University of Tehran Press

**Comparative Law Review**

**Online ISSN:** 2423-3404

**Volume:** 15, **Issue:** 1
Spring & Summer 2024

**Homepage: https://jcl.ut.ac.ir**

# Study of protection of citizens' privacy during Covid-19 period with emphasis on data processing (Comparative study of U.S., China, France, and Iran law)

**Mohsen Safari**[1]✉ **| Sajjad Ghasemi**[2]

1. Corresponding Author; Department of Private and Islamic Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran. Email: safarimohsen@ut.ac.ir
2. Department of Private Law, Department of Private and Islamic Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran. Email: sajjadghasemi@ut.ac.ir

**Article Info**

**Article Type:**
Research Article

**Received:**
2022/12/21
**Received in revised form:**
2023/10/10
**Accepted**:
2023/12/18
**Published online:**
2024/06/21

**Keywords**:
*Data processing, privacy, Corona, personal data.*

**Abstract**

Necessity of confrontation with coronavirus pandemic has moved governments toward taking a variety of actions in the field of defeating coronavirus (including data processing) which have influenced different aspects of life of citizens and caused many legal challenges in relation to the privacy of citizens in the time of corona outbreak. Comparative and descriptive-analytical method study of legal frameworks governing the right to privacy in the U.S., China, France, and Iran reveals that governments on the basis of special authorizations have taken actions during the pandemic which would be considered as violations to privacy in normal circumstances. French legal system has protected privacy in a centralized and transparent manner and based on accountability and responsibility which mostly is due to the existence of a controller entity. China law because of comprehensive legislations and regulations and citizens' trust in legal and political systems faced few challenges. Iranian law despite the legal and jurisprudential foundations for the protection of privacy is faced with legislation lack and absence of a controller and accountable entity for data processing, and in U.S. law there have been serious legal challenges because of the dual nature of federal and state system and lack of a holistic approach toward the right to privacy and lack of a supervisor entity on data processing. Furthermore, courts have limited the scope of the government's authority in dealing with the coronavirus in relation to privacy matters. In China and France, the government's entry into the field of privacy has been more serious, with the difference that transparency and compliance with the principles of citizen's rights have been in a better state in France. On the other hand, in American law, the least invasion of privacy has been done. In Iran, the lack of clear laws and guidelines can cause privacy concerns.

**How To Cite**

Safari, Mohsen; Ghasemi, Sajjad (2024). Study of protection of citizens' privacy during Covid-19 period with emphasis on data processing (Comparative study of U.S., China, France, and Iran law). *Comparative Law Review*, 15 (1), 93-119.
DOI: https://doi.com/10.22059/jcl.2023.352730.634451

**DOI**

10.22059/jcl.2023.352730.634451

**Publisher**

The University of Tehran Press

شاپا الکترونیکی: ۳۴۰۴-۲۴۲۳

# مطالعات حقوق تطبیقی

دوره: ۱۵، شماره: ۱
بهار و تابستان ۱۴۰۳

Homepage: https://jcl.ut.ac.ir

University of Tehran Press

# بررسی حفظ حریم خصوصی شهروندان در دورهٔ کرونا با تأکید بر مسئلهٔ پردازش داده‌ها (مطالعهٔ تطبیقی در امریکا، فرانسه، چین و ایران)

**محسن صفری[۱]✉ | سجاد قاسمی[۲]**

۱. نویسندهٔ مسئول؛ گروه حقوق خصوصی و اسلامی، دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران.
رایانامه: safarimohsen@ut.ac.ir

۲. گروه حقوق خصوصی، دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران. رایانامه: sajjadghasemi@ut.ac.ir

**اطلاعات مقاله**

**نوع مقاله:** پژوهشی

**تاریخ دریافت:**
۱۴۰۱/۰۹/۳۰

**تاریخ بازنگری:**
۱۴۰۲/۰۷/۱۸

**تاریخ پذیرش:**
۱۴۰۲/۱۰/۰۷

**تاریخ انتشار برخط:**
۱۴۰۳/۰۴/۰۱

**کلیدواژه‌ها:**
*اطلاعات شخصی، پردازش داده‌ها، حریم خصوصی، کرونا.*

**چکیده**

ضرورت مقابله با همه‌گیری کرونا دولت‌ها را به انجام اقدامات متعددی (ازجمله پردازش داده‌ها) سوق داده و بر عرصه‌های مختلفی از زندگی شهروندان تأثیر گذاشته و چالش‌های حقوقی فراوانی را در باب حریم خصوصی شهروندان در دورهٔ کرونا ایجاد کرده است. مطالعهٔ تطبیقی و مبتنی بر روش توصیفی- تحلیلی نظام حقوقی حاکم بر حریم خصوصی در دورهٔ شیوع کرونا در چهار کشور ایران، فرانسه و امریکا و چین، آشکار می‌سازد اقداماتی که در شرایط عادی ناقض حریم خصوصی محسوب می‌شد، در این دوره بر اساس مجوزهای خاص، از سوی دولت‌ها مبنای عمل قرار گرفته است. نظام حقوقی فرانسه به شیوه‌ای متمرکز، شفاف و مبتنی بر پاسخگویی و مسئولیت‌پذیری، حفظ حریم خصوصی را تضمین کرده که بخش مهمی از آن معلول وجود نهاد ناظر در زمینهٔ پردازش داده‌ها است. حقوق چین نیز به‌واسطهٔ قوانین و دستورالعمل‌های متعدد و نیز اعتماد شهروندان به نظام سیاسی و حقوقی با چالش‌های اندکی همراه بوده است. حقوق ایران علی‌رغم وجود مبانی حقوقی و فقهی در حمایت از حریم خصوصی، با خلأ تقنینی و نبود نهاد ناظر و مسئول در زمینهٔ پردازش داده‌ها مواجه بوده و در حقوق امریکا نیز به علت ماهیت فدرال و نیز نبود رویکرد کل‌نگر به مسئلهٔ حریم خصوصی و نهاد عام ناظر بر پردازش داده‌ها، چالش‌های حقوقی بسیار جدی وجود داشته است و دادگاه‌ها دایرهٔ اختیارات دولت در زمینهٔ مقابله با کرونا را در مسائل ناظر بر حریم خصوصی محدود کرده‌اند. در چین و فرانسه ورود دولت به عرصه‌های حریم خصوصی جدی‌تر بوده، با این تفاوت که در فرانسه شفافیت و رعایت اصول حقوق شهروندی در وضعیت بهتری قرار داشته است. در مقابل، در حقوق امریکا کمترین تعرض به حریم خصوصی صورت پذیرفته است. در ایران نیز فقدان قوانین و دستورالعمل‌های شفاف نگرانی‌هایی را در خصوص حفظ حریم خصوصی ایجاد کرده است.

**استناد**
صفری، محسن؛ قاسمی، سجاد (۱۴۰۳). بررسی حفظ حریم خصوصی شهروندان در دورهٔ کرونا با تأکید بر مسئلهٔ پردازش داده‌ها (مطالعهٔ تطبیقی در امریکا، فرانسه، چین و ایران). *مطالعات حقوق تطبیقی*، ۱۵ (۱)، ۹۳-۱۱۹.
DOI: https://doi.com/10.22059/jcl.2023.352730.634451

**DOI** 10.22059/jcl.2023.352730.634451

**ناشر** مؤسسه انتشارات دانشگاه تهران.

CC BY NC

## ۱. مقدمه

بخش مهمی از اقدامات دولت‌ها برای مقابله با همه‌گیری کرونا، مستلزم مداخله در اموری بوده که در چارچوب نظام حقوقی با مفهوم حریم خصوصی شهروندان ارتباط داشته است. ورود دولت به عرصهٔ حریم خصوصیِ شهروندان چالش‌های سیاسی و حقوقی مهمی را ایجاد کرده است. از یک سو، دولت‌ها وظیفهٔ تأمین سلامت شهروندان را برعهده داشتند و گستردگی شیوع کرونا به‌گونه‌ای بود که مسئلهٔ کنترل کرونا دارای ابعاد امنیتی و مرتبط با استراتژی‌های ملی سلامت عمومی درنظر گرفته می‌شد؛ از سوی دیگر، حفظ و احترام به حریم خصوصی شهروندان نیز وظیفهٔ مهمی است که متوجهٔ دولت‌ها می‌شود. تعارض بین حق بر سلامت و حق بر حریم خصوصی و همچنین ابعاد مختلف امنیتی و اجتماعی این تعارض، مسئلهٔ مهمی است که می‌تواند در نظام‌های حقوقی پاسخ‌های متفاوتی داشته باشد. از طرف دیگر، امکان سوءاستفادهٔ دولت‌ها و شرکت‌های خصوصی درگیر در پردازش داده‌های شهروندان با هدف مقابله با کرونا موجب نگرانی بسیاری از شهروندان شده بود. در این زمینه می‌توان به نامهٔ ۴۷۱ نفر از شخصیت‌های دانشگاهی فرانسه و ابراز نگرانی آنها از نقض حق حریم خصوصی شهروندان در برنامه‌های مقابلهٔ دولت با کرونا اشاره کرد. سازمان ملل متحد نیز در گزارشی در آوریل ۲۰۲۰ با عنوان «حقوق بشر و کرونا» در باب اقدامات نظارتی دولت‌ها در بحث شیوع کرونا و اثر آن بر حریم خصوصی بیان داشته که ظرفیت سوءاستفاده از این شیوه‌ها بسیار بالاست و آنچه امروز صرفاً در شرایط اضطراری موجه است، احتمال دارد با پایان شرایط اضطراری، عادی تلقی شود.

نگارندگان این پژوهش با هدف بررسی مسئلهٔ حفظ حریم خصوصی در دورهٔ شیوع کرونا با شیوهٔ تطبیقی در امریکا، فرانسه، چین و ایران به چند بحث خواهند پرداخت. ابتدا به‌عنوان بحث مقدماتی، توضیح مختصری دربارهٔ مفهوم حریم خصوصی و به‌طور کلی نظام حقوقی حاکم بر آن ارائه می‌شود. در بخش دوم تمرکز بر اقدام اصلی دولت‌ها در باب حریم خصوصیِ پردازش داده‌های شهروندان است. بخش سوم به ابعاد حقوقی این اقدامات می‌پردازد و در آن مبنای حقوقی اقدامات دولت‌ها را بررسی می‌کند. در بخش چهارم و در یک نگاه کلی، چارچوب حقوقی حمایت از حریم خصوصی در دورهٔ کرونا در کشورهای مورد مطالعه و اینکه دولت‌ها تا چه حد قادر به ورود به عرصهٔ حریم خصوصی بوده‌اند و نظارت‌ها، پاسخگویی‌ها و دایرهٔ اختیارات و تکالیف در این خصوص از منظر حقوقی چگونه بوده و چه نواقصی داشته است، بحث خواهد شد.

## ۲. حریم خصوصی و حمایت حقوقی از آن

حریم خصوصی ناظر بر بخش‌هایی از زندگی هر شخص است که علنی شدن و انتشار ابعاد آن باید با رضایت خود شخص باشد و دولت‌ها یا سایر اشخاص حق مداخله در این حوزه‌ها را جز در مواردی که

قانون مجاز بداند، نخواهند داشت. حریم خصوصی شامل مصادیق مختلفی ازجمله حریم منزل، حریم خصوصی مربوط به تمامیت جسمانی، حریم خصوصی داده‌های شخصی از قبیل داده‌های سلامت و حریم خصوصی مربوط به محل کار، ارتباطات و نیز حریم خصوصی مرتبط با تکنولوژی‌های جدید می شود. اصل مفهوم حریم خصوصی آن‌چنان در نظام‌های حقوقی محل اختلاف نیست، اما در خصوص اینکه آیا حریم خصوصی متضمن یک حق عام قابل حمایت است و یا اینکه مصادیق مختلفی دارد که باید به‌طور جزئی و به‌عنوان حقوقی مجزا و موردی تحت نظام‌های حمایتی متعدد قرار گیرد، محل بحث است که در ادامه به‌طور اجمالی در حقوق تطبیقی مورد بررسی قرار خواهد گرفت.

### ۲. ۱. امریکا

در فرهنگ‌های لغت حقوقی در تعریف حق بر حریم خصوصی گفته شده است که به معنای حق تنها بودن (Martin, 1977) و در معرض عمومی‌شدن قرار نگرفتن است (Black, 1968). در حقوق امریکا، در خصوص حریم خصوصی رویکرد تقلیل‌گرا پذیرفته شده است (Peikoff, 2008: 3)؛ به این معنا که اگرچه حریم خصوصی در امریکا مورد حمایت قرار می‌گیرد، اما ساختار حمایتی آن جزئی‌نگر است و درواقع چندین حق متمایز مرتبط با حریم خصوصی مورد شناسایی و حمایت نظام حقوقی قرار گرفته است (انصاری و عطار، ۱۴۰۱: ۹۲). برای مثال، در حوزهٔ مسئولیت مدنی به حقوق مربوط به محرمانگی و افشا و شهرت، و در حوزهٔ حقوق اساسی به حقوق مربوط به رفت و آمد و منع تجسس و... تقلیل یافته است و یک حق کلی با عنوان حریم خصوصی مورد شناسایی قرار نگرفته است (Beverley-Smith, 2005: 76).

شناسایی مفهوم حریم خصوصی شهروندان در نظام حقوقی امریکا در سال ۱۹۰۵ با رأی دیوان عالی ایالت جورجیا صورت گرفت. از منظر لایه‌های حمایتی از حریم خصوصی، در قانون اساسی امریکا اشاره صریحی به مفهوم حریم خصوصی نشده است. با این حال، دیوان عالی در سال ۱۹۶۵ در رأیی امکان حمایت از حریم خصوصی با استناد به قانون اساسی ایالات متحده را مورد شناسایی قرار داد (Cudd & Navin, 2018: 3). ویژگی خاص حقوق امریکا در حوزهٔ حریم خصوصی این است که به جای وضع مقررات جامع در باب حریم خصوصی و حفاظت از داده‌ها، قوانین خاصی برای حوزه‌های مختلف ارتباطی و اطلاعاتی و فناوری‌های متفاوت پیش‌بینی کرده است (Cortez, 2021: 234). در خصوص تعیین نهاد دولتی ناظر بر مسئلهٔ حفظ حریم خصوصی باید گفت که نبود رویکرد جامع‌نگر به مسئلهٔ حریم خصوصی در امریکا باعث شده است تا برخلاف کشورهای اروپایی، یک نهاد دولتی متمرکز برای نظارت بر مسئلهٔ حریم خصوصی وجود نداشته باشد.

### ۲. ۲. فرانسه

در فرهنگ‌های حقوقی فرانسه، مفهوم زندگی خصوصی در مقابل مفهوم زندگی عمومی قرار دارد و به اموری اشاره دارد که فرد این حق را دارد که بتواند مانع مداخله یا کسب اطلاع از سوی دیگران در خصوص آن بخش از زندگی خود شود (Guinchard et Debard, 2018). در حقوق فرانسه برخلاف حقوق امریکا حمایت از حریم خصوصی دارای مبنایی مستقل و متمایز است (Wiederkehr, 2019: 92). اولین نشانه‌ها از مفهوم حق بر حریم خصوصی در حقوق فرانسه در آرای دادگاه‌های پاریس و لیون در نیمهٔ قرن نوزدهم آشکار شده است (Rigaux, 1992: 3). در سطح قوانین برتر، در سال ۱۹۹۹ حق بر حریم خصوصی به‌عنوان یک حق مبتنی بر قانون اساسی از سوی شورای قانون اساسی به‌رسمیت شناخته شد. همچنین در سال ۱۹۷۰، مادهٔ ۹ قانون مدنی فرانسه به‌تصویب رسید که طبق آن هر شهروند از حق بر حریم خصوصی برخوردار است و شیوه‌ای خاص برای گرفتن دستور موقت از دادگاه‌های مدنی برای توقف نقض حریم خصوصی پیش‌بینی شده است:

«هر فردی از حق احترام نسبت به زندگی خصوصی خود برخوردار است... قضات می‌توانند اقداماتی را که موجب جلوگیری یا پایان دادن نقض حریم خصوصی زندگی شخصی دیگری می‌شود تجویز کنند» (Mbongo, 2012: 127).

با تصویب قانون فناوری اطلاعات و آزادی‌ها در سال ۱۹۷۴، یک نهاد ملی ناظر بر مسئلهٔ حریم خصوصی داده‌ها در فرانسه با عنوان کمیسیون ملی فناوری اطلاعات و آزادی‌ها تأسیس شد (Vitalis, 2009: 143). تصویب مقررات عمومی حفاظت از داده‌ها از سوی اتحادیهٔ اروپا در سال ۲۰۱۶ منجر به تصویب قانون جدید در سال ۲۰۱۸ در باب حریم خصوصی داده‌ها شد. در این قانون، وظایف کمیسیون یادشده و تعهدات ناظر بر حفاظت از حریم خصوصی جدی‌تر شده است (Cortez, 2021: 60).

### ۲. ۳. چین

توجه و اهتمام نسبت به مسئلهٔ حریم خصوصی و حفاظت از داده‌ها در چین به‌واسطهٔ مسائل فرهنگی و نیز محیط سیاسی این کشور، در مقایسه با سایر کشورهای توسعه‌یافته از نظر زمانی با تأخیر بیشتر و به لحاظ کیفی در سطح پایین‌تری بوده است و در دوره‌ای که وضع قوانین با هدف حمایت از حریم خصوصی در سطوح تقنینی ملی و بین‌المللی مورد توجه گسترده قرار گرفته بود، در چین حمایت از حریم خصوصی با کندی به سمت توسعه حرکت می‌کرد (Pernot-Leplay, 2020: 61). با این حال، توجه افکار عمومی و رسانه‌ها به مسئلهٔ حریم خصوصی از دههٔ ۱۹۸۰ به‌تدریج مسئلهٔ حمایت از حریم خصوصی را مورد توجه قانون‌گذار چین قرار داده است به شکلی که در بیش از ۲۰۰ قانون و مقررهٔ متفاوت به مسئلهٔ حریم خصوصی اشاره شده است (Jingchun, 2005: 645).

حقوق‌دانان چینی در تعریف حق بر حریم خصوصی گفته‌اند حقی است برای یک شخص حقیقی که بر مبنای آن امور و اطلاعات شخصی او نسبت به عمومی شدن و نیز تعرض و مداخلهٔ دیگران مصون باشد، مگر در فرض وجود نفع عمومی (Wang & Yang, 1997: 146). در این تعریف، اختصاص حریم خصوصی به اشخاص حقیقی، تأکید بر مفهوم عام زندگی خصوصی و شخصی و نیز استثنای نفع عمومی، قابل توجه است.

حق بر حریم خصوصی در قانون اساسی ۱۹۸۲ چین به‌عنوان یک حق مستقل مورد شناسایی قرار نگرفته و صرفاً در اصل ۴۰ به حریم خصوصی مکاتبات شهروندان اشاره شده است. مادهٔ ۱۰۱ قانون اصول کلی حقوق مدنی ۱۹۸۶ حق بر شهرت را مورد حمایت قرار داده و رویهٔ قضایی چین تعرض به حریم خصوصی و انتشار اطلاعات شخصی را از مصادیق نقض حق بر شهرت درنظر گرفته است. اولین اشاره صریح به حریم خصوصی در قانون مسئولیت مدنی ۲۰۱۰ صورت گرفته که طبق آن امکان مطالبهٔ خسارت در فرض نقض حریم خصوصی اشخاص پیش‌بینی شده است. در همین قانون، دسترسی و انتشار غیرمجاز اطلاعات و داده‌های سلامت بیماران و نیز سوابق پزشکی با ضمانت اجرا همراه شده است (Pernot-Leplay, 2020: 68). بالاترین و صریح ترین سطح حمایت از حریم خصوصی در قانون مدنی مصوب ۲۰۲۰ چین صورت گرفته و فصل ششم این قانون با عنوان حق بر حریم خصوصی و حفاظت از داده های شخصی از مواد ۱۰۳۲ تا ۱۰۳۹ بر بحث حریم خصوصی متمرکز شده است. همچنین در سال ۲۰۲۱ قانون حمایت از داده‌های شخصی شهروندان به‌تصویب رسیده که برخلاف رویکرد پیشین حقوق چین، حمایت از بخش‌ها و مصادیق مختلف داده‌ها را در قالب یک حق و نظام حمایتی جامع تعریف کرده و موجب نزدیک شدن رویکرد حقوق چین به حقوق حریم خصوصی اتحادیهٔ اروپا در مقایسه با رویکرد ایالات متحده شده است. همچنین، مشابه رویکرد اتحادیهٔ اروپا، نهاد ناظر بر مسئلهٔ رعایت حقوق شهروندی در بحث پردازش داده‌ها پیش‌بینی شده که بر اساس مادهٔ ۶۰ قانون حفاظت از اطلاعات شخصی، ادارهٔ امنیت سایبری چین است.

به این ترتیب، تحول نظام حقوقی چین به سمت پذیرش حق بر حریم خصوصی به‌عنوان یک حق عام و کلی با مصادیق متفاوت بوده است. البته باید توجه داشت که در حقوق چین، حق بر حریم خصوصی و حق بر حفاظت از داده‌های شخصی، دو حق مستقل و مجزا از هم محسوب می‌شوند که مورد حمایت قرار می‌گیرند (Lu Zhang, 2021).

### ۲. ۴. حقوق ایران

در حقوق ایران مفهوم حریم خصوصی و حمایت از آن به‌عنوان یک حق مستقل مورد شناسایی قرار نگرفته است. در قانون اساسی نیز تصریحی به حق حریم خصوصی نشده است (انصاری، ۱۳۹۰: ۱۰۹).

در قوانین عادی مسئلهٔ حریم خصوصی گاه به‌طور صریح و گاه به صورت ضمنی مورد حمایت قرار گرفته است که برای نمونه می‌توان به قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷، قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی مصوب ۱۳۸۲، مواد مرتبط با حقوق متهمان در قانون آیین دادرسی کیفری، مواد ۵۷۲ تا ۵۷۵ و ۵۸۰ و ۶۹۱ و ۶۹۲ و ۶۹۴ قانون تعزیرات و همچنین مواد ۱۰۰ و ۱۳۰ قانون برنامهٔ چهارم توسعه اشاره کرد. از جهت نهاد ناظر در بحث حریم خصوصی و داده‌ها، طبق مادهٔ ۱۸ قانون انتشار و دسترسی آزاد به اطلاعات، کمیسیون انتشار و دسترسی به اطلاعات تشکیل خواهد شد که وظیفهٔ ممانعت از دسترسی غیرمجاز به اطلاعات مرتبط با حریم خصوصی را برعهده دارد.

صرف‌نظر از حقوق موضوعه در باب حریم خصوصی که در حال تکوین و توسعه است، مسئلهٔ احترام به حریم خصوصی در اسلام مسبوق به سابقه بوده و این مسئله از مبنای نظری قابل‌توجهی برخوردار است. برای مثال، عبارت «و لا تَجَسَّسُوا» در آیهٔ ۱۲ سورهٔ حجرات مبنای مباحث مهمی در تفسیر و فقه در خصوص حریم خصوصی بوده است. شیخ طوسی تجسس را مترادف با تحسس و به معنای تبحث و جستجو دانسته و گفته است این یک تکلیف است برعهدهٔ مؤمن که از جستجوی بدی دیگران خودداری کند (طوسی، ۱۴۱۳: ۳۵۰). طبرسی یکی از احتمالات در خصوص دلالت آیه را منع جستجو از آنچه مخفی شده، دانسته است (طبرسی، ۱۴۱۵: ۵۳۸). گفته شده که موضوع عدم تجسس، اسرار و خفایای فردی و خانوادگی اشخاص است (مشکینی، ۱۴۳۴: ۱۲۸). فخر رازی دلالت آیه را نهی از گمانه‌زنی در خصوص عیوب مخفی مردم و نهی از جستجو برای کسب یقین در این زمینه دانسته است (فخر رازی، ۱۴۲۰: ۱۱۰). فقها نیز بر همین مبنا قائل به حرمت تجسس در امور مخفی و عیوب مردم هستند (نجفی، ۱۳۶۲، ۲۹۸). همچنین بیان شده است با توجه به عدم تقیید حرمت تجسس در آیه، منع تجسس به‌مثابه یک قاعدهٔ عام است (مکارم شیرازی، ۱۴۲۸: ۳۱۰). بعضی مقتضی حرمت تجسس را از مقتضی وجوب نهی از منکر اقوی و اهم دانسته و گفته‌اند حرمت تجسس مقدم بر وجوب نهی از منکر احتمالی است (مظفر، ۱۳۸۰: ۲۳۴). حرمت تجسس را شامل اعمال حکومت نیز دانسته‌اند (ایروانی، ۱۴۲۸: ۷۷۴). در ذیل عناوین دیگری نیز مسئلهٔ حریم خصوصی مطرح شده است. برای مثال، می‌توان به حرمت منزل (امام خمینی، ۱۳۶۸: ۴۶۷) و همچنین منع سوء ظن به دیگران که می‌تواند مقدمهٔ تجسس در خصوص امور مخفی آنان باشد، اشاره کرد (شهیدثانی، ۱۳۹۰: ۲۲). بر این اساس، مسئلهٔ حمایت از حریم خصوصی در حقوق ایران دارای مبنای مستحکم و پرسابقه‌ای در فقه اسلامی است که می‌تواند زمینهٔ مناسبی برای توسعهٔ ساختار حمایت حقوقی از حریم خصوصی شهروندان باشد.

به این ترتیب، حریم خصوصی برخلاف حقوق فرانسه و چین که یک حق مستقل و متمایز است، در حقوق امریکا و ایران با رویکردی تقلیل‌گرایانه در چندین حق و حریم متفاوت و پراکنده مورد شناسایی و حمایت قرار گرفته است. از نظر نهاد ناظر، کمیسیون ملی پیش‌بینی شده در حقوق فرانسه، دارای

رویکردی فعال در زمینهٔ صیانت از حریم خصوصی داده‌ها است. در چین نیز نهاد مشابهی پیش‌بینی شده است؛ درحالی که در حقوق امریکا چنین نهادی به‌طور متمرکز پیش‌بینی نشده است. در حقوق ایران کمیسیون مربوط به دسترسی آزاد به اطلاعات تا حدی می‌تواند خلأ نهاد ناظر را پر کند.

## ۳. پردازش داده‌های شهروندان در دورهٔ کرونا

اقدامات مقابله‌ای دولت‌ها را در زمینهٔ کرونا که با بحث حریم خصوصی مرتبط بوده است می‌توان در دو دستهٔ اقدامات درمانی و غیردرمانی قرار داد. ازجمله مهم‌ترین مصادیق اقدامات مرتبط با شیوه‌های غیردرمانی و دارویی کنترل بیماری در مورد حریم خصوصی، پردازش داده‌های شهروندان در قالب اپلیکیشن‌های رهگیری تماس‌های نزدیک بوده که ممکن است در تعارض با حریم خصوصی شهروندان باشد که در ادامه مورد بررسی قرار خواهد گرفت.

دولت‌ها برای تضمین اینکه فردِ مبتلا به کرونا در تماس با سایر افراد قرار نمی‌گیرد به‌دنبال پردازش اطلاعات شهروندان هستند؛ به این معنا که از طریق فناوری‌های نوین و به‌خصوص گوشی‌های موبایل با رهگیری فرد مبتلا و نیز موقعیت‌یابی افرادی که به فرد موردنظر نزدیک شده‌اند، هشدارهایی را برای شهروندان ارسال کنند. نظارت بر موقعیت مکانی شهروندان و تماس آنان با افراد مبتلا به کرونا به سه شیوه قابل انجام است: شیوهٔ اول، موقعیت‌یابی سنتی است که بر مصاحبه و کسب اطلاع فردی مبتنی است. شیوهٔ دوم، مدیریت دیجیتال است که به استفاده از ابزارهای دیجیتال برای ساده‌سازی و پردازش داده‌های مربوطه اشاره دارد. شیوهٔ سوم، اعلان هشدار درمعرض ابتلا قرار گرفتن با استفاده از فناوری بلوتوث و سامانهٔ موقعیت‌یاب جهانی (GPS) است (Yang, et al. 2020: 8).

شیوهٔ سوم دارای چالش‌های بیشتری دربارهٔ حریم خصوصی در دورهٔ کرونا است. در ۱۰ آوریل ۲۰۲۰ شرکت‌های گوگل و اپل از برنامهٔ مشترکی برای سیستم اعلان هشدار درمعرض ابتلا قرار گرفتن بر مبنای بلوتوث در سیستم عامل‌های اندروید و IOS با هدف توانمند ساختن مقامات عمومی حوزهٔ بهداشت و درمان برای پردازش برنامه‌های دنبال کردن ارتباطات و موقعیت مکانی شهروندان برای کنترل کرونا خبر دادند. شیوهٔ کار این سیستم به این صورت است که گوشی موبایل را قادر می‌سازد تا وجود سایر گوشی‌های موبایل در فاصله معینی از آن گوشی و در مدتی معین را مورد شناسایی قرار دهد. هنگامی که دو نفر در فاصلهٔ معینی به هم نزدیک شده، به‌اصطلاح «دست دادن» رخ می‌دهد که منظور برقرار تماس و ارتباط نزدیک است، این مسئله در گوشی ثبت می‌شود؛ به این صورت که هر فرد، دارای یک کد شناسایی به صورت رمزگذاری شده است که بر روی گوشی‌های آن دو نفر ذخیره می‌شود. وقتی فرد به کرونا مبتلا می شود، با ثبت بیماری خود در اپلیکیشن مربوطه یا بارگذاری اطلاعات از سوی نهادهای مربوطه، سیستم

اعلان هشدار به صورت روزانه با دریافت اطلاعات، هنگامی که متوجهٔ تست مثبت یک کد شناسایی می شود به‌طور خودکار یک هشدار به تمام گوشی‌هایی که آن کد شناسایی به‌واسطهٔ ارتباط و نزدیکی مکانی به آن فرد بر روی گوشی آنان ذخیره شده، ارسال می‌کند (Bradford, et al. 2020: 2).

علاوه بر مسئلهٔ داده‌های مکانی و ملاقات‌ها، لزوم دسترسی به نتایج تست‌های کرونا نیز در عملکرد این اپلیکیشن‌ها مهم است. این مسئله می‌تواند در تعارض با مسئلهٔ حریم خصوصی مرتبط با داده‌های سلامت اشخاص باشد. داده‌های سلامت که به وضعیت سلامت و درمان جسمی و روحی افراد اشاره دارد، زیرمجموعهٔ داده‌های شخصی قرار می‌گیرد و جزء حساس‌ترین حوزه‌های مربوط به حریم خصوصی اشخاص است (Levit & Gostin, 2009: 78). مفهوم داده‌های شخصی ابتدا در سال ۱۹۸۰ با متن «دستورالعمل‌های حفاظت از حریم خصوصی و گردش فرامرزی اطلاعات شخصی» که از سوی شورای سازمان همکاری اقتصادی و توسعه منتشر شد، مورد توجه قرار گرفت. اولین سند حقوقی دربردارندهٔ تعریف داده‌های شخصی کنوانسیون شمارهٔ ۱۰۸ شورای اروپا در خصوص حفاظت از اشخاص در برابر پردازش خودکار اطلاعات شخصی بود (Kindt, 2013: 90). در مادهٔ ۲ این کنوانسیون در تعریف داده‌های شخصی گفته شده است که به اطلاعاتی اشاره دارد که به یک فرد احرازِ هویت شده یا قابل احراز هویت مرتبط است. نکتهٔ مهم در این تعریف، قابلیت شناسایی و احراز هویت شخص موضوع داده‌ها است. رکن قابلیت شناسایی که معیار شمول قواعد حمایتی نسبت به اطلاعات شخصی است در مادهٔ ۴ قانون حفاظت از اطلاعات شخصی چین نیز مورد تأکید قرار گرفته است. در این کنوانسیون، طبق مادهٔ ۶، داده‌های مربوط به سلامت و درمان بیماران جزء داده‌های حساس قرار می‌گیرند که به حمایت بیشتری نیاز دارند. فعالیت اپلیکیشن‌های رهگیری نیازمند جمع‌آوری داده‌های مرتبط با وضعیت ابتلای شهروندان به کرونا است؛ درحالی که این موضوع می‌تواند به‌عنوان یک امر خصوصی مرتبط با پروندهٔ پزشکی افراد قرار گیرد.

مشخص است که چنین شیوه‌ای از نظارت بر شهروندان می‌تواند امکان کنترل و نظارت بی‌سابقه‌ای را برای نهادهای دولتی یا شرکت‌های خصوصی ایجاد کند که به‌راحتی محل رفت و آمد اشخاص و نیز افرادی را که مورد ملاقات قرار گرفته‌اند شناسایی نمایند. میزان به‌اشتراک‌گذاری این اطلاعات خصوصی شهروندان از سوی شرکت‌ها و توسعه‌دهندگان خدمات فنی این قبیل نظارت‌ها با نهادهای دولتی یا سایر اشخاص یا میزان دسترسی به این اطلاعات مسئله‌ای مهم و حساس در باب حریم خصوصی افراد در دورهٔ کرونا است (Scassa, et al. 2020: 3). اشتراک‌گذاری و انتقال اطلاعات بین گوشی‌ها و سیستم‌های عامل که به آن «تعامل‌پذیری» گفته می‌شود، می‌تواند زمینهٔ مستعدی برای سوءاستفاده از اطلاعات از سوی شرکت‌های فناوری را فراهم سازد. استفاده از تکنولوژی برای نظارت بر شهروندان با هدف کنترل کرونا، می‌تواند زمینهٔ عادی‌سازی نظارت و نقض حریم خصوصی شهروندان در آینده را

فراهم سازد (Scassa, et al. 2020: 11). در کنار استفاده از تکنولوژی مرتبط با گوشی‌های موبایل که بیشترین کاربرد را در دورهٔ کرونا داشته، موارد استفاده از زیرساخت‌های هوشمند شهری، ازجمله دوربین های مداربسته، تصاویر دریافت‌شده از پهپاد و استفاده از کارت های بانکی و خودپردازها نیز وجود داشته است (Mitchell, P. & Foth, M, 2022: 7).

به این ترتیب، باید گفت اقدامات دولت‌ها دامنهٔ وسیعی از حوزه‌های حریم خصوصی ازجمله حریم خصوصی مرتبط با وضعیت سلامت، محل رفت و آمد و حضور، حریم منزل خصوصی و افراد حاضر در آن، روابط دوستانه و صمیمانهٔ افراد و حریم خصوصی در محل کار و نیز به‌طور کلی داده‌های خصوصی را مورد مداخله قرار داده و چالش‌های مهمی در زمینهٔ مسائل حقوقی، سیاسی و فرهنگی در باب حریم خصوصی شهروندان ایجاد کرده است.

## ۴. نظام‌های حقوقی و چالش‌های حریم خصوصی در دورهٔ کرونا

چالش‌های موردبحث در باب نقض حریم خصوصی شهروندان در دورهٔ شیوع کرونا موجب شکل‌گیری مسائل حقوقی مهمی در کشورها در خصوص حدود اختیار دولت و حمایت‌های حقوقی از حریم خصوصی شده است. در ادامه، مهم‌ترین مسائل حقوقی مطرح‌شده در کشورهای امریکا، فرانسه، چین و ایران که ناظر بر پردازش داده‌ها است، مورد بررسی قرار خواهد گرفت.

### ۴. ۱. امریکا

اگرچه دولت فدرال به‌طور مستقیم از اپلیکیشن‌های موقعیت‌یاب استفاده نکرده، اما در سطح ایالت‌ها از چنین برنامه‌هایی بهره برده شده است. تا پایان سال ۲۰۲۰، نوزده ایالت از طریق توافق با شرکت‌های گوگل و اپل اقدام به راه‌اندازی چنین برنامه‌هایی کرده‌اند (Genia & Sabrina, 2022: 4). عمدهٔ نگرانی شهروندان امریکایی نسبت به نقض حریم خصوصی آنان معلول بی‌اعتمادی به شرکت‌های فناوری و نیز امکان سوءاستفادهٔ دولت فدرال است (Yang, et al. 2020: 10).

از نظر حقوقی، تنها قانون مرتبط با این مسئله در سطح ملی، قانون قابلیت انتقال و مسئولیت بیمهٔ سلامت است. در مواد ۲۶۱ تا ۲۶۴ این قانون به وزارت بهداشت مأموریت داده شده است تا معیارهای مشخصی برای حفاظت از داده‌های سلامت شهروندان پیش‌بینی کند. وزارت بهداشت در سال ۲۰۰۲ با انتشار متن معیارهای حریم خصوصی اطلاعات مربوط به سلامت اشخاصِ قابل شناسایی به این وظیفه عمل کرده است. حوزهٔ حریم خصوصی مورد حمایت طبق این قانون، محدود به اطلاعاتی است که از سوی ارائه‌دهندگان خدمات سلامت یا شرکت‌های به‌کار گرفته شده از سوی آنان جمع‌آوری شده است و

ناظر به فعالیت شرکت‌های فناوری مثل گوگل و اپل نیست (Bradford, et al. 2020: 7). با این حال، ازآنجا که اپلیکیشن‌های موقعیت‌یاب بر اساس اطلاعات مربوط به نتایج تست‌های کرونا فعالیت می‌کنند، حریم خصوصی مورد حمایت این قانون شامل نتایج تست‌های کرونا می‌شود. درنتیجه نهادهای دولتی و ایالتی نمی‌توانند به‌طور خودکار نتایج تست‌های کرونا را در اختیار دیگران قرار دهند. به همین جهت، تنها راه قانونی برای فعالیت این اپلیکیشن‌ها این است که خود شهروندان به‌طور داوطلبانه اطلاعات ابتلای خود به بیماری را در برنامه ثبت کنند. باید توجه داشت که نبود قوانین حمایتی مناسب در زمینهٔ حریم خصوصی موجب شده است تا رویهٔ قانونی مشخصی در این زمینه وجود نداشته باشد و درنتیجه نگرانی‌ها برای نقض حریم خصوصی بسیار بالا باشد.

به‌عنوان جمع‌بندی، ویژگی‌های نظام حقوقی حاکم بر حریم خصوصی در امریکا در دورهٔ شیوع کرونا را می‌توان در چند مورد اصلی خلاصه کرد: ویژگی اول، نبود قوانین جامع در باب حوزهٔ حریم خصوصی است که موجب عدم شفافیت و پیش‌بینی‌پذیری حقوقی دربارهٔ موارد نقض حریم خصوصی و حمایت‌های موجود می‌شود. عدم شفافیت در نظام دوگانهٔ فدرال– ایالتی آشکارکنندهٔ این امر است که اختلافات مهمی در زمینهٔ اقدامات ناظر بر کنترل کرونا و قواعد حاکم بر آن بین دولت فدرال و ایالت‌ها وجود داشته است. در این باره می‌توان به طرح دعوای دولت فدرال علیه ایالت میسوری در خصوص الزام به تزریق واکسن اشاره کرد. بر همین اساس، مداخلهٔ دادگاه‌ها نیز نشانگر نوعی آشفتگی حقوقی است. ویژگی دوم، محرمانگی اطلاعات مربوط به مبتلا شدن شهروندان به کرونا بر اساس حمایت از حریم خصوصی حوزهٔ داده‌های سلامت و درنظر گرفتن رضایت فرد مبتلا به‌عنوان تنها استثنا است که محدودیت مهمی در مسیر مقابلهٔ دولت با بیماری کرونا ایجاد می‌کند.

### ۴. ۲. فرانسه

در حوزهٔ اقدامات غیردرمانی، استفاده از برنامه‌های رهگیری مورد توجه دولت فرانسه بوده و در این زمینه بر لزوم پردازش داده‌ها از سوی نهادهای حاکمیتی تأکید شده است.

اولین اپلیکیشن ملی با عنوان StopCovid app در فرانسه راه‌اندازی شد که با موفقیت چندانی همراه نبود و بعد از مدتی نسخهٔ جدیدی با عنوان TousAntiCovid منتشر شد. مبنای حقوقی این برنامه در دستوری که نخست‌وزیر و وزرای مربوطه صادر کردند، ذکر شده است. در این دستور به قانون فناوری اطلاعات و آزادی‌ها و به‌طور خاص به قانون جدیدالتصویب مواجهه با همه‌گیری کرونا استناد شده است که طبق مادهٔ ۴ آن، امکان اعلام وضعیت اضطراری سلامت عمومی از سوی دولت و اتخاذ اقدامات ویژه برای مقابله با بیماری وجود دارد.

مهم‌ترین قانون در خصوص حفظ حریم خصوصی در فرانسه، مقررات عمومی حفاظت از داده‌ها در پارلمان اروپا بوده که جزئی از قانون مرتبط با حریم خصوصی داده‌ها مصوب ۲۰۱۸ است. بررسی مطابقت اپلیکیشن رهگیری با مقررات حمایتی حریم خصوصی برعهدهٔ نهاد کنترل‌کنندهٔ حریم خصوصی فرانسه یعنی کمیسیون ملی فناوری اطلاعات و آزادی‌ها است. کمیسیون در ۲۴ آوریل ۲۰۲۰ مطابقت اپلیکیشن یادشده با قواعد حمایتی حریم خصوصی را مشروط به رعایت توصیه‌ها و تضمین‌هایی در باب حفظ حریم خصوصی اعلام کرد. اولین مسئلهٔ حقوقی این است که آیا پردازش داده‌ها در اپلیکیشن پیش‌گفته مشمول حمایت‌های حریم خصوصی مندرج در مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا- که منبع اصلی حفاظت از حریم خصوصی داده‌ها در حقوق فرانسه است- می‌شود یا خیر. از منظر موضوع داده‌ها، طبق نظر کمیسیون، وضعیت ابتلای یک فرد به بیماری، جزء داده‌های مربوط به سلامت محسوب شده، درنتیجه مشمول حمایت‌های مقررات حفاظت از داده‌های اتحادیهٔ اروپا خواهد بود. از جهت اینکه آیا ماهیت داده‌های گردآوری‌شده، داده‌های شخصی محسوب می‌شوند یا خیر، باید توجه داشت که داده‌های مشمول حمایت این مقررات، داده‌های شخصی است که طبق بند ۱ مادهٔ ۴ مقررات، شامل داده‌هایی است که قابل انتساب به یک فردِ احراز هویت شده یا قابل احراز هویت هستند. بر این اساس، اطلاعاتی که در آن، فرایند ناشناس‌سازی داده‌ها به معنای حذف اطلاعات مؤثر در شناسایی افراد صورت می‌پذیرد، به‌گونه‌ای که تحت هیچ شرایطی قابل ربط دادن به یک فرد مشخص نباشد از شمول داده‌های شخصی و به تبع آن، از شمول حمایت این مقررات خارج است. اما با توجه به اینکه پردازش داده‌ها در این اپلیکیشن بر اساس شیوهٔ استفاده از کدهای شناسایی مستعار و مصنوعی یا به‌اصطلاح مستعارسازی می‌باشد و داده‌های مستعارسازی شده مشمول نظام حمایتی مقررات هستند، اپلیکیشن یادشده باید در چارچوب حمایتی این مقررات فعالیت کند. طبق بند ۵ مادهٔ ۴ مقررات، مستعارسازی به این معناست که پردازش اطلاعات به‌گونه‌ای انجام می‌شود که بدون استفاده از اطلاعات بیرونی نمی‌توان داده‌ها را به یک فرد معین منتسب کرد. در متن کمیسیون نیز بر مستعارسازی اطلاعات در فرایند پردازش اطلاعات از سوی اپلیکیشن تأکید شده است .

مسئلهٔ بعدی ناظر بر مبنای قانونی فعالیت این اپلیکیشن و جمع‌آوری داده‌ها از منظر حریم خصوصی است. مقررات حفاظت از داده‌ها در مادهٔ ۶، هفت جهت مشروع برای پردازش داده‌های شخصی را ذکر کرده است. کمیسیون اگرچه اولین مبنای قانونی را کاربرد اختیاری و داوطلبانهٔ این اپلیکیشن دانسته است، اما ازآنجا که باید یک مبنای مشخص از سوی کمیسیون انتخاب شود تا بتوان جزئیات و حدود اختیار را در تناسب با آن مبنا انتخاب کرد، کمیسیون مناسب‌ترین مبنای قانونی برای پردازش اطلاعات مربوط به سلامت شهروندان در دورهٔ کرونا را به‌انجام رساندن مأموریتی با هدف نفع عمومی که در بند «e» مادهٔ ۶ مقررات و مادهٔ ۵،۵ قانون داده‌ها و آزادی‌ها بیان شده است دانسته و بیماری کرونا به‌عنوان مصداقی از

مفهوم تهدیدات جدی فرامرزی علیه سلامت درنظر گرفته شده است کـه در مـادۀ ۹ مقـررات بـه‌عنـوان استثنای مرتبط با نفع عمومی در حوزۀ سلامت در زمینۀ پردازش اطلاعات شخصی ذکر شده است.

برای جمع‌بندی باید گفت، در فرانسه داده‌های سلامت نیز بر اساس استثنای مربوط به منافع عمومی و به صورت مستعارسازی شده می‌تواند از سوی دولت مورد استفاده قرار گیرد. در فرانسه، کمیسیون ملـی فناوری اطلاعات و آزادی‌ها با نظارت و دقت بر فعالیت‌های دولت، حفظ حریم خصوصی شـهروندان را از طریق قانون‌مداری، شفافیت و پاسخگویی تضمین کرده و مسـئلۀ حاکمیـت ملـی در پـردازش داده‌هـای شهروندان نیز مورد توجه این کمیسیون بوده است.

## ۴. ۳. چین

بررسی مواجهۀ چین با بیماری کرونا و تعارض آن با حقوق مرتبط با حریم خصوصی شهروندان- به‌ویـژه در بحث پردازش داده‌ها- هم به‌واسطۀ گستردگی شیوع و طولانی بودن مدت درگیری چـین بـا کرونـا و هم به سبب رویکردهای خاص سیستم سیاسی و قضایی چین در اولویت دادن به منافع و حقوق جمعی از اهمیت ویژه‌ای برخوردار است. دولت چین برای کنترل بیماری کرونا از ابزارهای نظارتی مختلفی از قبیل پهپادها، دوربین‌های مداربسته، بارکدهای دیجیتال و برنامه‌های موقعیت‌یاب گوشی‌های موبایـل بـه‌طـور گسترده استفاده کرده و سیستم جامعی از نظارت و کنترل را بر شهروندان خود اعمـال نمـوده اسـت کـه تشکیل‌دهندۀ سیاست کووید صفر در چین بوده است (Liu & Zhao, 2021: 744).

در چین پردازش داده‌های سلامت و مکانی شهروندان از طریق اپلیکیشن‌های مربوطه به‌طور گسترده انجام شده و برخلاف بسیاری از کشورها استفاده از این اپلیکیشن‌ها برای شهروندان الزامـی بـوده اسـت (Simko, et al. 2022: 4). یکی از ابتکارات خاص چین در زمینۀ پردازش داده‌ها، استفاده از کـد پاسـخ سریع سلامت بوده است که اطلاعات مربوط به محل اقامت، تزریق واکسن، علائم بیماری و رفت و آمد را مورد پردازش قرار داده تا میزان خطر و ریسک مبتلا بودن یک فرد قابل ارزیـابی باشـد (Cheng, et al. 2023: 3). شهروندان در اپلیکیشن خاصی که دارای تشخیص هویت بر اساس چهره بـوده، بایـد بـه صورت روزانه وضعیت سلامت خود را به‌روزرسانی می‌کردند و خود اپلیکیشن نیز موقعیت مکانی افـراد را مورد ارزیابی قرار می‌داد و درنهایت شهروندان در سه رنگ قرمز، زرد و سبز دسته‌بنـدی مـی‌شـدند. ایـن سازوکار در بیش از ۳۰۰ شهر چین و با مشارکت بیش از ۹۰۰ میلیون کاربر از سوی دولت چـین اجرایـی شد (Liang, 2020: 1).

در خصوص مبنای حقوقی و مشروعیت مداخلات دولت در بحث پردازش داده‌های شهروندان چینـی در دورۀ کرونا به قوانین و مقررات مختلفی در حقوق چین استناد شده که بر مبنـای آن بـرای دولـت اختیـارات

گسترده‌ای در زمینهٔ تأمین سلامت و نفع عمومی پیش‌بینی شده است. اصل ۲۱ قانون اساسی چین حفظ سلامت عمومی را از وظایف دولت دانسته و در مواد ۱۰۰۲، ۱۰۰۳ و ۱۰۰۴ قانون مدنی بر حق بر سلامت تأکید شده است. در قانون خلق چین در کنترل و جلوگیری از بیماری‌های مسری مصوب ۲۰۱۳ و نیز قانون پاسخ اضطراری مصوب ۲۰۰۷، اختیاراتی برای دولت در تأمین سلامت و انجام اقدامات لازم پیش‌بینی شده که به‌عنوان مبنای حقوقی اختیارات فراتر از حد معمول دولت در هنگام بیماری کرونا مورد استناد قرار گرفته است. به‌علاوه، دولت چین با هدف کنترل پاسخ به بیماری و نیز تأمین حقوق شهروندی، دستورالعمل ها و آیین‌نامه‌های متعددی را در دورهٔ کرونا صادر کرده است (Duan & Qin, 2022: 4).

ازجمله ویژگی‌های اصلی و منحصربه‌فرد مواجههٔ نظام حقوقی چین با مسئلهٔ حریم خصوصی در دورهٔ کرونا، عدم وقوع چالش‌های حقوقی جدی و پذیرش بالای اجتماعی و فرهنگی سیاست‌های دولت چین در زمینهٔ پردازش داده‌های شهروندان از سوی شهروندان چینی بوده است (Simko, et al. 2022: 5). بعضی از نویسندگان علت اعتماد شهروندان چینی به سیاست‌های پردازش داده‌ها از جانب دولت را معلول رویکرد اجتماع‌گرایی دانسته‌اند که در فرهنگ چین و سایر کشورهای آسیای شرقی قابل ملاحظه است و بر مبنای آن، منافع عمومی و جمعی بر منافع فردی اولویت دارد و نقطهٔ مقابل رویکرد آزادی‌گرایی فردی در نظام‌های غربی لیبرال است (Liu & Zhao, 2021: 746).

در این زمینه، آمادگی نظام حقوقی و سیاسی چین برای مواجهه با همه‌گیری کرونا را نیز باید ازجمله عوامل مؤثر در اعتماد جامعه به سیاست‌های دولت به‌خصوص در بحث حریم خصوصی دانست. چین ازجمله کشورهایی بود که پیش از شروع همه‌گیری کرونا دارای قوانین مشخص و نسبتاً جامعی در این زمینه بود و می‌توان گفت نظام حقوقی چین بسیار پیش‌تر از شیوع کرونا آماده رویارویی با یک همه‌گیری بوده است. به همین ترتیب، پس از شیوع کرونا نیز ۹ قانون و بیش از ۸۰ آیین‌نامهٔ دولتی در زمینهٔ مقابله با کرونا و تعیین حقوق و مسئولیت‌های دولت و شهروندان تصویب و منتشر شده و در آن بر عدم انتشار اطلاعات گردآمده از شهروندان تأکید شده است (Duan & Qin, 2022: 5, 7). از جملهٔ این اسناد می توان به هشدار مربوط به حفاظت از داده‌های شخصی و استفاده از کلان‌داده‌ها که در فوریه ۲۰۲۰ از سوی دفتر کمیتهٔ مرکزی امنیت سایبری و اطلاعات چین صادر شد، اشاره نمود (Wu, et al. 2020: 25).

در مقام جمع‌بندی باید گفت چین ازجمله کشورهایی بوده که در دورهٔ کرونا اقدامات گسترده‌ای را با هدف کنترل بیماری اجرا کرده که بر حوزهٔ حریم خصوصی شهروندان و پردازش داده‌ها اثری جدی داشته است. با این حال، انسجام نظام حقوقی، قضایی و سیاسی چین و نیز اعتماد شهروندان به حاکمیت موجب شده است که مداخلات دولت در امور خصوصی و پردازش داده‌های شهروندان با کمترین چالش حقوقی و سیاسی همراه باشد؛ اگرچه امکان سوءاستفاده دستگاه‌های دولتی از این اطلاعات وجود خواهد داشت.

### ۴. ۴. ایران

در زمینهٔ پردازش داده‌ها و استفاده از اپلیکیشن‌های موقعیت‌یاب و رهگیری تماس‌های نزدیک، اقدامات مختلفی در ایران صورت گرفته است که می‌توان به اپلیکیشن‌های «ریسک من»، «ماسک» و «سامانهٔ ایران من» اشاره کرد. برای مثال، اپلیکیشن «ریسک من» که آن را دستیار تشخیص و مراقبت کووید ۱۹ به کمک هوش مصنوعی دانسته‌اند، در اسفند ۱۳۹۹ در دانشگاه شهید بهشتی رونمایی شد. در توضیحات مرتبط با این برنامه آمده است که بیش از ۳ میلیون داده مربوط به ۱۰۰ هزار بیمار از ۷۵ بیمارستان استان تهران جمع‌آوری شده است تا در صورت ابتلای فرد به کرونا، بر اساس پردازش این داده‌ها، میزان ریسک و نوع علائم فرد مبتلاشده را پیش‌بینی کند. این داده‌ها شامل مواردی مثل سن، قد، بیماری‌های زمینه‌ای و سوابق دارویی می‌شود. مورد دیگر، اپلیکیشن «ماسک» است که از سوی بخش خصوصی و کارشناسان دانشگاه‌های صنعتی شریف و امیرکبیر طراحی شده و وزارت بهداشت نیز آن را توصیه کرده است. این اپلیکیشن با استفاده از بلوتوث، در صورت برقراری تماس نزدیک بین دو فردی که یکی از آنان به کرونا مبتلا بوده، هشداری را برای دیگری ارسال می‌کند و مشابه نمونه‌های خارجی است که پیش‌تر به آن اشاره شد. سازندگان در توضیح حفظ حریم خصوصی در این برنامه گفته اند: همهٔ دسترسی‌ها در این برنامه با اجازهٔ کاربر بوده است و کمیته‌ای متشکل از معتبرترین نهادهای تخصصی و علمی و مستقل کشور و نمایندگان چند خیریهٔ معتبر بر محرمانگی داده‌ها نظارت می‌کنند. مورد دیگر «سامانهٔ ایران من» است که به‌عنوان سکوی خدمات شهروندان در شرایط بحران‌های سلامت معرفی شده است. این سامانه فعلاً بر حوزهٔ حمل و نقل، اصناف، مسافران و مرزبانی متمرکز است. هدف این سامانه، ایجاد امکان استعلام برای شهروندان و صاحبان کسب و کارها در خصوص ابتلای مراجعان یا ارائه‌دهندگان خدمات به کرونا است. در مقطعی مجوز سفر نوروزی نیز منوط به ثبت پلاک در این سامانه شده بود. در این سامانه بر حریم خصوصی شهروندان تأکید شده است که اطلاعات هویتی حذف و داده‌ها به صورت ناشناس جهت ایجاد داده‌های تصمیم‌ساز ملی مورد استفاده قرار خواهد گرفت. همچنین تأکید شده است که تمامی داده‌ها با حفظ حقوق شهروندی در لایه‌های نقل و انتقال میان‌سازمانی نگهداری و با استفاده از امن‌ترین استانداردهای بین‌المللی رمزگذاری شده‌اند.

مسئلهٔ مهم از نظر حقوقی، بررسی حمایت‌ها از داده‌های شخصی شهروندان و مطابقت اپلیکیشن‌ها و سامانه‌های ایجادشده با ساختار حمایتی از داده در حقوق ایران است. طبق بند «ب» مادهٔ ۱ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷، اطلاعات شخصی شامل اطلاعات فردی، نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی های جسمی، شمارهٔ حساب بانکی و رمز عبور است. مادهٔ ۱۵ این قانون ارائهٔ اطلاعات شخصی از سوی

نهادهای دولتی را ممنوع کرده است؛ مگر اینکه شخص ثالث به نحو صریح و مکتوب به افشای اطلاعات راجع به خود رضایت داده باشد یا شخص متقاضی، ولی یا قیّم یا وکیل شخص ثالث در حدود اختیارات خود باشد و یا متقاضی یکی از مؤسسات عمومی باشد و اطلاعات درخواست‌شده در چارچوب قانون مستقیماً به وظایف آن به‌عنوان یک مؤسسهٔ عمومی مرتبط باشد. مسئله مهمی که باید به آن پرداخت این است که کدام دسته از اطلاعات جمع‌آوری شده در مسیر مقابله با کرونا، اطلاعات شخصی محسوب می‌شود و سپس باید دید آیا نحوهٔ جمع‌آوری و دسترسی‌ها در خصوص این داده‌ها منطبق با ساختار حمایتی اطلاعات شخصی بوده است یا خیر.

در خصوص مسئلهٔ اول، کمیسیون انتشار و دسترسی آزاد به اطلاعات که بر اساس مادهٔ ۱۸ قانون انتشار و دسترسی آزاد به اطلاعات تشکیل شد و وظایف مشخصی در حوزهٔ حمایت از داده‌ها دارد، مصوبه ای با عنوان شیوه‌نامهٔ تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی دارد که در آن تعریف و توضیح دقیق‌تری در خصوص اطلاعات شخصی آمده است. اولین نکته این است که طبق بند ۲ مادهٔ ۳ شیوه‌نامه، درصورتی که هویت افراد موجود در اطلاعات قابل تشخیص نباشد، این اطلاعات خصوصی یا شخصی محسوب نمی‌شود. این مورد مشابه مقررات اتحادیهٔ اروپا در تعریف داده‌های شخصی است. مادهٔ ۴ شیوه‌نامه، گروه خونی و مشخصات ژنتیکی؛ مادهٔ ۶ مکان‌های استفاده از وسیلهٔ ارتباطی و مکان‌های مراجعه افراد؛ و مادهٔ ۹ پروندهٔ پزشکی افراد، اطلاعات کلیهٔ بیماری‌های فرد اعم از واگیر و غیرواگیر و اطلاعات آزمایش‌های پزشکی را اطلاعات شخصی محسوب کرده است. به این ترتیب، نتیجهٔ آزمایش کرونا، مبتلا بودن و نیز عمدهٔ مکان‌های حضور افراد، اطلاعات شخصی محسوب شده، طبق مادهٔ ۱۵ قانون، پردازش داده‌ها با هدف کنترل کرونا در حقوق ایران یا باید مبتنی بر رضایت و اقدام داوطلبانهٔ شهروندان باشد و یا اینکه این پردازش داده‌ها از سوی یک مؤسسهٔ عمومی و در چارچوب وظایف قانونی آن مؤسسه انجام شود؛ درحالی که اپلیکیشن‌های معرفی‌شده در ایران از سوی بخش خصوصی تهیه شده است.

نکتهٔ دیگر این است که خصوصی و شخصی بودن نتیجهٔ تست کرونا و یا وضعیت تزریق واکسن بر اساس شیوه‌نامهٔ یادشده، مستلزم این است که افشای آن بر اساس مجوز قانونی باشد. این مجوز می‌تواند در دو صورت مطرح شود: اول مصوبهٔ ستاد کرونا بر مبنای اختیار قانونی شورای عالی امنیت ملی، و دوم مجوز مادهٔ ۱۵ قانون انتشار و دسترسی آزاد به اطلاعات که طبق آن، این اطلاعات باید در اختیار یک نهاد عمومی و در حوزهٔ وظایف قانونی آن نهاد قرار گیرد. بهترین شیوه این بود که یک نهاد عمومی بر اساس مصوبهٔ ستاد کرونا مسئولیت پردازش داده‌ها را برعهده گرفته، به‌طور مشخص در این حوزه پاسخگو باشد.

به‌عنوان جمع‌بندی باید گفت در خصوص پردازش اطلاعات، اطلاعات مربوط به مبتلا بودن شهروندان به کرونا جزء اطلاعات شخصی بوده و دسترسی به آن- که برای عملکرد اپلیکیشن‌های

مقابله با کرونا ضروری است- جز با رضایت هر شهروند یا پردازش آن داده‌ها از سوی مؤسسهٔ عمومی و در چارچوب وظایف قانونی ممکن نیست. نکتهٔ دیگر نبود یک قانون جامع و نهاد کنترل‌کننده و مسئول در بحث پردازش داده‌ها است. در کنار این مسئله باید توجه داشت با وجود عدم استفاده از اپلیکیشن‌های بین‌المللی، نقش نهادهای عمومی در پردازش داده‌ها و نظارت بر آن بسیار کم‌رنگ بوده است.

## ۵. ارزیابی و آسیب‌شناسی چالش‌های حقوقی در بحث حفظ حریم خصوصی مرتبط با پردازش داده‌ها در کشورها

پس از شناسایی چالش‌های حقوقی مرتبط با حریم خصوصی شهروندان در حوزهٔ پردازش داده‌ها در دورهٔ همه‌گیری کرونا و سپس طرح اقدامات اتخاذشده از سوی دولت‌ها، در این قسمت باید به ارزیابی و تحلیل وضعیت‌های حقوقی ایجادشده در اثر تعارض حریم خصوصی و اقدامات دولت‌ها پرداخته شود و نقاط ضعف و قوت پاسخ‌های حقوقی به چالش‌های ایجادشده از منظر آسیب‌شناختی و کاربردی و با نگاهی تطبیقی مورد توجه قرار گیرد.

### ۵. ۱. مبنای تحدید حق شهروندان بر حریم خصوصی مرتبط با پردازش داده‌ها (اصل قانونی بودن پردازش داده‌ها)

گفته شد است که در هر چهار نظم حقوقی داده‌های مربوط به نتیجهٔ تست کرونا و ابتلای افراد به بیماری و نیز سایر داده‌های شخصی، مثل محل حضور افراد درصورتی که بی‌نام نبوده و قابلیت انتساب به اشخاص و شناسایی صاحبان آن وجود داشته باشد، مربوط به حریم خصوصی و در چارچوب حمایت از اطلاعات شخصی قرار می‌گیرد. پرسش مهم این است که دولت‌ها بر چه مبنایی می‌توانند در شرایط اضطراری مثل همه‌گیری کرونا، اقداماتی انجام دهند که حق شهروندان در خصوص اطلاعات شخصی آنان را خدشه‌دار کند. در بخش قبلی، مبانی حقوقی و مقررات مورد استناد دولت‌ها در خصوص تحدید حق بر حریم خصوصی شهروندان بررسی شد و در اینجا به شکل مختصر سه رویکردی که در این خصوص دولت‌ها و نظام‌های حقوقی داشته‌اند، مورد ارزیابی قرار می‌گیرد.

#### ۵. ۱. ۱. رضایت شهروندان

در صورت رضایت شهروندان، پردازش داده‌های آنان از نظر حقوقی با مانعی مواجه نخواهد شد؛ چراکه هدف قوانین حریم خصوصی حمایت از اشخاص و آزادی و حقوق آنان است، آن‌چنان که در عمدهٔ تعاریف مرتبط با حق بر حریم خصوصی نیز بر خواست و ارادهٔ شهروندان در خصوصی بودن امور شخصی

زندگی آنان تأکید شده است. در قوانین نیز برای مثال، در متن مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا در بند «a» از شمارهٔ نخست مادهٔ ۶، یکی از موارد قانونی بودن پردازش داده‌های شهروندان رضایت آنان معرفی شده است. بند نخست از مادهٔ ۱۰۳۵ قانون حفاظت از اطلاعات شخصی چین نیز به مسئلهٔ رضایت به‌عنوان یکی از موارد تجویز پردازش اطلاعات شخصی اشاره کرده است. در حقوق ایران نیز به همین ترتیب در مادهٔ ۱۵ قانون دسترسی آزاد به اطلاعات، رضایت فرد در زمینهٔ دسترسی به اطلاعات شخصی مورد توجه قرار گرفته است.

با این حال، نکتهٔ بسیار مهم تفاوت رویکرد نظام حقوقی امریکا در این زمینه است. اگرچه در کشورها رضایت شهروندان مجوز قانونی بودن پردازش داده‌ها محسوب می‌شود، اما شرایط بحرانی کرونا و احتمال عدم همکاری برخی از شهروندان موجب شده است تا دولت‌ها به مبانی و مجوزهای دیگری برای توجیه قانونی تحدید حق بر حریم خصوصی شهروندان متوسل شوند. اما در ایالات متحده آن‌چنان که در بخش قبلی بحث شد، تنها مجوز نهادهای دولتی برای دسترسی به اطلاعات شهروندان و قانونی بودن پردازش داده‌ها، رضایت شهروندان است. این وضعیت دارای جنبه‌های مثبت و منفی است. جنبهٔ مثبت این رویکرد، محدود کردن دایرهٔ اختیارات دولت و حمایت حداکثری از حریم خصوصی و اطلاعات شخصی شهروندان است و جنبهٔ منفی آن، اولویت دادن به حقوق فردی نسبت به حقوق جمعی و منفعت عمومی است که می‌تواند مانعی در راه مقابلهٔ دولت با شرایط خاص بیماری کرونا باشد. به‌نظر می‌رسد این رویکرد حقوق امریکا مورد اقبال حقوق‌دانان و نظام‌های سیاسی و قضایی نبوده، بیشتر از آنکه مبتنی بر تکیه بر حقوق فردی و لیبرال شهروندان در بحث حریم خصوصی باشد، بازتاب‌دهندهٔ نبود رویکرد جامع و کل‌نگر در حقوق امریکا در بحث حریم خصوصی است که موجب ابهام در مسئولیت‌ها و حقوق مرتبط با حریم خصوصی و دامنهٔ اختیارات دولت فدرال در اقدامات مقابله‌ای با کرونا و نسبت آن با حریم خصوصی شده است.

### ۵. ۱. ۲. نفع عمومی و جمعی

در کنار عنصر رضایت فردی، تأمین منافع عمومی به‌خصوص در بحث حفظ و تأمین سلامت عمومی شهروندان ازجمله مبانی مهم در قانونی بودن پردازش داده‌ها از سوی دولت‌ها در شرایط اضطراری بوده است. در حقوق فرانسه با تکیه بر استثنای مربوط به منافع عمومی مندرج در مقررات اتحادیهٔ اروپا (بند «e» از شمارهٔ نخست مادهٔ ۶ مقررات عمومی حفاظت از داده‌ها) بدون نیاز به رضایت افراد، دولت می تواند این اطلاعات را در اختیار اپلیکیشن‌ها قرار دهد. در حقوق چین نیز استثنای مربوط به نفع عمومی در مقررات مربوط به حریم خصوصی در قانون مدنی وارد شده و بند ۳ مادهٔ ۱۰۳۶ همین قانون، پردازش

معقول داده‌ها با هدف تأمین منافع عمومی را از موانع مسئولیت دانسته است. تردیدی وجود ندارد که حفظ سلامت عمومی از سوی دولت‌ها می‌تواند در حد ضرورت مجوز مشروعی برای پردازش داده‌های شهروندان باشد؛ آن‌چنان که در متنی که از جانب کمیتهٔ حفاظت از داده‌های اتحادیهٔ اروپا منتشر شد نیز تأکید گردیده است که مقابله با بیماری کرونا یکی از اهداف مشترک بین ملت‌ها و دولت‌ها بوده و مقررات حمایتی اتحادیهٔ اروپا از حریم خصوصی به هیچ عنوان مانع فعالیت‌های دولت‌ها در این زمینه نمی‌شود. بر این اساس، نمی‌توان مجوز دولت در پردازش داده‌ها را صرفاً به فرض رضایت شهروندان محدود کرد و حتی در فرض عدم رضایت آنان، ضرورت‌های مقابله با کرونا که تأمین‌کنندهٔ نفع عمومی شهروندان باشد، یک مبنای حقوقی مشروع برای مجاز دانستن پردازش داده‌های شهروندان در چارچوب های حقوقی است.

### ۵. ۱. ۳. وظیفهٔ دولت در تأمین سلامت عمومی

این مبنا به‌نوعی مکمل مبنای قبلی است و بر اساس آن درصورتی که دولت یا نهاد دولتی وظیفهٔ قانونی خاصی را برعهده داشته باشد که انجام آن مستلزم پردازش داده‌های شهروندان باشد، این اختیار برای دولت وجود خواهد داشت که در حد لازم برای انجام وظیفهٔ خود (که معمولاً با منافع عمومی مرتبط است) به پردازش داده‌ها مبادرت ورزد. برای نمونه، می‌توان به بند «c» از شمارهٔ نخست مادهٔ ۶ مقررات حفاظت از دادهٔ اتحادیهٔ اروپا اشاره کرد. همچنین بر مبنای مادهٔ ۲۱ «شیوه‌نامهٔ تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی مصوب ۱۳۹۸»، ضرورت انجام وظیفه از سوی یک نهاد یا مؤسسهٔ عمومی می‌تواند مبنایی برای امکان دسترسی نهاد یادشده به اطلاعات شخصی باشد. به این ترتیب، دولت‌ها که موظف به تأمین سلامت عمومی هستند در شرایط بحرانی و اضطراری می‌توانند نسبت به پردازش داده‌های شهروندان اقدام کنند.

به‌طور کلی می‌توان گفت در حقوق فرانسه (و اتحادیهٔ اروپا)، چین و ایران، دولت‌ها می‌توانند در چارچوبی خارج از رضایت افراد بر مبنای تأمین منافع عمومی و حفظ سلامت جمعی برای مقابله با بیماری کرونا نسبت به پردازش داده‌ها اقدام کنند؛ درحالی که در ایالات متحده این امکان صرفاً در فرض رضایت شهروندان وجود دارد. نباید ازیاد برد که شرایط اضطراری اقتضای تصمیمات اضطراری را دارد و یک نظام حقوقی پیشرو، در کنار تأکید بر اصول و مبانی عام حمایت از حقوق شهروندان، باید از انعطاف‌پذیری لازم برای پاسخگویی به وضعیت‌های اضطراری برخوردار بوده، ساختار حقوقی نیز همانند سایر ساختارهای اجتماعی، درمانی و... در مسیر تلاش گستردهٔ دولت‌ها برای کنترل بیماری از هماهنگی و انعطاف‌پذیری لازم برخوردار باشد.

### ۵. ۲. رعایت اصول تضمین‌کنندهٔ حقوق شهروندان در پردازش داده‌ها

اگرچه شرایط اضطراری کرونا بستر حقوقی مشروعی برای ورود دولت‌ها به عرصهٔ حریم خصوصی شهروندان و اطلاعات شخصی آنان فراهم کرده است، اما مداخلهٔ دولت‌ها باید در چارچوب اصول حقوقی و در حد ضرورت و با رعایت ملاحظات مربوط به حقوق شهروندان باشد. در واقع، چالش بسیار مهم در این زمینه، تعارض و تزاحم بین حقوق شهروندی و منافع عمومی در مقابله با بیماری کروناست که باید به‌گونه‌ای مدیریت شود که بتوان دو هدف مورد تعارض را تا حد امکان باهم جمع کرد؛ به این معنا که هم پردازش داده‌ها از سوی دولت‌ها صورت پذیرد و هم نقض حقوق شهروندی مرتبط با حریم خصوصی شهروندان به‌حداقل رسیده، در حد امکان مانع از سوءاستفادهٔ دولت‌ها از مجوزهای اضطراری ناظر بر نقض حریم خصوصی در مقابله با کرونا شود. در ادامه بخشی از اصول و سازوکارهای تضمین‌کننده که مانع سوءاستفادهٔ دولت‌ها از پردازش داده‌ها می‌شود، مورد اشاره قرار خواهد گرفت.

ایجاد این تناسب و اعتدال مورد توجه کشورها نیز بوده است. برای مثال، کمیسیون ملی فناوری اطلاعات و آزادی‌ها که نهاد ناظر در زمینهٔ پردازش داده‌ها در فرانسه محسوب می‌شود در خصوص پردازش داده‌ها در دورهٔ کرونا از سوی دولت بر چند نکته تأکید کرده است که رعایت آن از سوی دولت، تضمین‌کنندهٔ حریم خصوصی شهروندان خواهد بود.

اولین نکته، لزوم توجه به مسئولیت‌پذیری در پردازش داده‌ها است. کمیسیون تأکید کرده است که مسئول اصلی رعایت مقررات حریم خصوصی باید یکی از نهادهای دولتی حوزهٔ بهداشت و درمان باشد. نکتهٔ دوم، لزوم انجام ارزیابی اثر پردازش داده‌ها بر موضوع حفاظت از داده‌ها است. این مسئله که در مادهٔ ۳۵ مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا مورد تأکید قرار گرفته، به این معناست که وقتی پردازش داده‌ها متضمن یک ریسک بسیار بالا و مرتبط با داده‌های حساس باشد، نهاد کنترل‌کنندهٔ ناظر بر حفاظت از داده‌ها باید پیش از شروع پردازش داده‌ها، آثار احتمالی و مخاطرات پردازش داده‌ها بر حریم خصوصی را با هدف به‌حداقل رساندن این مخاطرات، مورد بررسی قرار دهد. به عبارت دیگر، باید نقشهٔ راه مشخصی برای دولت‌ها در خصوص پردازش داده‌ها فراهم شود و وجود مخاطراتی که ناشی از امکان نقض حقوق شهروندان است، مورد توجه قرار گیرد.

نکتهٔ سوم، لزوم دقت و صحت داده‌ها و هشدارهایی است که بر اساس داده‌ها ارسال می‌شود. نکتهٔ چهارمِ مورد تأکید در متن کمیسیون، امنیت داده‌ها است. کمیسیون بر شیوهٔ رمزگذاری داده‌ها با هدف تأمین امنیت داده‌ها تأکید ویژه دارد. نکتهٔ پایانی نیز توجه به حق هر فرد در خصوص اطلاعات مربوط به خود آن فرد است که در چارچوب مواد ۱۲ تا ۱۴ مقررات عمومی مورد تأکید قرار گرفته و گفته شده است که کنترل افراد موضوع داده‌ها بر داده‌های خود یک تضمین اساسی برای تأمین اعتماد عمومی نسبت به اقدامات مقابله‌ای با کروناست.

نمونهٔ دیگری از این‌چنین اصول تضمین‌کننده‌ای را می‌توان در متن دستورالعمل‌های حفاظت از حریم خصوصی و گردش فرامرزی اطلاعات شخصی که از سوی شورای سازمان همکاری اقتصادی و توسعهٔ منتشر شده است، مشاهده کرد و با مبنا قرار دادن آن، نقطهٔ تعادلی بین حقوق شهروندی و مبارزه دولت‌ها با بیماری کرونا ایجاد کرد. در این متن تأکید شده که در مواردی که دولت‌ها مجاز به پردازش داده‌ها هستند، رعایت یک سری اصول ضروری است.

اولین اصل، محدودیت جمع‌آوری است که طبق آن باید محدودیت‌هایی برای جمع‌آوری داده‌ها تعیین شود و روش‌های جمع‌آوری داده‌ها نیز باید قانونی و منصفانه باشد. اصل دوم، مشخص کردن هدف است و بر اساس آن، داده‌های جمع‌آوری‌شده باید دقیقاً در راستای هدف تعیین‌شده باشند. برای مثال، در شرایط کرونایی صرفاً داده‌هایی که در مقابله با بیماری مؤثرند باید جمع آوری شوند و دولت‌ها نباید مجاز باشند به بهانهٔ مقابله با بیماری به پردازش داده‌ها در حوزه‌های غیرمرتبط اقدام کنند. اصل سوم، استفادهٔ محدود از داده‌هاست؛ به این معنا که داده‌های گردآوری‌شده باید صرفاً برای هدف تعیین شده مورد استفاده قرار گیرند و هر نوع استفادهٔ غیرقانونی یا غیرمرتبط با هدف مقابله با بیماری ممنوع است. اصل چهارم، ناظر بر تضمین‌های امنیتی است که بر حفاظت از داده‌ها در مراکز و نهادهای پردازش داده‌ها تأکید می‌کند که از هرگونه افشا یا استفادهٔ غیرمجاز از داده‌ها باید جلوگیری شود. اصل مهم دیگر، شفافیت است. طبق این اصل نهادهای دولتی باید نسبت به قوانین، رویکردها و سیاست‌های اتخاذشده در خصوص پردازش داده‌های شهروندان به شیوهٔ شفاف اطلاع‌رسانی کرده، شهروندان را از حدود و معیار ها و شیوه‌های پردازش داده‌ها آگاه کنند. این آگاهی می‌تواند زمینه‌ساز اعتماد شهروندان در همکاری با دولت‌ها باشد و در نهایت، اصل بسیار مهمِ پاسخگویی است که باید مورد توجه قرار گیرد و به معنای مسئول دانستن و اعمال نظارت بر نهادهای مسئول پردازش داده‌ها و وجود الزامات قانونی و ضمانت اجراها برای تضمین حفظ و عدم سوءاستفاده از اطلاعات شخصی شهروندان است.

برای پاسخ دقیق به این پرسش که اصول حقوقی یادشده تا چه حد مورد توجه کشورها بوده، نیاز به گذشت زمان است تا مشخص شود دولت‌ها با انبوه اطلاعات پردازش‌شده و ایجاد سازوکارهای مرتبط به چه اقداماتی دست خواهند زد؛ اما به‌اجمال می‌توان گفت در فرانسه تا حد زیادی این اصول مورد توجه قانون‌گذار و نیز نهاد ناظر بر پردازش داده‌ها قرار گرفته و پاسخ جامع و متمرکز نظام حقوقی فرانسه به ضرورت پردازش داده‌ها در دورهٔ کرونا و تعیین خطوط قرمز مرتبط با حقوق شهروندی در این زمینه می‌تواند الگوی قابل قبولی برای سایر نظام‌های حقوقی باشد. نکتهٔ قابل توجه این است که رعایت اصول تضمین‌کنندهٔ حقوق شهروندان در مورد حریم خصوصی که متضمن تعهدات مهمی برای نهاد مسئول پردازش داده‌هاست، نیازمند وجود مقررات مشخص و نیز اعمال نظارت‌های جدی است. از این رو، لازم است پردازش داده‌ها از سوی نهادهای دولتی و عمومی انجام شود تا امکان اعمال نظارت‌ها به‌درستی وجود داشته باشد.

### ۵. ۳. لزوم وجود قوانین جامع و کل‌نگر

وجود قوانین مناسبی که با نگاه عام و رویکرد کل‌نگر، چارچوب‌های حمایتی حریم خصوصی و تکالیف و حقوق نهادهای کنترل‌گر، تنظیم‌گر و پردازشگر داده‌ها را تعیین کنند و حمایت‌ها و اختیارات را در یک چارچوب حقوقی منعطف و مبتنی بر حقوق شهروندی تأمین نمایند، از ملزومات عدم تعدی حاکمیت‌ها به حریم خصوصی شهروندان در عین انجام اقدامات ضروری و نیز مدیریت بحران‌ها و چالش‌های حقوقی احتمالی است. چارچوب حقوقی حمایت از حریم خصوصی در دورهٔ کرونا در فرانسه که با وِیژگی‌های متمرکز بودن، شفافیت و قانون‌مداری همراه بوده، نشان‌دهندهٔ اهمیت وجود قوانین مادر و جامعی است که در آن، مفاهیم، حمایت‌ها، اختیارات و ضمانت اجراها در حوزهٔ حریم خصوصی و پردازش داده‌ها تعیین شود و در شرایط بحرانی که نیازمند اقدامات ویژه است در دسترس باشد. یکی از دلایل موفقیت نسبی چین در پاسخ یکپارچه به کرونا نیز انسجام نظام حقوقی حریم خصوصی بر اساس قوانین جامع در این زمینه بوده است. در مقابل، پراکندگی و ابهام‌های موجود در امریکا و ایران در خصوص دسترسی به اطلاعات و اختیارات قانونی در این زمینه ناشی از فقدان قوانین جامع حریم خصوصی است. در کنگرهٔ امریکا طرح‌هایی برای رفع این نقص ارائه شده است که ازجمله می‌توان به طرح «قانون حریم خصوصی اعلان هشدار درمعرض ابتلا قرار گرفتن» و طرح «قانون حریم خصوصی وضعیت اضطراری سلامت عمومی» اشاره کرد که هنوز به نتیجه نرسیده است، اما خلأ تقنین در حقوق امریکا و ضرورت وجود قوانین جامع در این زمینه را آشکار می‌کند (Yang, et al. 2020: 11). در همین راستا، لزوم تصویب قوانین جامع مرتبط با حریم خصوصی و اطلاعات شخصی در حقوق ایران نیز کاملاً ملموس است و یکی از عوامل مهمِ عدم شفافیت سازوکار حقوقی ایران در مواجهه با کرونا و نسبت آن با نقض حریم خصوصی شهروندان، نبود چنین قوانینی است.

### ۵. ۴. لزوم وجود نهاد ناظر بر پردازش داده‌ها

هنگامی که دولت‌ها بر اساس مجوزهای خاص قانونی یا استثناها اقداماتی را انجام می‌دهند که می‌تواند به نقض حریم خصوصی منجر شود، لازم است یک نهاد دولتی به‌طور مشخص مسئولیت نظارت بر پردازش داده‌ها و تضمین رعایت حریم خصوصی شهروندان را برعهده داشته باشد. در متن کمیسیون فناوری اطلاعات فرانسه تأکید شده است که این وظیفه باید به‌عهده وزارت بهداشت باشد. این درحالی است که اپلیکیشن‌های ساخته‌شده در ایران، نه‌تنها تحت نظارت نهادهای عمومی نبودند، بلکه تضمین حریم خصوصی نیز تعهدی خصوصی بود که به سازندگان برنامه‌ها مربوط می‌شد؛ درحالی که نهادهای عمومی در این حوزه مسئولیت مهم‌تری در حمایت از حقوق حریم خصوصی شهروندان دارند و باید در

قالب یک تعهد مثبت، نظارت و مداخله و نیز پاسخگویی و مسئولیت‌پذیری در زمینهٔ تضمین حق حریم خصوصی شهروندان را برعهده داشته باشند. همین مسئله در امریکا نیز قابل مشاهده است. در فرانسه به علت وجود کمیسیون ناظر، هم نظارت بیشتری بر تضمین حریم خصوصی وجود داشته و هم اقدامات صورت‌گرفته متمرکزتر بوده است. البته در ایران نیز به علت تمرکز تصمیم‌گیری در خصوص کرونا در یک ستاد، پراکندگی کمتری وجود داشته است، اما خلأ یک نهاد مسئول و پاسخگو در زمینهٔ اقدامات انجام‌شده که ممکن بود ناقض حریم خصوصی شهروندان باشد، حس می‌شد.

### ۵. ۵. مسئلهٔ حاکمیت ملی داده‌ها

توجه به حاکمیت ملی در بحث داده‌ها و تکیه بر نهادهای دولتی یا شرکت‌های پاسخگو به دولت موجب بیشتر شدن اعتماد شهروندان و افزایش نظارت دولت‌ها با هدف تضمین حفظ حریم خصوصی می‌شود. در بحث توجه به حاکمیت ملی بر داده‌ها، فرانسه و ایران هر دو به این مفهوم توجه داشته و پردازش داده ها در ذیل حاکمیت ملی و در داخل کشور انجام شده است. به این منظور، دولت فرانسه ابتدا وارد مذاکره با شرکت‌های گوگل و اپل شد، اما به علت تأکید فرانسه بر تکیه بر فناوری‌های بومی و تحت اقتدار حاکمیت دولت و عدم همکاری فناوری‌های بزرگ با دولت در این زمینه، فرانسه به سمت ساخت برنامهٔ رهگیری بومی رفت. مسئلهٔ اصلی ناظر بر این امر بوده که نباید جمع‌آوری و پردازش داده‌های شهروندان یک کشور و کم و کیف عملکرد برنامه‌های نصب‌شده، از سوی شرکت‌های فناوری چندملیتی غیردموکراتیکی که مقر اصلی آنان عمدتاً امریکا است، انجام و تعیین شود. سلطه و اقتدار شرکت‌های فناوری در این زمینه می‌تواند به نقض حاکمیت دولت‌ها بر داده‌های شهروندان منجر گردد. بی‌نتیجه بودن مذاکرات فرانسه با شرکت‌های فناوری و عدم همکاری آنان نشانگر سلطهٔ هژمونیک این فناوری‌ها بر داده‌ها و دستِ برتر داشتن به‌واسطه سلطه بر فناوری است (Yang, et al. 2020: 8). در چین نیز مسئلهٔ حاکمیت ملی داده‌ها در بالاترین سطح مورد توجه قرار گرفته است؛ درحالی که در امریکا شرکت های خصوصی‌ای که به دولت پاسخگو نبوده‌اند متولی پردازش داده‌ها شده‌اند.

باید توجه داشت که در ایران طبق مادهٔ ۱۵ قانون انتشار اطلاعات، پردازش داده‌های شخصی صرفاً از سوی مؤسسات عمومی باید انجام شود و حتی بخش خصوصی نمی‌تواند عهده‌دار این امر شود و این موضوع تأکید هرچه بیشتر بر حاکمیت بر داده‌ها را آشکار می‌کند. با این حال، پردازش اطلاعات از سوی شرکت‌های خصوصی بدون وجود نظارت مشخص از سوی دولت‌ها در ایران نگران‌کننده است و بهتر است طبق مادهٔ ۱۵ قانون انتشار اطلاعات، مؤسسات عمومی عهده‌دار این امر باشند.

### ۵. ۶. اهمیت توجه به ساختارها و سازوکارهای حقوقی

تجربهٔ حقوقی فرانسه در دورهٔ کرونا نشان داد حتی در شرایط بحرانی نیز می‌توان بسیاری از اقدامات خاص را بر اساس فرایندهای قانونی جلو برد. فرانسه از معدود کشورهایی بود که راه‌اندازی اپلیکیشن‌های رهگیری را منوط به تصویب پارلمان کرد. چنین رویکردی می‌تواند شفافیت و قانون‌مداری را افزایش داده، اعتماد شهروندان نیز جلب شود. در مقابل در ایران و امریکا، عمده اقدامات انجام‌شده از سوی دولت ها، ایالت‌ها و یا نهادهای خاص صورت پذیرفته، پارلمان و ساختار مردم‌سالار به علت ضرورت‌های خاص مقابله با کرونا کنار گذاشته شده‌اند. در ایران دولت می‌توانست با استناد به اصل ۷۹ قانون اساسی محدودیت‌ها بر حقوق و آزادی‌های شهروندان را به‌طور موقت از طریق مصوبهٔ مجلس اعمال کند؛ البته بدیهی است که در ماه‌های آغازین کرونا، عمدهٔ دولت‌ها ناچار به اتخاذ تصمیمات فوری بوده‌اند.

## ۶. نتیجه‌گیری

حریم خصوصی از مفاهیم بنیادین حقوق شهروندی و بشری بوده است که صرف‌نظر از تعریف‌های متفاوت، بر مفهوم عدم مداخله در حوزه‌های خصوصی زندگی و نیز داده‌های شخصی دلالت می‌کند. حمایت حقوقی از حریم خصوصی در فرانسه، امریکا، چین و ایران در سطوح مختلف پذیرفته شده است؛ با این تفاوت که در فرانسه حریم خصوصی به‌طور صریح در قانون اساسی تصریح شده و حمایت حقوقی از حریم خصوصی متمرکز و کل‌نگر است. در چین نیز تحول به سمت نگاه کل‌نگر و شناسایی حق عام حریم خصوصی بوده است. در مقابل در ایران و امریکا، قوانین مرتبط با حریم خصوصی، غیرمتمرکز و جزءنگر بوده و در قوانین اساسی دو کشور نیز تصریحی به مفهوم حریم خصوصی نشده است. با این حال، حمایت از حریم خصوصی از مبانی فقهی مستحکمی برخوردار است که می‌تواند مبنای قابل قبولی برای افزایش توجه قانون‌گذار به این حوزه باشد.

مقابلهٔ دولت‌ها با کرونا در قالب پردازش داده‌های سلامت و موقعیت مکانی و ارتباطات شهروندان با هدف جلوگیری از شیوع کرونا، ازجمله مهم‌ترین عرصه‌هایی بوده که موجب تعارض بین اقدامات دولت‌ها و حق بر حریم خصوصی شده است. اگرچه پردازش داده‌ها و تحدید حق بر حریم خصوصی شهروندان فرصت‌هایی را از منظر مقابله با کرونا برای دولت‌ها به‌وجود آورده، اما تهدیدهای جدی را در خصوص نقض بلاوجه حریم خصوصی و سوءاستفاده از داده‌های شخصی نیز ایجاد کرده است. چالش‌های حقوقی به‌وجود آمده در نظام‌های حقوقی در این خصوص، طرح دعاوی متعدد (به‌خصوص در ایالات متحده)، وضع قوانین جدید، و صدور آیین‌نامه‌ها و دستورالعمل‌های متعدد دربارهٔ ابعاد حقوقی مرتبط با حریم خصوصی، بازتاب‌دهندهٔ قابلیت‌های هر نظام حقوقی در مدیریت تعارض ایجادشده بوده است. جمع بین

پردازش داده‌های شهروندان و احترام حداکثری به حق بر حریم خصوصی، نیازمند وجود ظرفیت‌ها و سازوکارهایی در حقوق ملی است. ازجمله موارد بسیار مهم در این زمینه، توجه به اصول مرتبط با حقوق شهروندی در زمینهٔ پردازش داده‌هاست. مجوز قانونی دولت‌ها در پردازش داده‌ها در شرایط اضطراری باید متناسب با هدف تعیین شود و پردازش داده‌ها در حد ضرورت باشد و اصول مرتبط با شفافیت و مسئولیت پذیری مورد توجه قرار گیرد. تأمین شفافیت و مسئولیت‌پذیری در این زمینه مستلزم وجود قوانین و دستورالعمل‌های جامع و شفاف در خصوص پردازش داده‌هاست که بر مبنای آن، حقوق و تکالیف شهروندان و نهادهای مربوطه به‌طور کامل مشخص باشد. همچنین ضروری است تا نهادهای دولتی مسئول نظارت بر پردازش داده‌ها باشند. در این زمینه می‌توان به سازوکارهای حقوق فرانسه در دورهٔ کرونا اشاره کرد که یک پاسخ متمرکز و شفاف و قانون‌مدار را در باب حریم خصوصی و پردازش داده‌ها ارائه داده است. همچنین موفقیت چین در اعمال سیاست‌های محدودکنندهٔ حریم خصوصی و همراهی شهروندان با این سیاست‌ها تاحدی معلول انسجام نظام حقوقی چین در تعیین پاسخ مناسب به تعارض بین حریم خصوصی و اقدامات محدودکننده است. در مقابل، متمرکز نبودن راه‌حل‌های حقوقی در ایران و امریکا، ابهام و چالش‌های حقوقی را جدی‌تر کرده است. در این زمینه، ضروری است چند نکته مورد توجه قرار گیرد. اولین نکته، لزوم وضع قوانین جامع دربارهٔ حریم خصوصی و حفاظت از داده‌هاست که تعیین‌کنندهٔ حقوق و وظایف نهادهای پردازش‌کنندهٔ داده‌ها و نیز تضمین‌های حمایتی از شهروندان خواهد بود. نکتهٔ دوم، لزوم تعیین نهادهای ناظر بر امر پردازش داده‌ها و نیز نقش فعال نهادهای دولتی در پردازش داده‌هاست که درواقع عنصر پاسخگویی و مسئولیت‌پذیری را تضمین می‌کند؛ آن‌چنان که در چین و فرانسه نیز نهادهای دولتی وظایف اصلی در خصوص پردازش داده‌ها و نیز پاسخگویی در این زمینه را برعهده داشتند. درصورتی که در ایران نیز پردازش داده‌ها به‌طور کامل برعهدهٔ وزارت بهداشت قرار می‌گرفت و نظارت در این زمینه نیز به همین وزارت‌خانه محول می‌شد، وضعیت از نظر حقوقی شفاف‌تر بود و پاسخگویی در وضعیت بهتری قرار می‌گرفت.

## منابع

### الف) فارسی


۱. انصاری، باقر و عطار، شیما (۱۴۰۱). حمایت از داده‌ها در چین؛ مطالعهٔ تطبیقی با رویکرد حمایت از داده‌ها در امریکا و اتحادیهٔ اروپا. مطالعات حقوق تطبیقی، ۱۳(۱)، ۹۱-۱۱۳.

۲. انصاری، باقر (۱۳۹۰). حقوق حریم خصوصی. تهران: سمت.

۳. نجارزاده هنجنی، مجید (۱۳۹۹). تحلیل حقوقی وضع محدودیت‌های ناشی از همه‌گیری کرونا در حقوق ایران؛ در جستجوی ادارهٔ صلاحیت‌دار. فصلنامهٔ حقوق اداری، سال هفتم، (۲۳)، ۲۴۵-۲۲۵.

۴. واعظی، سید مجتبی و علی‌پور، سید علی (۱۳۸۹). بررسی موازین حقوق حاکم بر حریم خصوصی و حمایت از آن در حقوق ایران. مجلهٔ حقوق خصوصی، (۱۷)، ۱۳۳-۱۶۳.

## ب) عربی

۱. ایروانی، محمدباقر (۱۴۲۸). دروس تمهیدیهٔ فی تفسیر آیات الأحکام. ج ۲، قم: دار الفقه للطباعهٔ و النشر .
۲. خمینی، روح‌الله (۱۳۶۸). تحریر الوسیله. ج ۱، تهران: مؤسسهٔ تنظیم و نشر آثار امام خمینی.
۳. شهید ثانی، زین‌الدین بن علی (۱۳۹۰). کشف الریبه. قم: دار المرتضوی.
۴. طبرسی، فضل‌بن حسن (۱۴۱۵) مجمع البیان. ج ۱، بیروت: مؤسسهٔ الأعلمی للمطبوعات.
۵. طوسی، محمدبن حسن (۱۴۱۳). التبیان فی تفسیر القرآن. ج ۹، قم: مؤسسهٔ النشرالاسلامی.
۶. فخر رازی، محمدبن عمر (۱۴۲۰). مفاتیح الغیب. ج ۲۸، بیروت: دار إحیاء التراث العربی.
۷. مشکینی، علی (۱۴۳۴). مصطلحات الفقه. ج ۱، قم: مؤسسهٔ دارالحدیث العلمیه والثقافیه، مرکز للطباعه والنشر
۸. مظفر، محمدحسن (۱۳۸۰). دلائل الصدق فی نهج الحق. ج ۷، دمشق: مؤسسهٔ آل البیت.
۹. مکارم شیرازی، ناصر (۱۴۲۸). الاخلاق فی القرآن. ج ۳، قم: مدرسهٔ امام علی.
۱۰. نجفی، محمدحسن (۱۳۶۲). جواهر الکلام. ج ۹، بیروت: دار إحیاء التراث العربی.

## ج) لاتین

1. Bandelier, Silvia; Dressel, Charlotte; Lanier, Clément; Steger-Kicinski, Arthur (2022). Retour sur le passe vaccinal: libre disposition de son corps et consentement aux soins, La Revue des droits de l’homme, May 2022.
2. Beverley-Smith, Huw; Ohly, Ansgar; Lucas-Schloetter, Agne (2005). Privacy, Property and Personality; Civil Law Perspectives on Commercial Appropriation, New York: Cambridge university press
3. Black, Campbell M. A. (1968), Black’s law dictionary, West publishing co.
4. Bradford, Laura; Aboy, Mateo; Liddell, Kathleen (2020). COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes, Journal of Law and the Biosciences, Paper No. 23/2020
5. Cole, Jared P. & Swendiman, Kathleen S. (2014). Mandatory Vaccinations: Precedent and Current Laws, Washington: Congressional Research Service
6. Cornu, Gérard (2018). Vocabulaire juridique, Paris: Presses Universitaires de France
7. Cortez, Elif Kiesow (2021). Data Protection Around the World; Privacy Laws in Action, The Hague: T.M.C. ASSER PRESS, 2021
8. Cudd, Ann E. & Navin, Mark C. (2018). Core Concepts and Contemporary Issues in Privacy, Springer International Publishing
9. Duan, W. & Qin, T. (2022). The Impact of China’s Legal System on Public Health and Quality of Life during the COVID-19 Pandemic: An Empirical Study, Int. J. Environ. Res. Public Health, 19
10. Guide sur l’article 8 de la Convention européenne des droits de l’homme; Droit au

respect de la vie privée et familiale, du domicile et de la correspondence, (2022). Conseil de l'Europe/Cour européenne des droits de l'homme,
11. Guinchard, Serge & Debard, Thierry, (2018). Lexique des termes juridiques 2017-2018, Paris: Dalloz
12. Jingchun, Cao (2005), Protecting the Right to Privacy in China, Victoria University of Wellington Law Review 36(3)
13. Kostka, Genia & Habich-Sobiegalla, Sabrina (2022). In times of crisis: Public perceptions toward COVID-19 contact tracing apps in China, Germany, and the United States. New Media & Society
14. Liu, Jun & Zhao, Hui (2021). Privacy lost: Appropriating surveillance technology in China's fight against COVID-19, Business Horizons, Vol. 64, Issue 6
15. Martin, E. A., (1997). Oxford dictionary of law, New York: Oxford University Press
16. Mbongo, Pascal (2012). The French Privacy Law, The Right to Privacy in the Light of Media Convergence, Germany: de Gruyter
17. Mitchell, Mann; Mitchell, Peta; Foth, Marcus (2022). Between surveillance and technological solutionism: A critique of privacy-preserving apps for COVID-19 contact tracing, New Media and Society
18. Nass, SJ; Levit, LA; Gostin, LO (2009). Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research, Washington: National Academies Press
19. Peikoff, Amy L. (2008). Beyond Reductionism: Reconsidering the Right to Privacy, NYU Journal of Law and Liberty, Vol. 3, No. 1
20. Pernot-Leplay, Emmanuel (2020), China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? 8 PENN. ST. J.L. & INT'L AFF. 49
21. Rigaux, François (1992). La vie privée: Une liberté parmi les autres, Bruxelles: Larcier
22. Scassa, Teresa; Millar, Jason; Bronson, Kelly (2020). Privacy, Ethics, and Contact-tracing Apps, Vulnerable: The Law and Policy of COVID-19, University of Ottawa Press
23. Simko, Lucy; Chang, Jack; Jiang, Maggie; Calo, Ryan; Roesner, Franziska; Tadayoshi Kohno. (2022). COVID-19 Contact Tracing and Privacy: A Longitudinal Study of Public Opinion, Digital Threats, 3, Article 25
24. Vitalis, André (2009). Informatique et libertés: une histoire de trente ans, Hermès, La Revue 2009/1 (n° 53), pages 137 à 143
25. Wang, Limin & Yang, Lixin (eds) (1997), The Law of the Rights of The Person, Beijing: The Press of Laws
26. Warren, Samuel D. & Brandeis, Louis D., (1890). The Right to Privacy, Harvard Law Review, Vol. 4, No. 5., pp. 193-220.
27. Wiederkehr, Georges (2019). Code civil annoté, Paris: Dalloz
28. Wu, J.; Wang, J.; Nicholas, S.; Maitland, E.; Fan, Q. (2020). Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations, Journal of medical Internet research, 22(10)
29. Yue Yang; Baik, Jeeyun; Ahn, Soyun; Jang, Eugene (2020). Tracing Digital Contact Tracing: Surveillance Technology and Privacy Rights During COVID-19 in China, South Korea, and the United States, SSRN Electronic Journal