودی

قانون- لازم است داده‌های ورودی از طریق رابط‌های کاربری[۱] و انتقال از طریق API[۲]ها یا بین شبکه‌ها در سرویس‌ها و دستگاه‌ها اعتبارسنجی گردد. [۱۵]

سیستم‌ها ممکن است ازطریق داده‌های فرمت شده یا کدی که در میان انواع مختلف اینترفیس‌ها منتقل می‌شود، آسیب ببینند. اغلب ابزارهای خودکار توسط مهاجمان به‌منظور سوء استفاده از شکاف[۳]ها و ضعف‌های احتمالی به‌کار گرفته می‌شوند که درنتیجه عدم اعتبارسنجی داده‌ها پدید می‌آید. در ادامه مثال‌هایی ذکر می‌شود (اما به آنها محدود نمی‌شود)، داده‌هایی که عبارتند از:

- عدم نوع مورد انتظار: برای مثال کد قابل اجرا و نه متن ورودی کاربر.
- خارج از محدوده: برای مثال مقدار دمایی که بیشتر از محدوده اندازه‌گیری یک سنسور است.

فصل چهارم ـ چارچوب پیشنهادی برای مقرراتگذاری اینترنت اشیا در کشور

در این قسمت براساس یافته‌های قسمت‌های قبلی گزارش، چارچوبی برای مقرراتگذاری اینترنت اشیا در کشور پیشنهاد می‌شود. این چارچوب از چهار حوزه زیر تشکیل می‌شود:

۱. **نحوه اعمال قوانین به اینترنت اشیا:** بدین‌معنا که قوانینی که در ابتدا برای ارتباطات بین انسان‌ها طراحی شده‌اند در کاربردهای اینترنت اشیا نیز همان موارد اعمال می‌شوند، ازاین‌رو، هزینه انجام کسب‌وکار افزایش پیدا می‌کند و سبب تأخیر در پیاده‌سازی این فناوری می‌شود.

۲. **امنیت و حفاظت از داده و مصرف‌کننده:** برنامه‌های نرم‌افزاری در دستگاه‌های اینترنت اشیا مصرف‌کنندگان باید به‌طور امن و در زمان به‌موقع قابل به‌روزرسانی شوند تا از آسیب‌پذیری‌های نرم‌افزار جلوگیری شود. برقراری هر انتقال داده باید به‌صورت امن و رمزگذاری شده باشد تا در مقابل حملات نیز مقاوم باشد. درنظر گرفتن قوانینی برای حفاظت از داده‌های اینترنت اشیا سبب ایجاد امنیت و حفظ حریم خصوصی افراد خواهد شد. دستگاه‌های اینترنت اشیا برای فعالیت‌های پردازش داده لازم است تا رضایت کافی پیرامون داده را به‌صورت صریح و بدون ابهام از کاربران کسب کنند. پردازش داده‌های شخصی و رضایت مربوط به آن برای کودکان نیز باید قانونگذار به‌صورت صریح مشخص کند. دستورالعمل‌ها و مقرراتی مربوط به حفاظت از

---

[۱] User Interfaces

[۲] Application Programming Interface

[۳] Gap

مصرف‌کنندگان در اینترنت اشیا برای حوزه‌هایی ازقبیل آزاد بودن جریان داده‌های غیرشخصی، امنیت سایبری، حفاظت از داده، امنیت شبکه و سیستم‌های اطلاعاتی، حقوق مصرف‌کننده، مسئولیت محصول و مواردی از این دست مورد نیاز است. تولیدکنندگان دستگاه‌ها و ارائه‌دهندگان سرویس درخصوص اینکه اطلاعات شخصی مصرف‌کنندگان، توسط چه فردی و با چه هدفی استفاده می‌شود باید به آنها اطلاعات صریح و روشنی ارائه کنند و اطمینان ایجاد نمایند که اطلاعات شخصی آنها محافظت می‌شود.

۳. بی‌طرفانه بودن فناوری: یک تفاوت بی‌مورد در برخورد با فناوری‌های مختلف وجود دارد. به دلایل تاریخی، اغلب قوانین مختلف برای کاربردهای اینترنت اشیا متناظر با اینکه آنها ازطریق فناوری‌های سلولی یا فناوری‌های غیرسلولی به شبکه متصل هستند، اعمال می‌شوند. برخی از سیاست‌های بخش صنعت به‌صراحت طرفدار فناوری‌های غیرسلولی هستند. این موارد به‌طور قابل توجهی گزینه‌های سرمایه‌گذاری را با مشکل مواجه می‌کنند و مانع توانمندی‌های کشور در حفظ برتری خود در نوآوری و پذیرش اینترنت اشیا در میان رقبای منطقه‌ای خود می‌شود.

۴. مسئولیت و اتخاذ بهترین شیوه‌ها: درباره اشتراک داوطلبانه از داده‌های غیرشخصی تولید شده توسط دستگاه و تأکید قراردادی روی حل مسائل بالقوه پیرامون مسئولیت اینترنت اشیا که می‌تواند سبب تقویت رقابت‌پذیری در کشور و اعتماد کاربر نهایی در اینترنت اشیا شود، لازم است تا بهترین شیوه‌ها اتخاذ شوند. با ترویج این بهترین شیوه‌ها، حذف مسئولیت‌های غیرضروری و تضمین محرمانگی به مصرف‌کننده و کسب‌وکار ازطریق مقررات مؤثر، چارچوب جدید اقتصاد داده را ترویج خواهد کرد و سبب رشد بیشتر و افزایش منافع کسب‌وکارها و مصرف‌کنندگان خواهد شد. همچنین مسئولیت همه بازیگران در زنجیره ارزش اینترنت اشیا باید به‌طور صریح مشخص شود تا در زمان اتفاقی یک محصول مبتنی‌بر اینترنت اشیا منجر به خسارت شود مسئول این رویداد برای رسیدگی کاملاً مشخص باشد. ازاین‌رو، مسئولیت در رابطه با پیدایش موارد کاربردی ازجمله هواپیماهای بدون‌سرنشین یا خودروهای خودران باید به‌طور روشن در قوانین به‌طور شفاف بیان شود.

جمع‌بندی

ارزشی که اینترنت اشیا می‌تواند برای کشور به ارمغان آورد بسیار قابل توجه خواهد بود، از افزایش رشد تولید ناخالص داخلی (GDP) در اشتراک‌گذاری داده‌های غیرشخصی تولید شده توسط دستگاه‌ها گرفته تا زندگی بهتر ازطریق هوشمندسازی فرایندهایی که مردم در زندگی روزانه با آنها سروکار دارند و همچنین هوشمندسازی صنایع مختلف و ایجاد توسعه پایدار. اگر چشم‌انداز مقرراتی درستی وجود داشته باشد، تحقق این مزایا می‌تواند جایگاه کشور را در مقیاس جهانی و منطقه به‌طور قابل توجهی بهبود بخشد.

سیاست‌ها و مقررات مربوط به اینترنت اشیا هنوز در مرحله توسعه هستند و در بخش‌های مختلف گسترده شده‌اند. از یک‌سو، درخصوص موارد مهمی که باید در مقررات مرتبط با اینترنت اشیا در کشور اصلاح شوند و یا ارتقا یابند می‌توان به موارد زیر اشاره کرد:

○ مجوزدهی (تجمیع‌کننده‌های[۱] جدید اینترنت اشیا و دامنه مجوز)،

○ طیف فرکانسی (مقررات براساس سرویس و همچنین فناوری تغییر خواهند کرد، مانند فناوری‌های برد بلند[۲] در مقابل فناوری‌های برد کوتاه[۳]؛ همچنین مقررات براساس باند فرکانسی مورد استفاده (باند دارای مجوز در مقابل باند آزاد) نیز تغییر خواهند کرد)،

○ شماره‌گذاری و آدرس‌دهی (شناسه اینترنت اشیا)،

○ رومینگ بین‌المللی،

○ قابلیت همکاری و استانداردها،

○ حفاظت از داده، حریم خصوصی، حفاظت از مصرف‌کننده و امنیت،

○ رقابت (رقابت پلتفرم)،

○ حق استفاده از املاک دیگران: استفاده از مبلمان شهری.

ازسوی‌دیگر، لازم است تا در رابطه با موارد مهم زیر نیز مقرراتی پیرامون اینترنت اشیا وضع شود:

- مالکیت داده‌ها،
- حقوق مربوط به استفاده از مشتقات داده‌ها،
- حقوق تصمیم‌گیری پویا (تغییر در رضایت)،
- آگاهی مصرف‌کننده،
- حقوق حریم خصوصی،
- امنیت سایبری،
- مسئولیت (تصمیماتی که توسط هوش مصنوعی گرفته شده است به‌ویژه در حوزه سلامت و حمل‌ونقل)،
- استانداردهای دقیق و قابل اطمینان،
- آموزش،
- دفع زباله‌های الکترونیکی،
- جلوگیری از انحصار چندجانبه (تصرف شرکت‌های فناوری بزرگ)،
- امانت‌داری (مانند سرویس‌های مالی).

ازاین‌رو، کشور به یک چارچوب مقرراتی «طراحی شده برای اینترنت اشیا» نیاز دارد که موانع غیرضروری و غیرعمدی را حذف کند، بی‌طرفی فناوری را تضمین کند، نیازهای اینترنت اشیا را برآورده سازد، فرصت‌های دیجیتالی را برای افراد و کسب‌وکارها باز کند و کشور را به‌عنوان یک پیشتاز در حرکت به‌سمت جامعه دیجیتال قرار دهد.

---

[۱] Aggregators

[۲] LoRaWAN، سیگفاکس و اینترنت اشیا باند باریک.

[۳] RFID، بلوتوث و وای فای.

در این گزارش براساس بررسی‌های انجام شده یک چارچوب برای مقررات‌گذاری اینترنت اشیا مشتمل بر چهار بخش کلیدی پیشنهاد شد:

۱. نحوه اعمال قوانین به اینترنت اشیا،

۲. امنیت و حفاظت از داده و مصرف‌کننده برای حوزه‌هایی ازقبیل آزاد بودن جریان داده‌های غیرشخصی، امنیت سایبری، حفاظت از داده، امنیت شبکه و سیستم‌های اطلاعاتی، حقوق مصرف‌کننده، مسئولیت محصول،

۳. بی‌طرفانه بودن فناوری و پرهیز از برخی سیاست‌های بخش صنعت که به‌صراحت طرفدار فناوری‌های غیرسلولی هستند،

۴. مسئولیت و اتخاذ بهترین شیوه‌ها در رابطه با اشتراک داوطلبانه داده‌های غیرشخصی تولید شده توسط دستگاه و تأکید قراردادی بر روی حل مسائل بالقوه پیرامون مسئولیت اینترنت اشیا که می‌تواند سبب تقویت رقابت‌پذیری در کشور و اعتماد کاربر نهایی در اینترنت اشیا شود.

پی‌نوشت‌ها

[1] Ismail Shah, Policies and Regulations Pertaining to IoT, ITU, 2018.
[2] GSR discussion paper Regulation and the Internet of Things, 2015.
[3] Data Protection Regulations and International Data flows: Implications for trade and development, United Nations Conference on Trade and Development (UNCTAD) Report, 2016.
[4] A new IoT Regulatory Framework for Europe, Vodafone, White Paper, June 2019.
[5] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51633
[6] https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data ownership-interoperability-re-usability-and-access-data-and
[7] https://eur-lex.europa.eu/legal-content/EN/TXTPDF/?uri=CELEX:52018SC0125&rid=2
[8] https://www.privacyshield.gov/Program-Overview
[9] GDPR and the Internet of Things: 5 Things You Need to Know, McCann FitzGerald, European Union, May 2016.
[10] IDC, Customer Insights and Analysis, 2019.
[11] Analysys Mason, IoT forecast: connections, revenue and technology trends 2018–2027, March 2019.
[12] IoT measurement and applications, OECD Digital Economy Papers, No. 271, October 2018.
[13] Ericsson Mobility Report, June 2019.
[14] BEREC Report on Internet of Things indicators, BoR (19) 25, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8464-berec-report-on-internet-of-things-indicators
[15] Cyber; Cyber Security for Consumer Internet of Things, ETSI Technical Specification, TS 103 645 v1.1.1, 2019.

مرکز پژوهش‌ها
مجلس شورای اسلامی

شناسنامه گزارش

شماره مسلسل: ۱۷۰۱۲

عنوان گزارش: اینترنت اشیاء (۳): چارچوب مقرراتگذاری، امنیت سایبری و مقرراتگذاری داده در اینترنت اشیا برای ایران

نام دفتر: مطالعات انرژی، صنعت و معدن (گروه فناوری اطلاعات و ارتباطات)

مدیر مطالعه: پریسا علیزاده

تهیه و تدوین: محسن بنار

ناظران علمی: حسین افشین، علی‌اصغر اژدری

ویراستار تخصصی: ــــــــ

ویراستار ادبی: ــــــــ

واژه‌های کلیدی:

۱. امنیت سایبری
۲. اینترنت اشیا
۳. مقرراتگذاری

تاریخ انتشار: ۱۳۹۹/۲/۱۰