Iranian Journal of Public Policy
2023, Vol. 9 , No. 1 , 64-79

RESEARCH ARTICLE

The Ideal Model of Personal Data Protection Legislation in the Context of the Internet of Things in the Light of Comparative Studies

Behnaz Ahmadvand[1*], Artin Jahanshahi[2]

1- Assistant Professor of Public Law, National Research Institute for Science Policy, Tehran, Iran
2- Master of Private Law, University of Shiraz, Shiraz, Iran

*Corresponding Author's Email: **Behnazahmadvand@gmail.com**

Https://doi.org/10.22059/jppolicy.2023.92988

Received: 2 August 2022
Accepted: 5 December 2022

ABSTRACT

The Internet of Things as a new generation of connection and communication between intelligent objects through Internet is a concept that has recently entered the country's governance literature. Due to the possibility of identification and access to personal information through the analysis and combination of collected data, effective protection of personal data has been proposed as a must in the context of this technology. Iran's legal system lacks a law that is dedicated to the protection of citizens' personal data, only in the resolution of the Supreme Council of Cyberspace dated 2018-10-22, the requirements governing the Internet of Things in the National Information Network have been discussed. Based on the teachings of comparative law, we can benefit from the experiences of other systems to overcome similar challenges. Based on the descriptive analytical method, the current research has extracted the legislative patterns in the discussed field by examining all the laws and regulations of the legal systems of the European Union, the People's Republic of China, and the United States of America and answered the question of which type of legislative model is desirable for the legal system. It seems that among the proposed approaches, a combination of a comprehensive model and self-regulation with a broad definition of personal data can be a suitable option for drafting the law.

Keywords: Internet of Things, Personal Data Protection, Comprehensive Legislation, Diffuse Legislation, Self-Regulation.

فصلنامه سیاستگذاری عمومی

دوره ۹، شماره ۱، بهار ۱۴۰۲. صفحات ۷۹ - ۶۴

مقاله پژوهشی

الگوی مطلوب قانونگذاری حفاظت از داده شخصی در بستر اینترنت اشیا در پرتو مطالعات تطبیقی

بهناز احمدوند[۱*]، آرتین جهانشاهی[۲]

۱- استادیار حقوق عمومی مرکز تحقیقات سیاست علمی کشور، تهران، ایران

۲- کارشناسی ارشد حقوق خصوصی دانشگاه شیراز، شیراز، ایران

* رایانامهٔ نویسنده مسئول: Behnazahmadvand@gmail.com

تاریخ دریافت: ۱۱ مرداد ۱۴۰۱
تاریخ پذیرش: ۱۴ آذر ۱۴۰۱

Https://doi.org/10.22059/jppolicy.2023.92988

چکیده

اینترنت اشیا به عنوان نسل جدید اتصال و ارتباط اشیای هوشمند از طریق اینترنت، مفهومی است که به تازگی وارد ادبیات حکمرانی کشور شده است. با توجّه به امکان شناسایی هویّت و دسترسی به اطلاعات شخصی از طریق تحلیل و ترکیب داده‌های جمع‌آوری شده، حفاظت مؤثر از داده‌های شخصی به عنوان یک امر بایسته در بستر این فناوری مطرح شده است. نظام حقوقی ایران به علت نوپا بودن کشور در این حوزه فاقد قانونی می‌باشد که به حفاظت از داده‌های شخصی شهروندان در این مقوله اختصاص داشته باشد و صرفاً در مصوبه شورای عالی فضای مجازی به الزامات حاکم بر اینترنت اشیا در شبکه ملّی اطلاعات پرداخته شده است. پژوهش حاضر بر اساس روش تحلیلی- توصیفی با بررسی مجموع قوانین و مقررات نظام‌های حقوقی اتحادیه اروپایی، ایالات متحده آمریکا و جمهوری خلق چین، الگوهای قانونگذاری در حوزه مورد بحث را استخراج کرده است و در صدد پاسخگویی به این پرسش می‌باشد که کدام نوع الگوی قانونگذاری برای نظام حقوقی کشور، مطلوب می‌باشد. به نظر می‌رسد از میان رویکردهای مطرح شده، ترکیبی از الگوهای موجود، می‌تواند گزینه مناسبی برای تدوین قانون در کشور باشد.

واژگان کلیدی: اینترنت اشیا، حفاظت از داده شخصی، تقنین جامع، تقنین تفرُّقی، خودتنظیمی.

مقدمه

از مؤلفه‌های مُعرِّف دهه‌های اخیر که از آن تحت عنوان انقلاب صنعتی چهارم[1] یاد می‌شود می‌توان به رشد و گسترش تحوّلات و پیشرفت‌ها در حوزه فناوری اطلاعات و ارتباطات، اینترنت و اتوماسیون هوشمند اشاره کرد. چنان که گفته شده است امروزه استفاده از فناوری اطلاعات و ارتباطات دیگر یک انتخاب نیست بلکه یک امر واجب و اجتناب‌ناپذیر است (Ghanad & Aligholi, 2020:312) اینترنت اشیا از فناوری‌های نوظهور مبتنی بر اینترنت می‌باشد که با هدف اتصال دائمی بین اشیای هوشمند و تحلیل داده‌ها و تصمیم‌گیری خودکار بر اساس آن با حداقل دخالت انسان، خدماتی برای کاربران آن ارائه می‌دهد. موتور محرکه این فناوری پردازش[2] و تحلیل اطلاعات و داده‌های عظیم و کلانی است که از کاربر و محیط پیرامون او جمع‌آوری می‌گردد. فناوری‌های نوظهور علی‌رغم کاربردهای فراوانی که در زندگی انسان‌ها دارند چالش‌هایی نیز به همراه خود آورده‌اند که از جمله مهم‌ترین آن‌ها که در سطح بین‌المللی و داخلی مورد توجّه واقع شده، حفاظت از داده‌های اشخاص می‌باشد (European Commission, 2014). تدوین چارچوب حقوقی برای حفاظت از داده‌های اشخاص که متناسب با تحوّل‌های فعلی و پیش رو باشد، یک بایسته تلقی می‌گردد. همانطور که تکنولوژی به تغییر روش خود ادامه می‌دهد، ما نیز متقابلاً باید روش خود را تغییر دهیم. مهم آن است که ادراک تصورمان از حریم خصوصی در این فضا را به خوبی تکامل یافته نماییم و این را بدانیم که زمانی که ذهن خود را در حمایت از این حق اساسی طراحی می‌نماییم، تکنولوژی استعداد نهفته‌ای برای حمایت از مسأله امنیت و حریم خصوصی در این فضا خواهد داشت.(Pourghahramani & Sabernezhad, 2014: 161) اگرچه برخی به درستی به ابعاد حریم خصوصی و اهمیت حفاظت از آن در بستر اینترنت اشیا و در نتیجه به لزوم تدوین چارچوب قانونی اشاره کرده‌اند اما درباره اینکه این حمایت قانونی باید چه شاکله‌ای داشته باشند پاسخی نداده‌اند و برای قانونگذاری آتی به پیشنهاد چند مورد اکتفا کرده‌اند (Aghdasi, & Mohaghegh Damad, 2021:63). موضوع مقاله حاضر بررسی و استخراج الگوهای تقنینی در پرتو مطالعات تطبیقی و پیشنهاد برای قانونگذاری داخلی است. در حوزه قانونگذاری درباره موضوع حاضر نظام‌های حقوقی اتحادیه اروپایی، ایالات متحده آمریکا به علت داشتن سابقهٔ طولانی در این حوزه و گذر از آزمون و خطاها و نظام حقوقی چین به عنوان یکی از نظام‌های نوپا اما نظام‌مند اهمیت ویژه‌ای دارند. برخلاف نظام‌های اشاره شده؛ در ایران قانونی که به طور ویژه به حفاظت از داده‌های شخصی شهروندان در اینترنت اشیا اختصاص داشته باشد وجود ندارد و تنها در مصوبه شورای عالی فضای مجازی مورخ ۱۳۹۷/۷/۳۰ به الزامات حاکم بر اینترنت اشیا در شبکه ملّی اطلاعات پرداخته شده است. پژوهش حاضر به دنبال پاسخ به این پرسش می‌باشد که از میان الگوهای موجود برای حفاظت از داده شخصی کدام یک در نظام حقوقی کشور، مطلوب است؟ اهمیت پاسخ به پرسش مذکور در این نکته نهفته است که اینترنت اشیا در مراحل ابتدایی خود قرار دارد و در این مسیر با تغییرات گسترده در فناوری مواجه می‌باشد و از سوی دیگر پردازش داده‌ها به صورت کلان در حجم وسیع، شهروندان را با نگرانی‌هایی در مورد حریم خصوصی داده‌هایشان مواجه می‌کند. در معدود مطالعات صورت گرفته به خلاء قانونی موجود و لزوم تدوین چارچوب حقوقی اشاره شده است (Zareian & Vahed, 2020: 68) اما در این باره که قانون باید در چه ساختار و قالبی باشد و از چه داده‌های حمایت کند خلاء پژوهشی وجود دارد. در ابتدای مقاله به مفهوم و ساختار اینترنت اشیا و اهمیت حفاظت از داده‌های افراد در بستر این فناوری اشاره خواهد شد و در مبحث بعدی الگوهای قانونگذاری موجود در این حوزه مورد بررسی قرار گرفته و در نهایت الگوی مطلوب برای نظام حقوقی ایران پیشنهاد خواهد شد.

تبیین نظری مفاهیم اینترنت اشیا

در این مبحث در بادی امر به تعریف فناوری اینترنت اشیا پرداخته شده، در ادامه ساختار اینترنت اشیا و اهمیت حفاظت از داده شخصی در این بستر مورد بررسی قرار می‌گیرد.

1- Industry 4.0

۲- منظور از پردازش، هرگونه تحصیل، نگهداری، ساماندهی، ذخیره، حک و اصلاح، جایگزین کردن، استعمال، افشاء، انتقال، انتشار و اقدامات مشابه است.

تعریف اینترنت اشیا

در سال‌های گذشته پیشرفت فناوری ارتباطات بی‌سیم و شبکه به همراه کوچک‌تر شدن تجهیزات و دستگاه‌های الکترونیکی و حسگرها و نیز بهبود روش‌های محاسبات و پردازش داده از جمله رایانش ابری[1] باعث شده است موج جدیدی از نوآوری‌های مبتنی بر اینترنت که نحوه تعامل انسان با جهان اطراف خود را دستخوش تغییرات عمیقی می‌کند، پدیدار گردد. اصطلاح اینترنت اشیا به عنوان نسل جدید کاربردهای مبتنی بر اینترنت که از آن تحت عناوینی همچون شبکه اشیا[2] و اینترنت محتوی[3] نیز یاد می‌شود اوّلین بار توسط کوین اشتون در سال ۱۹۹۹ مطرح شد (Gubbi, 2013: 1646). جهان امروزی از مجموعه بی‌شماری از اشیای فیزیکی متّصل به اینترنت از گوشی موبایل، رایانه‌ها، تلویزیون‌های هوشمند، پوشیدنی‌های هوشمند، حسگرهای دارای قابلیت محاسباتی گرفته تا لوازم خانگی و خودران‌ها و خانه‌های هوشمندی که توانایی تحلیل و تصمیم‌گیری بدون دخالت یا با حداقل دخالت انسان دارند تشکیل یافته است. تعامل اشیای هوشمند با استفاده از فناوری‌های متعدد از جمله شبکه‌های بُرد کوتاه و بُرد بلند (Benar, 2019: 2) این امکان را فراهم می‌کند که فعالیت‌هایی نظیر نظارت بر محیط، ارائه گزارش از وضعیت و دریافت دستورالعمل‌ها را انجام دهند و از طریق تولید، جمع‌آوری، مبادله و تحلیل داده‌ها خدماتی را با کم‌ترین دخالت انسان به کاربران نهایی ارائه کنند. برای اینترنت اشیا تعاریف متعددی مطرح شده است؛ برای مثال اتحادیه بین‌المللی مخابرات[4] آن را یک زیرساخت جهانی برای جامعه اطلاعاتی که خدمات پیشرفته را با اتّصال چیزها (فیزیکی و مجازی) بر اساس فناوری‌های اطلاعاتی و ارتباطاتی موجود ارائه می‌دهد تعریف کرده است (ITU, 2012: 1). در برخی تعاریف دیگر نیز آمده است اینترنت اشیا به دنبال ایجاد پلی میان جهان واقع و جهان مجازی و محو مرز بین این دو و ارائه خدمات متنوع به کاربران از طریق ارتباطات ماشین به ماشین است (IEEE, 2015). به طور کلی می‌توان گفت اینترنت اشیا معماری نوظهور جهانی مبتنی بر اینترنت است که هدف آن اتصال و تسهیل ارتباط و تعامل بین اشیای متّصل به اینترنت و ارائه خدمات آنی به مصرف‌کنندگان به شیوه‌ای کاربردی و قابل اعتماد است. به عبارت دیگر اینترنت اشیا به ارتباط و تبادل اطلاعات سنسورها و دستگاه‌ها و تجهیزات از طریق اینترنت و تحلیل و تصمیم‌گیری خودکار داده‌ها برای ارائه خدمات منحصر به فرد اطلاق می‌گردد؛ این مفهوم می‌تواند به سادگی ارتباط یک گوشی هوشمند با تلویزیون، خانه هوشمند یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک باشد (Haller et.al, 2008:5). فناوری اینترنت اشیا با تبدیل بسیاری از شرکت‌ها به کسب و کارهای دیجیتال و تسهیل مدل‌های کسب‌وکار جدید، بهبود کارایی و افزایش تعامل کارکنان و مشتریان، تأثیر زیادی بر اقتصاد خواهد داشت. بر اساس آمارها و تخمین‌های موجود تا سال ۲۰۳۰ در کل جهان بیش از ۲۹,۴ میلیارد اشیای هوشمند به فناوری اینترنت اشیا متّصل خواهند شد (Statista, 2022). برنامه‌ریزی و سرمایه‌گذاری در پروژه‌های مبتنی بر فناوری‌های نوظهور به ویژه فناوری اینترنت اشیا در داخل کشور به طور جدی از سال ۱۳۹۵ آغاز شده است که از جمله می‌توان به طرح‌ها و استارت‌آپ‌های بخش حمل‌ونقل، محیط زیست، خودرو هوشمند، موقعیت‌یابی هوشمند، کشاورزی، مدیریت انرژی اشاره کرد. در حال حاضر بر اساس تصویب‌نامه مصوب جلسه مورخ ۱۴۰۰/۰۴/۰۲ هیأت وزیران درخصوص «تعیین فهرست اولویت‌های صنعتی» محصولات دانش بنیان با فناوری‌های پیشرفته از قبیل انرژی‌های تجدیدپذیر، مواد پیشرفته، پلتفرم‌های باتری به ویژه باتری‌های لیتیومی، فناوری‌های مرتبط با ژنوم و ژنتیک، سوئیچ و روتر مخابراتی، ذخیره‌سازها، پردازشگرها، فناوری‌های مرتبط با پنج جی، مودم، فناوری‌های مبتنی بر انقلاب صنعتی چهارم نظیر چاپگرهای سه بعدی، اینترنت اشیا، رایانش ابری، تحلیل کلان داده‌ها و حس‌گر(سنسور)ها به عنوان یکی از اولویت‌های اولیه صنعتی کشور محسوب می‌شوند. با شکل‌گیری شورای عالی فضای مجازی[5] اصطلاح اینترنت اشیا وارد گفتمان سیاستگذاری در کشور شده و در تعریف آن چنین آمده: «ارتباط/اتّصال اشیا

1- Cloud Computing
2- Web of Things
3- Internet of Content
4- International Telecommunication Union

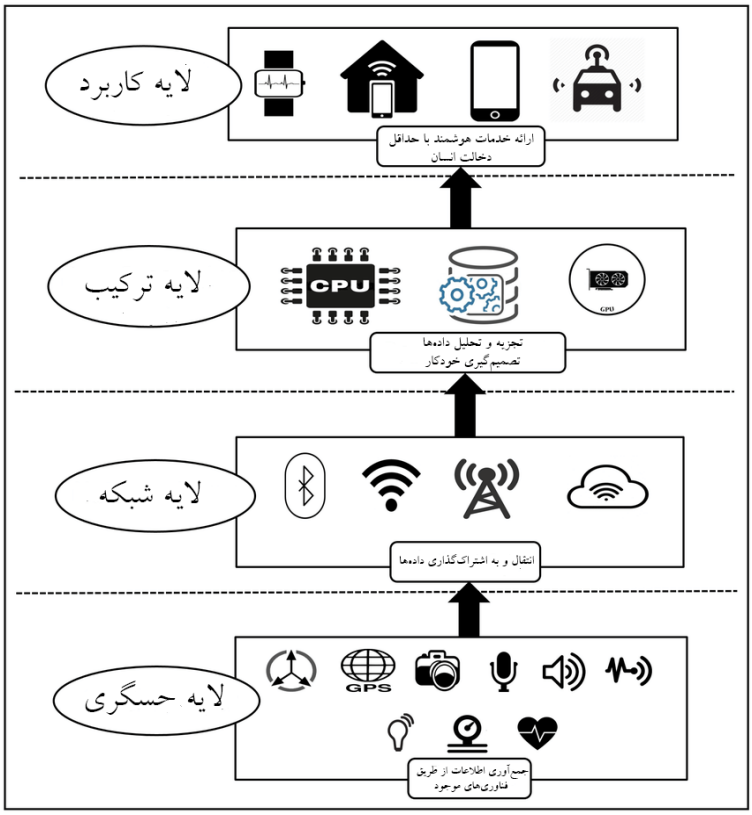
۵- شورای عالی فضای مجازی به علت گسترش فزاینده فناوری‌های اطلاعاتی و ارتباطاتی به ویژه شبکه‌ی جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی، و لزوم سرمایه‌گذاری وسیع و هدفمند در جهت بهره‌گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه‌ریزی و هماهنگی مستمر به منظور صیانت از آسیب‌های ناشی از آن با حکم حکومتی رهبر جمهوری اسلامی ایران تشکیل شده است (حکم تشکیل و انتصاب اعضای شورای عالی فضای مجازی).

با یکدیگر و با انسان‌ها که به عنوان جزئی از یک شبکه بزرگ‌تر(در هر مقیاسی) از طریق تبادل داده (به هر طریقی)، تعاملاتی میان این اشیا و انسان‌ها به عنوان سرویس‌دهنده/ سرویس‌گیرنده را با هر ساختاری فراهم می‌نماید».[۱]

ساختار اینترنت اشیا

برای نشان دادن نحوه کارکرد اینترنت اشیا معمولاً فرایند عملکرد آن را در قالب لایه‌هایی نشان می‌دهند. گرچه درباره مصادیق این لایه‌ها در معماری اینترنت اشیا اتفاق نظر وجود ندارد با این‌حال قدر متیقن همهٔ آنان را چنان که در شکل ۱ آمده است، می‌توان در چهار لایه ساختاری نشان داد: ۱. لایه حسگری دستگاه‌ها[۲] ۲.لایه مدیریت شبکه[۳] ۳. لایه ترکیب خدمات[۴] ۴. لایه کاربرد[۵](Lombardi et.al, 2021: 2). لایه اوّل از مجموعه‌ای از دستگاه‌های حسگر و سنجشگر هوشمند از جمله تلفن‌های هوشمند، برچسب‌های سامانه بازشناسی با امواج رادیویی[۶] و سامانه موقعیت‌یاب جهانی و غیره تشکیل یافته است. این مؤلفه‌ها می‌توانند به طور خودکار پارامترهای مختلف فیزیکی را به عنوان مثال دما، رطوبت، مکان و غیره را اندازه‌گیری و جمع‌آوری کنند. این دستگاه‌ها قابلیت آن را دارند که اطلاعات را در خود ذخیره کرده و با یکدیگر به اشتراک بگذارند. لایه دوّم ساختار اینترنت اشیا متشکل از شبکه‌های مختلف بی‌سیم و با سیم، رایانش ابری و بایگانی‌های کلان داده می‌باشد که کارایی اصلی آن مربوط به تجمیع داده‌ها و انتقال آن به لایه‌های بعدی است. شبکه‌های موجود در این لایه به طور بالقوه تجهیزات ناهمگن را با هم ترکیب می‌کنند و با استفاده از فناوری‌هایی مثل اینترنت نسل ۴ و ۵ و نیز سامانه جهانی ارتباطات سیار یا وایفای و بلوتوث داده‌ها را بین اجزای مختلف این لایه انتقال می‌دهند. لایه مدیریت شبکه پس از تجمیع داده‌های جمع‌آوری شده آن‌ها را به لایه سوّم انتقال می‌دهد که عملکرد اصلی آن تجزیه و تحلیل و پردازش داده‌هایی است که از لایه مدیریت شبکه جمع‌آوری شده است. این لایه بر اساس فناوری میان افزارها ساخته شده است و به تبادل اطلاعات برای برنامه‌های کاربردی اینترنت اشیا در بین اشیا ناهمگن و بدون نیاز به سخت‌افزار و نرم‌افزار خاص کمک می‌کند. چهارمین لایه ساختار اینترنت اشیا لایه کاربرد است که به موجب آن خدمات هوشمند اینترنت اشیا در اختیار کاربران قرار می‌گیرد. مؤلفه‌های اصلی این لایه کاربردهای مختلفی است که می‌تواند به عنوان مثال تحت عنوان خانه هوشمند، شهر هوشمند، حمل و نقل هوشمند، تجارت هوشمند و سلامت هوشمند و غیره طبقه‌بندی شود.

۱- مصوبه شماره ۲ جلسه ۵۳ مورخ ۹۷/۰۷/۳۰ شورای عالی فضای مجازی، الزامات حاکم بر اینترنت اشیا در شبکه ملّی اطلاعات.
2- Device Sensing Layer
3- Network Management Layer
4- Service Composition Layer
5- Application layer
6- Radio Frequency Identification Tags



شکل ۱ – معماری ساختاری و عملکردی اینترنت اشیا (Lombardi, et.al, 2021:3).

اهمیت حفاظت از داده شخصی در بستر اینترنت اشیا

در عصر فناوری اطلاعات و ارتباطات به ویژه اینترنت، شناسایی شدن هویّت و زندگی خصوصی از طریق داده‌ها و نیز دسترسی غیرمجاز یا سوء استفاده از آنها دغدغه اصلی کاربران تلقی می‌گردد. در بستر اینترنت اشیا که جزئی‌ترین اطلاعات افراد از صوت و تصویر گرفته تا عادات و الگوهای رفتاری و اطلاعات مربوط به سلامت جسمانی و هزاران اطلاعات دیگر جمع‌آوری می‌شود؛ نگرانی فوق دو چندان می‌گردد. علاوه بر موارد اشاره شده، از طریق برخی داده‌هایی که ظاهراً شخصی محسوب نمی‌شوند می‌توان به هویّت و اطلاعات مربوط زندگی خصوصی افراد دست یافت. برای مثال در خانه‌های هوشمند داده‌هایی همچون میزان مصرف انرژی، ساعات حضور در خانه، رطوبت و دمای محل و بسیاری از اطلاعات دیگر جمع‌آوری می‌شود که در ظاهر رابطهٔ مستقیمی با فرد ندارند با پیشرفت‌های موجود در حوزه فناوری به ویژه ترکیب و تحلیل داده‌ها می‌توان با کنارهم گذاشتن داده‌های متعدد به هویّت و اطلاعات شخصی افراد دست یافت. اگرچه ناشناس‌سازی[۱] به عنوان روشی برای حفاظت از داده‌های شخصی و حریم خصوصی پیشنهاد شده است با این‌حال توسعه روزافزون ابزارهای تحلیل داده و بازشناسی[۲] حاکی از آن است که حتی داده‌هایی که ناشناس شده‌اند همچنان امکان شناسایی مجدد هویّت افراد در آنها وجود را دارد. در کنار موارد مذکور، عدم آگاهی کاربران اینترنت اشیا از اینکه داده‌های آنان برای چه مقاصدی با اشخاص ثالث در میان گذاشته می‌شود به نگرانی های افراد دامن می‌زند. با توجّه به حساسیت داده‌های مربوط به افراد و اهمیت اقتصادی آن به ویژه برای مقاصد بازاریابی لازم می‌نماید نظام حقوقی برای حفاظت از داده‌های شخصی ایجاد شود. به طور کلی هدف از وضع قواعد مربوط به حمایت از داده شخصی پیش‌بینی الزامات و اصولی برای پردازش داده توسط کنترلگر و پردازشگر یا به

۱- یعنی پردازش داده‌های شخصی به گونه‌ای که دیگر نمی‌توان داده‌های شخصی را بدون استفاده از اطلاعات اضافی به یک موضوع خاص نسبت داد، مشروط بر اینکه این اطلاعات اضافی جداگانه نگهداری شوند و مشمول اقدامات فنّی و سازمانی باشند تا اطمینان حاصل شود که داده‌های شخصی به یک شخص حقیقی شناخته شده یا قابل شناسایی نسبت داده نمی‌شود.(ماده ۴ مقررات عمومی حفاظت از داده).

2- Re-Identification

عبارت دیگر افرادی که داده‌های افراد را برای اهداف مشخصی در اختیار دارند است، به گونه‌ای که افراد موضوع داده بتوانند نسبت به اینکه چه اطلاعات و به چه میزانی از آنان جمع‌آوری می‌شود و برای چه اهدافی مورد استفاده قرار می‌گیرد آگاهی داشته باشند و در صورت لزوم، عدم رضایت خود را اعلام دارند (European Union Agency for Fundamental Rights and Council of Europe, 2018).

الگوهای حاکم بر حفاظت از داده‌های شخصی در پرتو مطالعات تطبیقی

با توجّه به اهمیت و کارکرد داده‌های شخصی در عصر فناوری اطلاعات و ارتباطات، هر یک از نظام‌های حقوقی با توجّه به ارزش‌ها وهنجارهای پذیرفته شده در بستر اجتماعی خود، از طریق پیش‌بینی برخی الزامات درباره پردازش داده‌ها، نظام حمایت از داده‌های خود را در قالب قواعد حقوقی، تدوین کرده‌اند. بررسی قوانین و مقررات سابق و موجود نظام‌های حقوقی اتحادیه اروپایی، ایالات متحده آمریکا و جمهوری خلق چین نشان می‌دهد درباره اینکه باید از کدام یک از انواع داده‌ها در چه قالبی حفاظت و چه الزاماتی برای پردازش داده مقرر کرد، می‌توان دو رویکرد کلی را شناسایی نمود: قانونگذاری جامع و قانونگذاری تفرُّقی (Weber & Weber, 2010: 23). در الگوی اوّل با توجّه به اهمیت و حساسیت داده‌هایی که موجب شناسایی هویّت افراد می‌شوند یک قانون واحد با ارائه تعریفی جامع از داده‌های تحت حمایت قانون، رعایت الزامات پذیرفته شده در سطح بین‌المللی برای پردازش داده‌ها را به قید ضمانت اجرای قانونی به اشخاصی که داده‌های افراد را پردازش می‌کنند تحمیل می‌کند. به دنبال تصویب قوانین پراکنده با دامنه شمول مختلف توسط کشورهای اروپایی، اتحادیه اروپا با تصویب دستورالعمل در مورد محافظت از افراد در برابر پردازش داده‌های شخصی و جریان آزاد این داده‌ها[1] در سال ۱۹۹۵ انسجام‌گرایی در نظام حمایت از داده را آغاز نمود. در هر صورت اتحادیه اروپا با توجه به مسأله تجارت، قدم در راه تدوین دستورالعمل‌ها گذاشته است. به گفته لیمون دیوس[2] اگر حریم خصوصی حفاظت نشود، تجارت هم از بین خواهد رفت. دستورالعمل ۱۹۵۵ یک قانون قابل توجه و در عین حال هشداری بود، برای کشورهایی که در راستای حفاظت از اطلاعات شخصی قانون خاصی تدوین نکرده‌اند(Pourghahramani & Sabernezhad, 2014:148-149). اتحادیه اروپا در نهایت مقررات عمومی حفاظت از داده (G.D.P.R) مصوب ۲۰۱۶ را در قالب قانون لازم‌الاجرا در قوانین ملّی کشورهای عضو وضع و دو سال برای هماهنگ شدن با این قانون زمان تعیین کرد و قانون موصوف را از سال ۲۰۱۸ لازم‌الاجرا نمود. این نگاه به قانونگذاری بعدها توسط قانونگذار چین نیز مورد پذیرش قرار گرفت. در مقابل رویکرد اوّل، در الگوی تفرُّقی، تمامیِ داده‌هایی که موجب شناسایی افراد می‌شود مورد حمایت قرار نمی‌گیرد و تنها انواع خاصی از داده در حوزه‌های خاص تحت برخی الزامات قرار می‌گیرد (Ansari & Attar, 2022: 95). این الگو توسط قانونگذار فدرال ایالات متحده آمریکا اتخاذ شده است.

الگوی قانونگذاری جامع

تنظیم همه جوانب یک موضوع در قانون واحد، امر در خور تأکیدی در تقنین جامع به شمار می‌رود. این کار تلاشی است برای انسجام موضوع و مفاد قانون در یک سند واحد و ایجاد جایگاه منحصر به فرد برای آن در میان مجموعه قوانین دیگر. در این شیوه تقنین قانونگذار قواعد حقوقی و پیام‌های قانونی را در قالبی منسجم و نظام‌مند در یک سند جمع‌آوری کرده و به اشخاص تحت شمول ابلاغ می‌کند. در این نوع قانونگذاری افراد می‌توانند با مراجعه به قانون از حقوق و تکالیف قانونی خود به طور مشخص آگاه شوند. وجود یک پیام کلی واحد در قانون، افزون بر ایجاد قوام مفهومی و ساختار منطقی در محتوا، فهم و درک پیام‌های متعدد قانون را تسهیل می‌نماید؛ از حیث حقوقی نیز این امر موجب تقویت هماهنگی هنجاری، یکنواختی مفاهیم و تعمیم احکام آن به مصادیق مختلف تحت‌الشمول می‌شود و از حیث عملی نیز این الگو موجب تسهیل فهم پیام‌های قانون برای مخاطبان آن می‌شود و بستر انطباق آسان را فراهم می‌کند (Mousmouti, 2022: 119). فارغ از موارد اشاره شده، تعیین مرجع واحد نظارت بر اجرای قانون و مجرای رسیدگی به نقض مقررات در کاهش هزینه‌های اجرایی دولت نقش مؤثری

1- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.
2- Limon Davis

دارد. وجود یک قانون واحد که در آن حق بر حفاظت از داده برای تمامی اشخاص پیش‌بینی و الزاماتی برای آن تعیین شده باشد؛ می‌تواند در میان مردم، اعتماد عمومی لازم برای استفاده از فناوری‌های نوین را به وجود آورد. به عبارت دیگر، زمانی که شهروندان اطمینان حاصل نمایند که قانون از حقوق آنها درباره داده‌هایشان حمایت لازم را فراهم می‌کند به مرور به استفاده از فناوری‌های نوین همچون اینترنت اشیا رو می‌آورند. با توجّه به اهمیت موضوع در برخی نظام‌ها، حق حفاظت از داده‌های شخصی به عنوان یک حق مستقل در قانون مدنی پیش‌بینی شده است.[1] گذشته از این وجود قانون واحد باعث می‌شود تمام اشخاصی که داده‌های افراد را پردازش می‌کنند تحت تکالیف واحد و مشخص قرار بگیرند و با رجوع به قانون از تکالیف خود آگاه گردند. با وجود مزایای متعدد، این راهکار به دلایل مختلف نمی‌تواند همواره به عنوان یک راهکار عملی نتیجه‌بخش باشد: اوّلاً ممکن است پیام‌های قانونی از ابتدا نسنجیده باشند و یا بعضاً به سبب ماهیت ناهمگنی که دارند، نتوان آن‌ها را به طور یکپارچه در پیام واحد منتقل کرد؛ ارائه تعریف متناسب و موسع از داده‌های تحت حمایت می‌تواند به عنوان یک راهکار در این مورد کارساز باشد. ثانیاً قانون اغلب در فرایند تکاملی تدریجی قرار دارد و این در حالی است که ممکن است حسب ضیق وقت، ضرورت یا نیاز مبرم جامعه برای دستیابی به نتایج سریع قانونی، توسل به سایر راهکارها نیاز باشد؛ در چنین مواردی می‌توان از طریق تشویق خودتنظیمی خلاء موجود را رفع کرد. فارغ از موارد اشاره شده پیشرفت تدریجی و توسعه روزافزون فناوری اطلاعات و ارتباطات و به ویژه اینترنت اشیا در ظاهر امر، عدم قانونگذاری جامع را می‌طلبد با این توجیه که پیش‌بینی الزامات و ضمانت اجرا برای متولیان داده ممکن است مانعی بر سر راه توسعه فناوری باشد و همچنین موجب جاماندگی کشور از تحوّلات و نیازهای روز گردد و بعضاً باعث از بین رفتن خلاقیت شود، با این‌حال حساسیت حفاظت از داده‌های شخصی برای آحاد مردم جامعه و وقوع نقض‌های امنیتی گسترده در بستر اینترنت ایجاب می‌کند، قانونگذار الزاماتی کلی برای تمامی متولیان داده‌های افراد مقرر نماید. ارائه حمایت مؤثر قانونی از داده‌های شخصی می‌تواند نیاز شهروندان برای حفاظت از داده‌هایشان را فراهم کند. قانونگذاری جامع با توجّه به مزایای آن توسط اتحادیه اروپایی مورد پذیرش قرار گرفته است. تأثیر این الگو از زمان تصویب مقررات عمومی حفاظت از داده به اندازه‌ای بوده است که دیگر نظام‌های حقوقی غیراروپایی برای تدوین قوانین ملّی خود از آن به عنوان یک قاعده طلایی[2] الگوبرداری کرده‌اند که نمونه بارز آن قانون حمایت از اطلاعات شخصی جمهوری خلق چین است.

نظام حفاظت از داده‌های شخصی اتحادیه اروپایی

با توجّه به ارزش اقتصادی تجارت داده‌های اشخاص و نیز انتظار شهروندان از حمایت قانونی، اتحادیه اروپایی به عنوان نهاد تنظیم‌گر برای تسهیل جریان اطلاعات و نیز حفاظت از داده‌های اشخاص مقررات عمومی حفاظت از داده را به تصویب رسانده است. به طور کلی درباره چارچوب این مقررات می‌توان گفت قانونگذار سعی داشته است با پیش‌بینی ۳ مورد از داده‌های اشخاص حفاظت کند: ۱. پیش‌بینی اصول حاکم بر چرخه پردازش داده (اصل قانونی بودن، عدالت و شفافیت پردازش داده‌های شخصی، اصل هدف مشخص و اصل دقیق بودن داده‌های شخصی، اصل کمینه‌سازی و محدودیت ذخیره‌سازی، اصل امنیت و اصل مسئولیت پردازندگان) ۲. تجهیز افراد موضوع داده به حقوق ویژه (حق اطلاع و دسترسی به داده‌های شخصی، حق اصلاح و حذف، حق محدودسازی پردازش، حق انتقال داده‌های شخصی، حق اعتراض) ۳. پیش‌بینی نهاد ناظر مستقل و ضمانت اجراهای غیر کیفری و مجازات نقدی در صورت عدم رعایت قانون.[3] برای پاسخ به این سؤال که آیا داده‌هایی که در بستر اینترنت اشیا تولید و پردازش می‌شود تحت دامنه شمول این قانون قرار می‌گیرد یا خیر، باید داده شخصی تعریف گردد؛ بند ۱ ماده ۴ مقررات عمومی حفاظت از داده چنین بیان داشته است:«داده شخصی به معنای هر اطلاعاتی است که مربوط به شخص حقیقی شناخته شده یا قابل شناسایی (شخص موضوع داده) باشد. یک فرد حقیقی قابل شناسایی کسی است که به طور مستقیم یا غیرمستقیم، به ویژه با ارجاع به یک شناسه از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه آنلاین یا ارجاع به یک یا چند ویژگی خاص مانند هویّت فیزیکی، فیزیولوژیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی، شناسایی

۱- ماده ۱۰۳۴ قانون مدنی جدید جمهوری خلق چین مصوب سال ۲۰۲۰ و ماده ۲ قانون حمایت از اطلاعات شخصی مصوب ۲۰۲۱.

2- Golden rule

۳- برای مطالعه تفصیلی در این مورد رک: (Ghanad & Sharif, 2021)

شود». با توجّه به تعریف فوق هر گونه اطلاعات صرف‌نظر از شکل و قالب و محتوای آن به گونه‌ای که بتوان با استفاده از ابزارهایی یک فرد حقیقی را به طور مستقیم یا غیرمستقیم شناسایی کرد جزء داده‌های شخصی و تحت حمایت قانون قرار می‌گیرند. تعریف موسع از داده شخصی چنان که گفته شده است باعث انعطاف‌پذیری و سازگاری قانون با فناوری‌های روز می‌گردد(Allison, 2009: 49). این امر را به وضوح می‌توان در بستر اینترنت اشیا مشاهده کرد؛ به عنوان مثال در خانه‌های هوشمند که اطلاعات گوناگونی از محیط فرد گردآوری و مورد تحلیل قرار می‌گیرد (همچون رطوبت، دمای محل الگوی رفتاری، نوع تیپ شخصیتی، بررسی صحت کلی جسمی فرد، فرایند پیشروی بیماری، الگوی زمان خواب فرد) ممکن است با ترکیب با سایر داده‌ها موجبات شناسایی فرد را فراهم کنند. بر اساس تعریف مقررات عمومی حفاظت از داده ملاک اصلی شخصی بودن داده قابلیت شناسایی فرد است از این رو می‌توان گفت داده‌هایی که در جریان ارائه خدمات مبتنی بر اینترنت اشیا وارد چرخه داده می‌شوند شامل تعریف داده شخصی می‌شوند. این استدلال در نظریه شماره ۸/۲۰۱۴ کارگروه حفاظت از داده درباره تحوّلات اخیر درباره اینترنت اشیا نیز پذیرفته شده است.[1] با توجّه به تحوّل و پیشرفت تدریجی روش‌های بازشناسی داده در مقررات عمومی برای انعطاف‌پذیری هرچه بیشتر در برابر فناوری‌های روز مقرر شده است متولیان داده (کنترلگر و پردازشگر) باید با استفاده از ابزارهای مطابق فناوری‌های روز تعیین کنند که آیا یک داده خاص قابلیت شناسایی فرد را دارد یا خیر و در این تصمیم‌گیری باید عواملی همچون هزینه و مقدار زمان مورد نیاز برای شناسایی، با در نظر گرفتن فناوری موجود در زمان پردازش و پیشرفت‌های فناوری در نظر گرفته شود.[2]

نظام حفاظت از داده‌های شخصی جمهوری خلق چین

در حالی که کشورهای عضو اتحادیه اروپا و نیز نظام حقوقی ایالات متحده از سال‌ها پیش در حال گسترش قواعد حاکم بر حفظ حریم خصوصی خود بر داده‌های شخصی بودند جمهوری خلق چین تنها در چند سال اخیر توجّه خود را به موضوع معطوف کرده است. بر اساس آموزه‌های حقوق تطبیقی هر کشور در مواجهه با چالش‌های جامعه خود ابتدا سعی می‌کند به راهکارهای قانونی که در دیگر کشورها برای همان چالش استفاده شده است نظری بیندازند و سپس بر اساس مبانی خود آن راهکار را وارد نظام حقوقی خود کنند. نظام حقوقی چین به علت فقدان تجربه در این حوزه ابتدا با شیوه آزمون و خطا مسیر نظام حقوقی ایالات متحده را پیمود و همانند آن در برخی حوزه‌ها اقدام به قانونگذاری کرد. متأثر از این نگاه قانونگذار جمهوری خلق چین با توجّه به نوع صنعت و نوع اطلاعات، در بخش‌های مختلف بانکی، بیمه، پزشکی، اطلاعات کارت‌های اعتباری و ارتباطات از راه دور و اینترنت مقرراتی به طور پراکنده در چین وضع کرد که از جمله مهم‌ترین آنان می‌توان به موارد زیر اشاره کرد: مقررات برای تنظیم بازار خدمات اطلاعات اینترنتی مصوب ۲۰۱۲، مقررات حمایت از اطلاعات شخصی کاربران اینترنت و ارتباطات از راه دور مصوب ۲۰۱۳، مقررات مربوط به مدیریت سوابق پزشکی در مؤسسات پزشکی مصوب ۲۰۱۴، مقررات مربوط به خدمات اطلاعاتی برنامه های اینترنتی موبایل مصوب ۲۰۱۶ (Ansari & Attar, 2022: 95) با توسعه و رسوخ اصول بین‌المللی حاکم بر حفاظت از داده از یکسو و تصویب مقررات عمومی حفاظت از داده اتحادیه اروپایی به عنوان قانونی جامع و همه شمول در حوزه حفاظت از داده‌های شخصی از سوی دیگر، قانونگذار چین جهت همسو شدن با استانداردهای بین‌المللی پذیرفته شده در حوزه حفاظت از داده و تجمیع مقررات پراکنده موجود در یک قانون واحد با تاسی از مقررات عمومی حفاظت از داده اقدام به طرح مدل جدید خود کرد. قانونگذار جمهوری خلق چین پس از به رسمیت شناختن حق حریم خصوصی و حق حفاظت از اطلاعات شخصی در قانون مدنی خود در قالب حقوق مربوط به شخصیت افراد، قانون حمایت از اطلاعات شخصی جمهوری خلق چین و قانون امنیت داده جمهوری خلق چین به تصویب رساند. در تقنین قانون حمایت از اطلاعات شخصی از مقررات عمومی حفاظت از داده الگوبرداری شده است به گونه‌ای که می‌توان گفت اصول و الزامات حاکم بر پردازش داده و حقوق افراد موضوع داده هر دو قانون از حیث جامعیت حمایت قانونی مشابه یکدیگر می‌باشند (Molnár, 2021: 7). در این قانون نیز تعریف موسعی از داده‌های شخصی ارائه شده و همچون مقررات عمومی حفاظت از

۱- این کارگروه در ابتدا موجب ماده (۲۹) دستورالعمل حفاظت از داده مصوب سال ۱۹۹۵ تشکیل شد و پس از تصویب مقررات عمومی حفاظت از داده، کارگروه اروپایی حفاظت از داده جانشین آن شد.

2- Recital 26 of GDPR

داده معیار شناسایی یا احتمال شناسایی را برای شخصی تلقی کردن داده ملاک قرار داده است.[1] قانونگذار جمهوری خلق چین برای تطابق قوانین با ارزش‌ها و اهداف جامعه و توجّه به لزوم اعمال حاکمیت دولت در عرصه اطلاعات شهروندان در قانون امنیت داده جمهوری خلق چین برای کنترلگران و پردازشگران تعهدات مضاعفی در نظر گرفت. بر اساس این قانون، اشخاص مذکور موظف شده‌اند در سریع‌ترین زمان ممکن اطلاعات و داده‌هایی که توسط دولت معین می‌شوند در اختیار حکومت قرار دهند. این الزام اگرچه به ویژه برای سرمایه‌گذاران خارجی و شرکت‌های فعال و کسب و کارهای مبتنی بر داده در چین همواره منشأ نگرانی و تنش با دولت چین بوده است (Pernot-Leplay, 2020, P. 116) با وجود این به علت گستردگی موضوع و تأثیر آن بر زندگی خصوصی افراد از یکسو و نیز بحث رعایت منافع عمومی، اقتصادی، فرهنگی و ملّی کشور باعث شده است لزوم ایفای نقش گسترده دولت در حوزه حفاظت از داده بیش از پیش مورد تأکید قرار بگیرد. کشور چین از جمله نظام‌های حقوقی است که در آن برای حاکمیت نقش فعال و پویایی در راستای حفاظت از داده‌های شهروندان و امنیت ملّی پیش‌بینی شده است. طبق ماده ۱۳ قانون امنیت داده مصوب ۲۰۲۱ دولت موظف شده است یک برنامه کلی برای هماهنگی و توسعه امنیت داده‌ها تدوین کند و به موجب ماده ۱۷ نیز استانداردهایی را برای استفاده از داده‌های شخصی ایجاد کند. یکی از نوآوری‌های این قانون در مقایسه با نظام‌های حقوقی منتخب الزام دولت به ارائه طبقه‌بندی داده‌های شخصی بر اساس اهمیت داده‌ها در توسعه اقتصادی و اجتماعی و همچنین میزان آسیب به امنیت ملّی، منافع عمومی و حقوق و منافع قانونی افراد موضوع داده است. ماده ۲۱ قانون امنیت داده در این باره بیان می‌دارد داده‌های مربوط به امنیت ملّی، اقتصاد ملّی، جنبه های مهم زندگی مردم، منافع عمومی و غیره از جمله داده‌هایی می‌باشند که دولت برای محافظت از آنها باید سیستم مدیریت سختگیرانه‌ای را ایجاد کند. در قانون امنیت داده توضیح بیشتری درباره طبقه‌بندی داده‌ها ارائه نشده است و طراحی آن بر عهده دولت گذاشته شده است. از دیگر مسئولیت‌های دولت ایجاد نظامی برای پاسخگویی به خطرات امنیتی است. به موجب ماده ۲۲ دولت باید یک مکانیسم متمرکز، منسجم، مؤثر و معتبر برای ارزیابی، گزارش‌دهی، اشتراک اطلاعات، نظارت و هشدار اولیه در برابر خطرات امنیتی داده‌ها ایجاد کند. در این راستا ماده ۲۳ قانون امنیت اطلاعات اعلام می‌دارد در صورت وقوع یک حادثه امنیتی، ادارات ذی‌صلاح باید مطابق با قانون واکنش اضطراری را آغاز کنند و از جمله اقدامات مربوطه را برای جلوگیری از آسیب بیشتر و از بین بردن خطرات امنیتی انجام دهند و در صورت لزوم عموم مردم را از خطرات موجود مطلع کنند. شناسایی نقش گسترده برای دولت در حوزه حکمرانی فضای مجازی و نظارت بر داده‌های اشخاص و نیز پیش‌بینی مقررات سختگیرانه در خصوص انتقال داده‌های شهروندان چینی به خارج از کشور از جمله مواردی است که باعث می‌شود نظام حمایت از داده چین در مقایسه با سایر نظام‌ها ماهیت ویژه‌ای داشته باشد. (Pernot-Leplay, 2020, P. 103)

الگوی قانونگذاری تفرُّقی

تقنین تفرُّقی نوعی از قانونگذاری است که در آن قانونگذار با توجّه به اهمیت موضوع، قواعد جزئی برای مخاطبان خاص به طور پراکنده برای حوزه‌های خاص تصویب می‌کند. در این شیوه پیام‌های قانونگذار به صورت افقی (در بخش‌ها و حوزه‌های مختلف قانون) و به صورت عمودی (سطوح مختلف مقررات) توزیع می‌شود. مزیّت آشکار این رویکرد آن است که مقنن را قادر می‌سازد که پیام‌های قانونی را متناسب با پیچیدگی‌های موضوع تنظیم کند به گونه‌ای که برای مخاطبان خاص که موضوع احکام خاصی از قانون قرار می‌گیرند، بیشتر قابل فهم و تمیز باشند. این روش باعث می‌شود پیام قانون برای بخش‌های مقرر متمرکزتر و هدفمندتر شود و کسانی که طبق قانون عهده‌دار وظایف قانونی می‌باشند بتوانند با سهولت با تکالیف قوانین حوزه خود متابعت کنند (Mousmouti, 2022: 121). با وجود مزایای گفته شده به نظر می‌رسد این نوع از قانونگذاری در حوزه‌هایی که حقوق و منافع بیش و کم تمام شهروندان درگیر است نمی‌تواند گزینه مناسبی باشد. در بستر اینترنت اشیا که اطلاعات کاربر و غیرکاربر خدمات جمع‌آوری و پردازش می‌شود و در عمده موارد در اختیار اشخاص ثالث برای اهداف بازاریابی قرار می‌گیرد، حمایت از داده‌هایی خاص در حوزه‌های خاص نمی‌تواند پاسخگوی نیاز شهروندان برای حریم خصوصی اطلاعاتیشان باشد.

۱- ماده ۴ قانون حمایت از اطلاعات شخصی:«اطلاعات شخصی به انواع مختلفی از اطلاعات مربوط به اشخاص حقیقی شناخته شده یا قابل شناسایی اشاره دارد که از طریق الکترونیکی یا وسایل دیگر ثبت شده است، به استثنای اطلاعاتی که به صورت ناشناس پردازش می‌شوند».

علاوه بر این، پیش‌بینی مقررات پراکنده مستلزم ایجاد نهادهای نظارتی متکثر برای ارزیابی اجرای قانون و رسیدگی به تخلفات است که لازمه آن صرف هزینه‌های هنگفت اجرایی می‌باشد. نمونه‌ای از قانونگذاری تفرُّقی درباره حفاظت از داده در سطح فدرال ایالات متحده آمریکا مشاهده می‌شود (Ansari & Attar, 2022: 95). قانونگذار فدرال بی آنکه حق مشخصی تحت عنوان حق حفاظت از داده‌های شخصی پیش‌بینی کرده باشد، در قوانین متعدد برخی از انواع داده‌ها که اهمیت بیشتری دارند به ویژه اطلاعات مربوط به حوزه سلامت، بهداشت، بیمه، حریم خصوصی آنلاین کودکان، گزارش‌های مالی و اعتباری را تحت حمایت قانونی قرار داده و الزاماتی برای اشخاص مشمول قوانین مقرر کرده است. از میان قوانین فدرال اشاره شده می‌توان به قانون مسئولیت‌پذیری و انتقال‌پذیری بیمه سلامت مصوب ۱۹۹۶، قانون حفاظت از حریم خصوصی آنلاین کودکان، مصوب ۱۹۹۸ اشاره کرد. با توجّه به این موارد می‌توان گفت در حال حاضر نظام حفاظت از داده در سطح فدرال فاقد یکنواختی می‌باشد. به دلیل خلاءهای قانونی موجود و ضعف مقررات فدرال در حمایت از داده‌های شخصی افراد در بستر فناوری‌های نوین، کمیسیون تجارت فدرال به دنبال برگزاری کنفرانسی درباره اینترنت اشیا طی توصیه‌ای به کنگره پیشنهاد داد قوانین منعطف، مستحکم و یکنواخت برای حفاظت از داده‌های شهروندان آمریکایی تصویب کند (FTC, 2015, P. 27). از آنجا که در بسیاری از موارد کسب و کارها خارج از شمول قوانین خاص حفظ حریم خصوصی موجود هستند در بسیاری موارد منبع اصلی تنظیم‌گری در ایالات متحده کمیسیون تجارت فدرال است. (Solove & Hartzog, 2013, p. 588). کمیسیون اشاره شده بر خلاف قوانین فدرال محدود به حوزه خاصی از کسب و کار و تجارت نمی‌باشد و صلاحیت آن بر تمام شرکت‌هایی که در حوزه تجارت فعالیت می‌کنند تسری دارد. با توجّه به اختیارات و وظایف گسترده کمیسیون تجارت فدرال، این نهاد در مقام نظارت بر اجرای حقوق مصرف‌کننده ارتکاب اعمال یا اقدامات ناعادلانه توسط شرکت‌ها و تولیدکنندگان و ارائه‌دهندگان خدمات را که با داده‌های افراد سر و کار دارند ممنوع اعلام داشته است. این کمیسیون با اقدامات و توصیه‌های خود سعی کرده است خلاءهای موجود در حفاظت قانونی از داده‌های افراد را هر چند به طور جزئی مرتفع نماید. در رابطه با خط مشی‌های حفاظت از حریم خصوصی اطلاعاتی افراد کمیسیون تجارت فدرال اعلام داشته است شرکت‌ها و ارائه دهندگان خدمات هنگامی که برخلاف تعهدات خود در خط مشی‌های حریم خصوصی عمل می‌کنند یا هنگامی که علی‌رغم اعلام تعهدشان مبنی بر حفاظت و تأمین امنیت داده‌های شخصی نتوانند در برابر دسترسی‌های غیرمجاز از اطلاعات افراد محافظت کنند اقداماتشان گمراه کننده و فریبنده تلقی می‌شود و کمیسیون صلاحیت دارد تحقیقات و اقدامات لازم از جمله طرح دعوی را انجام دهد. به عبارت دیگر در صورتی که اطلاعات افراد را برخلاف موارد مندرج در خط مشی حفاظت از حریم خصوصی جمع‌آوری، ذخیره، استفاده و افشاء کنند یا این اطلاعات را با اشخاص ثالث برای اهداف دیگر به اشتراک بگذارند اقداماتشان تحت شمول مفهوم اعمال گمراه کننده قرار می‌گیرد. الگوی ایالات متحده آمریکا که از آن تحت عنوان مدل مینیمالیستی[1] حفاظت از داده نیز یاد می‌شود (Pernot-Leplay, 2020, P. 53) برای مدتی سرمشق برخی از نظام‌های حقوقی به ویژه چین بوده است (Ansari & Attar, 2022: 95) با این وجود تجربه هر دو نظام نشان می‌دهد وضع قوانین پراکنده بدون تبیین مصادیق داده شخصی، حقوق مشخص برای افراد و الزامات ویژه برای پردازندگان داده‌ها نمی‌تواند به عنوان راهکار مناسب برای حفاظت از داده‌های شخصی مطابق با تحوّلات موجود در حوزه فناوری اطلاعات و ارتباطات و توسعه اینترنت اشیا باشد و از داده‌های شخصی افراد حفاظت مؤثری به عمل آورد (Levin & Nicholson, 2005, P. 357).

خودتنظیمی

خودتنظیمی یا وضع قواعد هنجاری توسط اعضای یک گروه برای اداره امور خود در دکترین حقوقی مبتنی بر این ایده است که زمانی که اعضای یک جامعه خاص با توجّه به نیازهای واقعی خود اقدام به تنظیم روابط امور و حل مسائل می‌کنند در عمل به نتایج اثربخش و مطابق با مقتضیات نیازهای خود می‌رسند. بر این اساس مداخله دولت تنها زمانی تجویز می‌شود که مشارکت‌کنندگان یک جامعه خاص نتوانند خودشان راه حل‌های مناسب (ساختارها، رفتارها) را برای رتق و فتق امور خود بیابند (Weber, 2002: 79). در عمل با توجّه به مزایای خودتنظیمی از جمله کم هزینه بودن اجرای آن در مقایسه با

1- Minimalistic Approach

مقررات‌گذاری توسط دولت، پویایی در برابر تحوّلات فناوری اطلاعات و ارتباطات و نیز پذیرش و انطباق سریع افراد با قواعدی که خودشان تنظیم کرده‌اند باعث شده است به عنوان یکی از راهکارها برای حفاظت از داده افراد در اینترنت اشیا مطرح شود. بر اساس این روش، کسب و کارها و شرکت‌های ارائه‌دهنده خدمات مبتنی بر داده و اینترنت اشیا برای حصول اطمینان کاربران از اینکه داده‌های آنان در فرایندی قانونی و شفاف استفاده می‌شود اقدام به تنظیم خط‌مشی‌های حفظ حریم خصوصی[1] می‌کنند و پیش از ارائه خدمات کاربر یا مصرف‌کننده را ملزم به مطالعه و اعلام رضایت می‌کنند. در خط‌مشی‌های حفظ حریم خصوصی توضیح داده می‌شود که کدام یک از داده‌های فرد برای کدام اهداف گردآوری و پردازش می‌شود. به عبارت دیگر در خط‌مشی‌های حفظ حریم خصوصی که از آن تحت عنوان رویکرد اطلاع–تصمیم[2] نیز یاد می‌شود (Solove & Hartzog, 2013: 592) به روش‌هایی که اطلاعات افراد را جمع‌آوری، استفاده و با اشخاص ثالث برای اهداف مشخص (از جمله بازاریابی) به اشتراک می‌گذارند و نیز شیوه‌های حفاظت از اطلاعات افراد بیان می‌شود. در بخش دیگری از این سیاست‌ها برای افراد این امکان پیش‌بینی می‌شود که عدم تمایل خود به جمع‌آوری و استفاده از اطلاعاتشان را اعلام بدارند، در این صورت شرکت ارائه‌دهنده خدمات طبق تعهد خود نمی‌تواند از اطلاعات افراد استفاده کرده یا آن را با هدف بازاریابی در اختیار اشخاص ثالث قرار دهد. گنجاندن این سیاست‌ها در فعالیت شرکت دفاع از این دیدگاه است که صنعت می‌تواند فعالیت‌های خود را بدون نیاز به دخالت قانونگذار ساماندهی کند. در نظام حقوقی ایالات متحده با توجّه به محدود بودن دامنه مقررات حفاظت از داده‌ها بسیاری از افراد تنها متکی به سیاست‌های حفظ حریم خصوصی شرکت‌ها و کسب و کارهای مبتنی بر داده و الزامات محدود پیش‌بینی شده در آن می‌باشند (Congressional Research Service, 2019: 7). عدم رعایت موارد مندرج در سیاست‌های حفظ حریم خصوصی توسط شرکت‌ها از طریق انتقال و فروش داده‌ها بدون رضایت فرد و نیز استفاده از داده‌های شخصی برای اهدافی به غیر از مواردی که فرد به پردازش آن رضایت داده است باعث شده است برخی از قانونگذاران ایالتی به موضوع مداخله کرده و قوانین مدونی در این باره به تصویب برسانند. ایالت کالیفرنیا یکی از اوّلین ایالت‌هایی می‌باشد که به دنبال رسوایی فروش اطلاعات شهروندان آمریکایی توسط فیسبوک اوّلین قانون جامع در ایالات متحده آمریکا تحت عنوان «قانون حریم خصوصی مصرف‌کننده کالیفرنیا» را به تصویب رساند.(Baik, 2020: 3) در این قانون به طور واضح از الگوی قانونگذاری جامع استفاده شده است. از خلاءهای اصلی شیوه خودتنظیمی فقدان یک نهاد خاص و مستقل از نهاد متولی داده برای نظارت بر اجرای صحیح مفاد سیاست‌های حفظ حریم خصوصی است. فقدان نهاد نظارتی ویژه و مجرای رسیدگی به درخواست‌های مربوط به نقض داده‌ها باعث می‌شود در عمل اشخاصی که داده‌های کاربران را در اختیار دارند به سادگی از آنان برای اهداف دیگر و کسب منافع مالی استفاده کنند بی آنکه نظارتی بر اعمال آنان باشد. با توجّه به ماهیت ویژه اینترنت اشیا و وسعت عظیم پردازش اطلاعات در این بستر لازم می‌نماید مجرایی پیش‌بینی گردد که افراد موضوع داده بتوانند بدون اتلاف وقت حقوق شناخته شده خود را به اجرا بگذارند به ویژه اینکه تعلل در اعمال کنترل بر داده توسط فرد ممکن است آثار زیانبار جبران‌ناپذیری در پی داشته باشد.

جدول ۱ – مقایسه تطبیقی قوانین و قواعد حاکم بر حفاظت از داده شخصی در نظام‌های حقوقی منتخب (Kelly, 2022)

نظام حقوقی	نام قانون یا مقرره	داده‌های تحت حمایت قانون	الزامات کلی
اتحادیه اروپایی	مقررات عمومی حفاظت از داده مصوب ۲۰۱۶	داده‌های شخصی مربوط به شخص حقیقی (فرد موضوع داده) شناخته شده یا قابل شناسایی به طور مستقیم یا غیرمستقیم.	اصول پردازش: اصل قانونی بودن، عادلانه بودن و شفافیت پردازش، اصل هدف مشخص و اصل دقیق بودن داده شخصی، اصل کمینه‌سازی و محدودیت ذخیره‌سازی، اصل امنیت داده، اصل مسئولیت‌پذیری (مواد ۵ الی ۱۱). حقوق افراد موضوع داده: حق اطلاع و دسترسی (مواد ۱۲ الی ۱۵)، حق اصلاح و حذف داده‌های شخصی(ماده ۱۶ و ۱۷)، حق محدودسازی پردازش (ماده ۱۸) حق انتقال داده‌ها (ماده ۲۰)، حق اعتراض (ماده ۲۱) نهاد نظارتی مستقل: (ماده ۵۱)

1- Privacy Policies
2- Notice-Choice

جمهوری خلق چین	قانون مدنی جدید چین مصوب ۲۰۲۰	اطلاعات شخصی که به صورت الکترونیکی یا به روش‌های دیگر ثبت می‌شود و می‌تواند به تنهایی یا در ترکیب با اطلاعات دیگر موجب شناسایی شخص شود.	به موجب ماده (۱۰۳۵) پردازش اطلاعات شخصی باید مطابق با اصول قانونی بودن و توجیه پردازش بوده و در بازه زمانی محدود به مقدار کافی انجام شود و علاوه بر این شرایط ذیل باید احراز گردد: ۱. رضایت از شخص طبیعی یا سرپرست وی اخذ شده باشد مگر اینکه قوانین یا مقررات اداری ترتیب دیگری مقرر کرده باشند ۲. قواعد مربوط به پردازش اطلاعات منتشر شده باشد ۳. هدف، روش و دامنه پردازش اطلاعات به وضوح بیان شده باشد ۴. پردازش اطلاعات شخصی در تعارض با قوانین یا مقررات اداری یا مخالف با توافق بین طرفین نباشد.
	قانون حمایت از اطلاعات شخصی مصوب ۲۰۲۱	انواع مختلفی از اطلاعات مربوط به اشخاص حقیقی شناخته شده یا قابل شناسایی که از طریق الکترونیکی یا وسایل دیگر ثبت شده است، به استثنای اطلاعاتی که به صورت ناشناس پردازش می‌شوند	اصل قانونی بودن، عادلانه بودن و شفافیت پردازش، اصل هدف مشخص و اصل دقیق بودن داده شخصی، اصل کمینه‌سازی و محدودیت ذخیره‌سازی، اصل امنیت داده، اصل مسئولیت‌پذیری.(مواد ۵ الی ۱۰). حقوق افراد موضوع داده: حق اطلاع و دسترسی، حق اصلاح و حذف داده‌های شخصی، حق محدودسازی پردازش، حق انتقال داده‌ها، حق اعتراض (مواد ۴۴ الی ۵۰) نهاد نظارتی مستقل: (مواد ۶۰ ال ۶۵)
ایالات متحده آمریکا	قانون مسئولیت‌پذیری و انتقال‌پذیری بیمه مصوب ۱۹۹۶	هرگونه اطلاعاتی که: ۱. توسط یک ارائه‌دهنده مراقبت‌های بهداشتی، برنامه بهداشتی، اداره بهداشت عمومی یا سایر مراکز ذی‌ربط ایجاد یا دریافت می‌شود و ۲. مربوط به سلامت جسمی یا روانی گذشته، حال یا آینده فرد و پرداختی‌های آن فرد برای امور بهداشت و سلامت می‌باشد و ممکن است منجر به شناسایی یک فرد یا احتمال شناسایی یک فرد گردد.	تمامی اطلاعات مربوط به سلامت افراد باید توسط نهادهایی که این اطلاعات را در اختیار دارند به طور محرمانه نگه داشته شوند و نمی‌توانند از این اطلاعات استفاده یا آنها را افشاء کنند مگر با رضایت کتبی فرد. طبق ماده (۱۶۰،۱۰۳) آیین‌نامه مذکور افشای اطلاعات به معنای انتشار، انتقال، تأمین دسترسی یا علنی ساختن هر نوع اطلاعات به خارج از نهادی است که اطلاعات را در اختیار دارد.
	قانون حفاظت از حریم خصوصی آنلاین کودکان مصوب ۱۹۹۸	اطلاعاتی که به صورت آنلاین جمع‌آوری می‌شود، از جمله نام و نام خانوادگی، آدرس خانه و محل سکونت، شماره تلفن، شماره تأمین اجتماعی، عکس و فیلم و صدای حاوی کودک، اطلاعات جغرافیایی و سایر اطلاعات مربوط به کودک یا والدین او.	اپراتورهای وب‌سایت یا خدمات آنلاین نمی‌توانند اطلاعات مربوط به کودک را جمع‌آوری یا استفاده کنند مگر اینکه پیش از آن از والدین کودک رضایت معتبر اخذ نمایند. منظور از اپراتور به معنای هر شخصی است که یک وب‌سایت واقع در اینترنت یا یک سرویس آنلاین را اداره می‌کند و اطلاعات شخصی را از یا در مورد کاربران یا بازدیدکنندگان از چنین وب‌سایت یا سرویس آنلاین جمع‌آوری یا نگهداری می‌کند.
	قانون کمیسیون تجارت فدرال مصوب ۱۹۱۴	ممنوعیت طیف گسترده‌ای از شیوه‌های ناعادلانه و گمراه کننده در تجارت و رقابت که باعث تضرر مصرف‌کننده می‌شود.	نظارت بر نحوه اجرای سیاست‌های حفظ حریم خصوصی و اقامه دعوی در صورت لزوم برای جریمه نقدی.

الگوی مطلوب حفاظت از داده‌های شخصی در نظام حقوقی ایران

شناخت وضع موجود از یک‌سو و بهره‌گیری از فواید مقایسه تطبیقی از سوی دیگر، ما را در رسیدن به خاستگاه پژوهش حاضر که همانا دستیابی و تدوین الگوی مطلوب و مدل بومی مبتنی بر نظام حقوقی کشور در این موضوع است یاری می‌نماید. اکثر نظام‌های حقوقی موجود در دنیا به مسئله حریم خصوصی و حفاظت از داده‌های شخصی در متون قانونی خود، کم و بیش اشاره نموده‌اند لیکن همان‌گونه که مسلم است نظام‌های حقوقی مختلف در دنیا بنابر شرایط فرهنگی، تاریخی، ایدئولوژیکی، اقتصادی و... راهکارهای متفاوتی را اعمال می‌نمایند. با عنایت به تفارق نظام‌های حقوقی در دنیا، بهره‌گیری از یک الگوی موفق در یک کشور، الزاماً مستلزم همان نتیجه برای کشور دیگر نخواهد بود. بنابراین تناسب و عدم تناسب رویکردهای حاصله از

بررسی‌های تطبیقی با وضعیت حقوقی ایران و شناسایی مزایا و معایب هرکدام و چگونگی تبلور آن در نظام حقوقی کشورمان، جهت تدوین مدل مفهومی موضوع در نظام حقوقی کشور مقوله‌ای بسیار حائز اهمیت و دشوار می‌باشد. در راستای توسعه اینترنت اشیا و سیاستگذاری در این حوزه، شورای عالی فضای مجازی به عنوان مرجع سیاستگذار فضای مجازی کشور گام‌های مؤثری برداشته است که از جمله مهم‌ترین آنها می‌توان به مصوبه جلسه پنجاه و سوم مورخ ۱۳۹۷/۰۷/۳۰ شورای عالی فضای مجازی با موضوع «الزامات حاکم بر اینترنت اشیا در شبکه ملّی اطلاعات» و مصوبه نود و نهمین جلسه مورخ ۱۴۰۰/۱۰/۶ تحت عنوان «دستورالعمل بکارگیری خدمات شبکه‌های ارتباطی برای کمک به توسعه صنعت خودروهای متّصل» اشاره کرد. در کنار شورای عالی فضای مجازی، شورای اجرایی فناوری اطلاعات نیز حسب مورد برای دستگاه‌های قوه مجریه اقدام به تنظیم‌گری می‌کند. با این حال لازم به ذکر است وجود خلاءهای قانونی به دلیل پیشرفت سریع تکنولوژی در حوزه فناوری اطلاعات، از یک‌سو و عدم تکافوی سیاستگذاری شورای عالی فضای مجازی که فقط سیاستگذاری کلان را مشخص می‌کند و فاقد حکم اجرایی و عملی است از سوی دیگر و روند کند قانونگذاری در کشور باعث شد که شورای اجرایی فناوری اطلاعات زیر مجموعه وزارت ارتباطات و فناوری اطلاعات به تصویب پراکنده و غیرمتمرکز احکام مورد نیاز در حوزه فناوری اطلاعات و ارتباطات بپردازد و از آنجا که این مقررات‌گذاری صرف، فقط برای دستگاه‌های درون قوه مجریه لازم الاجراست، بقیه نهادهای کشور در این حوزه بلاتکلیف می‌باشند. ارائه حمایت قانونی مؤثر برای داده‌های اشخاص به گونه‌ای که منطبق با واقعیت‌های روز باشد در ابتدا بیش از هرچیزی نیازمند شناسایی حق بر حفاظت از داده‌های شخصی می‌باشد؛ در نظام داخلی منشورحقوق شهروندی در ماده ۳۵ حفاظت از داده‌های شخصی را حق شهروندان اعلام داشته است با این حال با توجّه به ماهیت سند مذکور، شناسایی این حق در قوانین موضوعه یک بایسته می‌باشد. در قوانین فعلی نظام حقوقی ایران از جمله قانون انتشار و دسترسی آزاد به اطلاعات، قانون تجارت الکترونیکی، قانون جرایم رایانه‌ای مصادیقی یافت می‌شود که شباهت‌هایی با قواعد بین‌المللی از حیث اصول پردازش و حقوق افراد موضوع داده دارند(Raisi & Ghassemzadeh Liyasi, 2020: 134)، لذا می‌توان گفت ادبیات حقوق داخلی با آنچه که در قوانین نظام‌های منتخب وجود دارد چندان بیگانه نیست و می‌توان با استخراج اصول و قواعد از قوانین موجود در نظام داخلی و عاریه برخی موارد از نظام‌های منتخب نظام اثربخشی برای حفاظت از داده‌های شخصی تدوین کرد. از بین الگوهای قانونگذاری در حوزه حفاظت از داده‌های شخصی، ترکیبی ازالگوهای موجود برای نظام حقوقی ایران پیشنهاد می‌گردد. با عنایت به تأسی بسیاری از نظام‌های حقوقی دنیا از مدل اتحادیه اروپایی و با توجّه به این نکته که نظام حقوقی ایران بر مبنای نظام حقوقی رومی-ژرمن و مبتنی بر حقوق نوشته است؛ لذا مدل اتحادیه اروپا با توجّه به آنچه پیشتر به طور مبسوط مورد بررسی قرار گرفت، به عنوان یکی از موفق‌ترین رویکردهای موجود در حوزه حفاظت از داده می‌تواند الگوی مناسبی برای نظام حقوقی ایران باشد. آشنایی ذهنی شهروندان، شرکت‌ها، بخش‌های مختلف دولتی و خصوصی و قضات با این مدل نیز در پذیرش آن به عنوان الگوی مناسب برای ایران، بی‌تأثیر نیست. در این مدل، مفهوم حق حریم خصوصی، حق بر حفاظت داده به وضوح تبیین و به رسمیت شناخته شده است. این حقوق به درستی از یکدیگر تفکیک شده، سپس چارچوب حفاظت از داده و قواعد آن به رشته تحریر درآمده و قواعد به طور متمرکز در یک متن واحد قرار گرفته و از تصویب مقررات پراکنده و جزئی پرهیز شده است. در این رویکرد حق‌محور، اصول پردازش داده‌های شخصی، حقوق و تکالیف کنترل‌گران و پردازش‌گران داده به تدقیق مورد بررسی و قاعده‌گذاری قرار گرفته؛ حقوق افراد موضوع داده برای حفاظت از اقراد در برابر پردازش داده‌های شخصی مشخص شده است. استفاده از ماده واحده‌ای جهت شمولیت احکام مواد قوانین مرتبط به داده در حوزه اینترنت اشیا، نظیر مدل اروپایی می‌تواند در مدل ایران راهگشا باشد. قانونگذاری تفرُّقی به علت ارائه حمایت قانونی محدود و جزئی نمی‌تواند مناسب برای حفاظت از داده شخصی باشد؛ لیکن به‌نظر می‌رسد اقتباس از مقررات سخت‌گیرانه ایالات متحده امریکا در مورد مسائل مربوط به حفاظت از داده‌های شخصی در حوزه بهداشت و کودکان برای تدوین مدل ایران مطلوب و مورد استفاده باشد. الگوی خودتنظیمی گرچه در ابتدا به عنوان یکی از راهکارهای حفاظت از داده شهروندان مطرح شده است با اینحال به نظر می‌رسد اتکای صرف به رویکرد خودتنظیمی برای کشورهایی همچون ایران که به تازگی وارد این حوزه شده‌اند مناسب نمی‌باشد چراکه باید توجّه داشت در داخل کشور اینترنت اشیا در مراحل اولیه خود قرار دارد و استفاده مطلوب از آن مستلزم جمع‌آوری داده‌های شخصی و تحلیل کلان داده‌ها به عنوان زیرساخت این فناوری می‌باشد؛

نیل به این هدف تنها از طریق جلب و کسب اعتماد کاربران برای استفاده از این خدمات و فرهنگ‌سازی میان مردم حتّی پیش از تصویب قانون (Ghanad & Aligholi, 2020:319) است که به نظر نمی‌رسد به آسانی کسب شود زیرا شکل‌گیری نگرش شهروندان نسبت به فناوری‌های نوین در این موارد طی یک چرخه اتفاق میفتد؛ در این چرخه به طور معمول شاهد مقاومت اولیه، انطباق تدریجی و در نهایت همگون‌سازی می‌باشیم (Faqihi & Nafei, 2015: 11). با این وجود در کنار ارائه حمایت قانونی می‌توان از ظرفیت‌های خودتنظیمی ارائه‌دهندگان خدمات اینترنت اشیا در کاهش هزینه‌های اجرایی و نظارتی دولت و نیز کاهش زمان و هزینه‌ها اعمال حقوق توسط افراد موضوع داده از طریق پیش‌بینی برخی امتیازات قانونی سود جست. وارد نمودن کدهای دستوری خودتنظیم‌گری در برخی موارد درکسب‌وکارهای آنلاین در ایران آغاز شده است هرچند از غنای مطلوبی برخوردار نیست لیکن می‌تواند به‌عنوان مقدمه، زمینه‌هایی برای آشنایی نظام حقوقی کشور، شهروندان و قضات با خودتنظیم‌گری را فراهم نماید. با توجّه به رویکرد سخت‌گیرانه امنیتی که چین در پیش‌گرفته باید به قانونگذار ایران هشدار داد که پررنگ کردن نقش دولت و سخت‌گیری شدید امنیتی در این حوزه منجر به شکست شرکت‌های فعال و کسب و کارهای مبتنی بر داده در بازار و تهدیدی برای سرمایه‌گذاری خارجی در کشور باشد. مزیتی که رویکرد امنیت‌محور چین دارد و برای ایران نیز قابل بهره‌برداری می‌باشد این نکته است که در ماده ۱۷ قانون امنیت داده جمهوری خلق چین مصوب ۲۰۲۱، دولت به ارائه طبقه‌بندی داده‌های شخصی بر اساس اهمیت داده‌ها در توسعه اقتصادی و اجتماعی و همچنین میزان آسیب به امنیت ملّی، منافع عمومی و حقوق و منافع قانونی افراد موضوع داده، ملزم شده است. بنابراین استفاده از این روش و طبقه‌بندی داده‌ها در نظام حقوقی کشور می‌تواند مرز مداخله دولت را تعیین نماید و از حساسیت‌ها و نگرانی‌های بخش خصوصی و شهروندان در خصوص دسترسی و سوء استفاده‌های احتمالی دولت در این حوزه را کاهش دهد.

نتیجه‌گیری

رشد فناوری‌ها و گسترش طرق جمع‌آوری و پردازش اطلاعات افراد به ویژه از طریق اینترنت اشیا باعث شده است حفاظت از داده‌های شخصی بیش از پیش مورد توجّه قانونگذاران قرار گیرد. توسعه فناوری‌های نوین و کسب و کارهای مبتنی بر آنان در گرو جلب اعتماد کاربران می‌باشند. جلب رضایت افراد زمانی محقق می‌گردد که اطمینان داشته باشند قانونگذار به شیوه‌ای مؤثر از حقوق و منافع ایشان حمایت می‌کند. قانونگذاری و مقررات‌گذاری در حوزه حفاظت از داده‌های اشخاص در بخش‌های مختلف باید با در نظر گرفتن این نکته همراه باشد که قانون قطعاً نمی‌تواند همسو با رشد فناوری اطلاعات و ارتباطات باشد و برای جلوگیری از جمود قانونی و اجرایی و پویایی نظام حقوقی در برابر تغییرات، لازم است مقررات مربوط به حفاظت از داده‌های اشخاص به گونه‌ای خنثی نگاشته شوند. فارغ از این نکته باید به این موضوع توجّه شود که استفاده از فناوری‌های نوین و داده‌های اشخاص می‌تواند منبعی برای رشد و گسترش تجارت و بازاریابی باشد، از این رو مقررات‌گذاری باید به گونه‌ای باشد که مانع شکل‌گیری بستر تجارت نگردد. حفاظت مؤثر از داده‌های شخصی افراد زمانی محقق می‌گردد که قانونی منسجم و جامع تدوین گردد و در آن حقوق و اختیارات افراد در رابطه با داده‌های خود و نیز تعهدات و تکالیف پردازندگان داده‌ها در قالب الزامات قانونی همراه با ساز و کارهای رسیدگی و نظارت مستقل و ضمانت اجراهای غیرکیفری پیش‌بینی گردد. در تدوین مدل مفهومی ایران، تلفیقی از رویکردهای سه‌گانه با ابتنای اصلی بر نظام اتحادیه اروپایی پیشنهاد می‌شود. استفاده از رویکرد خود تنظیم‌گری آمریکایی در شرکت‌ها، استفاده از ماده واحده‌ای جهت شمولیت احکام مواد قوانین مرتبط به داده در حوزه اینترنت اشیا نظیر مدل اروپایی، اقتباس از مدل امریکایی نسبت به حساسیت در مورد حفاظت از داده‌های مربوط به حوزه سلامت و بهداشت عمومی و کودکان و اقتباس از مدل چین در طبقه بندی اطلاعات و عدم تجربه سیستم قانون‌گذاری تفرقی پیشنهاد شده است.

References

1- Aghdasi, F & Mohaghegh Damad, MS. (2021). Legal Aspects of Internet of Things Privacy. Interdisciplinary Legal Research, 2 (2): 49-67. [in Persian]

2- Allison, S. (2009), "the Concept of Personal Data Under the Data Protection Regime". Edinburgh Student Law Review 1: 48–65.
3- Ansari, B., & Attar, S. (2022). Data Protection in China; A Comparative Study of the Data Protection Approach in the United States and the European Union. Comparative Law Review, 13(1), 91-113. [in Persian] doi: 10.22059/jcl.2022.333708.634275
4- Baik, J. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). Telematics and Informatics, Volume 52. Doi: 10.1016/j.tele.2020.101431
5- Benar, M. (2019). Internet of Things: Technologies, Standards and Challenges (Report)". Office of Energy, Industry and Mining Studies of the Research Center of the Islamic Council. [in Persian]
6- Congressional Research Service. (2019). Data Protection Law: An Overview. 1-75.
7- European Union Agency for Fundamental Rights and Council of Europe. (2018). Handbook on European data protection law, Luxembourg: Publications Office of the European Union.
8- Faqihi, M., & Nafei, N. (2015). Internet of Things (Report). New Technologies Studies Office of the Research Center of the Islamic Council. [in Persian]
9- Federal Trade Commissio. (2015). Internet of Things: Privacy & Security in a Connected World.
10- Ghanad, F., & Sharif, E. (2021). Comprehensive Study of Personal Data Protection in Iran's Legal System and European General Data Protection Regulations. ModernTechnologies Law, 2(4), 1-22. [in Persian] doi: 10.22133/clj.2021.244608.1020
11- Ghanad, F., & Aligholi, A. (2020). The Notion and Importance of Personal Data and Privacy and Their Various Protections in Cyber Space. ModernTechnologies Law, 1(1), 297-322. [in Persian] doi: 10.22133/clj.2020.243290.1016
12- Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29, 7, pp. 1645–1660. Doi: 10.1016/j.future.2013.01.010
13- Haller, S., Karnouskos, S. & Schroth, C. (2008). The Internet of Things in an Enterprise Context. Future Internet - FIS 2008, First Future Internet Symposium, 1-15. Doi: 10.1007/978-3-642-00985-3_2
14- https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/#:~:text=The%20number%20of%20Internet%20of,around%205%20billion%20consumer%20devices.
15- IEEE. (2015). Internet of Things/M2M from Research to Standards: The Next Steps.
16- International Telecommunication Union (ITU) (2012). Overview of the Internet of things.
17- Kelly, C. (2022). Data Privacy Regulations in the United States, China, and the European Union. Honors College Theses, Georgia Southern University. (756)
18- Levin, A. & Nicholson, M. (2005). Privacy law in the United States, the EU and Canada: the allure of the middle ground. University of Ottawa Law & Technology Journal, 2, 357-395.
19- Lombardi, M., Pascale, F. & Santaniello, D. (2021). Internet of Things: A General Overview between Architectures, Protocols and Applications. Information, 12, 2, pp. 1-20. Doi:10.3390/info12020087
20- Molnár, P. (2021). Comparison of the new Chinese Personal Data Protection Law (PIPL) with GDPR and CCPA. KRE-Dit Online Tudományos folyóirat, 1-12.
21- Mousmouti, M. (Jahanshahi, A. & Petoft, A. (trans)). (2022). Designing Effective Legislation, Tehran: Library, Museum and Document Center of IRAN Parliament.
22- Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things 2014.
23- Pernot-Leplay, E. (2020). China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?. Penn. St. J.L. & Int'l Aff, 49, 49-117.
24- Pourghahramani, B & Sabernezhad, A. (2014). Privacy in Cyberspace from the Perspective of International Law. Tehran: Majd. [in Persian]
25- Raisi, L., & Ghassemzadeh Liyasi, F. (2020). The Challenges of the Iranian Legal System in Violating the Personal Data and Privacy in - Cyber Space. The Judiciarys Law Journal, 84(110), 119-142. [in Persian] doi: 10.22106/jlj.2020.88629.2213
26- Smith, N. (2019). Protecting Consumers in the Age of the Internet of Things. St. JOHN's L. REV, 93, 851-881.
27- Solove, D. & Hartzog, W. (2013). The FTC And The New Common Law Of Privacy. SSRN Electronic Journal, 114, 583-676. Doi: 10.2139/ssrn.2312913
28- Weber, R,. & Weber, R. (2010). Internet of Things: Legal Perspectives, Berlin: Springer.
29- Weber, R. (2002). Regulatory Models for the Online World, Zurich: Schulthess luristische Medien.
30- Zareian, D., & vahed, F. (2020). Legal Review of Data Regulatory Protection. Rasaneh, 31(1), 47-72. [in Persian]