Interdisciplinary Legal Research
Jul 2021, 2(2): 49-67
Available online on: www. ilrjournal.ir
e-ISSN:2717-1795

ORIGINAL RESEARCH PAPER

Legal Aspects of Internet of Things Privacy

Fatemeh Aghdasi [1*], ***Maryam Sadat Mohaghagh Damad*** [2]

Received:
05 Apr 2021
Revised:
02 May 2021
Accepted:
16 May 2021
Available Online:
01 Jul 2021

Abstract

Background and Aim: The Internet of Things is a broad concept with high potential that is dynamically evolving and developing that is not easy to identify in all its dimensions. In such an information exchange space, paying attention to the privacy of personal information is very important for consumers. Obviously, due to the wide scope of this issue, privacy has been studied internationally in scientific conferences and at the global and regional levels. In this article, an attempt has been made to examine the concept and examples and the scope of privacy of individuals, especially privacy in the Internet of Things, and to distinguish it from the concept of security.

Materials and Methods: The method of descriptive-analytical research is referring to the existing laws in Iran and studying the regulations of leading countries in the field of study.

Ethical Considerations: Ethical considerations related to writing texts and referring to sources was observed.

Findings: Privacy is essential in today's new information space. The important point in providing protection is to pay attention to efficiency, that is, to create a reasonable balance between maintaining the privacy of individuals and the free flow of information. Paying attention to this makes it possible to use the Internet of Things efficiently and fairly.

Conclusion: Some suggestions have been made in order to develop an appropriate legal framework to protect the privacy of individuals in the Internet of Things for Iran.

Keywords:
IoT,
Privacy,
Security,
Data,
Legal Framework.

1* M.A., Department of Communication Law, Faculty of Law, Allameh Tabatabai University, Tehran, Iran. (Corresponding Author)
Email: F.aghdasi@mohagheglaw.com *Phone: +982126116284*
2 Assistant Professor, Department of Private Law, Faculty of Law, Imam Sadegh University, Tehran, Iran.

Please Cite This Article As: Aghdasi, F & Mohaghegh Damad, MS (2021). "Legal Aspects of Internet of Things Privacy". *Interdisciplinary Legal Research*, 2 (2): 49-67.

This is an open access article distributed under the terms of the Creative Commons Attribution (CC BY 4.0)

مقاله پژوهشی
(صفحات ۴۹-۶۷)

ابعاد حقوقی حریم خصوصی در اینترنت اشیا

فاطمه اقدسی[۱]، مریم سادات محقق داماد [۲]

۱. کارشناس ارشد، گروه حقوق ارتباطات، دانشکده حقوق، دانشگاه علامه طباطبایی، تهران، ایران. (نویسنده مسؤول)
Email: F.aghdasi@mohagheglaw.com

۲. استادیار، گروه حقوق خصوصی، دانشکده حقوق، دانشگاه امام صادق (ع)، تهران، ایران.

دریافت: ۱۴۰۰/۱/۱۶ ویرایش: ۱۴۰۰/۲/۱۲ پذیرش: ۱۴۰۰/۲/۲۶ انتشار: ۱۴۰۰/۴/۱۰

چکیده

زمینه و هدف: اینترنت اشیا مفهومی گسترده با پتانسیل‌های بالایی را شامل می‌شود که به صورت پویا در حال شکل‌گیری و توسعه است که شناسایی تمامی ابعاد آن، چندان آسان نیست. در چنین فضای تبادل اطلاعاتی، توجه به حریم خصوصی حاکم بر اطلاعات شخصی برای مصرف‌کنندگان دارای اهمیت بسیار بالایی است. بدیهی است به دلیل گستردگی ابعاد این موضوع، حریم خصوصی در سطح بین‌المللی در کنفرانس‌های علمی و در سطح جهانی و منطقه‌ای مورد بررسی قرار گرفته است. در مقاله حاضر، تلاش شده تا مفهوم و مصادیق و یا چیستی و دامنه حریم خصوصی افراد به‌خصوص حریم خصوصی در اینترنت اشیا مورد بررسی قرار گیرد و تفاوت آن از مفهوم امنیت مشخص گردد.

مواد و روش‌ها: روش پژوهش توصیفی_تحلیلی با مراجعه به قوانین موجود در کشور ایران و مطالعه مقررات کشورهای پیشرو در حوزه مورد مطالعه است.

ملاحظات اخلاقی: ملاحظات اخلاقی مربوط به نگارش متون و نیز ارجاع‌دهی به منابع رعایت گردید.

یافته‌ها: حفاظت حریم شخصی در فضای نوین اطلاعاتی کنونی امری ضروری است. نکته مهم در تأمین حفاظت توجه به کارآمدی است، یعنی توازن منطقی بین حفظ حریم شخصی افراد و گردش آزاد اطلاعات، ایجاد گردد. توجه به این نکته بهره‌مندی کارآمد و عادلانه از اینترنت اشیا را میسر می‌نماید.

نتیجه‌گیری: تدوین چارچوب حقوقی مناسب در جهت حفظ حریم خصوصی افراد در فضای اینترنت اشیا ضروری است.

کلمات کلیدی: اینترنت اشیا، حریم خصوصی، امنیت، داده، چارچوب حقوقی.

مقدمه

۱- بیان موضوع

ممنوعیت از تجسس، افشای اسرار، تصرف بدون اذن، استراق سمع و بصر و... در طول تاریخ دارای اهمیت بوده است، اما تحولات نوین ابزارهای ارتباطی و ظهور موضوع اینترنت اشیا موجب شده تا این دسته از موضوعات اهمیت دوبرابری پیدا کنند. احترام به حریم خصوصی افراد در مجموعه حفظ اسرار ناشی از زندگی خصوصی اشخاص قرار می‌گیرد (انصاری، ۳۹:۱۳۸۲). تاکنون مطالعاتی در رابطه با حریم خصوصی در فضای سایبری انجام شده است اما آنچه این مقاله را از سایر موارد مشابه متمایز می‌سازد توجه به حریم خصوصی در فضای اینترنت اشیا (IoT)[1] است. سوال‌های اصلی این مقاله عبارتند از: مفهوم و ارکان دقیق حریم خصوصی چیست؟ آیا حریم خصوصی دقیقاً همان امنیت داده است؟ آیا در داخل کشور و یا در سطح بین‌المللی به شکل تام حریم خصوصی افراد حمایت شده است؟ برای پاسخ به این پرسش‌ها و موارد مشابه دیگر در ادامه مفهوم و مصادیق امنیت و حریم خصوصی بیان می‌گردد. پس از آن با نگاهی گذرا به موضوع حریم خصوصی در اسناد بین‌المللی نحوه حمایت آن در این حوزه تحلیل می‌شود. و در نهایت پیشنهادات اصلاحی در رابطه با قوانین و مقررات داخل کشور ارائه خواهد شد.

۲- تبیین مفاهیم

۲-۱- اینترنت اشیا یا همان IOT، به شبکه‌ای متشکل از اشیاء فیزیکی است که قادر به جمع‌آوری و به اشتراک‌گذاری اطلاعات الکترونیکی هستند، اطلاق می‌شود. اینترنت اشیا شامل طیف گسترده‌ای از دستگاه‌های «هوشمند»[2] است، از دستگاه‌های صنعتی که اطلاعات مربوط به فرآیند تولید را منتقل می‌کنند، تا حسگرهایی که اطلاعات مربوط به بدن انسان را منتقل می‌کنند؛ شامل این مفهوم هستند (Kenton, 2020:1).

اینترنت اشیا یک معماری اطلاعاتی در حال تکامل مبتنی بر بستر اینترنت است که برای تسهیل تبادل کالا و خدمات عرضه شده است (Weber, 2009:522). هدف اینترنت اشیا، تسهیل تبادل «اشیا» با زیرساخت فناوری اطلاعات در یک مسیر امن و قابل اعتماد است و وظیفه آن غلبه بر فاصله فیزیکی موجود بین اشیا و ارائه آن‌ها به شیوه‌ای نوین در فضای سیستم‌های اطلاعاتی است (Haller *et al*., 2008: 15).

واضح است که در رابطه با اینترنت اشیا گذشته از مباحث فنی و زیرساختی که دارای اهمیت غیرقابل انکار است، مباحث حقوقی از جمله حریم خصوصی، امنیت نیز دارای اولویت فراوانی هستند. بر کسی پوشیده نیست که امروزه سنسورهای موجود در تلفن‌های هوشمند حجم بالایی از اطلاعات شخصی افراد را در بر دارند مواردی از قبیل درجه استرس، نوع تیپ شخصیتی، اختلال دو قطبی، جمعیت‌شناسی (اطلاعاتی نظیر جنسیت، وضعیت تأهل، شغل، سن)، عادات سیگار کشیدن، بررسی کلی صحت جسمی فرد، فرآیند پیشروی بیماری پارکینسون، الگوی زمان خواب فرد، میزان خوشحالی فرد، میزان و نوع تحرکات جسمی و ورزش‌های فرد و ... که به راحتی در گوشی افراد ذخیره می‌شوند؛ تنها مثال کوچکی از اطلاعات شخصی افراد در بستر اینترنت اشیا است (Weber, 2010: 44).

در کشور ایران هرچند عبارت «حریم خصوصی» به‌طور خاص در ماده قانونی تعریف نشده است اما در موارد متفاوتی به اهمیت آن اشاره‌هایی شده است به‌طور مثال در ماده ۱ قانون «تجارت الکترونیک» چنین مقرر می‌دارد: قانون حاضر مجموعه اصول و قواعدی است برای مبادله آسان و ایمن اطلاعات در واسطه‌های الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به کار می‌رود. کلمه ایمن در این

---

[1]- The Internet of Things.
[2]- Smart.

ماده توجه قانونگذار به امنیت داده و حریم خصوصی را نشان می‌دهد.

۲-۲- مفهوم امنیت

از آنجا که مفهوم حریم خصوصی و امنیت بسیار نزدیک به هم می‌باشد و حتی در برخی از متون به اشتباه از این دو عبارت به جای هم استفاده می‌کنند، لازم است به شکلی دقیق‌تر به مقوله امنیت و حریم خصوصی توجه کرد. امینت در لغت از ریشه امن به معنای در امان بودن و مصون بودن از هر گونه تهدید و ترس است (جهان بزرگی، ۳۱:۱۳۸۸). امنیت در اینجا قواعدی است که مانع تهدید اینترنت اشیا در قالب یک سیستم می‌شود. به دلیل اینکه اطلاعات در این حالت به شکل کامل در دسترس قرار دارد، می‌تواند منجر به حمله به سیستم شود که در نتیجه آن خسارات مالی زیادی وارد آورد یا امنیت ملی و بین‌المللی به خطر اندازد (Benjamin & Günther,2009:123). مسلماً به موازات توسعه فناوری‌های نوین، ابزار جدید سوءاستفاده نیز توسعه پیدا می‌کند. امنیت گاهی به معنی حفظ محرمانگی، یکپارچگی و در دسترس بودن اطلاعات به صورت توأمان[1] است (Baldini & Peirce, 2015:14) .

علی‌رغم منافع بسیار ارزشمندی که اینترنت اشیا، برای زندگی کنونی بشر به ارمغان آورده است؛ واضح است که افزایش ارتباط بین وسایل، مخاطراتی را در زمینه امنیتی ایجاد می‌نماید. در ادامه در رابطه با هر یک از موارد مذکور توضیحاتی بیان می‌شود.

نکته بسیار مهم این است که هرچند که در بسیاری از موارد امنیت و حریم خصوصی با یکدیگر هم‌پوشانی دارند اما تفاوت اصلی حریم خصوصی از مسائل امنیتی در این است که حریم خصوصی به حق انفرادی شخص در حفظ اطلاعات شخصی خود در هر فضایی اشاره دارد. از طرفی با وجود اینکه امنیت با محرمانگی اطلاعات فرد در ارتباط است اما همه‌ی هدف آن حفظ این مورد نیست. در واقع هدف اصلی امنیت حفظ سیستم و تشکیلات از آسیب‌ها و نفوذهای احتمالی است.

۲-۳- مفهوم حریم خصوصی

حریم در لغت به محدوده‌ای از پیرامون چیزی گفته می‌شود که برای صیانت از حقوق و بهره‌برداری از آن لازم است[2] (فیومی، بی‌تا: ۱۳۳). این موضوع در رابطه با انسان، دارای صفتی است که شخص نسبت به آن حساس بوده و برای حفظ آن به دفاع بر خیزد (واسطی، ۱۳۵:۱۴۱۴؛ شیرازی، ۳۴:۱۴۲۸). با توجه به این مقدمات «حریم خصوصی، قلمرویی از زندگی شخصی است که هر فرد نوعاً و عرفاً یا با اعلان قبلی از دیگران انتظار دارد بدون رضایت او به اطلاعات در مورد این قلمرو مانند ارتباطات خصوصی وارد نشوند و نظارت نکنند و به‌طور کلی از تعرض مصون باشد.» (قنواتی و جاور، ۸:۱۳۹۰؛ انصاری، ۱۳۹۱: ۱۱-۳۸).

واژه حریم خصوصی در برگیرنده مفاهیم و ایده‌های فراوانی است. به‌طور کلی در فضایی سایبری[3] هر فرد خواهان کنترل و در اختیار داشتن اطلاعات شخصی خود می‌باشد. حریم خصوصی در سه رویکرد قابل تحلیل است (Jerry, 1998:1202–1211)

در یک نگاه حریم خصوصی را می‌توان همچون سپری مقابل اشیا و سیگنال‌های ناخواسته دانست. این برداشت بیشتر به زیرساخت‌های امنیتی و حفاظتی اشاره دارد.

در نگاه دوم حریم خصوصی همان قدرت تصمیم‌گیری در رابطه با اطلاعات فردی است. در این برداشت حمایت از فرد به شکلی است که بتواند بدون دخالت دولتی محدوده اطلاعات فردی خود را تعیین نمایند.

---

[1]- Confidentiality, Integrity and Availability (CIA)

[2] - (حَرِيمُ الشيء) مَا حَوْلَهُ مِنْ حُقُوقِهِ و مَرَافِقِهِ سُمِّيَ بذَلِكَ لأَنَّهُ يَحْرُمُ عَلَى غَيْرِ مَالِكِهِ أَنْ يَسْتَبِدَّ بِالانْتِفَاعِ به

[3] - Cyber Space

در نگاه سوم حریم خصوصی، کنترل شخصی فرد بر تحلیل اطلاعات شخصی او است. در این برداشت مباحثی همچون حصول، افشا و استفاده از اطلاعات فردی مطرح است.

به شکل کلی سه شاخصه اصلی از حریم خصوصی باید همواره مورد توجه واقع شود:

– اختفا، در رابطه با اطلاعاتی که شخصی تلقی می‌شود؛

– عدم ذکر نام افراد، در رابطه با هویت خود فرد؛

– جای خلوت، در رابطه با دسترسی به مکان افراد (Weber.2016:237).

حق حفاظت از حریم خصوصی را می‌توان در زمره حقوق بنیادین و مسلم بشر دانست و یا به‌عنوان حق شخصی و از جمله حقوق مالکیت به حساب آورد. به خصوص اطلاعات حساس ممکن است از ارتباط مطلق با فرد تا مسائل مهم اجتماعی در جریان باشد. در نهایت مهم‌ترین موضوع در رابطه با حریم خصوصی، ممانعت از استفاده نابجا از اطلاعات شخصی است.

۳– روش تحقیق: روش پژوهش توصیفی–تحلیلی با مراجعه به قوانین موجود در کشور ایران و مطالعه مقررات کشورهای پیشرو در حوزه مورد مطالعه است.

بحث و نظر

۱– تهدیدهای امنیتی در فضای اینترنت اشیا

لازم به ذکر است که مخاطرات موجود در سیستم‌های قدیمی اینترنتی نیز وجود داشته است اما با توضیحاتی که در ادامه بیان می‌گردد، پر اهمیت شدن این موارد پس از ایجاد اینترنت اشیا مشاهده می‌گردد. متخصصان بر این باورند که اینترنت اشیا مخاطرات بالقوه زیادی برای مشترکین در زمینه امنیتی ایجاد می‌نماید، از جمله این موارد می‌توان به موارد زیر اشاره کرد. (Weber, 2010: 44)

۱–۱– امکان دسترسی غیرمجاز و سوءاستفاده از اطلاعات شخصی

اینترنت اشیا در وسایلی همچون کامپیوترهای شخصی یا لپ‌تاپ‌ها، به دلیل فقدان امنیت کافی می‌تواند منجر به دسترسی و سوءاستفاده از اطلاعات شخصی جمع‌آوری‌شده یا منتقل‌شده از کامپیوتری به کامپیوتر دیگر شود. برای مثال تلویزیون‌های هوشمند جدید امکان اتصال به اینترنت، خرید و فروش و به اشتراک‌گذاری تصاویر را همانند کامپیوتر، به وجود آورده است. ازاین‌رو هر نوع آسیب‌پذیری که در رابطه با اطلاعات ذخیره‌شده یا منتقل‌شده در کامپیوترها موجود است در این نوع تلویزیون‌ها نیز قابل تعمیم است. اگر این تلویزیون‌های هوشمند یا سایر وسایل این‌چنینی در برگیرنده اطلاعات مهمی همچون حساب‌های مالی، رمز عبور[1] و غیره باشند؛ اشخاص غیرمجاز می‌توانند بهره‌برداری‌های نادرستی از اطلاعات در جهت جعل یا سرقت هویت، نمایند. بنابراین هرچه تعداد وسایل هوشمند موجود در خانه‌ها بیشتر گردد، امکان سوءاستفاده افراد غیرمجاز از اطلاعات شخصی افراد بیشتر می‌گردد.

۱–۲– تسهیل نفوذهای سایبری به سیستم سایرین

آسیب‌پذیری امنیتی موجود در برخی از وسایل امکان حمله یا نفوذ به شبکه‌هایی که مشترکین به آن‌ها متصل هستند را افزایش می‌دهد. برای مثال، وسایلی که به وسیله اینترنت به یکدیگر متصل شده‌اند می‌توانند به راحتی مورد استفاده در جهت ارسال ایمیل‌های مخرب قرار گیرد.

۱–۳– ایجاد مخاطرات امنیتی

در این مورد نیز اینترنت موجود می‌تواند امکان امنیت اشیا را بر هم زند. برای مثال یک هکر می‌تواند از راه دور موجب شود تا داروی مورد تقاضا به دست مصرف‌کننده آن نرسد. و یا حتی به شبکه خودرویی وارد شده و مسیر آن را تغییر دهد

[1] - Passwords

بدون اینکه حتی تماس فیزیکی با آن داشته باشد. همچنین می‌تواند با ورود به سیستم کنترل خودرو با استفاده از دستگاه‌های مسیریابی نصب شده بر روی خودرو میزان فاصله فرد تا منزل مسکونی او را تخمین زند.

۲- تهدیدهای حریم خصوصی در فضای اینترنت اشیا

در کنار مسائل مرتبط به امنیت، برخی از مخاطرات مستقیم با اطلاعات حساس گردآوری شده افراد در ارتباط است. از جمله منطقه جغرافیایی دقیق فرد، شماره حساب مالی افراد، اطلاعات مربوط به سلامت فرد و مواردی از قبیل اطلاعات شخصی، عادات، موقعیت مکانی و شرایط فیزیکی فرد در طول زمان؛ ممکن است در اختیار نهادهای متفاوتی که ارتباط مستقیم با این اطلاعات ندارند؛ قرار گیرد.

یونسکو در رابطه با حریم خصوصی اشاره کرده است که کشورهای پیشرفته در رأس آنها آمریکا شبکه‌های اطلاعاتی در اختیار دارند که روزانه بیش از سه میلیارد پیام تلفنی، دورنگار و پست الکترونیکی در سرار دنیا را شنود، کنترل و پردازش می‌کنند (معتمدنژاد،۱۳۸۴:۳۳۲).

حجم داده‌ای که حتی یک وسیله کوچک می‌تواند در خود ذخیره کند شگفت‌انگیز است. یکی از متخصصین تخمین زده است که کمتر از ۱۰۰۰۰ خانواری که از محصولات IOT استفاده می‌کنند، ۱۵۰ میلیون داده به صورت مجزا روزانه تولید می‌کنند و یا به‌طور تقریبی در هر شصت ثانیه یک داده توسط هر یک از خانوارها تولید می‌گردد.

چنین حجم عظیمی از داده‌های مجزا به کسانی که نیازمند تجزیه و تحلیل رفتار بازار هستند این امکان را می‌دهد که نسبت به زمانی که حجم داده‌ها کمتر است، بررسی مناسب‌تری داشته باشند. نکته مهم در این رابطه این است که هرچند ارائه این اطلاعات برای مصرف‌کنندگان سودمند است اما از طرفی می‌تواند مورد سوءاستفاده افراد سودجو قرار گیرد. به عبارتی دیگر اینترنت اشیا می‌تواند اطلاعات بسیار حساس الگوی رفتاری افراد را در اختیار افراد نامناسب قرار دهد. برخی از افراد مخاطراتی که این اطلاعات گردآوری شده برای حریم خصوصی ایجاد می‌کند را در قالب مثالی این‌گونه مطرح کرده‌اند که گویا ماهیگیری تور خود را بدون در نظر گرفتن شکار خاصی بی‌هدف در همه جا گسترده باشد. در واقع میزان خسارتی که این ماهیگیر برای محیطزیست ایجاد می‌کند مشابه با میزان خسارت اینترنت اشیا برای حریم خصوصی افراد است!

برخی دیگر معتقدند شرکت‌ها نیز همچون افراد عادی می‌توانند از این اطلاعات استفاده کنند؛ به این صورت که برای ارائه خدمات بیمه یا خدمات اعتباری و یا استخدام افراد در شرکت‌ها، از اطلاعات شخصی آن‌ها استفاده شود. برای مثال شرکت‌های بیمه ممکن است از بیمه‌شدگان بخواهند که با نصب نرم‌افزاری اطلاعات مربوط به عادات رانندگی خود را به بیمه‌گذار بدهند. این اطلاعات می‌تواند شامل مواردی از قبیل تعداد ترمزهای سخت و ناگهانی وسیله نقلیه، میزان مسافتی که وسیله نقلیه طی کرده است، میزان زمانی که از نیمه شب تا چهار صبح وسیله نقلیه مورد استفاده قرار گرفته است، باشند؛ که بیمه‌گذار می‌تواند در میزان بیمه خود این موارد را در نظر بگیرد. ممکن است در نگاه اول این اطلاعات مفید به نظر برسد اما می‌تواند مشکل‌ساز نیز باشد چنانچه این اطلاعات بدون اطلاع یا رضایت مصرف‌کننده اخذ شود و یا از صحت این اطلاعات نتوان اطمینان حاصل کرد (Weber, 2010: 45).

به‌عنوان مثالی دیگر می‌توان گفت ورزش و فعالیت‌های جسمی ممکن است از نظر یک فرد تنها مربوط به سلامت جسمی او باشد، اما اطلاعات جمع‌آوری‌شده مرتبط به این موضوع می‌تواند برای شرکت‌هایی که برای سلامت افراد پولی می‌پردازند؛ مهم باشد. شرکت‌های بیمه یا شرکت‌هایی که می‌خواهند نیروی سالم و فعال برای انجام کارهای خود استخدام کنند از جمله مواردی هستند که برای اطلاعات

سلامت افراد اهمیت ویژه‌ای قائل هستند. ایراد عمده افشای این‌گونه اطلاعات آنگاه مشخص می‌شود که شرکتی بر مبنای اطلاعات سلامت جسمانی یک فرد او را از تصدی شغلی محروم کند و یا علیه طبقه خاصی از افراد تبعیض قائل شود.

در همین راستا در کشور آمریکا قانون گزارش منصفانه اعتبارات[۱] تصویب گردید و محدودیت‌های خاصی برای استفاده از اطلاعات افراد وضع گردید. برای مثال یک شرکت بیمه می‌تواند از متقاضی بیمه بخواهد یک ردیاب تناسب اندام هوشمند به تن کند اما در عوض این کار بیمه‌گذار، باید میزان حق بیمه سلامت فرد را تا حد ممکن کاهش دهد.

علاوه بر مواردی که ذکر شد «استراق سمع» همواره به‌عنوان یکی از مهم‌ترین خطرات حریم خصوصی قابل بحث است. در واقع صنایع مرتبط به اینترنت اشیا مدت‌ها است که می‌دانند که چگونه از طریق وسایل ارتباط جمعی پنجره‌ای به خانه‌های شخصی افراد بگشایند. محققین در آلمان موفق به تولید تلویزیونی شده‌اند که می‌تواند آنچه را که هر یک از مخاطبین از بین برنامه‌ها انتخاب می‌کنند، تعیین کند. این تلویزیون‌ها می‌توانند به‌عنوان یک جاسوس درون خانه افراد فعالیت کنند.[۲]

در رابطه با حریم خصوصی در سال ۲۰۰۲ در کشور امریکا موسسه **پونمون**[۳] توسط دکتر **لری پونمون**[۴] تأسیس گردید. این موسسه یک مرکز تحقیقاتی در رابطه با سیاست‌گذاری در حوزه حریم خصوصی، امنیت و حفاظت از داده‌ها است. در یکی از تحقیقات انجام‌شده در این موسسه در سال ۲۰۱۷ که نتایج آن در سال ۲۰۱۸ ارائه شد، از ۱۱۰۰ کاربر اینترنت اشیا موجود در کشور امریکا، اروپا، خاورمیانه و شمال آفریقا پیرامون اینترنت اشیا با تمرکز اصلی بر حریم خصوصی نظرسنجی‌هایی صورت گرفت. از میان افراد مورد پرسش در این تحقیق ۸۲٪ افراد اعتقاد دارند با ظهور اینترنت اشیا میزان کنترل آن‌ها بر حریم خصوصی‌شان بسیار کم خواهد شد. و ۸۰٪ آنها اعتقاد داشته‌اند که در نتیجه نفوذ اطلاعاتی به شرکتهای آنها فاجعه‌ای رخ خواهد داد (Ponemon Institute Research Report, 2018:1).

۳- شاخص‌های حریم خصوصی در اینترنت اشیا

بنابر اصول فوق الذکر، تعدادی از شاخص‌های اصلی که به‌عنوان نقاط عطف حریم خصوصی در سیستم‌های آنلاین و به‌طور خاص اینترنت اشیا عبارتند از:

- حق انتخاب: هر فرد باید حق داشته باشد تا میان اطلاعات قابل اشتراک‌گذاری و غیرقابل اشتراک‌گذاری تفکیک قائل شود.
- کاربری آسان: سیستم از لحاظ تکنیکی باید به گونه‌ای طراحی شده باشد که حق انتخاب افراد در راستای حفاظت از حریم خصوصی‌شان به آسانی صورت گیرد.
- اطلاع‌رسانی: هرگونه استفاده از اطلاعات افراد باید به اطلاع مالک آن برسد.
- بازبینی: چارچوب حقوقی مناسب باید روش‌های بازبینی اطلاعات را داشته باشد تا از اجرای سیاست‌های حمایت از حریم خصوصی اطمینان حاصل کند.
- ضمانت اجرا و جبران خسارت: چارچوب حقوقی مناسب باید امکان طرح دعوی در صورت نقض حریم خصوصی را برای افراد ایجاد نماید (Basho, 2000:1510).

در رابطه با حفاظت از حریم خصوصی افراد دو نکته زیر حائز اهمیت است:

- این حفاظت ممکن است منجر به کنترل بیش از حد اطلاعات توسط افراد شود و صحت این‌گونه اطلاعات را به

---

[1]- Fair Credit Reporting Act (“FCRA”)

[۲] - برای مطالعه بیشتر ر.ک: The Federal Fair Credit Reporting Act (FCRA)

[3]- Ponemon Institute

[4]- Dr. Larry Ponemon

خطر اندازد. در همین راستا فعالیت‌های مجرمانه نیز ممکن است مخفی باقی بماند.

– حفاظت بیش از حد ممکن است در دراز مدت به قرنطینه شدن اطلاعات بیانجامد. در نتیجه لازم است تا چارچوب قانونی مناسبی برای حفاظت از حریم خصوصی با محدوده معقول پیش‌بینی شود.

۴– ارکان حفاظت از حریم خصوصی در اینترنت اشیا

با توجه به مطالعات بین‌المللی صورت گرفته در این مقاله، پنج رکن اصلی و مهمی که قوانین آینده حریم خصوصی و حفاظت داده در حوزه‌ی اینترنت اشیا باید در نظر گیرند، بیان می‌گردد. (Schmid, 2008:208)

– حق دانستن: هدف این حق، آگاه کردن افراد است. به عبارت دیگر کاربر باید بداند کدام اطلاعات او گردآوری می‌شود و توانایی این را دارد که پس از استفاده از دستگاه‌ها آن را غیرفعال کند.

– ممنوعیت قانونی: این مورد ممنوع یا محدود بودن استفاده از دستگاه‌ها را در بخش‌های خاص مطرح می‌نماید.

– امنیت فناوری اطلاعات: بهره‌برداری از برخی استانداردهای امنیتی فناوری اطلاعات که دستگاه‌ها را از خوانده شدن و بازنویسی اطلاعات آن توسط افراد غیر مجاز محفوظ می‌نماید. این نوع استانداردها می‌تواند توسط قانون‌گذار دولتی و یا نظام‌نامه‌های صنفی معرفی گردد.

– بهره‌برداری: در اینجا بیشتر تمرکز بر استفاده مناسب از دستگاه است. در واقع این رویکرد برخلاف ممنوعیت قانونی است و بر ساخت دستگاه تمرکز دارد. آنچه در این بخش اهمیت دارد ایجاد تناسب بین میزان بهره‌برداری و ممنوعیت است.

– نیروی الزام‌آوری: در این بخش مقررات قانونی از بخش فنی حمایت می‌کند تا با سرمایه‌گذاری در بخش تحقیقات، چالش‌های قانونی مربوط به دستگاه را مورد بررسی قرار دهند. در بسیاری از قوانین ملی و دستورالعمل‌های اروپایی قانون‌گذاری در بخش حریم خصوصی به شخص حقیقی محدود گشته است. اما به‌طور خاص در زمینه اینترنت اشیا، اشخاص حقوقی همچون شرکت‌ها نیز دارای حقوقی در زمینه حریم خصوصی هستند.

این موضوع بر کسی پوشیده نیست که با ظهور اینترنت اشیا، رویکرد قانون‌گذاری نوینی نیاز است تا حریم خصوصی و امنیت افراد اعم از حقیقی و حقوقی تضمین شود. ماهیت اینترنت اشیا چارچوب حقوقی متفاوتی می‌طلبد که هم‌زمان جهان‌شمول، ماندگار، فراگیر و با توجه به استانداردهای فنی در حوزه اینترنت اشیا باشد. در ادامه هر یک از این ویژگی‌ها توضیح داده شده است. (Schmid, 2008:205)

– جهان‌شمول: مسلماً کالا و خدمات در بستر اینترنت اشیا به شکل جهانی مبادله و جابجا می‌شود و الزامات فنی موجود در آن در تمام جهان ثابت است. در نتیجه چنانچه چارچوب حقوقی حاکم بر اینترنت اشیا تنها به قوانین ملی محدود شود مبادله و تجارت این‌گونه اشیا پیچیده و دشوار می‌گردد. اگر این دستگاه‌ها در سطح بین‌المللی تولید و بهره‌برداری شود مسلماً سیستم حقوقی آن نیز باید بین‌المللی باشد.

– ماندگاری: به معنی دوام بالقوه ابزار است. به‌طور خاص در این رابطه بسیار اهمیت دارد که نه تنها در چرخه تولید و بهره‌برداری دارای ماندگاری بالا باشد بلکه حتی پس از استفاده نیز قابلیت بازیافت داشته باشند.

– فراگیر: به شکل فنی اینترنت اشیا همانطور که از نامش آشکار است باید قابلیت استفاده برای اشیا، گیاهان، حیوانات و حتی انسان را نیز داشته باشد.

– استانداردهای فنی: رعایت استانداردهای فنی یکی از مهم‌ترین عوامل حفظ حریم خصوصی افراد است.

نباید فراموش کرد که علاوه بر روش‌های فنی و حقوقی که پیش‌تر در رابطه با آن‌ها توضیح داده شد، روش‌های فرهنگی نیز دارای اهمیت هستند. در همین راستا بیان تهدیدات

احتمالی که در حوزه اینترنت اشیا می‌تواند حریم خصوصی افراد را در معرض خطر قرار دهد نیز می‌تواند راه‌گشا باشد. چنانچه کاربران از مقوله اینترنت اشیا و عملکرد آن به خوبی آگاه شوند تا حدودی می‌توانند تشخیص دهند که چه فعالیت‌هایی را انجام ندهند تا ریسک انتشار اطلاعات محرمانه آن‌ها کاهش یابد. لازم است آگاه‌سازی افراد به شکل مناسب و استانداری صورت گیرد زیرا بیان بیش از حد تهدیدات می‌تواند نوعی ترس غیرعادی در کاربران ایجاد کرده و صنایع مرتبط با اینترنت اشیا را با خطر ورشکستگی مواجه سازد.

با توجه به مفهوم و ارکان حریم خصوصی و تهدیدهای احتمالی اینترنت اشیا برای آن، که تا بدینجا ذکر گردید؛ با بررسی حریم خصوصی در اسناد بین‌المللی و داخلی ابزار حمایت از آن بررسی خواهد شد.

۵- حمایت از حریم خصوصی در سطح بین‌المللی

در ماده ۱۲ اعلامیه جهانی حقوق بشر[1]، ماده ۱۷ از میثاق بین‌المللی حقوق مدنی و سیاسی[2] و ماده ۸ کنوانسیون اروپایی حقوق بشر[3] حریم خصوصی از جمله حقوق اساسی و اولیه بشر مطرح گردیده است. علاوه بر موارد مطرح شده آنچه که بیشتر با چارچوب مبحث اینترنت اشیا در ارتباط است، حکم دادگاه عالی آلمان در فوریه ۲۰۰۸ است. در این حکم به حریم خصوصی به‌عنوان یک حق اساسی و مستقل در رابطه با سیستم‌های فنی مرتبط با اطلاعات اشخاص؛ توجه ویژه گردیده است (Decision 1 BvR 370/07 and 1 BvR 595/07).

حریم خصوصی در واقع به معنی محفوظ بودن حریم هر فرد از مداخله ملی و یا بین‌المللی است. امروزه سرعت بالای پردازش اطلاعات در حوزه فناوری اطلاعات و به خصوص در زمینه انگشت‌نگاری، مدیریت شبکه، سیستم‌های زیست آگاهی،[4] پردازش الکترونیک داده‌ها و پایگاه‌های اطلاعاتی گسترده نه‌تنها جمع‌آوری و ذخیره‌سازی اطلاعات شخصی بلکه پردازش و اشتراک‌گذاری آن‌ها را نیز تسهیل نموده است.

در چنین جامعه اطلاعاتی، حفاظت از اطلاعات شخصی باید به‌عنوان موضوع مهمی مدنظر قرار گیرد. حفاظت از اطلاعات شخصی باید در واقع ایجاد توازن بین آزادی شخصی همراه با رعایت موارد امنیتی کند به گونه‌ای که حفاظت از حریم خصوصی و سهولت در جابجایی اطلاعات توأمان رعایت شود. از این‌رو پیشنهادهایی در اتحادیه اروپا در راستای حفاظت از حریم خصوصی بیان شده است: یکی از راه‌های حفاظت از حریم خصوصی می‌تواند تشکیل کمیته ضد نظارت باشد. این کمیته می‌تواند نظارت ملی و بین‌المللی را به حداقل کاهش دهد و در راستای تدوین قانون حفاظت از حریم خصوصی کمک کند. یکی دیگر از روش‌های حفاظت از حریم خصوصی می‌تواند این‌گونه باشد که هر فردی توانایی غیرفعال کردن دستگاه‌ها مرتبط به اطلاعات شخصی خود را داشته باشد. این فرایند به نام «سکوت تراشه‌ها»[5] معروف شده است.

دامنه کاربرد حقوق بشر امروزه نسبت به گذشته تغییراتی کرده است. در گذشته این باور وجود داشت که تنها ارکان دولتی امکانات و قابلیت صدمه زدن به حقوق بشر و از جمله آن حریم خصوصی را دارند. در نتیجه تنها فرد یا افراد غیردولتی شایستگی حفاظت از حریم خصوصی را دارند اما امروزه با گسترده شدن امکانات و پیشرفت تکنولوژی هر فرد حقیقی یا حقوقی امکان تعرض به حریم خصوصی دیگران را

---

[1] - Universal Declaration of Human Rights (UDHR), 1948.

[2] - International Covenant on Civil and Political Rights, 1966.

[3] - European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

[4] - Bio-awareness Systems.

[5] - Silence of the Chips.

دارد و در نتیجه حفاظت از آن به مراتب دشوارتر و با اهمیت‌تر گردیده است.

هرچند موارد پراکنده‌ای از اسناد حمایتی حریم خصوصی بیان گردید اما به‌طور کلی در سطح بین‌المللی هنوز سند جامعی که در برگیرنده مفهوم حریم خصوصی و حفاظت از داده‌ها باشد تدوین نگردیده است. با وجود اینکه قوانین حقوق بشری در ذات خود به حریم خصوصی اشاره داشته‌اند اما از بسیاری از جهات حفاظت مذکور کافی نمی‌باشد. بنابراین به‌طور کامل آشکار است که مشارکت در قانون‌گذاری در سطح بین‌المللی برای اجرای کارآمد اصول حریم خصوصی در دنیای مجازی لازم است.

از آنجایی که مصادیق امنیت و حریم خصوصی در هر کشور با کشور دیگر متفاوت است، پیشنهاد می‌شود اصول کلی و اولیه مربوط به این حوزه توسط قوانین بین‌المللی تدوین گردد و جزئیات قوانین توسط بخش خصوصی شرح و توسعه یابد. در نهایت نباید فراموش کرد که امنیت و حریم خصوصی موضوعاتی نیست که تنها محدود به مباحث قانون‌گذاری باشد بلکه محققین حوزه فناوری اطلاعات باید عواقبی که هر اختراع جدید در حوزه اخلاق ایجاد می‌کند را نیز در نظر گیرند.

۶- حفاظت از حریم خصوصی در قوانین ایران

۶-۱- پیشینه حفاظت از حریم خصوصی در ایران

قانون اساسی ایران به حریم خصوصی از طریق بیان مصادیق توجه داشته است. اصول قانون اساسی به‌ویژه در فصل حقوق ملت با مفهوم حریم خصوصی در ارتباط و وابستگی‌اند و در عین حال هیچ اصلی به‌صراحت به مسئله حریم خصوصی نپرداخته است. با این حال شاید بتوان اصل‌های ۲۲، ۲۳ و ۲۵ قانون اساسی را مرتبط‌ترین اصول با حریم خصوصی افراد دانست:

اصل بیست و دوم: «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند.»

اصل بیست و سوم: «تفتیش عقاید ممنوع است و هیچ‌کس را نمی‌توان به صرف داشتن عقیده‌ای مورد تعرض و مؤاخذه قرار دارد.»

اصل بیست و پنجم: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق سمع و هر گونه تجسس ممنوع است مگر به حکم قانون.»

نحوه نگارش اصل هیچ منعی برای گسترش دایره شمول آن به مصادیق جدید نظیر نامه‌های الکترونیک ایجاد نمی‌کند. استثنای پایانی مگر به حکم قانون خود دایره وسیعی از اقدامات قانونی ـ قضایی را لازم می‌آورد. این استثنا به این معنا است که موارد چنین تجسسی باید دقیقاً در قانون روشن شود و در هر مورد خاصی باید با حکم پیشین مقام قضایی وفق شرایط قانونی انجام گردد.

ماده ۱۰۰ قانون برنامه پنج ساله چهارم، دولت را مکلف به تدوین لایحه منشور حقوق شهروندی کرد. یکی از محورهایی که باید در این قانون تعریف و مورد حمایت قرار می‌گرفت، حفظ و صیانت از حریم خصوصی افراد بود. دولت در آن زمان، لایحه حمایت از حریم خصوصی را همراه چند لایحه دیگر تقدیم مجلس شورای اسلامی کرد. با این حال مجلس هیچ‌گاه وارد بررسی این لایحه نشد، زیرا از طرفی نمایندگان مجلس با آن از در مخالفت وارد شدند و از طرف دیگر دولت جدید در فروردین ۱۳۸۵ اقدام به استرداد آن نمود. این در حالی بود که گزارش کارشناسی مرکز پژوهش‌های مجلس به شماره مسلسل ۷۵۹۱ از آن لایحه استقبال کرد. لایحه مذکور دارای ۷ فصل و ۸۳ ماده و با سرفصل‌هایی همچون حریم خصوصی جسمانی، حریم خصوصی اماکن و منازل، حریم خصوصی در محل کار، حریم

خصوصی اطلاعات، حریم خصوصی ارتباطات و مسؤولیت‌های ناشی از نقض حریم خصوصی توصیف کرده بود. در آن لایحه مجازات نقض‌کنندگان هر یک از موارد حریم خصوصی جداگانه تشریح شده بود که حبس از سه ماه تا سه سال و انفصال از خدمت و محرومیت سه تا پنج سال از جمله آن مجازات‌ها بود.

در قانون آیین دادرسی کیفری در موارد مختلف همچون مواد ۵۵، ۵۶، ۵۷، ۵۸، ۱۱۹، ۱۲۴ و... به مسأله حریم خصوصی توجه نشان داده شده است. مثلاً قانون، مقامات قضایی را مکلف می‌کند بازرسی و تفتیش اماکن با رعایت ضوابط قانونی عنداللزوم در اوقات روز و نه شب صورت بگیرد.

این توجه در قوانین دیگر نیز صورت گرفته است. در بهمن ۱۳۸۷ قانون انتشار و دسترسی آزاد به اطلاعات از تصویب مجلس شورای اسلامی گذشت. بر اساس این قانون **«مؤسسات عمومی مکلف‌اند اطلاعات موضوع این قانون را در حداقل زمان ممکن و بدون تبعیض در دسترسی مردم قرار دهند.»** در مقابل این تکلیف چنین حقی نیز برای شهروندان تدارک دیده شده است که **«هر شخص ایرانی حق دسترسی به اطلاعات عمومی را دارد، مگر آن که قانون منع کرده باشد.»**

با این حال انتشار عمومی اطلاعات استثنائاتی دارد که در فصل چهارم، ماده ۱۴ این قانون پیش‌بینی شده است. یکی از این استثنائات، حفظ حریم خصوصی افراد است: **«چنانچه اطلاعات درخواست شده مربوط به حریم خصوصی اشخاص باشد یا در زمره اطلاعاتی باشد که با نقض احکام مربوط به حریم خصوصی تحصیل شده است، درخواست دسترسی باید رد شود.»** البته امکان افشای این اطلاعات با رضایت شخصی که حریم خصوصی او در معرض نقض قرار دارد، پیش‌بینی شده است.

در ماده ۲۲ کنوانسیون حقوق افراد دارای معلولیت که در آذر ۱۳۸۷ از تصویب مجلس شورای اسلامی گذشته است، مسأله حفظ حریم خصوصی افراد دارای معلولیت مطرح شده است. این قبیل افراد باید از دخالت خودسرانه در حریم خصوصی مصون باشند و به‌طور برابر با دیگران در کنف حمایت‌های دولت برای حفظ حریم خصوصی قرار گیرند.

۶-۲- حفاظت از حریم خصوصی در حوزه اینترنت اشیا ازمنظر حقوق ایران

مطالعات تطبیقی که در این مقاله به آن اشاره شد نشان می‌دهد اصول و قواعد بین‌المللی به صورت عام در راستای حفظ حریم خصوصی به‌عنوان یکی از مصادیق حقوق بشر دارای اهمیت است. از طرفی بحث‌های منطقه‌ای در محدوده اتحادیه اروپا و کنفرانس‌های پراکنده‌ای در ایالات متحده آمریکا و سایر کشورها لزوم تدوین چارچوب کارآمد و حفاظت از حریم خصوصی را مورد تأکید قرار داده‌اند. در این میان تدوین یک چارچوب حقوقی مناسب به گونه‌ای متعادل که تضمین‌کننده گردش اطلاعات و حفاظت اطلاعات به شکل موازی باشد، داری اهمیت ویژه‌ای است.

در داخل کشور ایران نیز به تعدادی از مهم‌ترین مفاد قانونی مرتبط به حریم خصوصی اشاره شد اکنون به نظر می‌رسد قانونی که بیشترین ارتباط با حوزه اینترنت اشیا را دار است، قانون تجارت الکترونیک است و همچنین مصوبه سازمان تنظیم مقررات و ارتباطات رادیویی است که در ادامه توضیحات بیشتری پیرامون آن‌ها ارائه می‌گردد.

قانون تجارت الکترونیک: جمهوری اسلامی ایران در سال ۱۳۸۲ قانونی را تحت عنوان «قانون تجارت الکترونیک» به منظور شناسایی معاملات و اسناد الکترونیکی به تصویب رساند. ماده ۱ چنین مقرر می‌دارد که **این قانون مجموعه اصول و قواعدی است که برای مبادله آسان و ایمن اطلاعات در واسطه‌های الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به کار می‌رود.** مفاد این ماده قانونی در دو جنبه بسیار مهم است:

- قلمرو این قانون، محدود به فعالیت‌های تجاری نمی‌باشد. مقررات ماده مذکور شامل فعالیت‌های تجاری و غیر تجاری است.

– همچنین قلمرو اجرای این قانون محدود به اینترنت و شبکه‌های کامپیوتری نمی‌گردد، بلکه شامل هر گونه واسطه الکترونیکی دیگر علاوه بر اینترنت، از جمله سیستم‌های مبادله الکترونیکی داده‌ها و انتقال وجوه، پست الکترونیکی، فاکس، تلفن و غیره می‌گردد.

قانون‌گذار در ماده ۱ الفاظ عام «مبادله آسان و ایمن اطلاعات» را به کار برده است و در مفاد این ماده، الفاظی چون تجار، روابط تجار، اعمال تجاری و امور تجاری دیده نمی‌شود و با توجه به این که مقنن بدون اشاره به واسطه الکترونیکی خاص از کلمه «واسطه‌های الکترونیکی» استفاده کرده است؛ لذا عنوان «قانون ارتباطات الکترونیک» با مفاد ماده ۱ و سایر مواد دیگر این قانون سازگاری بیشتری دارد تا عنوان «قانون تجارت الکترونیک» (ساورایی،۱۳۹۱:۵۳۳). عام بودن قلمرو این قانون از این جهت دارای اهمیت است که می‌توان در رابطه با موضوع اینترنت اشیا از بسیاری از مفاد این قانون بهره جست و این موضوع بسیار امیدبخش است زیرا در چنین حوزه جدید و روزآمدی که بسیاری از کشورهای پیشرفته نیز به دلیل گستردگی بحث هنوز قانون جامعی ندارند، در کشور ایران، قانونی موجود است که تا حدودی مرتبط به این حوزه است. در ادامه مفاد مرتبط به حوزه اینترنت اشیا مورد بررسی قرار می‌گیرد.

در ماده ۲ قانون مذکور بند الف، تعریف واژه **«داده پیام» بیان می‌دارد: هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسائل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.**

همان‌طور که مشاهده می‌شود داده پیام در متن ماده به گونه‌ای تعریف شده است که در بحث اینترنت اشیا بسیار کارآمد است. اطلاعات فردی که در حوزه حریم خصوصی و حفاظت از آن دارای اهمیت بسیار زیادی است؛ در قالب همین داده پیام‌ها در فضای اینترنت قرار می‌گیرد و این اطلاعات به راحتی قابل سوء استفاده توسط تولیدکنندگان و صاحبان صنایع و یا سایر کاربران فضای مجازی، می‌باشد. اما در فصل سوم تحت عنوان حمایت از داده پیام‌های شخصی، به نوعی از حریم خصوصی افراد حمایت شده است. ماده ۵۸ از همین فصل بیان می‌کند: «**ذخیره، پردازش و یا توزیع داده پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیر قانونی است.**»

ماده مذکور ذخیره، پردازش و توزیع داده‌های شخصی را مشروط به رضایت افراد نموده است. اما در ماده بعدی از همین قانون برای داده‌هایی که رضایت اشخاص را نیز دارد شروطی بیان داشته است. طبق ماده ۵۹ «**در صورت رضایت شخص موضوع داده پیام نیز به شرط آن که محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع داده پیام‌های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:**

– اهداف آن مشخص بوده و به‌طور واضح شرح داده شده باشند.

– داده پیام باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع داده پیام شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.

داده پیام باید صحیح و روزآمد باشد.

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

– شخص موضوع داده پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه در خواست محو کامل پرونده رایانه‌ای داده پیام‌های شخصی مربوط به خود را بنماید.

شرایط مذکور مطرح شده در قانون تجارت الکترونیک، مشابه کارگاه آموزشی است که در ۱۹ نوامبر سال ۲۰۱۳ با عنوان «اینترنت اشیا: امنیت و حریم خصوصی در جهان متصل»[1] در

[1]- The Internet of Things: Privacy and Security in a Connected World.

آمریکا برگزار شد. اعضای این کارگاه در رابطه با اصول اجرایی اطلاعات منصفانه‌ای (FIPPs[1]) که عبارتند از آگاهی، حق انتخاب، حق دسترسی، صحت، به حداقل رساندن اطلاعات، امنیت و مسؤولیت در صورت نقض حقوق دیگران در فضای اینترنت اشیا می‌باشد، بحث و گفت‌وگو کردند. شرط (الف) همان چیزی است که در مذاکرات موجود در کارگاه آموزشی از آن به‌عنوان Transparency (شفافیت) یاد می‌شود؛ شرط (ب) همان Data Minimization است؛ مورد (ج) در بیشتر متون لاتین در حوزه اینترنت اشیا با کلمه Accuracy بیان شده است؛ مورد آخر نیز بیان کننده کلمات Choice و Access می‌باشد. می‌توان نتیجه گرفت شروط مذکور در قانون، هم‌خوانی مناسبی با مباحث مطرح شده در نشست‌های بین‌المللی در حوزه اینترنت اشیا دارد، که این هم‌خوانی نوید بخش کارآمدی قانون مذکور است.

ماده ۶۰ قانون، ذخیره، پردازش و یا توزیع داده پیام‌های مرتبط به سوابق پزشکی و بهداشتی افراد را تابع آیین‌نامه‌ای دانسته است که توسط وزارت بهداشت، درمان و آموزش پزشکی پیشنهاد شود و توسط سازمان مدیریت و برنامه‌ریزی کشور تهیه و به تصویب هیأت وزیران برسد.

با توجه به حوزه بحث ماده مذکور که در رابطه با سوابق پزشکی و بهداشتی افراد است و این حوزه همان‌طور که پیش‌تر اشاره شد در فضای اینترنت اشیا بسیار در معرض تهدید است و می‌تواند یکی از عوامل مهم در تعیین نرخ بیمه مؤسسات مرتبط باشد، شایسته است که آیین‌نامه مذکور تطبیق تشریفات بیان شده به سرعت تهیه و تصویب شود.

ماده ۶۱، بررسی سایر موارد راجع به دسترسی به موضوع داده پیام را موکول به آیین‌نامه‌های مربوطه کرده است. هرچند که قانون تجارت الکترونیک در برخی مواد اشاراتی راه‌گشا به حوزه حفاظت از داده پیام‌های شخصی در بستر معاملات الکترونیکی داشته است اما بسیار واضح است که این مواد مختصر پاسخ‌گوی تمام نیازهای موجود در بحث اینترنت اشیا نمی‌باشد. از طرف دیگر، ماده ۶۱ به گونه‌ای تدوین شده است که در زمان کوتاه می‌توان نیاز فوری در این حوزه را با تصویب آیین‌نامه‌ای تحت عنوان حفاظت از داده پیام‌های شخصی در حوزه اینترنت اشیا، پاسخ گفت.

با توجه به اینکه حریم خصوصی در موضوع اینترنت اشیا تنها معطوف به شخص حقیقی نیست و حریم خصوصی شخص حقوقی را نیز در برمی‌گیرد ماده فصل دوم قانون تجارت الکترونیک تحت عنوان حمایت از اسرار تجاری است که در بحث اینترنت اشیا نیز می‌تواند راه‌گشا باشد.

ماده ۶۴ بیان می‌دارد که «**به منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و مؤسسات برای خود و یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب کننده به مجازات مقرر در این قانون خواهد رسید.**»

ماده ۶۵ در تعریف اسرار تجاری الکترونیکی بیان می‌کند که «**اسرار تجاری الکترونیکی داده‌پیامی است که شامل اطلاعات، فرمول‌ها، الگوها، نرم‌افزارها و برنامه‌ها، ابزار و روش‌ها، تکنیک‌ها و فرآیندها، تألیفات منتشر نشده، روش‌های انجام تجارت و داد و ستد، فنون، نقشه‌ها و فراگردها، اطلاعات مالی، فهرست مشتریان، طرح‌های تجاری و امثال این‌ها است، که به‌طور مستقل دارای ارزش اقتصادی بوده و در دسترس عموم قرار ندارد و تلاش‌های معقولانه‌ای برای حفظ و حراست از آن‌ها انجام شده است.**»

هر چند بهتر بود ابتدا تعریف بیان می‌شد سپس حمایت از آن، اما به همین منوال نیز مشخص است که حریم خصوصی و اسرار تجاری اشخاص حقوقی تحت حمایت قانونی واقع شده است.

در مواد ۶۷ و ۶۸ کلاهبرداری و جعل مشمول مجازات مطرح شده است که با توجه تفاوت‌هایی که این جرایم در حوزه اینترنت اشیا با روش‌های کلاهبرداری سنتی دارد، لازم است آئین‌نامه مربوطه به آن تصویب شود (قاسم زاده، رئیسی

[1]- Fair Information Practice Principles (FIPPs).

درزکی، ۶۱۱:۱۳۹۹). باب چهارم در قانون مذکور در رابطه با جرائم و مجازات‌ها است. در این قسمت مجازات هر یک از تخلفات موجود در این قانون تعیین گردیده است. با توجه به حوزه بحث حاضر مجازات‌های مرتبط به شرح زیر است:

فصل دوم- نقض حمایت از داده‌پیام‌های شخصی/ حمایت داده

ماده ۷۱: هر کس در بستر مبادلات الکترونیکی شرایط مقرر در مواد ۵۸ و ۵۹ این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود.

ماده ۷۲: هرگاه جرائم راجع به داده‌پیام‌های شخصی توسط دفاتر خدمات صدور گواهی الکترونیکی[1] و سایر نهادهای مسئول ارتکاب یابد، مرتکب به حداکثر مجازات مقرر در ماده ۷۱ این قانون محکوم خواهد شد.

ماده ۷۳: اگر به واسطه بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی الکترونیکی جرائم راجع به داده‌پیام‌های شخصی روی دهد، مرتکب به سه ماه تا یک سال حبس و پرداخت جزای نقدی معادل پنجاه میلیون (۵۰۰۰۰۰۰۰) ریال محکوم می‌شود.

مبحث چهارم- نقض حفاظت از داده‌پیام در بستر مبادلات الکترونیکی

فصل دوم- نقض اسرار تجاری

ماده ۷۵: متخلفین از ماده ۶۴ این قانون و هرکس در بستر مبادلات الکترونیکی به منظور رقابت، منفعت و یا ورود خسارت به بنگاه‌های تجاری، صنعتی، اقتصادی و خدماتی، با نقض حقوق قراردادهای استخدام مبنی برعدم افشای اسرار شغلی و یا دستیابی غیرمجاز، اسرار تجاری آنان را برای خود تحصیل نموده و یا برای اشخاص ثالث (۵۰۰۰۰۰۰۰) ریال محکوم خواهد شد.

ملاحظه می‌شود که مواد بالا به جرم‌انگاری بیشتر تخلفاتی که حریم خصوصی را در معرض خطر قرار می‌دهند، پرداخته است. بهتر بود قانون‌گذار جز در مواردی همچون جعل و کلاهبرداری، از جرم‌انگاری در سایر موارد خودداری می‌کرد و به مسؤولیت مدنی و پرداخت جریمه اکتفا می‌نمود با این وجود توجه به این موارد صرف نظر از انتقاداتی مذکور، شایسته است.

نتیجه‌گیری

در این مقاله مفهوم حریم خصوصی و امنیت و تهدیدهای احتمالی آنها در حوزه اینترنت اشیا بیان گردید. پس از بررسی تفاوت‌های موجود پیرامون مفهوم این دو مقوله می‌توان گفت امنیت همان قواعدی است که مانع تهدید شدن اینترنت اشیا در قالب یک سیستم می‌شود. عنصر اصلی در این مفهوم تأکید بر ممانعت و جلوگیری سیستماتیک است در حالی که حریم خصوصی در زمره حقوق بنیادین و مسلم بشر است و می‌توان آن را به‌عنوان حق شخصی از جمله حقوق مالکیت به حساب آورد. مهم‌ترین موضوع در رابطه با حریم خصوصی، توانایی حفظ اطلاعات فردی و ممانعت از استفاده نابجا از این‌گونه اطلاعات توسط دولت‌ها و افراد سودجو است.

آشکار است که حریم خصوصی در فضای نوین اینترنت اشیا بسیار بیشتر از گذشته در معرض تهدید و سوءاستفاده قرار گرفته است. از این‌رو لزوم حفاظت از آن به خوبی احساس می‌شود. روش‌های حفاظت از حریم خصوصی در سه حوزه فنی، حقوقی و فرهنگی قابل دسته‌بندی می‌باشد که فصل مشترک تمامی آن‌ها توجه به حفاظت حداکثری اطلاعات فردی در کنار استفاده کارآمد از اینترنت اشیا است. در واقع آنچه دارای اهمیت است ایجاد توازن بین حفظ حریم شخصی افراد و گردش آزاد اطلاعات -لازمه اصلی اینترنت اشیا- است. توجه به همین توازن بهره‌مندی کارآمد و عادلانه از اینترنت اشیا را میسر می‌نماید.

بررسی‌های صورت گرفته در قوانین داخلی پیرامون حریم خصوصی حاکی از این حقیقت است که کمبود قانون اختصاصی با عنوان حمایت از حریم خصوصی همگام با پیشرفت‌های اخیر فنی کاملاً محسوس می‌باشد. قانون مد

[1]- ماده ۳۱ قانون تجارت الکترونیکی: دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی‌های اصالت (امضای) الکترونیکی می‌باشد.

نظر در این حوزه باید به صورت پویا و قابل انطباق با قواعد دسترسی به اطلاعات باشد. در شرایط فعلی و با توجه به اینکه تصویب قانون جدید ممکن است زمان‌بر باشد، از این‌رو اصلاح قانون موجود پیشنهاد می‌گردد.

همگامی با استانداردهای فنی و اطلاع‌رسانی و فرهنگ‌سازی در حفظ حریم خصوصی دارای اهمیت فراوان است و البته واضح است که فقدان قانون حریم خصوصی در این حوزه محسوس است لذا پیشنهاد می‌شود در صورت اقدام برای تصویب قانون مذکور موارد زیر که حاصل مطالعات تطبیقی می‌باشد نیز مد نظر قرار گیرد:

الف. پیش از هرچیز لازم است مفهوم حریم خصوصی و قلمرو آن تعیین گردد.

ب. فردی که اطلاعاتش در فضای اینترنت اشیا موجود است دارای حقوقی است که در گام اول حمایت از حریم خصوصی رعایت آن‌ها الزامی است. این حقوق عبارت‌اند از:

– حق دانستن: فرد باید به شکل کاملی بداند که اطلاعات او تا چه میزان و برای چه هدفی نگه‌داری می‌شود؛

– حق انتخاب: پیرو حق دانستن فرد باید حق داشته باشد تا چنانچه لازم دید از میان اطلاعات شخصی خود آن مواردی که قابل اشتراک‌گذاری نیست را تفکیک کند؛

– حق دسترسی: فرد باید به اطلاعات خود دسترسی داشته باشد؛

– حق اصلاح: پیرو حقوق مذکور در بندهای قبلی فرد باید حق اصلاح، به‌روزرسانی و حذف اطلاعات شخصی خویش را داشته باشد.

ج. پس از بیان حقوق فردی، داده‌های فردی قطعاً از موارد دارای اهمیت است که باید مورد حمایت قانون‌گذار قرار گیرد. از منظر قانونی داده‌ها باید دارای صحت، شفافیت، تا حد امکان مختصر و در ارتباط با هدف تصریح‌شده باشند.

د. در نهایت لازم است اپراتور و یا شخص مسؤول در قانون معرفی شود. پس از آن میزان مسؤولیت و نحوه جبران خسارت باید توسط قانون‌گذار معرفی گردد. در همین راستا لازم است استانداردهای فنی و زیرساختی لازم برای حفظ امنیت داده‌های شخصی کاربران معرفی گردد.

ه. پر واضح است که مقوله اینترنت اشیا یک فضای جهانی و گسترده است و محیطی چنان گسترده الزاماً نیازمند تطابق با استانداردهای جهانی و شرکت در کنفرانس‌ها و نشست‌های بین‌المللی مرتبط به این موضوع را دارا می‌باشد.

ملاحظات اخلاقی: در ابتدا تا انتهای این تحقیق، اصول صداقت و امانتداری رعایت گردیده است

تعارض منافع: تدوین این مقاله، فاقد تعارض منافع بوده است.

سهم نویسندگان: نویسنده مسؤول هفتاد درصد و نویسنده دوم، سی درصد در تهیه مقاله حاضر مشارکت داشته‌اند.

تشکر و قدردانی: از کلیه‌ی کسانی که در تهیه این مقاله ما را یاری رساندند، تشکر می‌نماییم.

تأمین اعتبار پژوهش: این پژوهش فاقد تأمین کننده مالی می‌باشد.

منابع و مآخذ

الف. منابع فارسی

۱- کتب و مقالات

- انصاری، باقر (۱۳۸۲). «مقدمه‌ای بر مسؤولیت مدنی ناشی از ارتباطات اینترنتی». *مجله دانشکده حقوق*، ۶۲(۰): ۹-۲۵

- انصاری، باقر (۱۳۹۱). *حقوق حریم خصوصی*. تهران: سازمان مطالعه و تدوین کتب علوم انسانی (سمت).

- جهان بزرگی، احمد (۱۳۸۸). *امنیت در نظام سیاسی اسلام*. تهران: انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.

- حسینی شیرازی، سید محمد (۱۴۲۸). *من فقه الزهرا*. جلد دوم، چاپ اول، قم: رشید.

- حسینی واسطی زبیدی حنفی، محب الدین سید محمد مرتضی (۱۴۱۴). *تاج العروس من جواهر القاموس*. جلد هشتم، بیروت: دارالفکر للطباعه و التوزیع.

- ساورایی، پرویز (۱۳۹۱). «قلمرو قانون تجارت الکترونیک ایران تحلیل حقوقی ماده یک». *مجله تحقیقات حقوقی*، ۱۵(۵۷): ۴۹۵-۵۳۲

- فیومی، احمد بن محمد مقری (بی‌تا). *المصباح المنیر فی غریب الشرح الکبیر للرافعی*. جلد اول، قم: منشورات دارالرضی.

- قاسم زاده لیاسی، فلور و رئیسی درزکی، لیلا (۱۳۹۹). «کاربست قوانین ومقررات ارتباطی در صیانت از حریم خصوصی شهروندان در فضای سایبر». *مجله مطالعات حقوق عمومی*، ۵(۲): ۵۹۷-۶۱۶

- قنواتی، جلیل و جاور، حسین. (۱۳۹۰). «حریم خصوصی، حق یا حکم». *مجله حقوق اسلامی*، ۸(۳۱): ۷- ۳۲

- معتمدنژاد، کاظم (۱۳۸۴). *جامعه اطلاعاتی، اندیشه‌های بنیادی، دیدگاه‌های انتقادی و چشم اندازهای جهانی*. تهران: پدیده.

۲- قوانین و مقررات

قانون اساسی.

قانون انتشار و دسترسی آزاد به اطلاعات.

قانون آیین دادرسی کیفری.

قانون برنامه پنج ساله چهارم.

قانون تجارت الکترونیک.

کنوانسیون حقوق افراد دارای معلولیت.

ب. منابع انگلیسی

1- Books & Articles

- Basho, K (2000). "The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?" *California Law Review*, 88(5): 1507-1545

- Fabian, B & Günther, O (2009). "Security Challenges of the EPCglobal Network". *Communications of the ACM*, 52(7): 121-125

- Haller, S; Karnousjos, S & Schroth, Ch (2008). "The Internet of Things in an Enterprise Context". *John Dominigue/Dieter Fensel/Paolo Traverso (Eds)*: 14-28.

- Schmid, V (2008). "Radio Frequency Identification Law Beyond 2007". *Chrstian Floerkemeier Marc Langheinrich Elgar Fleisch Friedemann Matttern Sanjay E. Sarma* (Eds.):196-213.

- Weber, R. H. & Weber, R (2010). *Internet of Things, Legal Perspectives*. Berlin: Springer-Verlag.

- Weber, R.H. (2009). “Internet of Things- Need for a New Legal Environment?” *Computer & Security Report*, 25(6): 522-527.

2- Documents

- Assembly Resolution 217 (III), UN Doc. A/810 (1948), UN GOAR, 3rd Sess. Supp. No. 13, available at: http://un.org/Overview/rights/html.

- Council of Europe Contribution to the 2nd Preparatory Committee for the WSIS, Democracy, Human Rights and the Rule of Law in the Information Society, section 18.

- Decision 1 BvR 370/07 and 1 BvR 595/07; to this decision see Weber, Vertraulichkeit und Integrität; Stögmüller; Holznagel/Schumacher.

- European Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, ETS No. 5, 213 UNTS 221.

- Gianmarco Baldini/Trevor Pierce, (January 2015), IOT Governance, Privacy and Security Issues, European Reaearch Cluster on Internet of Things.

- Ponemon Institute Research Report, (2018), Global Megatrends in Cybersecurity: available at: https://www.raytheon.com/cyber/cyber_megatrends

- International Covenant on Civil and Political Rights, GA Res. 2200 Annex (XXI), UN GAOR, 21st Session, Supp. No. 16, opened for signature December 16, 1966, 999 UNTS 171.

- Universal Declaration of Human Rights (UDHR), December 10, 1948, adopted by the General.

3- Websites

- https://www.investopedia.com (Last revised: 2021)

References

- Ansari, B (2003). "Introduction to Civil Liability Due to Internet Communications". *Journal of the Faculty of Law*, Tehran University of Tehran Press, 62(512): 9-25. (Persian)

- Ansari, B (2012). *Privacy Law*. Tehran: Organization for the Study and Compilation of Humanities Books. (Persian)

- Assembly Resolution 217 (III), UN Doc. A/810 (1948), UN GOAR, 3rd Sess. Supp. No. 13, available at: http://un.org/Overview/rights/html.

- Basho, K (2000). "The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?" *California Law Review*, 88 (5): 1507-1545

- Council of Europe Contribution to the 2nd Preparatory Committee for the WSIS, Democracy, Human Rights and the Rule of Law in the Information Society, section 18.

- Decision 1 BvR 370/07 and 1 BvR 595/07; to this decision see Weber, Vertraulichkeit und Integrität; Stögmüller; Holznagel/Schumacher.

- European Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, ETS No. 5, 213 UNTS 221.

- Fabian, B & Günther, O (2009). "Security Challenges of the EPCglobal Network". *Communications of the ACM*, 52(7): 121-125

- Fiyumi, A (N.D.). *Al-Misbah Al-Munir Fi Gharib Al-Sharh Al-Kabir Lel Rafi'i*. Vol 1, Qom: Manshourate Dar Al-Razi Publications. (Arabic)

- Gianmarco Baldini/Trevor Pierce, (2015), IOT Governance, Privacy and Security Issues, European Reaearch Cluster on Internet of Things.

- Haller, S; Karnousjos, S & Schroth, Ch (2008). "The Internet of Things in an Enterprise Context". *John Dominigue/Dieter Fensel/Paolo Traverso (Eds)*: 14-28.

- Hosseini Shirazi, SM (2007). *Men Fiqh Al-Zahra*. Vol 2, 1st ed. Qom: Rashid. (Arabic)

- Hosseini Wasiti Zubidi Hanafi, M (1993). *Taj ul Arous Men Javahere al Ghamous*. vol. 8, Beirut: Dar al-Fikr lel Tabayeh va Touzie. (Arabic)

- https://www.investopedia.com (Last revised: 2021)

- International Covenant on Civil and Political Rights, GA Res. 2200 Annex (XXI), UN GAOR, 21st Session, Supp. No. 16, opened for signature December 16, 1966, 999 UNTS 171.

- Jahan Bozorgi, A (2009). *Security in the Islamic Political System*. Tehran: Publications of the Institute of Islamic Culture and Thought. (Persian)

- Motamednejad, K (2005). *Information Society, Fundamental Thoughts, Critical Perspectives and Global Perspectives*. Tehran: Padideh. (Persian)

- Ponemon Institute Research Report, (2018), Global Megatrends in Cybersecurity: available at: https://www.raytheon.com/cyber/cyber_megatrends

- Qanawati, J & Javar, H (2011). "Privacy, Right or Rule". *Journal of Islamic Law*, 8(31): 7-32. (Persian)

- Qasemzadeh Liasi, F & Raeisi Darzaki, L (2020). "Application of Communication Laws and Regulations in Protecting the Privacy of Citizens in Cyberspace". *Journal of Public Law Studies*, 5(2): 597-616. (Persian)

- Savaraei, P (2012). "The Realm of Iranian Electronic Commerce Law, Legal Analysis Article 1", *Journal of Legal Research,* 15(57): 495-532. (Persian)

- Schmid, V (2008). "Radio Frequency Identification Law Beyond 2007". *Chrstian Floerkemeier Marc Langheinrich Elgar Fleisch Friedemann Matttern Sanjay E. Sarma* (Eds.): 196-213.

- Universal Declaration of Human Rights (UDHR), December 10, 1948, adopted by the General.

- Weber, R. H. & Weber, R (2010). *Internet of Things, Legal Perspectives*. Berlin: Springer-Verlag.

- Weber, R.H. (2009). "Internet of Things- Need for a New Legal Environment?" *Computer & Security Report*, 25(6): 522-52.