Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/MTLJ.2022.361434.1123

Requirements for Exercising the Right to Privacy in the Field of Internet of Things in Iran's law

Mohaddeseh Moeinifar[1]*, Delaram Vahidzadeh[2]

[1] Assistant Professor of Theology and Islamic Thought (Islamic Jurisprudence and Fundamentals of Islamic law)/Faculty of Islamic Sciences and Researches/ Imam Khomeini International University (IKIU), Qazvin, Iran

[2] M.A. in Financial and Economic Law/ Faculty of Law/ Islamic Azad University Central Tehran Branch, Tehran, Iran

Article Info

Original Article

Received:
09-09-2022

Accepted:
03-11-2022

Keywords:
Internet of Things
Internet
Right
Privacy
Iran

Abstract

The Internet of Things is the technology of connecting things, humans and animals in a network that has wide dimensions in current human life. Its importance has increased as the issue of protecting people's rights, such as protecting their privacy, has grown. Accordingly, this paper's fundamental question is the relationship between the right to privacy as a human right and the right to the internet of things in Iran's legal system. The right to privacy is one of the first-generation rights that conflict with the right to enjoy the Internet of Things. The second right relates to economic and social rights, whose proof was disputed under international law. In addition, the rank of this right was lower compared to other examples of social and economic rights. In the future, it may be possible to ignore the fulfilment of the right to privacy if it becomes one of the necessities of human life. The content of the right to privacy in the area of the Internet of Things included the management and monitoring of one's data on the one hand and, on the other hand, compliance with security in the three areas: security of the Internet of Things systems and related systems against hacking and intrusion, security and observance of the principles during the legal collection of data and security during the storage and use of data. In addition, they should observe legal and ethical principles during collecting and using personal data in Iran. Other examples of violating individuals' privacy rights in the field of the Internet of Things in Iran are insulting people, obtaining unauthorised access to data on the Internet of Things system, making data publicly available, deleting or destroying data, disrupting or disabling Internet of Things systems, etc. We conclude that approving laws and cultural policies is the best solution to support this right.

***Corresponding author**
e-mail: moeinifar@isr.ikiu.ac.ir

How to Cite:
Moeinifar, M., & Vahidzadeh, D. (2022). Requirements for Exercising the Right to Privacy in the Field of Internet of Things in Iran's law. *Modern Technologies Law*, *3*(6), 61-75.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

حقوق فناوری‌های نوین، ۱۴۰۱، ۳(۶) https://www.mtlj.usc.ac.ir

حقوق فناوری‌های نوین

http://doi.org/10.22133/MTLJ.2022.361434.1123

الزامات استیفای حق بر حریم خصوصی در بستر اینترنت اشیا از منظر حقوق ایران

محدثه معینی‌فر[1]*، دل‌آرام وحیدزاده[2]

[1] استادیار گروه فقه و حقوق اسلامی، دانشکدهٔ علوم و تحقیقات اسلامی، دانشگاه بین‌المللی امام خمینی (ره)، قزوین، ایران

[2] کارشناس ارشد حقوق مالی ـ اقتصادی، دانشکدهٔ علوم انسانی، دانشگاه آزاد اسلامی، تهران، ایران

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۶/۱۸

تاریخ پذیرش:
۱۴۰۱/۸/۱۲

واژگان کلیدی:
اینترنت اشیا
اینترنت
حق
حریم خصوصی
ایران

چکیده

اینترنت اشیا فناوری به‌هم‌رساندن اشیا، انسان‌ها و حیوانات در یک شبکه است که به‌علت ابعاد گسترده‌ای که در زندگی کنونی بشر دارد، بسیار حائز اهمیت است و این اهمیت در موضوع حفظ حق‌های افراد مانند حفظ حریم خصوصی آن‌ها بیشتر است. بر همین مبنا، سؤال اساسی این پژوهش نسبت میان استیفای حق حریم خصوصی به‌منزلهٔ حق بشری و استیفای حق بر اینترنت اشیا در نظام حقوقی ایران است. حق حریم خصوصی از انواع حق‌های نسل اول است که در تزاحم با حق بهره‌مندی از اینترنت اشیا قرار گرفته است. حق دوم در زمرهٔ حق‌های اقتصادی و اجتماعی است که اثبات آن در حقوق بین‌الملل محل نزاع است. به‌علاوه، رتبهٔ این حق در مقایسه با سایر مصادیق حق‌های اجتماعی و اقتصادی پایین‌تر است، اما اگر استیفای این حق از ضروریات زندگی بشر در آینده شود، شاید بتوان از استیفای حق حریم خصوصی چشم‌پوشی کرد. محتوای حق حریم خصوصی در حوزهٔ اینترنت اشیا شامل مدیریت و نظارت فرد بر داده‌های شخصی خود از یک‌سو و از سوی دیگر، رعایت امنیت در سه حوزهٔ امنیت خود سامانه‌های اینترنت اشیا و سامانه‌های مرتبط با آن در مقابل هک و نفوذ، امنیت و رعایت اصول در هنگام جمع‌آوری قانونی داده‌ها و امنیت در هنگام نگه‌داری و استفاده از داده‌ها است و مصادیق نقض حق حریم خصوصی افراد در حوزهٔ اینترنت اشیا در قوانین ایران شامل هتک حرمت و حیثیت افراد، دسترسی غیرمجاز به داده‌ها در سیستم اینترنت اشیا، در دسترس قراردادن داده‌های موجود در سیستم اینترنت اشیا، حذف یا تخریب یا مختل یا غیرقابل پردازش کردن داده‌های موجود در سیستم اینترنت اشیا، ازکارانداختن یا مختل‌کردن سامانه‌های اینترنت اشیا و... است که بهترین راهکار برای حمایت از این حق در برابر نقض آن، تصویب قوانین و سیاست‌گذاری‌های فرهنگی است.

* **نویسندهٔ مسئول**

رایانامه: moeinifar@isr.ikiu.ac.ir

نحوهٔ استناددهی:

معینی‌فر، محدثه و وحیدزاده، دل‌آرام (۱۴۰۱). الزامات استیفای حق بر حریم خصوصی در بستر اینترنت اشیا از منظر حقوق ایران. *حقوق فناوری‌های نوین*، ۳ (۶)، ۷۵-۶۱.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

مقدمه

فناوری شمشیر دولبه‌ای است که منافع و مضراتی دارد. این موضوع در مورد اینترنت اشیا نیز صادق است. با توجه به گسترهٔ جرائم رایانه‌ای که غالباً با تضییع حقوق افراد همراه است، معرفی فناوری اینترنت اشیا نیز ممکن است بر دامنهٔ این جرائم بیفزاید؛ یعنی افزایش این جرائم که در قالب سوءاستفاده از این فضا پیش خواهد آمد پیوند عمیقی با حفظ حقوق افراد دارد.

اینترنت اشیا ارتباط اشیای دیجیتالی با استفاده از اینترنت است که سهم بسیار زیادی در تبادل اطلاعات و ارتباطات بین افراد دارد، بدون آن‌که میان انسان‌ها ارتباطی مستقیم و رودررو برقرار شود و حتی بدون دخالت و نظارت مستقیم بر آن‌ها. ناتوانی در مدیریت این اشیا این موضوع را به موضوعی مهم بدل کرده است، زیرا این وضعیت ایجاب می‌کند که در این فضا از زندگی فردی و اجتماعی افراد به‌نحوی محافظت و حمایت شود که ضمانت اجرا داشته باشد و این خواسته فقط با توسل به قانون و تصویب قوانین در این خصوص توسط قانونگذار محقق می‌شود. پرداختن به اینترنت اشیا در قوانین کشورها، با توجه به گسترش کاربرد اینترنت و اهمیت آن در زندگی روزمره و اجتماعی افراد، بسیار مهم و دارای آثار مالی، اجتماعی، حقوقی و فردی بسیاری خواهد بود. برای نمونه، «اتحادیهٔ اروپا در سال ۲۰۱۶، با بازنگری سند EU/46/95 سال ۱۹۹۵، حمایت افراد در برابر پردازش داده‌های شخصی و انتقال آن را مورد تأکید قرار داد و برابر این سند، حق استفاده و پردازش داده‌های شخصی، بدون کسب رضایت صریح شخص، غیرمجاز است و در صورت کسب اجازه هم صرفاً برای هدف مورد رضایت شخص می‌تواند مورد بهره‌برداری قرار گیرد که مفاد این سند، با استقبال اکثر کشورهای جهان به‌استثنای کشورهای معدودی، مانند آمریکا همراه شد و آن کشورها، قوانین و مقررات خود را در حمایت از داده‌های شخصی، مطابق با این سند تصویب یا اصلاح کردند» (رئیسی و قاسم‌زاده، ۱۳۹۹، ص ۱۳۰). بر همین مبنا، هدف از این پژوهش بررسی حقوقی وضعیت قوانین ایران دربارهٔ حق حریم خصوصی در حوزهٔ اینترنت اشیا است.

با مروری بر پژوهش‌های پیشین دربارهٔ اینترنت اشیا باید اذعان کرد که عمدهٔ پژوهش‌ها بر محور توضیح ابعاد فناورانهٔ آن انجام شده و کمتر مقاله‌ای است که ابعاد حقوقی این مسئله را بررسی کرده باشد. مقالات حوزهٔ حریم خصوصی و اینترنت اشیا نیز بسیار محدود است. همین موضوع اهمیت این پژوهش را نشان می‌دهد. در ذیل به برخی از پژوهش‌های صورت‌گرفته اشاره می‌شود:

اقدسی و محقق داماد (١٤٠٠) در مقاله‌ای با عنوان «ابعاد حقوقی حریم خصوصی در اینترنت اشیا»، پس از بیان مسئله، به تعریف مفاهیمی چون اینترنت اشیا و حریم خصوصی پرداخته‌اند و ذیل عنوان تهدیدهای امنیتی در فضای اینترنت اشیا به مصادیق فنی و فناورانهٔ این تهدیدات اشاره کرده‌اند. سپس از حق انتخاب، کاربری آسان، اطلاع‌رسانی، بازبینی و ضمانت اجرا و جبران خسارت با عنوان شاخص‌های حریم خصوصی در اینترنت اشیا و دربارهٔ حق دانستن، ممنوعیت قانونی، امنیت فناوری اطلاعات، بهره‌برداری، نیروی الزام‌آوری، جهان‌شمولی، ماندگاری، فراگیری و استانداردهای فنی بحث کرده‌اند. درنهایت، پس از طرح حمایت‌های بین‌المللی از این حق، پیشینهٔ این حق را با محوریت قانون تجارت الکترونیک مطرح کرده‌اند. به‌نظر می‌رسد، علاوه‌بر تفاوت روال بحث در این دو مقاله، در مقالهٔ پیش‌رو تأکید بر قانون جرائم رایانه‌ای است و راهبردهای حل مسئله از منظری دیگر بررسی شده‌اند.

آقایی طوق و ناصر (۱۳۹۹)، در مقاله‌ای با عنوان «چالش‌های حفاظت از داده‌های خصوصی در حوزهٔ اینترنت اشیا: مطالعهٔ تطبیقی حقوق ایران و اتحادیهٔ اروپا»، تلاش کرده‌اند چالش‌های مختلف اینترنت اشیا مانند امکان افشای اطلاعات خصوصی اشخاص یا تحدید حقوق مالکانهٔ آن‌ها یا حتی روابط میان پردازنده و کنترل‌کننده و مسئلهٔ مسئولیت مدنی آن‌ها در برابر مصرف‌کنندگان را بررسی کنند. آنان درنهایت نتیجه گرفته‌اند که مدیریت این چالش‌ها نیازمند برخورداری از نظام حقوقی مشخصی است که بتواند احکام لازم را در راستای مدیریت مسائل مربوط به اینترنت اشیا در خود جای دهد. قانونگذار ایران می‌تواند تجربهٔ مقررات‌گذاری اتحادیهٔ اروپا در این خصوص را مدنظر قرار دهد.

فرحزادی و ناصر (۱۴۰۰) ،در مقاله‌ای با عنوان «حق بر تبادل داده‌های خصوصی و راهکارهای رفع چالش‌های آن در سازوکار عملکرد ابزارهای اینترنت اشیا»، پژوهش خود را با این پیش‌فرض به انجام رساندند که مطابق با مفاد مادهٔ ۲۰ آیین‌نامهٔ عمومی حفاظت از اطلاعات اتحادیهٔ اروپا مصوب ۲۰۱۶، حق بر تبادل داده‌های خصوصی به‌منزلهٔ انتقال حق نظارت و کنترل اطلاعات جمع‌آوری‌شده از سوی ابزار اینترنت

اشیا از کنترل‌کنندهٔ اولیه به ثانویه است. از دیدگاه آنان، اجرای این حق با چالش‌هایی مانند محدودهٔ اجرای مقررات حق مزبور، استثنائات حاکم بر اصول مقدماتی اجرای حق مزبور و سازوکار تبادل بدون بازگشت پردازش داده‌های خصوصی اشخاص از یک کنترل‌کننده به کنترل‌کنندهٔ دیگر روبه‌رو است. آنان درنهایت نتیجه گرفته‌اند که اجرای این حق در نظام حقوقی ایران منوط به اجرای برخی سیاست‌گذاری‌های تقنینی ازجمله اصلاح قوانین موجود، پیاده‌سازی زیرساخت‌های به‌کارگیری ابزارهای اینترنت اشیا، آگاهی‌بخشی به مردم و نظارت مراجع صلاحیت‌دار است. این دو پژوهش نیز بیشتر بر قوانین اروپا در این حوزه تمرکز داشته‌اند و کمتر به قوانین ایران در این زمینه توجه کرده‌اند.

بر همین مبنا، سؤال اساسی این پژوهش نسبت میان استیفای حق حریم خصوصی به‌منزلهٔ حق بشری و استیفای حق بر اینترنت اشیا در نظام حقوقی ایران است و فرضیات آن نیز به شرح زیر است:

هرچند در نظام حقوقی ایران به موضوع حق حریم خصوصی افراد اهمیت داده شده است، اما اصل به‌روزبودن قوانین برای حمایت از حق‌های افراد ایجاب می‌کند که قانونگذار، با معرفی فناوری‌های نوین مانند اینترنت اشیا، قوانین کارآمد و متناسب با آن را به تصویب برساند تا افراد در تزاحم میان استیفای حق حریم خصوصی و حق بهره‌مندی از اینترنت اشیا آسیب نبینند.

مفهوم اینترنت اشیا و کاربردهای آن

هرچند به‌علت نوپایی و وجود طیف گسترده‌ای از اینترنت اشیا تعریف یکسانی از آن در جهان وجود ندارد (Poudel, 2016, p.1000)، به برخی تعاریف از آن اشاره می‌شود. اصطلاح اینترنت اشیا سامانه‌ای متشکل از حس‌گرهای شبکه و محرک‌ها و اشیای هوشمند را توصیف می‌کند که هدف آن‌ها اتصال همه‌چیز، شامل اشیا، در زندگی روزمره و صنعت است، به‌گونه‌ای که آن‌ها را هوشمند، قابل‌برنامه‌ریزی و توانمندتر در تعامل با انسان و سایر ابزارها می‌نماید. همچنین، اینترنت اشیا فناوری‌ای است که دستگاه‌های محاسباتی قابل‌شناسایی را قادر می‌سازد که از طریق شبکه‌ها (سیمی یا غیرسیمی) به رابط‌های دیگر (مانند انسان‌ها و ماشین‌ها) متصل شوند تا با هدف جمع‌آوری داده‌ها از محیطی که در آن به‌کار گرفته شده است شبکه‌ای اطلاعاتی برای ارائهٔ مدل‌های تجاری، خدماتی و عملکردهای جدید الکترونیکی ایجاد کند (Fornasier, 2019, p.298-299).

در تعریفی دیگر، اینترنت اشیا را چنین توصیف کرده‌اند: «دنیای امروز متشکل از مجموعه‌ای از اشیای فیزیکی شامل ماشین‌آلات، کالاها، زیرساخت‌ها و دستگاه‌هایی است که با شبکه‌ای از حسگرها و عامل‌های هوشمند تجهیز شده‌اند و این امر آن‌ها را به فعالیت‌هایی نظیر نظارت بر محیط، گزارش وضعیت، دریافت دستورالعمل‌ها و حتی نشان‌دادن عکس‌العمل بر اساس اطلاعات جمع‌آوری‌شده قادر می‌سازد.» (فقیهی و نافعی، ۱۳۹۵، ص ۳)

برخی نیز در تعریفی کلی آن را مظهر شبکه‌ای فراگیر می‌دانند که در هر زمان، هر مکان، هر کسی و هر وسیله‌ای را با استفاده از هر مسیر یا شبکه و هر سرویسی به هم متصل می‌کند (Poudel, 2016, p.1009). تعاریف اینترنت اشیا را می‌شود به چند گروه تقسیم کرد: گروه نخست بر موضوع ارتباط اشیا باهم از طریق اینترنت بدون مداخلهٔ انسان تأکید دارد، درحالی‌که گروه دوم بر فناوری‌هایی تأکید دارد که اینترنت اشیا بر اساس آن‌ها شکل می‌گیرد.

فناوری اینترنت اشیا اساساً از سه عنصر تشکیل شده است: ۱) دستگاه‌های هوشمند، ۲) پروتکل‌هایی برای تسهیل ارتباط بین دستگاه‌های هوشمند و ۳) سامانه‌ها و روش‌های ذخیره‌سازی و تجزیه‌وتحلیل داده‌های به‌دست‌آمده توسط دستگاه‌های هوشمند (Robinson, 2015, p.657). اینترنت اشیا، در زندگی افراد و جامعه، در مواردی چون حوزهٔ تبلیغات محصولات و رونق کسب‌وکار، حوزهٔ هواشناسی و حمایت از جان افراد و سرمایه‌های کشور، حوزهٔ سلامت و تجهیزات پزشکی، حوزهٔ خدمات حمل‌ونقل، منازل هوشمند، حوزهٔ ورزش، حوزهٔ آموزش و شهر هوشمند کاربرد دارد.

ماهیت حق حریم خصوصی افراد در بستر اینترنت اشیا

برای تبیین ماهیت حق حریم خصوصی در حوزهٔ اینترنت اشیا بهتر است به تقسیم حق از نظر تاریخ پیدایش آن توجه کرد. حق‌های نسل نخست، یعنی حق‌های مدنی و سیاسی، عمدتاً از جنس حق‌های سلبی‌اند که نباید مانع اجرای آن‌ها توسط صاحبان حق شد. این حق‌ها همان آزادی‌های سنتی و امتیازات شهروندی‌اند.

حق‌های نسل دوم حق‌های اجتماعی و اقتصادی و به‌طور عمده از جنس حق‌های ایجابی‌اند که تحقق آن‌ها منوط به فراهم‌آمدن مجموعه‌ای از شرایط و امکانات است. این ادعاهای اجتماعی و اقتصادی شامل حق آموزش، مسکن، مراقبت‌های بهداشتی، اشتغال و سطح مناسب زندگی است.[1] هر دو نوع این حق‌ها در این مشترک‌اند که صاحبان آن‌ها افرادند (حق‌های فردی)؛ اما حق‌های نسل سوم حق‌هایی هستند که ادعا می‌شود جامعه از حیث جامعه‌بودن صاحب آن‌ها است، مانند حق نسبت‌به محیط‌زیست (والدرون، ۱۳۸۱، ص ۱۵۸-۱۵۹). میثاق بین‌المللی حقوق مدنی و سیاسی و میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی به‌صورت جداگانه و نسبی دربارهٔ حق‌های نسل نخست و دوم بحث و از آن‌ها حمایت می‌کنند. در هر دوی این اسناد، به حق بهره‌مندی مردم از ثروت‌ها و منابع طبیعی کامل و آزادانه اشاره شده است که می‌شود آن را بنیانی برای این گروه حق‌ها به‌شمار آورد، هرچند این نسل از حق‌ها همچنان در حال پیشرفت است (Robb, 1998, p.286). اگرچه این‌گونه پنداشته می‌شود که حق‌های نسل دوم ادعاهای رادیکال‌تری هستند که موجب پیدایش دولت مداخله‌جو[2] می‌شوند، به لحاظ محتوا اساساً حق‌های فردی‌اند؛ بدین معنا که این رفاه مادی هر فرد (زن یا مرد) است که باید به‌وسیلهٔ حقوق یادشده تضمین شود. به همین علت، دربارهٔ اصل وجود حق‌های مذکور تردید و نزاع وجود دارد (والدرون، ۱۳۸۱، ص ۱۵۸).

حق بر حریم خصوصی از انواع حق‌های نسل اول یا سلبی است؛ درحالی‌که حق بهره‌مندی از اینترنت اشیا در زمرهٔ حق‌های نسل دوم یا ایجابی است. حضور این دو حق در کنار هم مؤید وجود تزاحمی میان آن‌هااست، زیرا حق‌های نسل دوم غیرعملی و بسیار پرهزینه‌اند (مالایطاق) و بسیاری از دولت‌ها منابع کافی برای فراهم‌آوردن حداقل امنیت اقتصادی برای اکثریت شهروندان خود را ندارند، چه رسد به آن‌که زمینهٔ بهره‌مندی فردی هر شخص از اینترنت اشیا را در اماکن خصوصی فراهم آورند. البته بحث دربارهٔ استحقاق افراد نیست، بلکه باید میان دو مرحلهٔ استحقاق حق و استیفای آن تفاوت قائل شد؛ این بدان معنی است که افراد استحقاق برخورداری از این حق‌ها را در تمامی کشورها دارند، اما در مرحلهٔ استیفا موانعی وجود دارد که مانع دستیابی آنان به حق‌های خود می‌شود. پس این حق‌ها جهان‌شمول‌اند و همهٔ انسان‌ها استحقاق آن‌ها را دارند.

همچنین، ریشهٔ تزاحم میان این دو حق این است که از دیدگاه برخی «حق‌های نسل نخست فقط حکومت‌ها را از انجام اقدامات مستبدانه و خشونت‌آمیز گوناگون بازمی‌دارد؛ درنتیجه، حق‌هایی «منفی» یا سلبی‌اند که لازمهٔ تکلیف «ترک فعل»اند، حال آن‌که لازمهٔ حق‌های اجتماعی ـ اقتصادی تکلیف مثبت (ایجابی) به کمک است. یکی از مزایای حق‌های منفی این است که این حق‌ها هرگز باهم تعارض نمی‌کنند، زیرا انسان می‌تواند در هرزمانی بی‌نهایت ترک فعل انجام دهد، ولی در مورد حق‌های مثبت همیشه باید مسئلهٔ کمبود منابع و خدمات لازم را مدنظر قرار داد» (والدرون، ۱۳۸۱، ص ۱۷۵). در پاسخ باید گفت، «تلازم میان حق‌های نسل نخست و دوم به‌ترتیب با تکالیف ترک فعل و تکالیف مثبت به کمک همیشه درست نیست. بسیاری از حق‌های نسل نخست (مانند حق رأی) مستلزم تلاش بسیار برای برپایی و نگه‌داری چارچوب‌های سیاسی است. تکالیف ملازم با حق‌های نسل دوم نیز با توجه به شرایط می‌توانند تکالیف مثبت یا منفی باشند» (والدرون، ۱۳۸۱، ص ۱۷۵).

از مجموع آنچه بیان شد، چند نکته قابل‌بیان است:

۱. هرچند حق حریم خصوصی از انواع حق‌های نسل اول است، لوازم استیفای آن محدود به ترک فعل نیست، بلکه نیازمند انجام تکالیف مثبت از سوی دولت‌ها است تا در حوزهٔ اینترنت اشیا این حق به‌خوبی استیفا شود.

---

۱. از این دو نوع حق با عناوین «حقوق انتخابی» (Option Rights) و «حقوق رفاهی» (Welfare Rights) نیز یاد می‌شود (گلدینگ، ۱۳۸۱، ص ۱۸۵)؛ اما در تعریف این دو حق باید گفت حقوق انتخابی اساساً با مفاهیم آزادی و انتخاب (دامنهٔ آزادی انتخاب فرد و عمل بر اساس آن انتخاب) و حقوق رفاهی با حق برخورداری از کالا یا منفعت معینی ارتباط دارند، مانند حق آموزش ابتدایی، حق مسکن مناسب و حق مراقبت‌های بهداشتی کافی (گلدینگ، ۱۳۸۱، ص ۱۹۰-۱۸۹).

2. Interventionist

۲. میان حق حریم خصوصی و حق بهره‌مندی از اینترنت اشیا نمی‌توان تزاحمی را تصور کرد؛ زیرا نخست، در اصل وجود حق‌های نسل دوم مانند حق بهره‌مندی از اینترنت اشیا تردید وجود دارد. دوم، برفرض وجود این نوع از حق‌ها، به‌نظر می‌رسد در مرتبه‌بندی میان انواع حق‌های نسل دوم، حق بهره‌مندی از اینترنت اشیا در مرتبه‌ای بسیار پایین‌تر از مصداقی چون حق تأمین امنیت اقتصادی برای مردم توسط دولت قرار دارد؛ بنابراین، حتی در صورت وجود تزاحم، قطعاً حق حریم خصوصی مقدم خواهد بود، مگر آن‌که زندگی بشر تا حد زیادی وابسته به این فناوری شود و با نبود آن مختل شود. سوم، استیفای حق‌های نسل دوم هزینه‌ای بسیار دارد که مانع اساسی استیفای این حق‌ها در عمل است و تزاحم هم درجایی واقع می‌شود که اساساً دو حکم (مانند دو حق) را نمی‌توان باهم به انجام رساند، زیرا در مرحلهٔ استحقاق این دو حق تزاحمی وجود ندارد. پس، بر اساس قاعدهٔ اهم و مهم در فقه و همچنین مادهٔ ۴ میثاق بین‌المللی حقوق مدنی و سیاسی، با توجه به شرایط و مقتضیات زمان و مکان می‌توان تقدم یکی از این دو حق را بر دیگری تعیین کرد. البته در فقه از روش‌های دیگر هم می‌توان برای حل تزاحم میان این دو بهره برد، مانند تقدم حقوق مربوط به حق حیات و حیثیت، استصحاب حق گذشته نسبت‌به حق فعلی، تقدم حق قوی‌تر بر حق دیگر، تقدم مصالح عامه بر مصالح خاصه و درنهایت، قاعدهٔ لا ضرر و لا ضرار فی الاسلام. با کمی تأمل می‌توان بر اساس تقدم حقوق مربوط به حق حیات و حیثیت، استصحاب حق گذشته نسبت‌به حق فعلی و تقدم حق قوی‌تر بر حق دیگر حق بر حریم خصوصی را مقدم دانست و بر مبنای دو راهکار دیگر می‌توان تقدم حق بهره‌مندی از اینترنت اشیا را انتخاب کرد. البته بهره‌بردن از قاعدهٔ لا ضرر در این تزاحم تقدم هریک را بر دیگری تأیید می‌کند، زیرا در هر دو طرف ضرر محتمل موجود است، اما این‌که کدام ضرر مهم‌تر دانسته شود، محل بحث خواهد بود.

۳. متعهد یا من علیه الحق در هردوی این حق‌ها دولت و سپس دیگران‌اند که تکلیف سلبی به عدم‌مداخله باید هم از سوی دولت و هم از سوی اشخاص حقیقی و حقوقی به اجرا درآید و تکلیف مثبت نیز از سوی دولت از طریق سیاست‌گذاری در دو حوزهٔ قانونگذاری و فرهنگی تحقق خواهد یافت. در اسناد بین‌المللی نیز بر انجام این دو نوع از تکلیف از سوی دولت‌ها تأکید شده است. البته دولت می‌تواند، با اتخاذ رویکردی میانه، شرکت‌های خصوصی تولیدکنندهٔ فناوری اینترنت اشیا را نیز در حوزهٔ سیاست‌گذاری وارد کند تا قوانین مطابق با پیشرفت فناوری متحول و اجرا شوند.

محتوای حق حریم خصوصی افراد در بستر اینترنت اشیا

تضمین امنیت خدمات و کاربردهای اینترنت اشیا در ایجاد اعتماد در کاربران و افزایش به‌کارگیری این بستر بسیار مهم است. کاربران باید اطمینان داشته باشند که اینترنت و تجهیزاتی که در حوزهٔ اینترنت اشیا به آن متصل است برای انجام فعالیت‌های برخط به‌اندازهٔ کافی در برابر تهدیدات موجود امن است.

هرچه سامانه‌های امنیتی و تجهیزات متصل به اینترنت پیشرفته‌تر و کارآمدتر باشند، به‌طوری‌که احتمال خطا و آسیب‌پذیری در آن‌ها کم باشد، همین‌قدر امنیت آن‌ها بیشتر می‌شود و سرقت اطلاعات کاربران و تخطی به حریم خصوصی و داده‌های آنان کمتر می‌شود؛ این درحالی است که تجهیزاتی که ازنظر امنیتی ضعیف‌اند مانع عملکرد صحیح سیستم و درنتیجه سرقت داده‌های کاربران خواهند شد. علاوه‌براین، این تجهیزات آسیب‌پذیری‌های امنیتی ایجاد می‌کنند یا آسیب‌پذیری امنیتی موجود را در برخی وسایل افزایش می‌دهند.

هر کاربر باید این امکان را داشته باشد که اطلاعاتی را که دوست دارد به اشتراک گذارد و آن‌هایی را که نمی‌خواهد، از دسترس دیگران خارج کند. همچنین، برای آن‌دسته از اطلاعاتی که در دسترس قرار می‌دهد این امکان وجود داشته باشد که به‌محض استفادهٔ دیگری حتماً در جریان استفاده از آن‌ها قرار گیرد و بتواند دسترسی بعضی از افراد و سازمان‌هایی را که نمی‌خواهد به آن‌ها محدود سازد. برای مثال، یک هکر می‌تواند از راه دور موجب اختلال در روند سفارش مصرف‌کننده شود، بدون این‌که هیچ ارتباط دیداری و شنیداری بین آن‌ها باشد و مسیر و جریان کار را به‌کلی دگرگون سازد یا می‌تواند وارد شبکهٔ بانکی شود و با هک‌کردن اطلاعات افراد ضررهای هنگفت مالی به افراد و نظام بانکی کشور و خسارت جبران‌ناپذیری به زندگی شخصی و اجتماعی افراد وارد کند.

همچنین، با توجه به کاربرد اینترنت اشیا در منازل و سایر اماکن خصوصی، علاوه‌بر اطلاعات خصوصی افراد، موضوع حریم جسمانی آنان نیز مطرح می‌شود. بنابراین، در صورت هک‌شدن سامانه‌های اینترنت اشیا در هر حوزه‌ای که کاربرد دارند، تعرض به حریم خصوصی افراد را می‌توان طی مراحل زیر تصور نمود:

۱. هک و نفوذ: نفوذ به معنای ورود غیرقانونی به سامانه‌های اینترنت اشیا است.

۲. جمع‌آوری داده‌ها: به معنای جمع‌آوری داده‌ها از منازل یا لوازمی چون ساعت یا سایر لباس‌های پوشیدنی است که ممکن است با اهداف مختلفی چون قتل، اخاذی و کلاه‌برداری مورد سوءاستفاده قرار گیرند.

۳. تغییر داده‌ها: تغییر داده‌ها ممکن است با اهدافی چون قتل، صدمات مالی به شرکت‌ها، تولیدکنندگان و حتی مصرف‌کنندگان، و کلاه‌برداری صورت گیرد.

٤. انتقال داده‌ها: انتقال داده‌ها در اینترنت اشیا ممکن است توسط خود شرکت تولیدکننده یا رقبای آن‌ها صورت گیرد که در هر صورت به‌علت رضایت‌نداشتن مشتری جرم تلقی می‌شود. به‌علاوه، موضوع انتقال داده‌های خصوصی افراد ممکن است به موضوعی در حوزهٔ امنیت ملی هم تبدیل شود و هر کشور طبق قواعد و مقررات خود می‌تواند مانع انتقال داده‌های مربوط به ملت خود به دیگر کشورها شود. برای نمونه، «استرالیا طبق قوانین خود اجازهٔ انتقال داده‌های مربوط به سلامت شهروندان خود را به سایر کشورها نمی‌دهد یا در کانادا انتقال اطلاعات شخصی افراد به خارج از کشور ممنوع است» (Chander, 2019, p.14). البته این نداشتن مجوز مضراتی دارد، مانند افزایش هزینهٔ ارائهٔ خدمات برای ایجاد سامانه‌های حفظ و نگه‌داری داده‌ها در هر کشور و همچنین، افزایش خطر هک یا نفوذ مجدد در سامانه‌های جدید (Chander, 2019, p.15).

۵. افشای غیرمجاز داده‌ها که ممکن است شامل تصاویر خصوصی افراد و سایر اطلاعاتی باشد که به فرد یا سازمان یا شرکتی تعلق دارد و می‌تواند حیات آن فرد یا سازمان یا شرکت را به خطر اندازد.

٦. استفاده از داده‌های جمع‌آوری‌شده برای هک و نفوذ در سامانه‌های دیگر.

۷. زیرنظرگرفتن افراد.

علاوه‌بر این موارد می‌توان این سه مورد را هم افزود: «سرقت هویت، جمع‌آوری نامحدود رسا و استفاده از تصمیم‌گیری الگوریتمی برای تصمیم‌گیری‌های بعدی» (Tschider, 2018, p.117). بر همین اساس، شاید بتوان با کمک منشور حق حریم خصوصی مصرف‌کننده[1] محتوای حق حریم خصوصی افراد را در حوزهٔ اینترنت اشیا شامل این موارد دانست:

۱. مدیریت ایمن و مسئولانهٔ اطلاعات و داده‌هایی که شرکت‌ها دربارهٔ افراد جمع‌آوری می‌کنند (McMeley, 2014, p.72; Smith, 2019, p.870)؛

۲. دسترسی آسان به اطلاعات مربوط به اقدامات امنیتی یک نهاد در حوزهٔ حریم خصوصی (McMeley, 2014, p.72)؛

۳. جمع‌آوری و بازیابی اطلاعات افراد فقط در موارد ضروری (McMeley, 2014, p.72)؛

٤. دسترسی به اطلاعات شخصی خود (Smith, 2019, p.870) و امکان اصلاح اطلاعات نادرست (McMeley, 2014, p.72)؛

۵. اعمال محدودیت‌های معقول در میزان داده‌هایی که جمع‌آوری و نگه‌داری می‌شود (McMeley, 2014, p.72)؛

٦. ضمانت اجرای مناسب برای استیفای این حق (McMeley, 2014, p.72)؛

۷. اطلاع از فروش یا افشای اطلاعات و همچنین، شخص خریدار یا سایر مخاطبان (Smith, 2019, p.870)؛

۸. حق نپذیرفتن فروش اطلاعات شخصی (Smith, 2019, p.870)؛

1. Consumer Privacy Bill of Rights

۹. دسترسی برابر به خدمات و قیمت مناسب، حتی در صورت استیفای حق حریم خصوصی خود بر اساس این قانون (Smith, 2019, p.870).

محتوای این حق به دو بخش عمده تقسیم می‌شود: بخش اول مربوط به جمع‌آوری داده‌ها و رعایت اصول مربوط به آن است (معمولاً یا به‌صورت قانونی یا غیرقانونی جمع‌آوری می‌شوند) و بخش دوم، سایر اعمال و افعالی است که در ارتباط با داده‌ها ممکن است اتفاق بیفتد. درواقع بخش دوم مربوط به منافع مربوط به داده‌ها است که ممکن است مورد سوءاستفادهٔ اشخاص ثالث اعم از حقوقی و حقیقی قرار گیرد.

اصول حاکم بر جمع‌آوری و حفظ داده‌ها در بستر اینترنت اشیا

برخی اصول حاکم بر جمع‌آوری داده‌ها را راهکاری برای افزایش امنیت در اینترنت اشیا می‌دانند، زیرا مهم‌ترین مرحله از مراحل مزکور همین مرحلهٔ جمع‌آوری داده است که به‌صورت قانونی توسط شرکت ارائه‌کنندهٔ خدمت صورت می‌گیرد. این اصول شامل موارد زیر است:

الف) اطلاع‌رسانی به کاربران و انتخاب کاربران: کاربران باید از جمع‌آوری داده‌های مربوط به خود مطلع شوند و بتوانند دربارهٔ ثبت و ضبط داده‌های مربوط به خود تصمیم بگیرند.

ب) تعیین هدف از جمع‌آوری داده‌ها و محدودیت‌های کاربرد داده‌ها: شرکت‌ها باید هر زمان که داده‌های کاربران را جمع‌آوری می‌کنند به کاربر اطلاع دهند و هدف از جمع‌آوری داده‌ها را توضیح دهند. کسب‌وکارها نیز باید متعهد شوند که با اطلاع کاربر و فقط به‌صورت محدود از داده‌ها استفاده می‌کنند.

ج) به حداقل رساندن میزان جمع‌آوری داده‌ها: کسب‌وکارها، در زمانی‌که داده‌ها را از کاربران جمع‌آوری می‌کنند، فقط باید مواردی را بازیابی کنند که برای عملکرد سامانه‌های آن‌ها ضروری است.

د) مسئولیت و امنیت: داده‌ها خصوصی و متعلق به کاربرند؛ بنابراین، کسب‌وکارها در قبال آنچه جمع‌آوری می‌کنند مسئول‌اند و باید با دقت امنیت داده‌ها را در برابر مداخلهٔ طرف سوم تضمین کنند (Fornasier, 2019, p.313). به‌علاوه، یکی از قواعد اساسی در استفاده از اینترنت اشیا، خصوصاً در روابط بین‌المللی که باید همواره رعایت شود، داشتن حسن نیت است. حسن نیت در حقوق به معنای تأثیر اخلاق در حقوق است. بر همین اساس، در مادهٔ ۳ قانون تجارت الکترونیکی چنین بیان شده است: «در تفسیر این قانون همیشه باید به خصوصیت بین‌المللی، ضرورت توسعهٔ هماهنگی بین کشورها در کاربرد آن و رعایت لزوم حسن نیت توجه کرد.». این بیانگر توجه تجارت الکترونیک بر حسن نیت و ضرورت وجود آن در روابط بین کشورها است.

حسن نیت یعنی کاربر با اطمینان به فضای اینترنت و داده‌های رایانه‌ای از این فناوری‌ها استفاده کند و اطمینان داشته باشد که برنامهٔ اینترنت اشیا به‌صورتی طراحی شده است که امنیت اطلاعات کاربر خود را تأمین کند و کسی به اطلاعات شخصی وی دسترسی ندارد و شرکت ارائه‌کنندهٔ خدمات در این راه متعهد است که برای حفظ حریم خصوصی مشتریان نهایت تلاش خود را خود صرف کند. این حاصل قاعدهٔ حسن نیت و اعتماد متقابل در روابط طرفین است.

البته هرچند در ایران قانونی عام دربارهٔ حسن نیت وجود ندارد که همهٔ قراردادها را دربر گیرد، قانونگذار در برخی قوانین صراحتاً اصطلاح حسن نیت را به‌کار برده است؛ مانند مادهٔ ۸ قانون مسئولیت مدنی مصوب ۱۳۳۹ (اَعمالِ مخالف حسن نیت)، مادهٔ ٤٠ قانون دریایی مصوب ۱۳۴۳ (طلبکار با حسن نیت)، مواد ٦ و ١٦ قانون صدور چک مصوب ۱۳۴۴ (وجود حسن نیت در صادرکنندهٔ چک) و مواد ۳ و ۳۵ قانون تجارت الکترونیک مصوب ۱۳۸۲ (لزوم رعایت حسن نیت در تفسیر این قانون). بر همین اساس، در موضوع اینترنت اشیا نیز اگر قراردادی میان مصرف‌کننده و تولیدکننده بسته شود، باید طبق اصل حسن نیت حریم خصوصی مصرف‌کننده رعایت شود.

به‌طور کلی، امنیت در سه مرحله در اینترنت اشیا مطرح است:

۱- امنیت خود سامانه‌های اینترنت اشیا و سامانه‌های مرتبط با آن در مقابل هک و نفوذ: امنیت در این حوزه بیشتر مربوط به فناوری است و راهکارهای فنی در این زمینه راهگشا است و باید از شرکت‌ها خواسته شود تا در این زمینه امنیت را تضمین کنند.

۲- امنیت و رعایت اصول در هنگام جمع‌آوری قانونی داده‌ها: در این مورد، علاوه بر راهکارهای فنی، رعایت برخی اصول اخلاقی و حقوقی هم لازم است؛ مانند رعایت حقوق مصرف‌کنندگان مثل حق آگاهی، حق مالکیت بر داده‌ها و سایر حق‌های مشابه.

۳- امنیت در هنگام نگه‌داری و استفاده از داده‌ها: هرچند امنیت داده‌ها در مرحلهٔ نگه‌داری نیز منوط به راهکارهای فنی است، در مرحلهٔ استفاده از داده‌ها آنچه حاکم است اصول اخلاقی و حقوقی است.

انواع داده‌های افراد با توجه به کاربردهای مختلف اینترنت اشیا

داده‌های مربوط به افراد در حوزهٔ اینترنت اشیا به چند گروه تقسیم می‌شود که در جدول ۱ آمده است:

جدول ۱: انواع داده‌های کاربردی در اینترنت اشیا

انواع کاربرد اینترنت اشیا	انواع داده‌ها	سوءاستفاده‌کنندگان احتمالی
سلامت و درمان پزشکی	رفتارهای فرد و ویژگی‌های روانی و علائم جسمی مانند خلق‌وخو، میزان استرس، اطلاعات جمعیت‌شناختی (مانند جنسیت، وضعیت تأهل، وضعیت شغلی و سن)، عادت به سیگار کشیدن، سلامت عمومی، نوع شخصیت روانی فرد، میزان ورزش، انواع فعالیت بدنی یا حرکات روزانه تا اطلاعات مهم‌تر مانند پیشرفت پارکینسون و/ یا بیماری آلزایمر، اچ‌آی‌وی، سرطان، صرع و اسکیزوفرنی	اشخاص حقیقی اشخاص حقوقی مانند شرکت‌های بیمهٔ سلامت شرکت‌های داروسازی شرکت‌های صاحب فناوری اینترنت اشیا دولت یا حکومت دولت‌های دیگر (در این صورت، موضوع مربوط به امنیت ملی خواهد بود)
منازل هوشمند	خودکارسازی خانگی (دستگاه‌های خودکارسازی خانگی با ارائهٔ خدماتی چون پاسخ‌دادن به سؤالات، گزارش اخبار، پخش موسیقی و کنترل سایر ابزارها و لوازم‌خانگی در منزل به کاربران کمک می‌کنند) نظارت و امنیت منازل (با استفاده از فناوری خودبرنامه‌ریزی برای نظارت و تغییر دمای خانه و ارسال هشدارهای دیجیتالی به مصرف‌کننده، به‌عنوان یک سامانهٔ امنیتی در صورت تشخیص دود، مونوکسید کربن یا دمای بسیار کم که ممکن است باعث ترکیدن لوله‌ها شود) شبکهٔ خانگی (وای‌فای و جعبهٔ تلویزیون کابلی)	اشخاص حقیقی اشخاص حقوقی مانند شرکت‌های صاحب فناوری اینترنت اشیا شرکت‌های لوازم‌خانگی شرکت‌های مهندسی ساختمان دولت یا حکومت
اتومبیل هوشمند	دو نوع رایج از حسگرهای خودرو عبارت‌اند از: ضبط‌کنندهٔ داده‌های رویداد و تصادف (جمع‌آوری داده‌های خودرو برای شناسایی مسائل ایمنی خودرو و درنهایت بهبود ایمنی جاده و ثبت اطلاعات فنی خودرو و سرنشین برای مدت کوتاهی (ثانیه، نه دقیقه) قبل، حین و پس از تصادف) و دستگاه‌های مخابراتی بیمهٔ خودکار (ثبت نحوهٔ رانندگی ایمن مصرف‌کنندگان).	اشخاص حقیقی اشخاص حقوقی مانند شرکت‌های بیمهٔ خودرو شرکت‌های صاحب فناوری اینترنت اشیا دولت یا حکومت
محل کار هوشمند یا حس‌گرهای محل کار یا کارخانه‌های هوشمند	نظارت بر عملکرد و فعالیت کارمندان نظارت بر فرایندهای تولید محصولات	اشخاص حقیقی اشخاص حقوقی مانند شرکت‌های خصوصی دولت یا حکومت

انواع کاربرد اینترنت اشیا	انواع داده‌ها	سوءاستفاده‌کنندگان احتمالی
اجرای قانون	نظارت بر موقعیت و رفتار مجرمان یا متهمان و سایر شهروندان و حتی خود مقامات قضایی و اجرایی کشور در جهت رعایت حقوق متهمان در هنگام انجام فرایندهای قضایی	اشخاص حقیقی دولت یا حکومت
آتش‌نشانی	استفاده از فناوری پوشیدنی برای واکنش سریع‌تر به آتش‌سوزی و سایر شرایط اضطراری با استفاده از نمایش‌گرهای هدآپ برای به‌دست‌آوردن بازخوانی‌های فوری نقشهٔ ساختمان یا شرایط محیطی	اشخاص حقیقی دولت یا حکومت
شهر هوشمند	پایش و مدیریت ترافیک خودروها و سامانه‌های حمل‌ونقل، نیروگاه‌های برق، تأسیسات شهری، شبکه‌های تأمین آب، مدیریت پسماند، سامانه‌های اطلاعاتی، مدارس، کتابخانه‌ها، بیمارستان‌ها و دیگر خدمات اجتماعی	اشخاص حقیقی اشخاص حقوقی مانند شرکت‌های طرف قرارداد با شهرداری‌ها دولت یا حکومت
آموزش هوشمند	مدیریت یادگیری رسمی و یادگیری غیررسمی مدیریت و نظارت بر فعالیت‌های آموزشی و فرهنگی در دانشگاه‌ها، مدارس، فرهنگ‌سراها و کتابخانه‌ها	اشخاص حقیقی اشخاص حقوقی دولت یا حکومت
کشاورزی هوشمند	مدیریت تولید بهینهٔ محصولات کشاورزی، خطرات زیست‌محیطی، مصرف آب و انرژی، کود دهی، دما و رطوبت و موارد مشابه	اشخاص حقیقی اشخاص حقوقی دولت یا حکومت دولت‌های دیگر (امنیت ملی)

مصادیق نقض حق حریم خصوصی افراد در بستر اینترنت اشیا

برای تعیین مصادیق باید به این نکته اشاره کرد که برخی مصادیق نقض این حق در حوزهٔ اینترنت اشیا به‌صورت غیرمستقیم از قوانین برداشت می‌شوند و برخی نیز به‌صورت فرضی مطرح می‌شوند که نیازمند تصویب قوانین‌اند:

مصادیق ذکرشده در قوانین ایران

هتک حرمت و حیثیت افراد: طبق اصل ۲۲ قانون اساسی و با توجه به اطلاق این اصل و همچنین قانون جرائم رایانه‌ای، در صورتی که به‌واسطهٔ هک یا نفوذ در سامانهٔ اینترنت اشیا به حرمت یا حیثیت فردی تعدی شود، مشمول منع موضوع این اصل خواهد بود.

ضبط و فاش‌کردن، و سانسور و مخابره‌نکردن مکالمات تلفنی و شنود غیرمجاز در سامانهٔ اینترنت اشیا: طبق اصل ۲۵ قانون اساسی و با توجه به اطلاق این اصل و همچنین مواد ۱۶ و ۱۷ قانون جرائم رایانه‌ای، وقوع هریک از این موارد در سامانهٔ اینترنت اشیا جرم و مشمول منع قانونی است.

دسترسی غیرمجاز به داده‌ها در سامانهٔ اینترنت اشیا: طبق مادهٔ ۱ قانون جرائم رایانه‌ای، دسترسی غیرمجاز به داده‌ها در سامانهٔ اینترنت اشیا به‌منزلهٔ نوعی از سامانه‌های رایانه‌ای جرم‌انگاری شده است.

در دسترس قراردادن داده‌های موجود در سامانهٔ اینترنت اشیا: طبق بند الف مادهٔ ۳ قانون جرائم رایانه‌ای، در دسترس قراردادن داده‌های موجود در سامانهٔ اینترنت اشیا جرم است.

حذف یا تخریب یا مختل یا غیرقابل‌پردازش کردن داده‌های موجود در سامانهٔ اینترنت اشیا: طبق مادهٔ ۸ قانون جرائم رایانه‌ای، این امور نیز در زمرهٔ جرائم در این حوزه قرار می‌گیرد.

ازکارانداختن یا مختل‌کردن سامانه‌های اینترنت اشیا: طبق مادهٔ ۱۳ قانون جرائم رایانه‌ای، ازکارانداختن یا مختل‌کردن سامانه‌های اینترنت اشیا، فردی یا ملی، از جرائم رایانه‌ای و حتی جرائم علیه امنیت کشور به‌شمار می‌رود. منظور از ملی هوشمندسازی فرایندهای توزیع آب، برق و گاز یا حمل‌ونقل و درنهایت اختلال در آن‌ها است.

نقض حق ممانعت از انتشار اطلاعات خصوصی خود: در مادهٔ ۳ قانون انتشار و دسترسی آزاد به اطلاعات این بُعد مطرح شده است.

رد یا پذیرش درخواست افراد یا سراچه‌های درخواست‌کنندهٔ اطلاعات شخصی افراد توسط خود این افراد: مادهٔ ۱٤ قانون انتشار و دسترسی آزاد به اطلاعات به این بُعد اشاره کرده است.

فروش یا انتشار یا در دسترس قراردادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند: طبق بند ب مادهٔ ۲۵ قانون جرائم رایانه‌ای، این مورد جرم‌انگاری شده است که علاوه بر این‌که خود نقض حریم خصوصی افراد به‌شمار می‌رود، در نقض مصادیق دیگر این حق نیز به‌کار گرفته می‌شود.

سایر مصادیق

منظور از این مصادیق مصادیقی است که در قوانین به آن‌ها اشارهٔ مستقیم و غیرمستقیم نشده است، اما نیازمند قانونگذاری ویژه در این زمینه‌اند:

انتقال غیرمجاز داده‌ها از یک سامانهٔ اینترنت اشیا به سامانه‌ای دیگر: یکی از حق‌هایی که باید برای مشتریان در سامانهٔ اینترنت اشیا ملاحظه شود حق انتقال داده‌ها است. انتقال غیرمجاز داده‌ها از یک سامانهٔ اینترنت اشیا به سامانهٔ دیگر نیز از مصادیق نقض حریم خصوصی افراد است.

دسترسی‌نداشتن به اطلاعات خصوصی خود در سامانهٔ اینترنت اشیا: هر فرد حق دارد یک نسخه از اطلاعاتی را که در سامانه‌های اینترنت اشیا وجود دارد دریافت کند، مگر این‌که مانع قانونی وجود داشته باشد. ممانعت از این دسترسی یکی از مصادیق نقض حق حریم خصوصی است.

نبود امکان اصلاح اطلاعات خصوصی نادرست برای خود مشتری در سامانهٔ اینترنت اشیا: افراد باید این حق را داشته باشند که برای اصلاح اطلاعات غلط یا ناقصی که دربارهٔ خودشان در سیستم اینترنت اشیا ذخیره کرده‌اند به شرکت خدمات‌دهنده درخواست بدهند و امکان اصلاح این اطلاعات وجود داشته باشد. ممانعت از این کار از موارد نقض حریم خصوصی افراد به‌شمار می‌رود.

نبود امکان محدودکردن استفاده از اطلاعات خصوصی مشتریان در سامانهٔ اینترنت اشیا: هر فرد این حق را دارد که از شرکت خدمات‌دهنده بخواهد روند پردازش همه یا بخشی از اطلاعات خصوصی او را محدود کند و در صورت نادرست‌بودن این اطلاعات، شرکت ازنظر قانونی نباید از این اطلاعات استفاده کند یا در صورت نیاز مشتری برای حفظ اطلاعات خود با هدف تثبیت، پیگیری یا دفاع از یک پروندهٔ قانونی باید این اطلاعات را نگه‌داری کند. همچنین، مشتری باید این حق را داشته باشد که در هر موقعیت که حق حریم خصوصی او با منافع قانونی شرکت خدمات‌دهنده برای استفاده از اطلاعات مشتری در زمینه‌ای مشخص در تعارض است بتواند نظر خود را به شرکت مذکور اعلام کند.

نبود امکان حذف اطلاعات خصوصی مشتریان در سامانهٔ اینترنت اشیا: نبود امکان حذف همه یا بخشی از اطلاعات خصوصی مشتریان در موارد مشخص از موارد نقض حق حریم خصوصی افراد است.

نبود امکان اعتراض به استفاده از اطلاعات خصوصی مشتریان در سامانهٔ اینترنت اشیا: افراد این حق را دارند که در صورت نیاز به استفادهٔ شرکت خدمات‌دهنده از اطلاعات خود اعتراض کنند، گرچه ممکن است ارائهٔ خدمات به آنان را تحت تأثیر قرار دهد.

چالش‌های حقوقی، اخلاقی و قانونگذاری دربارهٔحق حریم خصوصی در بستر اینترنت اشیا در ایران

با توجه به اهمیت حق بر حریم خصوصی و درعین‌حال، ارتباط آن با اینترنت اشیا در این بخش از مقاله به مهم‌ترین چالش‌های پیش‌رو اشاره می‌شود:

ـ چالش‌ها در گسترهٔ نظری: این چالش‌ها که به‌صورت مشترک در حیطه‌های مذکور مطرح است شامل این موارد می‌شود: عدم تبیین مناسب مفهوم حق بر حریم خصوصی در قوانین و نظریات حقوقی و اخلاقی به‌طور کلی، عدم تبیین مناسب مصادیق حق بر مفهوم خصوصی در قوانین و نظریات حقوقی و اخلاقی به‌طور کلی، عدم تبیین ماهیت مفهوم حق بر حریم خصوصی در قوانین و نظریات حقوقی و اخلاقی به‌طور کلی، عدم تعیین حدود و ثغور حق بر حریم خصوصی در قوانین و نظریات حقوقی و اخلاقی به‌طور کلی، عدم تبیین رابطهٔ حق حریم خصوصی با سایر حق‌ها، عدم تبیین رابطهٔ حق حریم خصوصی با حوزهٔ سلامت و اخلاق عمومی، عدم تبیین رابطهٔ حق حریم خصوصی با حوزهٔ امنیت ملی، عدم تبیین مناسب مفهوم حق بر حریم خصوصی در بستر فناوری اینترنت اشیا، عدم تبیین مناسب مصادیق حق بر مفهوم خصوصی در بستر فناوری اینترنت اشیا، عدم تبیین ماهیت مفهوم حق بر حریم خصوصی در بستر فناوری اینترنت اشیا، عدم تبیین مناسب نسبت میان حق بر حریم خصوصی و حق بهره‌مندی از اینترنت اشیا، عدم تبیین مفهوم و مصادیق داده‌های شخصی، عدم تبیین رابطه و نسبت میان حق حریم خصوصی و داده‌های شخصی و... .

ـ چالش‌ها در گسترهٔ عملی و کاربردی: این چالش‌ها عبارت است از: آسیب‌پذیری اینترنت اشیا در برابر حملات سایبری به‌علت ضعف پروتکل‌ها و سیاست‌های امنیتی، مدیریت امنیت دستگاه‌های اینترنت اشیا، امکان دسترسی از طریق اینترنت ناشناس با ارتباط متقابل شبکه‌ها در فناوری اینترنت اشیا، تأثیر ضعف امنیتی بر امنیت کل سیستم در سطح بین‌المللی، سرقت یا جعل هویت در اینترنت اشیا، فقدان رویهٔ قضایی مناسب در دادگاه‌ها برای پرونده‌های مرتبط با فناوری اطلاعاتی مانند اینترنت اشیا، فقدان سیاست‌گذاری واحد و کلان در حوزهٔ فناوری‌های اطلاعاتی، ضعف قوانین دربارهٔ فناوری‌های مرتبط به اینترنت به‌ویژه اینترنت اشیا، نداشتن سرعت کافی قانونگذار برای اصلاح قوانین گذشته یا تصویب قوانین جدید دراین‌باره، بی‌توجهی قانونگذار به پیوست فرهنگی لازم برای استفاده از فناوری‌ها به‌ویژه اینترنت اشیا، بی‌توجهی قانونگذار به حق آگاهی به‌عنوان الزام و مقدمهٔ استیفای درست سایر حق‌ها مانند حق حریم خصوصی در اینترنت اشیا، جرم‌خیزبودن عرصه‌های مربوط به حریم خصوصی و فناوری‌هایی چون اینترنت اشیا و... .

راهکارهای حفظ حق حریم خصوصی در بستر اینترنت اشیا

هرچند برخیْ هنجارهای فرهنگی، فشار عمومی و تحریم‌های اجتماعیِ خودجوشِ «تنظیم‌کنندهٔ» نوآوری‌ها و نحوهٔ استفادهٔ مردم از ابزارهای جدید را بسیار قوی‌تر از راهکار تصویب قوانین و تنظیم مقررات می‌دانند (Thierer, 2014, p.111)، اما سه مکتب فکری عمده در عرصهٔ تصویب قوانین در مورد روش مدیریت حریم خصوصی برخط در آینده وجود دارد:

دیدگاه نخست «تنظیم از بالا به پایین» است که از نظارت دقیق بر شرکت‌ها با هدف الزام آن‌ها به پیروی از حداقل استانداردهای کاملاً تعریف‌شدهٔ حریم خصوصی حمایت می‌کند. نمونهٔ عملی این دیدگاه چارچوب حریم خصوصی اتحادیهٔ اروپا است که بر مشارکت دولت در تنظیم حریم خصوصی برخط تأکید دارد.

دیدگاه دوم با وضع قوانین اجباری برای حفاظت از حریم خصوصی مخالف است. حامیان این دیدگاه عبارت‌اند از دولت‌های مستبد و دیکتاتور، افراد یا گروه‌هایی که دولت و شرکت‌ها را غیرقابل‌اعتماد می‌دانند و سرمایه‌داران بازار آزاد که معتقدند بازار باید به حال خود رها باشد.

دیدگاه سوم، از خودتنظیمی شرکت‌ها و ارائه‌دهندگان خدمات برخط حمایت می‌کند؛ زیرا شرکت‌های فناور نسبت‌به دولت در موقعیت بهتری برای ایجاد قوانین حفظ حریم خصوصی، نظارت و مدیریت بر اجرای قوانین قرار دارند. طرف‌داران این دیدگاه را می‌توان به‌نوعی طرف‌دار دو دیدگاه قبل دانست، زیرا آن‌ها ضمن آن‌که خواهان حمایت قوی از مصرف‌کننده‌اند، در مقابلِ اجرای از بالا به پایین مقررات مقاومت می‌کنند (Wafa, 2009, p.150).

اما آنچه دربارهٔ فناوری‌های نوین در ایران باید حاکم باشد سیاست‌گذاری مناسب در دو حوزهٔ فرهنگی و تصویب قوانین است. بر همین اساس و با توجه به رویکرد حقوقی مقاله، برای حفظ حریم خصوصی شهروندان در ارتباط با اینترنت اشیا باید قانون مناسب در این زمینه تدوین شود که ویژگی‌های زیر را داشته باشد:

الف) توجه به اتخاذ رویکرد خودتنظیمی از سوی فناوران این حوزه با شیوه‌هایی چون تأمین امنیت داده‌ها (برای نمونه، از طریق رمزگذاری)، جمع‌آوری حداقل داده‌ها[1] بر اساس درخواست مشتریان، اطلاع‌رسانی، انتخاب (Smith, 2019, p.865)، تنظیم شیوه‌نامهٔ استفادهٔ صحیح از سامانهٔ اینترنت اشیا، شفافیت، فراهم‌آوردن امکان انتقال داده‌ها بر اساس درخواست مشتریان و هشدارهای امنیتی مداوم و به‌روز (Thierer, 2014, p.91-92) در کنار تصویب قانون به روش سنتی.

ب) لزوم وجود ضمانت اجرای قوی برای قانون مصوب.

ج) لزوم انعطاف‌پذیری و بی‌طرفی قانون ازلحاظ فناوری (Smith, 2019, p.865)

د) شناسایی مسئولیت مدنی و کیفری برای شرکت‌های ارائه‌دهنده یا تولیدکنندهٔ خدمات اینترنت اشیا. این موضوع به دو علت زیر دارای اهمیت است:

اول، از سوءاستفادهٔ تولیدکنندگان و اشخاص ثالث از داده‌های شخصی پیشگیری می‌کند.

دوم، برخلاف مقررات مربوط به اعلام و کسب رضایت، بار حمایت از مصرف‌کننده را بر دوش شرکت‌ها قرار می‌دهد، زیرا زمان و تلاش کافی را برای انجام این کار صرف نمی‌کنند (Smith, 2019, p.877).

هـ) توجه به نحوهٔ جبران ضرر، زیرا در احکام دادگاه‌ها ممکن است روش مناسب جبران ضرر ملاحظه نشود (Smith, 2019, p.875).

پس از تصویب قوانین، موضوع مهم دیگر رویهٔ قضایی است و بر همین مبنا، اختصاص دادگاه‌های ویژه برای رسیدگی به دعاوی این موضوع و موضوعات مشابه حائز اهمیت است. درنهایت، در حوزهٔ سیاست‌گذاری فرهنگی، آموزش شهروندان و شرکت‌ها برای حمایت از خود در ارتباط با اینترنت اشیا (Smith, 2019, p.866) با تأکید بر این امور (راهبردهای سواد رسانه‌ای، مهارت‌های تفکر انتقادی و شهروندی دیجیتال) (Thierer, 2014, p.85) مهم است؛ زیرا علاوه‌بر ناآگاهی، طبق پژوهش‌ها، بی‌تفاوتی مصرف‌کننده به این موضوع نیز وجود دارد (Smith, 2019, p.875).

نتیجه‌گیری

در تعریف اینترنت اشیا از دیدگاه‌های مختلف به دو عامل ارتباط اشیا باهم و فناوری‌های به‌کاررفته در آن توجه شده است، درحالی‌که اینترنت اشیا از سه عنصر دستگاه‌های هوشمند، پروتکل‌ها و سامانه‌های ذخیره‌سازی داده‌ها تشکیل شده است. بر اساس همین تفاوت دیدگاه، تعاریف متفاوتی از اینترنت اشیا در حوزهٔ فناوری مطرح شده است.

حق حریم خصوصی از انواع حق‌های نسل اول بود که در تزاحم با حق بهره‌مندی از اینترنت اشیا قرار گرفته بود. حق دوم در زمرهٔ حق‌های اقتصادی و اجتماعی بود که اثبات آن در حقوق بین‌الملل محل نزاع بود. به‌علاوه، رتبهٔ این حق در مقایسه با سایر مصادیق حق‌های اجتماعی و اقتصادی پایین‌تر بود، اما اگر استیفای این حق از ضروریات زندگی بشر در آینده شود، شاید بتوان از استیفای حق حریم خصوصی چشم‌پوشی کرد.

محتوای حق حریم خصوصی در حوزهٔ اینترنت اشیا شامل مدیریت و نظارت فرد بر داده‌های شخصی خود از یک‌سو و از سوی دیگر، رعایت امنیت در سه حوزهٔ امنیت خود سامانه‌های اینترنت اشیا و سامانه‌های مرتبط با آن در مقابل هک و نفوذ، امنیت و رعایت اصول در هنگام جمع‌آوری قانونی داده‌ها و امنیت در هنگام نگه‌داری و استفاده از داده‌ها است.

اصول حاکم بر جمع‌آوری و نگه‌داری داده‌ها شامل مواردی چون اطلاع‌رسانی به کاربران و انتخاب کاربران، تعیین هدف از جمع‌آوری داده‌ها و محدودیت‌های کاربرد داده‌ها، به حداقل رساندن میزان جمع‌آوری داده‌ها و مسئولیت و امنیت است که در حقوق ایران دچار نقص جدی است و تمامی وجوه به‌طور کامل پیش‌بینی نشده است که به‌علت فقدان همین مقررات جامع درزمینهٔ حریم خصوصی حمایت کامل و جامعی از حریم خصوصی افراد در این خصوص از طرف کاربر احساس نمی‌شود و کاربر اطمینان کامل به حفظ حقوق خود ندارد.

1. Data Minimization

نقض حریم خصوصی افراد، به‌منزلهٔ اصلی بسیار مهم در فضای اینترنت و به‌تبع آن در حوزهٔ اینترنت اشیا، موضوع بسیار مهمی است که پیامدهای اجتماعی، سیاسی و فرهنگی دارد و جرم‌انگاری و وضع قوانین دقیق و جزئی در این خصوص موجب رعایت انصاف و حمایت از افراد در برابر آسیب‌های احتمالی است که گاهی ممکن است سالیان سال زندگی فردی و اجتماعی فرد را تحت تأثیر قرار دهد.

در این مقاله، مصادیق نقض حق حریم خصوصی افراد در حوزهٔ اینترنت اشیا به دو حوزهٔ مصادیق ذکرشده در قوانین ایران و سایر مصادیق تقسیم شده است. در گروه نخست، مصادیقی چون هتک حرمت و حیثیت افراد، ضبط و فاش‌کردن و سانسورکردن و مخابره‌نکردن مکالمات تلفنی، شنود غیرمجاز در سامانهٔ اینترنت اشیا، دسترسی غیرمجاز به داده‌ها در سامانهٔ اینترنت اشیا، در دسترس قراردادن داده‌های موجود در سامانهٔ اینترنت اشیا، حذف یا تخریب یا مختل یا غیرقابل‌پردازش کردن داده‌های موجود در سامانهٔ اینترنت اشیا، ازکارانداختن یا مختل‌کردن سامانه‌های اینترنت اشیا، ممانعت از انتشار اطلاعات خصوصی خود و رد یا پذیرش درخواست افراد یا سراچه‌های درخواست‌کنندهٔ اطلاعات شخصی افراد توسط خود این افراد مطرح شده است. در گروه دوم نیز به مواردی مانند انتقال غیرمجاز داده‌ها از یک سامانهٔ اینترنت اشیا به سامانه‌ای دیگر، دسترسی‌نداشتن کاربر به اطلاعات خصوصی خود در سامانهٔ اینترنت اشیا، نبود امکان اصلاح اطلاعات خصوصی نادرست از سوی خود مشتری در سامانهٔ اینترنت اشیا، نبود امکان محدودکردن استفاده از اطلاعات خصوصی مشتریان در سامانهٔ اینترنت اشیا، نبود امکان حذف اطلاعات خصوصی مشتریان در سامانهٔ اینترنت اشیا و نبود امکان اعتراض به استفاده از اطلاعات خصوصی مشتریان در سامانهٔ اینترنت اشیا اشاره شده است.

در پایان، پیشنهادهای زیر دربارهٔ حفظ حریم خصوصی افراد در اینترنت اشیا مطرح می‌شود:

– شناسایی چالش‌ها، تهدیدها و فرصت‌ها درخصوص اینترنت اشیا و تدوین راهکار برای حفظ اطلاعات شخصی و حمایت از حقوق افراد.

– ایجاد فرصت‌های پژوهشی در مراکز علمی و دانشگاهی و حقوقی کشور و اجرای پروژه‌های علمی و حقوقی دربارهٔ اینترنت اشیا و حقوق افراد و ارتباط با مراکز علمی و دانشگاهی و حقوقی بین‌المللی به‌منظور تبادل اطلاعات.

منابع

آقایی طوق، مسلم و ناصر، مهدی (۱۳۹۹). چالش‌های حفاظت از داده‌های خصوصی در حوزهٔ اینترنت اشیا: مطالعهٔ تطبیقی حقوق ایران و اتحادیهٔ اروپا. *حقوق اداری*، *۷* (۲۳)، ۳۳-۵۵.

اقدسی، فاطمه و محقق داماد، مریم‌السادات (۱٤۰۰). ابعاد حقوقی حریم خصوصی در اینترنت اشیا. *پژوهش‌های حقوقی میان‌رشته‌ای*، ۲ (٦)، ٦۷-۵۰.

رئیسی دزکی، لیلا و قاسم‌زاده لیاسی، فلور (۱۳۹۹). چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر. *حقوقی دادگستری*، *۸۴*(۱۱۰)، ۱۲۳-۱۴۶.

فرحزادی، علی‌اکبر و ناصر، مهدی (۱۴۰۰). حق بر تبادل داده‌های خصوصی و راهکارهای رفع چالش‌های آن در سازوکار عملکرد ابزارهای اینترنت اشیا. *دوماهنامه بررسی‌های بازرگانی*، *۱۹* (۱۰۹)، ۱۱۵-۱۲۹.

فقیهی، مهدی و نافعی، نوشین (۱۳۹۵). اینترنت اشیا. گزارش‌های کارشناسی (مرکز پژوهش‌های مجلس شورای اسلامی).

گلدینگ، مارتین پی (۱۳۸۱). *مفهوم حق (۱): درآمدی تاریخی، حق و مصلحت*. محمد راسخ (مترجم). تهران: طرح نو.

والدرون، جرمی (۱۳۸۱). *فلسفه حق، حق و مصلحت*. محمد راسخ (مترجم). تهران: طرح نو.

Chander, A. (2019). The internet of things: both goods and services. *World Trade Review*, *18*(Supplement), S9-S22.

Fornasier, M. D. O. (2019). The Applicability of the Internet of Things (IoT) between Fundamental Rights to Health and to Privacy. *Revista de Investigacoes Constitucionais*, 6(2), 297-321.

McMeley, C. S. (2014). Protecting consumer privacy and information in the age of the internet of things. *Antitrust*, *29*(1), 71-78.

Poudel, S. (2016). Internet of things: underlying technologies, interoperability, and threats to privacy and security. *Berkeley Technology Law Journal*, *31*(Annual Review 2016), 997-1022.

Robb, C. S. (1998). Liberties, claims, entitlement and trumps, reproductive rights and ecological responsibilities. *The Journal of Religious Ethics*, *26*(2), 283-294.

Robinson, W. K. (2015). Patent law challenges for the internet of things. *Wake Forest Journal of Business and Intellectual Property Law*, *15*(4), 655-670.

Smith, N. (2019). Protecting consumers in the age of the internet of things. *St. John's Law Review*, *93*(3), 851-882.

Thierer, A. D. (2014). The internet of things and wearable technology: addressing privacy and security concerns without derailing innovation. *Richmond Journal of Law & Technology*, *21*(2), 1-118.

Tschider, C. A. (2018). Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age. *Denver Law Review*, *96*(1), 87-144.

Wafa, T. (2009). Global internet privacy rights: apragmatic approach. *Intellectual Property Law Bulletin*, *13*(2), 131-158.