فصلنامهٔ علمی دیدگاه‌های حقوق قضائی
مقالهٔ پژوهشی، دورهٔ ۲۷، شمارهٔ ۹۷، تابستان ۱۴۰۱، صفحات ۱۴۵ تا ۱۷۴
تاریخ دریافت: ۱۳۹۹/۰۹/۲۲ - تاریخ پذیرش: ۱۴۰۱/۰۶/۱۲

حفاظت از داده‌ها در بحران همه‌گیری ویروس کووید-۱۹؛ مطالعه تطبیقی اتحادیه اروپا و جمهوری اسلامی ایران

| **سیدمحمدمهدی غمامی** | استادیار گروه حقوق عمومی، دانشکده معارف اسلامی و حقوق، دانشگاه امام صادق (ع)، تهران، ایران
| **سجاد خلیلی‌نژاد** * | دانشجوی دکتری حقوق عمومی، دانشکده معارف اسلامی و حقوق، دانشگاه امام صادق (ع)، تهران، ایران

چکیده

در مواجهه با بحران همه‌گیری کووید-۱۹، روابط اجتماعی مختلف با سرعتی مضاعف بر بستر فضای مجازی منتقل می‌شود. از طرفی یکی از راه‌کارهای مهم مبارزه با همه‌گیری کووید-۱۹ راهکارهای مبتنی بر فناوری اطلاعات است. به همین دلیل جریان داده در بحران کووید-۱۹ به‌صورت تصاعدی درحال افزایش است. رژیم‌های حقوقی حفاظت از داده؛ جمع‌آوری، انتقال و پردازش داده‌ها را تنظیم‌گری می‌کند و به حقوق کاربران در این حوزه می‌پردازد. در این مقاله، نگارنده با روشی تحلیلی توصیفی و رویکردی تطبیقی درصدد پاسخگویی به این پرسش است که: «الزامات و قواعد حقوقی حفاظت از داده‌ها در شرایط اضطراری بحران همه‌گیری کووید-۱۹، در اتحادیه اروپا و جمهوری اسلامی ایران چیست؟» با بررسی اسناد حقوقی اتحادیه اروپا، مراعات الزامات حفاظت از داده در مقابله با بحران همه‌گیری کووید-۱۹ هم‌چنان لازم‌الاجراست و قوانین حفاظت از داده در اتحادیه اروپا استثنائات و انعطاف‌پذیری لازم برای مقابله با بحران همه‌گیری را درنظر گرفته‌اند. همچنین در ایران به‌دلیل عدم وجود نظام منسجم حفاظت از داده، پیشنهاد می‌شود کمیته فناوری اطلاعات ستاد ملی مقابله با کووید-۱۹ برای صیانت از حقوق شهروندان در بحران کووید-۱۹ با استناد به اصول کلی حقوقی و قوانین پراکنده قابل‌استناد برای حفاظت از داده‌ها، دستورالعمل موقت حفاظت از داده‌ها در بحران کووید-۱۹ را تهیه و به‌تصویب ستاد ملی مقابله با کووید-۱۹ برساند.

---

* نویسندهٔ مسئول؛ ***Email:*** sakhne@ gmail.com

واژگان کلیدی: حفاظت از داده‌ها، بحران همه‌گیری ویروس کووید-۱۹، رهگیری تماس، اتحادیه اروپا، جمهوری اسلامی ایران.

مقدمه

با گسترش روزافزون فضای مجازی در جهان و کوچ بسیاری از روابط اجتماعی بر بستر فضای مجازی و انتقال بسیاری از نظامات اجتماعی از دنیای فیزیکی به فضای مجازی، حقوق و تکالیف مختلفی که در دنیای فیزیکی برای اشخاص متصور بود، به فضای مجازی نیز تعمیم پیدا کرد. یکی از مهم‌ترین مصادیق حقوق بشر و شهروندی اشخاص حقیقی در دنیای فیزیکی، حق بر حریم خصوصی است که اصل آن در بیشتر کشورها، با وجود تفاوت در قلمرو، پذیرفته شده است. بنابراین همان‌طور که باید این حقوق در عرصه فضای مجازی نیز تعمیم پیدا کند، برای تکلیف متقابل آن نیز باید نظامی حقوقی تدارک دید تا این حقوق نقض نشود.

امروزه سازمان‌های عمومی و خصوصی صاحب‌نفوذ، سازمان‌های اطلاعاتی و جاسوسی و شرکت‌های بزرگ فناوری اطلاعات و ارتباطات می‌توانند در کسری از ثانیه، داده‌های مربوط به خصوصی‌ترین اطلاعات یک فرد، همچون اطلاعات مربوط به وضعیت سلامت جسم و روان، دارایی‌های مالی و بانکی، سوابق تحصیلی و سوابق سفرهای خارجی دسترسی پیدا کنند. اطلاعاتی که مالک داده حتی از اینکه چه هنگام توسط چه کسی گردآوری شده یا مورد استفاده قرار می‌گیرد، خبردار نیست. بنابراین نظام‌های حقوقی مختلف در پی حمایت از این حقوق، قوانین مختلفی وضع کردند که به قوانین حفاظت از داده‌ها شهرت پیداکرده است. البته باید توجه داشت که هرچند هسته اصلی قوانین حفاظت از داده‌ها، حریم خصوصی می‌باشد، اما رابطه این دو، عموم و خصوص من‌وجه است و نقاط افتراق زیادی دارند.

در اواخر سال ۱۳۹۸ هجری شمسی و اوایل سال ۲۰۲۰ میلادی، بحران همه‌گیری ویروس کوید-۱۹ به مهم‌ترین چالش بین‌المللی و ملی در سطح جهان تبدیل شد و دولت‌ها تمام امکانات خود را برای مبارزه با این ویروس به میدان آوردند. یکی از ابزارهایی که کمک شایانی به مبارزه با همه‌گیری می‌کند، ابزارهای فناوری اطلاعات و ارتباطات است که مستلزم گردآوری، پردازش و ذخیره‌سازی داده‌ها می‌باشد. بنابراین پرسش اصلی این پژوهش چیستی الزامات حقوقی حفاظت از داده‌ها در بحران همه‌گیری کووید-۱۹ در اتحادیه اروپا و ایران است. پیرو سؤال اصلی، سؤالات فرعی این پژوهش مطرح می‌شود که آیا قواعد حفاظت از داده‌ها در نظام‌های حقوقی مختلف هم‌چنان هم لازم‌الاجراست یا می‌توان برای مقابله با همه‌گیری ویروس کووید-۱۹ برخی از قواعد و الزامات حفاظت از داده‌ها را تعلیق کرد؟ حدود این تعلیق به چه نحوی است؟ به‌طور اساسی آیا

قوانین حفاظت از داده‌ها، چنین استثنایی را پیش‌بینی کرده‌اند؟ این پژوهش با رویکردی توصیفی - تحلیلی و به‌صورت تطبیقی به مطالعه الزامات حفاظت از داده‌ها در بحران کووید-۱۹ در اتحادیه اروپا و جمهوری اسلامی ایران می‌پردازد.

پاندمی کووید-۱۹ یکی از چالش‌های مهم پیش‌روی حفاظت از داده است که به‌علت جدید بودن این موضوع هنوز تألیفات قابل‌توجهی صورت نگرفته است. درخصوص حفاظت از داده‌ها منشورهای حقوقی مختلفی در اتحادیه اروپا، چه در سطح اتحادیه مانند مقررات GDPR[1] و چه در سطح ملی کشورهای عضو اتحادیه مانند قانون حفاظت از داده‌ها در آلمان (BDGS) که هریک تکالیفی را برای حفاظت از داده‌ها در شرایط خاص مقرر کرده‌اند. ونترلا[2] با تعمیم اصول لازم برای پردازش داده‌های شخصی در قوانین حفاظت از داده، به پردازش داده‌ها در شرایط اضراری معتقد است در بحران‌های همه گیری نیز تا جای ممکن باید به اصول حفاظت از داده پایبند بود (Ventrella, 2020). مکلسون و دیگران، با تأکید بر ضروری بودن حفظ حریم خصوصی و پای‌بندی به قواعدحفاظت از داده‌ها در شرایط پاندمی، نقش نهادهای رگولاتور در این زمینه را برجسته می‌کند و آن‌ها را مسئول رعایت حداکثری مقررات حفاظت از داده در شرایط پاندمی می‌داند (Mikkelsen & others, 2020).

این مقاله از سه بخش تشکیل شده است؛ قسمت نخست به تبیین مختصرموضوع حفاظت از داده‌ها در اتحادیه اروپا و ایران می‌پردازد، در قسمت دوم چالش‌های مرتبط با داده‌ها در بحران کووید-۱۹ تشریح می‌شود و قسمت سوم به بررسی الزامات و وضعیت حفاظت از داده‌ها در بحران کووید-۱۹ در اتحادیه اروپا و ایران، اختصاص دارد.

۱- نظام‌های حقوقی حفاظت از داده‌ها

اعلامیه جهانی حقوق بشر در ماده ۳ چنین بیان می‌کند: «هر فردی حق زندگی، آزادی و امنیت شخصی دارد». ماده ۱۲ نیز مداخله خودسرانه در زندگی خصوصی، امور خانوادگی، اقامتگاه و مکاتبات را منع کرده است. در اعلامیه حقوق بشر اسلامی قاهره نیز در ماده ۱۸ قسمت «ب» حق استقلال اشخاص در زندگی خصوصی شناسایی‌شده و نظارت و جاسوسی در آن منع شده است. اظهارنظر عمومی شماره ۱۶ کمیته حقوق بشر در مورد حق حفظ حریم خصوصی طبق مفاد میثاق بین‌المللی حقوق مدنی و سیاسی در ماده ۱۰ بیان می‌کند: «جمع‌آوری و نگهداری اطلاعات شخصی در رایانه‌ها، بانک‌های داده و سایر دستگاه‌ها، چه توسط مقامات دولتی صورت پذیرد یا اشخاص خصوصی یا ارگان‌ها، باید توسط قانون تنظیم شود. [...] برای مهیا کردن مؤثرترین راه برای

1. General Data Protection Regulation
2. Emanuele Ventrella

حفاظت از زندگی خصوصی، هر فرد باید این حق را داشته باشد که به‌طور دقیق و مشخص بداند که چه داده‌های شخصی از او به‌صورت خودکار در فایل‌های داده ذخیره می‌شود و این ذخیره‌سازی برای چه هدفی صورت می‌پذیرد» (HCR, 1988).

با بررسی رویکرد کلی نظام‌های حقوقی حفاظت از داده‌ها، به‌نظر می‌رسد دنیای حفاظت از داده‌های کاربران در فضای مجازی دوقطبی شده است. در یک‌سوی این معادله، ایالات‌متحده آمریکا قرار دارد و در سوی دیگر، دیدگاه اروپایی دیده می‌شود. سیاست‌ها و قوانین ایالات‌متحده دارای خلأهای زیادی در حوزه حفاظت از حریم خصوصی کاربران در فضای مجازی است. ایالات‌متحده آمریکا به‌دلیل اتخاذ روش موردی برای قانون‌گذاری درخصوص حریم خصوصی و رویکرد خودتنظیمی در بخش‌های مختلف این موضوع، فاقد قانونی جامع در این زمینه می‌باشد (نوری و نخجوانی، ۱۳۸۲: ۱۰۶). نقطه مقابل رویکرد آمریکایی در باب حفاظت از داده، رویکرد اروپایی است. رهیافت اروپایی درباره حفاظت از داده‌های کاربران در فضای مجازی رهیافتی جامع‌نگر می‌باشد. در این رویکرد، قوانین جامع و فراگیر در زمینه حمایت از داده‌ها، تعیین مراجع عمومی برای ثبت داده‌ها، پایگاه داده، حل اختلاف، اخذ رضایت قبلی در مورد پردازش برخی داده‌ها و جزئیات زیادی مدنظر قرار می‌گیرد (محسنی، ۱۳۹۴: ۵۴۰). البته رویکرد سومی در حفاظت از داده قابل‌تصور است که مبنی بر عدم قانون‌گذاری در حوزه حفاظت از داده‌ها و حریم خصوصی در نظام حقوقی می‌باشد که هم‌چنان برخی کشورها در این دسته قرار می‌گیرند.

۱-۱. نظام حقوقی حاکم بر حفاظت از داده‌ها در اتحادیه اروپا

قواعد حقوقی حفاظت از داده در اتحادیه اروپا قدمت ۵۰ ساله دارد به‌نحوی‌که اولین قانون حفاظت از داده در جهان در سال ۱۹۷۰ میلادی در ایالت هسن آلمان به تصویب رسید (Raul, 2020: 195). در سال ۱۹۸۰، OECD مجموعه ای از دستورالعمل‌های بین المللی حریم خصوصی و حفاظت از داده‌ها را منتشر کرد که به عنوان «دستورالعمل‌های مربوط به حفاظت از حریم خصوصی و جریان فرامرزی داده‌های شخصی»[1] شناخته می‌شود. این دستورالعمل‌ها چندین اصل مهم حفاظت از داده و حریم خصوصی را ایجاد کرده اند که امروزه در مقررات GDPR منعکس شده است (Karmer & Hoar, 2017: 2). در ۲۵ ژانویه ۲۰۱۲، کمیسیون اروپا اعلام کرد که تلاش می‌کند قوانین حفاظت از داده‌ها را در اتحادیه اروپا از طریق قانون پیشنهادی موسوم به «مقررات عمومی حفاظت از داده» یا GDPR متحد کند. اهداف اتحادیه اروپا برای این قانون جدید شامل موارد زیر است:

---

1. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2013 https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

- هماهنگی مقررات ملی اعضای اتحادیه اروپا در حفاظت از داده‌ها در یک مقرره واحد؛
- بهبود قوانین انتقال داده‌های شرکت‌ها در خارج از اتحادیه اروپا؛ و
- بهبود کنترل کاربر بر داده‌های شناسایی شخصی.[1]

در ۲۷ آوریل ۲۰۱۶، پس از چهارسال مذاکره، نسخه نهایی مقررات GDPR توسط پارلمان اتحادیه اروپا تصویب شد[2] و طبق ماده ۹۹ این قانون مقرر شد پس از یک دوره گذار دوساله، این مقرره در ۲۵ مه ۲۰۱۸ به‌طور کامل اجرا شود.

آئین‌نامه عمومی حفاظت از داده‌های اتحادیه اروپا جامع‌ترین چارچوب جهانی در حفاظت از داده‌های شخصی را ارائه می‌دهد. این مقررات شامل ۹۹ ماده است که سخت‌گیرانه‌ترین رژیم حقوقی حفاظت از داده‌ها تاکنون (۲۰۲۱) را اعمال می‌کند. اکنون این مقررات در کشورهای عضو اتحادیه اروپا لازم‌الاجراست، هم‌چنین بسیاری از کشورها از این مقررات برای تدوین قوانین ملی خود، بهره‌برداری کرده‌اند (Kittichaisare, 2017: 60). برای مثال آرژانتین با بهره‌برداری از مقررات GDPR سند قانونی ملی خود در زمینه حفاظت از داده را تنظیم کرده است. هم‌چنین در کشورهایی نظیر برزیل، ژاپن، کره جنوبی، تایلند، شیلی نیوزلند، هند و آفریقای جنوبی شاهد قوانین مشابهی با GDPR هستیم (Simmons, 2019). در واقع می‌توان گفت پذیرش قواعد و الزامات GDRP به‌مرور به یک رویه بین‌المللی تبدیل خواهد شد.

موضوع مقررات GDPR، حمایت از داده‌های شخصی است که در بند ۱ ماده ۴ از این مقررات چنین تعریف‌شده است: «داده‌های شخصی به‌معنای هرگونه اطلاعات مربوط به یک شخص حقیقی شناسایی‌شده یا قابل‌شناسایی (موضوع داده) گفته می‌شود؛ منظور از شخص حقیقی قابل‌شناسایی، شخصی است که می‌تواند به‌طور مستقیم یا غیرمستقیم مشخص شود، به‌ویژه با ارجاع به یک شناسه مانند نام، شماره شناسایی، داده‌های مکان‌محور، یک شناسه برخط یا چند عامل خاص برای هویت جسمی، فیزیولوژیکی، ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی آن شخص حقیقی». با توجه به مقررات GDPR و ادبیات مربوط به حفاظت از داده‌های کاربران، به‌نظر می‌رسد این حفاظت در ۴ حوزه باید انجام گیرد: گردآوری داده‌ها؛ ذخیره‌سازی داده‌ها؛ پردازش داده‌ها؛ استفاده از داده‌ها.

---

1. EC, European Commission. (2012). Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data (General Data Protection Regulation). Brussels: European Commission.
2. Regulation, E. G. D. P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) 2016 .OJ L ,119 (1)

براساس ماده ۳ مقررات GDPR، قلمرو اعمال این مقررات تا جایی است که کنترل‌کننده داده (سازمانی که اطلاعات ساکنان اتحادیه اروپا را جمع‌آوری می‌کند) یا پردازش‌کننده داده (سازمانی که از طرف کنترل‌کننده داده، داده‌ها را پردازش می‌کند، مانند ارائه‌دهندگان خدمات ابری) یا موضوع داده (شخص) از اتباع اتحادیه اروپا باشد. البته ماده ۳ مقررات GDPR به‌نوبه خود، برای کنترل‌کننده‌ها، پردازش‌کننده‌ها یا نظارت‌کننده‌های داده‌های افراد که در اتحادیه اروپا نیستند، اما پردازش آن‌ها مرتبط با ارائه کالا یا خدمات به اشخاص دارای تابعیت یک یا چند کشور عضو اتحادیه اروپا می‌باشد، نیز حاکم است.

طبق این قانون باید مشخص شود اطلاعات شخصی کاربران چه مدت توسط شرکت‌ها نگهداری شده و این داده با چه کسانی یا شرکت‌هایی به اشتراک گذاشته می‌شود. در واقع طبق این قانون، رضایت کاربر در همه این موارد یک اصل ضروری و اساسی محسوب می‌شود و شرکت‌ها بدون اخذ رضایت صریح و آگاهانه از کاربر، حق جمع‌آوری اطلاعات از او را ندارند. از سوی دیگر کاربران شاهد افزایش پیغام‌های هشدار در ارتباط با حریم خصوصی هستند و برای دسترسی به سایت‌ها باید پیام‌های زیادی را تأیید کنند (جلیلی، ۱۳۹۷).

۱-۲. نظام حقوقی حاکم بر حفاظت از داده‌ها در جمهوری اسلامی ایران

در نظام حقوقی جمهوری اسلامی ایران، تاکنون رژیم قانونی و حقوقی منسجمی برای حفاظت از داده‌ها و حریم خصوصی تدارک دیده نشده است و قانون جامعی که به‌صورت منسجم به حفاظت از داده‌ها یا حریم خصوصی بپردازد موجود نیست. هرچند لایحه صیانت از داده‌ها شخصی در ایران در سال ۱۳۹۷، توسط وزارت ارتباطات رونمایی شد (وزارت ارتباطات، ۱۳۹۷)، اما تاکنون پس از گذشت دوسال، در هیئت دولت تصویب نشده (۱۳۹۹/۹) و به مجلس شورای اسلامی ارسال نشده است. درواقع در دسته‌بندی مذکور در ارتباط با مواجهه کشورها در ارتباط با حفاظت از داده‌ها، جمهوری اسلامی ایران در جایگاهی بین دسته دوم و سوم قرار می‌گیرد، یعنی بین عدم وجود نظام حقوقی حفاظت از داده و نظام افتراقی و موضوعی حفاظت از داده.

به‌علت رشد پایگاه‌های داده اینترنتی و نبود نظام حفاظت از اطلاعات شخصی کاربران، نبود فرهنگ ارزشمندی داده‌ها در سطح جامعه، عدم برخورد با شرکت‌هایی که به‌علت ضعف در امنیت، اطلاعات کاربران‌شان لو رفته است و نبود اکوسیستم امنیت اطلاعات، شاهد افزایش تعداد نشت‌های اطلاعات در فضای مجازی در کشور هستیم. ازجمله این اتفاقات می‌توان به «نشت اطلاعات شناسنامه‌ای ۸۰ میلیون کاربر ایرانی از طریق سرورهای سازمان ثبت‌احوال و وزارت بهداشت، افشای بانک اطلاعاتی حاوی اطلاعات شمار زیادی از کاربران ایرانی پیام‌رسان تلگرام و شماری از

کاربران یکی از بازارهای ایرانی نرم‌افزارهای آیفون، افشای اطلاعات کاربران یکی از اپراتورهای موبایل و سرقت پایگاه داده سازمان امور دانشجویان وزارت علوم، پایگاه ایرانداک و برخی شرکت‌های هواپیمایی و بانک‌ها» (بخشی پور، ۱۳۹۹) اشاره کرد.

یکی از دلایلی که انگیزه شرکت‌ها برای پرداختن به حفاظت از داده‌های کاربران و هم‌چنین حفظ امنیت اطلاعات کاربران را کاهش می‌دهد، این است که این اقدام برای آن‌ها هزینه‌بر است و از طرفی جرم‌انگاری و ضمانت‌اجرای حقوقی بازدارنده‌ای در این خصوص برای سهل‌انگاری آن‌ها صورت نگرفته است، اما همین موضوع در اتحادیه اروپا و ذیل GDPR تعبیه شده است و سازمان‌ها و شرکت‌ها را موظف می‌سازد تا درصورت نشت اطلاعات کاربران پاسخگو باشند و جریمه پرداخت کنند. جریمه‌ای که مطابق با بند ۶ ماده ۸۳ مقررات GDPR تا ۲۰ میلیون یورو و برای شرکت‌ها تا حداکثر ۴٪ از کل گردش مالی سالانه جهانی در سال مالی قبل آن‌ها را درصورتی‌که از ۲۰ میلیون یورو بالاتر باشد، دربرمی‌گیرد. بنابراین عدم محکوم شدن به این جریمه سنگین انگیزه بسیار مهمی برای حفاظت از داده‌های کاربران در اتحادیه اروپا می‌باشد. اما در ایران جرم‌انگاری بازدارنده در این زمینه صورت نگرفته است و کاربران تنها با استناد به قوانین عمومی و اصول حقوقی مانند ورود ضرر و مسئولیت مدنی امکان پیگیری این اهمال‌کاری و ترک فعل را دارند.

اصل ۲۲ قانون اساسی بیان می‌کند: «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی‌که قانون تجویز کند». این اصل مهمترین سند در مورد حریم خصوصی در جمهوری اسلامی ایران می‌باشد که در عین موجز و کلی بودن آن به ابعاد مختلفی از حریم خصوصی توجه شده است مانند حریم خصوصی معنوی، حریم خصوصی جسمانی، حریم خصوصی مکانی در این ماده قید شده است.

اما قوانین، مقررات و احکام شرعی مختلفی در ایران به‌صورت پراکنده و افتراقی به برخی حقوق شهروندان در حریم خصوصی و حفاظت از داده‌ها اشاره کرده است. برای مثال اصل ۲۳ قانون اساسی ناظر بر منع تفتیش عقاید؛ امکان جبران خسارت واردشده به داده‌های شخصی یا خسارت‌های ناشی از انتشار داده‌ها از طریق مواد ۱ و ۱۰ قانون مسئولیت مدنی و ماده ۷۸ قانون تجارت الکترونیک؛ عدم امکان استفاده از داده‌های تجمیع شده افراد در محلی که رضایت نداشته باشند، براساس ماده ۱۷ جرائم رایانه‌ای؛ حق برخورداری از امنیت سایبری و حفاظت از داده‌های شخصی و حریم خصوصی مطابق با ماده ۸ منشور حقوق شهروندی؛ قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی مصوب، ۱۳۸۳؛ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۸ و آئین‌نامه اجرایی این قانون مصوب ۱۳۹۳؛ هم‌چنین فتاوای معتبری از مراجع تقلید در منع

نقض حریم خصوصی وجود دارد[1] که براساس اصل ۱۶۷ جزء منابع نظام حقوقی جمهوری اسلامی ایران محسوب می‌شود. بااین‌حال چطور می‌توان انتظار داشت که حفاظت از داده‌ها و حریم خصوصی کاربران فضای مجازی در ایران حفظ شود، درحالی‌که برای بسیاری از مصادیق نقض حریم خصوصی و حفاظت از داده‌ها در فضای مجازی هنوز احکام قانونی وجود ندارد؟

۲- چالش‌های حفاظت از داده‌ها در بحران همه‌گیری کووید-۱۹

پس از شیوع کووید-۱۹، به‌علت کاهش تعاملات انسانی در محیط فیزیکی، تعاملات اجتماعی با روندی تصاعدی بر بستر فضای مجازی شکل گرفت که مهم‌ترین نتیجه آن در بُعد فنی، افزایش حجم زیادی جریان داده‌ها بود، به‌شکلی که بسیاری از ارائه‌دهندگان خدمات در فضای مجازی با مشکلاتی ازجمله پهنای باند و عدم ظرفیت زیرساخت‌ها مواجه شدند. هم‌چنین بسترهای مختلف فضای مجازی ازجمله؛ پیام‌رسان‌های اجتماعی، شبکه‌های اجتماعی، پلتفرم‌های تجارت الکترونیک و بسترهای آموزش مجازی با استقبال زیادی مواجه شدند. این روند تغییرات پرشتاب نگرانی‌های مهمی ایجاد کرد که مبادا این تغییر سریع، منجربه نادیده گرفتن حقوق کاربران شود.

از طرفی یکی از ابزارهای مهمی که امروزه برای مقابله با همه‌گیری‌ها وجود دارد، ابزار فناوری اطلاعات است که با ره‌گیری افراد و نظارت بر داده‌ها، امکان قرنطینه هوشمند را فراهم می‌کند. در بحران کووید-۱۹ نیز فناوری اطلاعات کمک‌های مختلفی برای جلوگیری از شیوع ویروس کووید-۱۹ انجام داد. برای مثال برنامه‌های ردیابی تماس، برنامه‌های خوداظهاری سلامت، نظارت بر سلامتی کارمندان، نقشه‌های عبور و مرور افراد و مناطق آلوده، آموزش مجازی و دورکاری کارکنان کمک شایانی به پیشگیری از ابتلا به ویروس کووید-۱۹ کردند. اما هم‌زمان با افزایش نقش فناوری اطلاعات در پیشگیری از همه‌گیری و گسترش جریان داده‌ها، نگرانی‌هایی در جهت حفظ حریم خصوصی و حقوق حفاظت از داده‌های شهروندان ایجادشده است که مبادا به بهانه مقابله با همه‌گیری، حقوق قانونی شهروندان در حفاظت از داده‌ها و حریم خصوصی، توسط دولت‌ها و شرکت‌های خصوصی مورد تعرض قرار گیرد. برای نمونه در ایران برای اجرای قرنطینه هوشمند، مشخصات بیماران کووید-۱۹ای به ارائه‌دهندگان خدمات حمل‌ونقل ریلی، هوایی و زمینی ارائه شد

---

۱. برای مثال مقام معظم رهبری در دیدار با مسئولان در ۱۳۹۷/۱/۲۰ بیان کردند: «تعرض به امنیت و حریم داخلی مردم «حرام شرعی» است و نباید انجام شود.» هم‌چنین آیت‌الله مکارم‌شیرازی در فتوایی در ۱۳۹۷/۱/۲۹ بیان می کنند: «شکی نیست که تعرض به حریم خصوصی افراد چه در فضای مجازی باشد، چه در غیر آن شرعاً جایز نیست و مسئولیت شدید دارد.»

تا از ورود آن‌ها به وسایل حمل‌ونقل مزبور ممانعت به‌عمل آید.[۱] اما تاکنون مصاحبه یا سندی از مسئولان منتشر نشده که شفاف‌سازی کند، چه نهادهایی، چه داده‌هایی را جمع‌آوری، پردازش و استفاده کرده‌اند. هم چنین الزامی قانونی برای حفاظت از داده‌های کاربران در این زمینه وجود ندارد.

لزوم رعایت الزامات حفاظت از داده‌ها به معنای ممانعت از استفاده از داده‌ها نیست بلکه مقامات دولتی باید بتوانند با استفاده از داده‌ها، ازجمله داده‌های بهداشتی، بهترین اقدامات را برای کاهش شیوع ویروس تعیین کنند و مشخص کنند که چه اقداماتی باید برای حفاظت از مردم و حقوق آن‌ها در طول بحران و پس‌ازآن انجام شود. اما تدابیر اعمال‌شده باید شفاف، ضروری و متناسب باشد و درصورت وجود، قوانین حفاظت از داده‌ها و حریم خصوصی باید استثناهای روشنی داشته باشند که در مورد بحران‌های بهداشت عمومی اعمال می‌شود تا امکان استفاده بیشتر از داده‌ها از حد معمول فراهم شود. حقِ دانستن یکی از حقوق اساسی انسان است که در اصل ۱۹ بیانیه حقوق بشر نیز بر آن تأکید شده است و همه کشورها ازجمله ایران آن را پذیرفته‌اند. از طرفی شفافیت اقدامات دولت از اصول اجماعی حکمرانی در عصر حاضر است که در اسناد مختلف ملی و بین‌المللی تعبیه شده است. هم‌چنین قانون انتشار و دسترسی آزاد به اطلاعات احکام بسیاری در این زمینه دارد.

امروزه فناوری اطلاعات و ارتباطات کاربردهای گسترده‌ای دارد و در ابعاد مختلف زندگی بشر، راه‌کارهای نوینی برای تسهیل امور ارائه می‌کند، ازجمله در بحران‌های همه‌گیری فناوری اطلاعات و ارتباطات می‌تواند ابزار مناسبی برای رصد الگو و کنترل شیوع بیماری باشد. در این خصوص فناوری‌های مختلفی برای رهگیری تماس افراد ابداع شده است که علاوه‌بر مزایای مذکور می‌تواند بحرانی برای حفاظت از داده‌ها و حریم خصوصی ایجاد کند که نیازمند بررسی حقوقی بیشتر می‌باشد. از طرفی بحران همه‌گیری کرونا منجربه افزایش و تحول جریان داده‌ها در سطح جوامع شده است. بسیاری از امور که تا پیش از این از طریق حضور فیزیکی انسان‌ها در کنار یکدیگر انجام می‌شد، درحال حاضر به‌صورت مجازی برگزار می‌شود، مانند آموزش مجازی که حجم داده بسیار زیادی را بر شبکه‌ها تحمیل کرده است. در مورد دیگر، تمایل شرکت‌ها، ادارات دولتی و کارمندان به دورکاری می‌باشد که علاوه بر حفاظت از سلامتی افراد، منجربه کاهش هزینه‌ها نیز می‌شود، اما هریک الزامات جدیدی در حفاظت از داده‌ها و حریم خصوصی ایجاد کرده است که باید مورد بررسی حقوقی قرار گیرد.

---

۱. ابلاغیه شماره ۳۰۰/۳۱۰۹ وزارت بهداشت، درمان و آموزش پزشکی: «از تاریخ ۲۸ آبان ۱۳۹۹ هرگونه جابه‌جایی مسافر به‌صورت هوایی، زمینی و دریایی، بدون دریافت نتیجه تست کرونا ممنوع است».

۲-۱. نرم‌افزار ردیابی تماس هوشمند

از زمان انتشار ویروس کووید-۱۹ در اوایل سال ۲۰۲۰ در سراسر اروپا، بحث‌های عمومی و سیاسی به‌طور فزاینده‌ای حول یک راه‌حل تکنولوژیکی برای این مهم‌ترین مسئله متمرکز شده است. آیا می‌توان با استفاده از نرم‌افزارهای ردیابی در تلفن‌های هوشمند همه، همه‌گیری را مهار کرد؟ این سیستم‌ها به‌طور خودکار تمام تماس‌های بین فردی کاربران را ثبت می‌کنند و بنابراین ردیابی سریع زنجیره‌های ابتلا را امکان‌پذیر می‌کند. سپس، افراد بالقوه در معرض خطر را می‌توان به‌طور مؤثر ردیابی کرد تا در مراحل اولیه ابتلا آن‌ها را جدا کند (Bock et al., 2020: 5). در اجرای ماده ۸ منشور حقوق اساسی اتحادیه اروپا، GDPR شرایطی را برای حمایت از حقوق و آزادی‌های اشخاص حقیقی فراهم می‌کند که امکان پردازش داده‌های شخصی را فراهم می‌کند. این امر همچنین در پردازش داده‌های شخصی در زمینه اقدامات انجام‌شده برای مهار و کنترل COVID-19 به‌ویژه به‌واسطه استفاده از یک نرم افزار، اعمال می‌شود (Bock et al., 2020: 45).

در این میان، طیف وسیعی از فعالیت‌های پردازشی با پشتیبانی فناوری در تعداد زیادی از کشورها ازجمله جمهوری خلق چین، کره جنوبی، سنگاپور و اتریش معرفی‌شده است که در این کشورها الزامات حفاظت از داده‌ها سخت‌گیرانه نیست و سطح حفاظت از داده‌ها و حریم خصوصی در این کشورها با اروپا متفاوت می‌باشد، ازاین‌رو در استفاده از فناوری برای مقابله با کووید-۱۹ دو رویکرد اروپایی و غیراروپایی وجود دارد، که رویکرد اروپایی مطابق و هماهنگ با قواعد حفاظت از داده‌های این اتحادیه است و رویکرد غیراروپایی الزامات ضعیف‌تری در ارتباط با حفاظت از داده‌ها و حریم خصوصی درنظر می‌گیرد (Bock et al., 2020: 24).

بسیاری از کشورهای اتحادیه اروپا درحال حاضر بر روی نرم‌افزارهایی باهدف تسهیل مبارزه با بحران کووید-۱۹ کار می‌کنند. برخی از آن‌ها مبتنی بر موقعیت جغرافیایی هستند، مانند Coronamadrid و StopCovid19 در اسپانیا، درحالی‌که برخی دیگر مبتنی بر فناوری بلوتوث شناخته‌شده به‌عنوان «دست دادن دیجیتال»[1] هستند، مانند Stopp-CoronaApp در اتریش، StopCovid در فرانسه، ProteGo در لهستان، یا نرم افزاری که توسط سرویس بهداشت ملی (NHS) در انگلیس درحال‌توسعه است. فناوری «Apple/Google ENS»[2] قابلیت همکاری بین دستگاه‌های

---

1. digital handshake

۲. سیستم اطلاع‌رسانی قرار گرفتن در معرض (Exposure Notification System)، به‌عنوان پروژه ردیابی تماس با حفظ حریم خصوصی شناخته می‌شود که یک چارچوب و پروتکل است که توسط شرکت‌های Apple و Google برای تسهیل ردیابی تماس‌های دیجیتالی در طول همه‌گیری COVID-19 توسعه یافته است که با استفاده از فناوری ←

اندروید و iOS و برنامه‌ها را برای ردیابی با استفاده از فناوری بلوتوث «تماس با رویدادها»[1] بین دستگاه‌ها را فراهم می‌کند. در این پروژه مشترک اعلام شده است که فقط برنامه‌های تعیین‌شده توسط مقامات بهداشت عمومی به این چارچوب دسترسی خواهند داشت و چنین برنامه‌هایی باید معیارهای خاصی در مورد حریم خصوصی، امنیت و کنترل داده‌ها را داشته باشند (Bradford, 2020: 3).

شرکت‌های اپل و گوگل ادعا می‌کنند که داده‌های کاربری که از طریق ENS آن‌ها پخش می‌شود، به‌دلیل هویت زدایی و عدم تمرکز، «ناشناس» شده است و به همین دلیل تحت شمول مقررات GDPR قرار نمی‌گیرد. از طرفی شورای حفاظت از داده‌های اروپا به‌صراحت اعلام کرده است که ناشناس ماندن قطعی داده‌های واقعی استاندارد بسیار بالایی است و کنترل‌کننده‌های داده معمولاً از بی‌هویت‌سازی داده‌ها کوتاهی می‌کنند (Guidelines 2020/04, 2020).

در نهایت براساس اطلاعات موجود، اعلان خودکار با استفاده از ENS و برنامه‌های مرتبط، یک سیستم پردازش اطلاعات شخصی است که تحت شمول GDPR است. ماده ۲۴ GDPR دستور می‌دهد که کنترل‌کننده‌های داده، ازجمله کنترل‌کننده‌های مشترک، اقدامات فنی و سازمانی مناسبی را برای اطمینان از انجام پردازش مطابق با مقررات را تدارک ببینند، هم‌چنین کلیه اصول مندرج در ماده ۵ مقررات GDPR ازجمله: قانونی بودن، انصاف و شفافیت؛ محدودیت هدف؛ به حداقل رساندن داده‌ها؛ صحت داده‌ها؛ محدودیت ذخیره‌سازی؛ یکپارچگی و محرمانه بودن و پاسخگویی، باید در طراحی و اجرای این سیستم‌ها رعایت شود (Bradford, 2020: 3).

پروژه‌های دیگری برای انطباق مقررات حفاظت از داده‌ها با نرم‌افزارهای ردیابی تماس طراحی شده است، ازجمله پروژه «چارچوب اروپایی حفظ حریم خصوصی در ردیابی مجاورت (PEPP-PT)»، قصد دارد مکانیسم‌ها و استانداردهای فنی را ارائه دهد که به‌طور کامل از حریم خصوصی حفاظت می‌کند. این پروژه نوید اجرای حفاظت از داده‌ها، ازجمله ناشناس ماندن داده‌ها، با رعایت GDPR و الزامات امنیت اطلاعات را می‌دهد. تلفن‌های هوشمندی که برنامه‌ها را اجرا می‌کنند شناسه‌های موقتاً معتبر «ناشناس» را ارسال می‌کنند که توسط سایر تلفن‌های هوشمند دریافت و ذخیره می‌شوند. این پروژه نوید می‌دهد که هیچ‌کسی، ازجمله خود کاربران، نمی‌توانند به سابقه تماس فرد با دیگران دسترسی داشته باشند. همچنین حوادث قدیمی در تاریخ به‌محض اینکه ازنظر اپیدمیولوژی بی‌اهمیت می‌شوند، حذف می‌شوند. درصورت آلوده شدن کاربران این برنامه، با آن‌ها

---

bluetooth، ارتباطات صاحبان ابزارهای فناوری اطلاعات و ارتباطات با یکدیگر را به‌صورت شبکه‌ای و توزیع یافته به‌واسطه فناوری رمزنگاری جمع‌آوری و رصد می‌کند که این رمزنگاری می‌تواند عامل حفظ حریم خصوصی باشد.

1. contact events

تماس گرفته می‌شود تا بتوانند سبب اطلاع‌رسانی مخاطبان خود شوند. برنامه‌ها به‌طور مرتب به‌روزرسانی را از سرور بارگیری می‌کنند، ازجمله شناسه مخاطبان کاربران آلوده که به کاربران امکان می‌دهد دریابند که با افراد آلوده در تماس بوده‌اند. هر برنامه‌ای که طبق این استاندارد ساخته‌شده باید توسط کنسرسیوم PEPP-PT تأیید شود (Bradford, 2020: 17).

۲-۲. خوداظهاری سلامت

براساس شواهد جمع‌آوری‌شده توسط آژانس حقوق اساسی اتحادیه اروپا، نرم‌افزارها و وب‌سایت‌های خوداظهاری بهداشت در بلغارستان، کرواسی، دانمارک، آلمان، یونان، ایتالیا، اسلوونی و اسپانیا وجود دارد. این برنامه‌ها با برنامه‌های ردیابی متفاوت است. در این شیوه کاربران به‌صورت داوطلبانه داده‌ها و علائم خود را بارگذاری می‌کند تا نقشه COVID-19 را ترسیم کنند و این اطلاعات را به‌صورت ناشناس یا عمومی در اختیار مقامات بهداشتی قرار دهند. برای مثال، در اسپانیا، یک نرم‌افزار موجود گزارش روزانه علائم ویروس کووید-۱۹، دریافت مشاوره و اطلاعات بهداشتی را فراهم کرده، اما همچنین ردیابی جغرافیایی را برای هشدارهای محلی نیز امکان‌پذیر می‌کند. در آلمان، این برنامه ادعا می‌کند که علائم اولیه COVID-19 را شناسایی کرده و نقشه جغرافیایی گسترش ویروس را ترسیم می‌کند (EUAFR v.2, 2020: 54). بنابراین اقدامات سایت‌ها و نرم افزارهایی که به‌صورت خود اظهاری و با رضایت کاربران، بر داده‌ها صورت می‌گیرد، براساس مواد ۵ و ۶ مقررات GDPR مشروع و قانونی است، اما باید سایر الزامات حفاظت از داده‌ها را رعایت کنند.

۲-۳- حفاظت از داده‌ها در آموزش مجازی

بحران همه‌گیری کووید-۱۹ نقطه عطفی برای آموزش مجازی بود و در بسیاری از کشورها مدارس، دانشگاه‌ها و مؤسسات آموزشی، از بسترهای آموزش مجازی استفاده کرده و می‌کنند. انتقال یک‌باره و ناگهانی فعالیت‌های آموزشی به بسترهای آموزش مجازی، مشکلات فراوانی در زیرساخت‌ها و نرم‌افزارهای آموزش مجازی را عیان کرد. علاوه بر این نگرانی‌هایی در رابطه با حریم خصوصی، حفاظت از داده‌ها و رعایت حقوق کاربران مطرح می‌شود؛ چراکه بسترهای آموزش مجازی اطلاعات مهمی در ارتباط با دانش‌آموزان و دانشجویان در اختیار دارند. برای نمونه برای احراز هویت کاربران در این بستر اطلاعات مهم شخصی افراد مبادله می‌شود. هم چنین داده‌های مختلفی ازجمله، صوت، تصویر، متن، نمرات، امتحانات و داده‌های مختلف دیگری در این بستر منتقل می‌شود که به‌صورت جدی نیازمند رعایت الزامات حفاظت از داده‌ها است.

همچنین انتخاب یک مبنای حقوقی مناسب برای پردازش داده‌ها از اهمیت اساسی برخوردار است، به‌ویژه هنگامی‌که کودکان درگیر آموزش مجازی می‌شوند، در صورت لزوم برای پردازش داده‌های موردنظر در زمینه آموزش آنلاین، نقش والدین به عنوان سرپرست قانونی کودکان اهمیت پیدا می‌کنند. بنابراین برای حفظ حریم خصوصی کاربران و حفاظت از داده‌های کاربران که در این بستر اهمیت ویژه‌ای پیدا می‌کند، علاوه بر قوانین و مقررات عمومی حفاظت از داده‌ها، قوانین و دستورالعمل‌های ویژه‌ای ایجاد شده است بطور مثال می‌توان به رهنمودهای UNICEF با عنوان «حریم خصوصی کودکان و آزادی بیان»[1] در سال ۲۰۱۸؛ توصیه‌نامه شورای اروپا با عنوان «توصیه CM/ Rec (2018) 7 کمیته وزیران به کشورهای عضو درباره رهنمودهایی برای احترام، محافظت و تحقق حقوق کودک در محیط دیجیتال»[2]؛ «مقررات مربوط به حفاظت سایبری از اطلاعات شخصی کودکان» در چین در سال ۲۰۱۹ اشاره کرد.

۳- الزامات حقوقی حفاظت از داده‌ها در بحران همه‌گیری کووید-۱۹

قوانین بین‌المللی و ملی تشخیص داده‌اند که شرایط اضطراری به اقدامات فوق‌العاده‌ای نیاز دارند که در نهایت وضعیت اضطراری را شکل می‌دهد، وضعیت اضطراری در یک تعریف عبارت است از عکس‌العمل قانونی دولت‌ها که به‌صورت موقت و برای پاسخ به تهدیدها و خطرات گسترده، صورت می‌گیرد و در پی آن آزادی‌های بیشتری نسبت به شرایط عادی محدود می‌شود (کرمی و شریفی طرازکوهی، ۱۳۹۷: ۱۶۴). این بدان معناست که برخی از حقوق اساسی، ازجمله حقوق حریم خصوصی و حفاظت از داده‌ها، ممکن است برای حل بحران بهداشتی همه‌گیری محدود شود. یک دستور حقوقی خاص مانند اعلام وضعیت اضطراری یا وضعیت بحران، یک وضعیت فراقانونی نیست، بلکه در این شرایط هم قاعده حاکمیت قانون حاکم و جاری است و این شرایط باید از نظر گستردگی و زمانی، محدود و موقت باشد (قربان‌نیا، ۱۳۸۶: ۴۲). هم‌چنین ایجاد یک وضعیت حقوقی مانند وضعیت اضطراری نمی‌تواند توجیه‌کننده تمام اقدامات ذیل آن باشد، بلکه در شرایط وضعیت اضطراری نیز قانون حاکم می‌باشد و تمامی اقدامات باید در محدوده قانون باشد. البته حقوق معینی وجود دارد که هیچ‌گاه عدول از آن‌ها جایز نیست، مانند حق حیات، ممنوعیت شکنجه و رفتار غیرمجاز و غیرانسانی یا تحقیرآمیز، ممنوعیت بردگی و اصل قبح عقاب بلابیان (OHCHR, 2003: 833).

---

1. Children's Online Privacy and Freedom of Expression (2018)
https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf
2. Guidelines to respect, protect and fulfil the rights of the child in the digital environment - Recommendation CM/Rec(2018)7 of the Committee of Ministers (2018)
https://edoc.coe.int/en/module/ec_addformat/download?cle=ad62cfd33e3870262d6bf5331c1f13b0&k=055587731e6f9e137b8324fb13cfe4fe

کمیساریای عالی حقوق بشر در سازمان ملل متحد بیان می‌کند در مواقع همه‌گیری جهانی مانند COVID-19، مشروط بر رعایت قواعد بین‌المللی حقوق بشر و سایر استانداردهای داخلی، دولت‌ها می‌توانند اختیارات خاصی را در اختیار بگیرند تا اقدامات فوق‌العاده‌ای را برای جلوگیری و کاهش بحران بهداشت انجام دهند.[1] هم‌چنین دادگاه اروپایی حقوق بشر بیان می‌کند: «اختیارات و اقدامات فوق‌العاده به‌صورت دقیق به‌عنوان اشکال خاصی از دستورات قانونی توسط قانون اساسی ملی و رژیم‌های قانونی تعریف‌شده و در قوانین بین‌المللی و منطقه‌ای حقوق بشر پذیرفته‌شده است، ازجمله در ماده ۴ میثاق بین‌المللی حقوق مدنی و سیاسی، ماده ۱۵ معاهده اروپایی حقوق بشر و ماده ۲۷ معاهده حقوق بشر آمریکا».[2]

۳-۱. الزامات حقوقی اتحادیه اروپا برای حفاظت از داده‌ها در بحران کووید-۱۹

در مبارزه با COVID-19، داده‌ها می‌توانند جان انسان‌ها را نجات دهند. از طرفی این امکان، حل تعارض حفاظت از داده‌ها و استفاده از داده‌ها برای جلوگیری از بحران را در اولویت پاسخ به همه‌گیری قرار می‌دهد. به همین دلیل نهادهای مختلف مرتبط با حفاظت از داده‌ها در سطح بین‌المللی و اتحادیه اروپا، در جریان بحران همه‌گیری ویروس کووید-۱۹، بیانیه‌هایی صادر کردند و دیدگاه تفسیری خود را نسبت به اعمال قواعد حفاظت از داده‌ها بیان کرده‌اند. نهادهایی مانند مجمع جهانی حریم خصوصی[3]، شورای حفاظت از داده‌های اروپا[4]، شورای اروپا[5] و تنظیم‌کنندگان ملی حفاظت از داده‌ها بیانیه‌هایی صادر کردند و در آن تأیید کردند که الزامات حفاظت از داده‌ها، جمع‌آوری و پردازش امن و قابل‌اعتماد داده‌ها را تضمین می‌کند.

در بند ۴ مقدمه GDPR بیان‌شده است: «پردازش اطلاعات شخصی باید به‌گونه‌ای باشد که به بشریت خدمت کند. حق حفاظت از داده‌های شخصی یک حق مطلق نیست. باید متناسب با عملکرد آن در جامعه موردتوجه قرار گیرد و مطابق با اصل تناسب در برابر سایر حقوق اساسی متعادل

---

1. United nation Human rights office of the high commissioner. COVID-19: states should not abuse emergency measures to suppress human rights, 2020.
https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E.
2. European Court of Human Rights. Guide on Article 15 of the European Convention on Human Rights, 2019.
https://www.echr.coe.int/Documents/Guide_Art_15_ENG.pdf
3. Global Privacy Assembly (2020), Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic, 17 March 2020.
4. European Data Protection Board (2020), Statement on the processing of personal data in the context of the COVID-19 outbreak, 19 March 2020.
5. Council of Europe (2020), Joint statement on the right to data protection in the context of the COVID-19 pandemic, 30 March 2020.

شود». بنابراین مقررات GDPR برای حفظ حقوق و آزادی‌های شهروندان طریقیت دارد و اگر در موردی رعایت این قانون برخلاف منافع اساسی اشخاص و حقوق اساسی بشر مانند حق بر حیات، حق بر سلامتی و حق بر برخورداری از روش درمانی مؤثر بود، می‌توان از استثنائات قانونی مندرج در همین قانون استفاده کرد.

در اتحادیه اروپا بحران جهانی همه‌گیر کووید-۱۹ اولین مانع برجسته‌ای است که مقررات GDPR، از زمان لازم‌الاجرا شدن، با آن مواجه است. این یک فرصت عالی برای به نمایش گذاشتن انعطاف‌پذیری این مقررات برای تأمین منافع عمومی است و همچنین برای نشان دادن انعطاف‌پذیری این مقررات در بازگشت از محدودیت‌های موقت، این یک فرصت طلایی محسوب می‌شود (Deloitte, 2020: 4).

قوانین حفاظت از داده‌ها (مانند GDPR) مانع اقدامات لازم در مبارزه با بیماری همه‌گیر COVID-19 نمی‌شوند بلکه سازوکارهایی مبنی بر استفاده از داده‌ها در شرایط اضطراری در این قوانین تعبیه‌شده است. مقررات GDPR یک قانون گسترده است و مقررات مختلفی را در برمی‌گیرد که اجازه می‌دهد پردازش داده‌های شخصی، به‌منظور تحقیقات علمی مرتبط با بیماری همه‌گیر COVID-19 با رعایت حریم خصوصی و حفاظت از داده‌های شخصی صورت پذیرد.[۱] مقررات GDPR همچنین پیش‌بینی ویژه‌ای در مورد منع پردازش برخی دسته‌های خاص داده‌های شخصی، مانند داده‌های بهداشتی، در مواردی‌که برای این اهداف تحقیق علمی لازم است، دارد.[۲]

فراتر از پیش‌شرط‌های قانونی که باید برای پردازش داده‌های شخصی رعایت شود، پردازش اطلاعات شخصی در دسته‌های مشخص‌شده در بند ۱ ماده ۹ GDPR ازجمله «داده‌های بیومتریک» و «داده‌های مربوط به‌سلامتی» نیاز به توجیه ویژه دارد. در اصل، پردازش آن‌ها ممنوع است، مگر اینکه یکی از استثناهای مندرج در بند ۲ همین ماده اعمال شود.

در بند ۱۴ ماده ۴ «داده‌های بیومتریک» این‌گونه تعریف‌شده است: «داده‌های بیومتریک به‌معنای داده‌های شخصی ناشی از پردازش فنی خاص مربوط به خصوصیات جسمی، فیزیولوژیکی یا رفتاری یک شخص طبیعی است که شناسایی منحصربه‌فرد آن شخص طبیعی را امکان‌پذیر یا تأیید می‌کند، مانند تصاویر صورت یا داده‌های داکتیلوسکوپی». هم‌چنین در بند ۱۵ ماده ۴ «داده‌های مربوط به‌سلامتی» به این شیوه تعریف‌شده است: «داده‌های مربوط به‌سلامتی به معنای داده‌های

---

۱. برای مثال به ماده ۵ (۱) (ب) و (ه)، ماده ۱۴ (۵) (ب) و ماده ۱۷ (۳) (د) از مقررات GDPR مراجعه کنید.

۲. برای مثال به ماده ۹ (۲) (j) و ماده ۸۹ (۲) از مقررات GDPR مراجعه کنید.

شخصی مربوط به‌سلامت جسمی یا روانی یک فرد حقیقی است، ازجمله ارائه خدمات مراقبت‌های بهداشتی، که اطلاعات مربوط به وضعیت سلامتی وی را نشان می‌دهد». داده‌های مربوط به‌سلامتی مستحق حفاظت بیشتری هستند، زیرا استفاده از چنین داده‌های حساس ممکن است تأثیرات سوء قابل‌توجهی برای افراد داده داشته باشد. هم‌چنین رویه مربوط به دیوان دادگستری اروپا (ECJ)، بیانگر این است که اصطلاح «داده‌های مربوط به بهداشت» باید تفسیر گسترده‌ای داشته باشد.[1]

اما در بند ۲ ماده ۹ استثناناتی برای بند ۱ در نظر گرفته است که درصورتی‌که این استثنائات حاکم باشد، امکان پردازش و استفاده از داده‌هایی نظیر داده‌های بیومتریک و داده‌های مربوط به‌سلامتی وجود خواهد داشت. در بخش g از بند ۲ ماده ۹ بیان‌شده است که به‌دلیل حفظ منافع عمومی اساسی می‌توان از ممنوعیت پردازش داده‌های خاص چشم پوشید، البته مشروط به اینکه پردازش متناسب با هدف دنبال شده باشد، به اصل حق حفاظت از داده احترام بگذارد و اقدامات لازم برای حفاظت از حقوق اساسی و منافع موضوع داده را درنظر بگیرد. در بخش h از بند ۲ ماده ۹ پردازش داده‌های خاص برای اهداف پزشکی پیشگیرانه یا شغلی، برای ارزیابی توانایی کار کارمند، تشخیص پزشکی، ارائه خدمات بهداشتی یا اجتماعی یا درمان یا مدیریت سیستم‌ها و خدمات بهداشتی و درمانی اجتماعی ممنوع نیست، مشروط بر اینکه براساس قانون اتحادیه اروپا یا کشور عضو یا طبق قرارداد با یک متخصص بهداشت و تحت شرایط و ضمانت‌های ذکرشده در بند ۳ این ماده صورت پذیرد. در بخش i از بند ۲ ماده ۹ پردازش داده‌های خاص به‌دلیل منافع عمومی در زمینه بهداشت عمومی مجاز است مشروط بر اینکه پردازش داده بر اساس قانون اتحادیه اروپا یا کشور عضو که اقدامات مناسب و مشخصی را برای حفاظت از حقوق و آزادی‌های موضوع داده به‌ویژه در رابطه با منع افشای اسرار پزشکی بیماران، درنظر گرفته است، باشد.

پردازش و جمع‌آوری داده‌ها برای اهداف تحقیقاتی، باید در دوره‌های ذخیره‌سازی (جدول زمانی) خاصی تنظیم شود و باید متناسب باشد. برای تعریف چنین دوره‌های ذخیره‌سازی، معیارهایی مانند طول و هدف تحقیق باید درنظر گرفته شود. مقررات ملی ممکن است قوانینی راجع‌به دوره نگهداری پیش‌بینی کند که باید موردتوجه قرار گیرند (Guidelines 2020/03, 2020).

در اصل، شرایطی که در شیوع COVID-19 حاکم است، امکان استفاده موضوع داده‌ها از حقوق خود را طبق ماده ۱۲ تا ۲۲ GDPR به حالت تعلیق درنمی‌آورد یا محدود نمی‌کند. بااین‌حال، بند ۲ ماده ۸۹

1. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (2020, April 21). European Data Protection Board.
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

GDPR به قانون‌گذار ملی اروپایی اجازه می‌دهد تا برخی حقوق موضوع داده را همان‌طور که در فصل ۳ GDPR تنظیم شده است، محدود کند. به همین دلیل، محدودیت‌های حقوق اشخاص داده ممکن است، بسته به قوانین مصوب کشور عضو خاص متفاوت باشد (Guidelines 2020/03, 2020).

در سطح اتحادیه اروپا، آندره جلینک[1]، رئیس وقت هیئت حفاظت از داده‌های اروپا (EDPB) در تاریخ ۱۶ مارس بیانیه رسمی در مورد پردازش اطلاعات شخصی در زمینه شیوع COVID-19 را منتشر کرد. در این بیانیه تأکید شده است که حفاظت از داده‌ها مانعی برای سلامت عمومی نیست. هیئت حفاظت از داده‌های اروپا این بیانیه را در تاریخ ۱۹ مارس به‌روز کرد و مقرر شد، حتی در زمان وقوع بحران‌ها و شرایط اضطراری، کنترل‌کننده و پردازنده داده‌ها باید از حفاظت از اطلاعات شخصی موضوع داده اطمینان حاصل کنند. هیئت حفاظت از داده‌های اروپا همچنین اظهار داشت که «شرایط اضطراری یک شرط قانونی است که می‌تواند به محدودیت آزادی‌ها مشروعیت بدهد، مشروط بر اینکه این محدودیت‌ها متناسب و محدود به دوره شرایط اضطراری باشند». به همین دلیل، برای اطمینان از پردازش قانونی داده‌های شخصی، رعایت ملاحظاتی لازم می‌باشد. کارفرمایان و مقامات بهداشت عمومی لازم نیست در مورد مبانی قانونی که برای پردازش داده‌های شخصی در محدوده یک بیماری همه‌گیر به رضایت فرد استناد کنند، اما می‌توانند به ماده ۶ و ۹ GDPR استناد کنند.[2]

کمیته اخلاق زیستی شورای اروپا در بیانیه‌ای اصول اساسی مبتنی بر احترام به کرامت انسانی و حقوق بشر را در مقابله با همه‌گیری کووید-۱۹، بیان می‌کند که باید تصمیمات و اقدامات پزشکی در متن بحران موجود را هدایت کند. با استفاده از معاهده حقوق بشر و زیست پزشکی موسوم به معاهده اویدو[3]، کمیته اخلاق زیستی شورای اروپا بیان می‌کند: «جمع‌آوری و پردازش داده‌های مربوط به‌سلامت، که در مبارزه با COVID-19 ضروری است، باید تحت شرایط حفاظتی خاصی باشد و هرگونه محدودیت در اعمال حقوق باید توسط قانون تعیین شود و هدف آن حفاظت از منافع جمعی، ازجمله بهداشت عمومی باشد». سرانجام، کمیته اخلاق زیستی در برنامه اقدام استراتژیک

---

1. Andrea Jelinek
2. Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. (2020, March 16). European Data Protection Board. https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en#:%7E:text=COVID%2D19%20outbreak-,Statement%20by%20the%20EDPB%20Chair%20on%20the%20processing%20of%20personal,of%20the%20COVID%2D19%20outbreak&text=Andrea%20Jelinek%2C%20Chair%20of%20the,fight%20against%20the%20coronavirus%20pandemic.
3. Oviedo Convention

حقوق بشر و فن‌آوری‌های زیست پزشکی (۲۰۲۰-۲۰۲۵) این تبادل اطلاعات را تسهیل و چالش‌های اخلاقی مطرح‌شده در طی این بیماری همه‌گیر و پس‌ازآن را تجزیه‌وتحلیل می‌کند.[۱]

هر محدودیتی باید به اصل حق محدودشده احترام بگذارد. بنابراین محدودیت‌هایی که عمومی، گسترده یا متعارض باشند تا حدی که محتوای اصلی حق اساسی را باطل کنند، قابل توجیه نیستند و در صورت به خطر افتادن اصل حق، این محدودیت بدون نیاز به ارزیابی بیشتر در مورد اینکه آیا منافع عمومی را تأمین می‌کند یا معیارهای ضرورت و تناسب را برآورده می‌کند، باید غیرقانونی تلقی شود.[۲]

مقررات GDPR انعطاف‌پذیری لازم را برای تصویب قوانین مناسب در شرایط اضطراری فراهم می‌کند. طبق بند ۱ ماده ۲۳ GDPR، حقوق داده‌های شخصی ممکن است به دلایل بهداشت عمومی محدود شود. ماده ۱۵ دستورالعمل حریم خصوصی الکترونیک[۳] در اتحادیه اروپا نیز به‌طور استثنایی به مقامات اجازه می‌دهد تا از طریق ارائه‌دهندگان خدمات مخابراتی به داده‌های ترافیکی و مکان‌محور اشخاص حقیقی در تهدیدات علیه امنیت عمومی یا ملی یا پیشگیری، تعقیب، تحقیق و مجازات جرائم جدی، دسترسی پیدا کرده و پردازش کنند. چنین پردازش‌هایی برای حمایت از حقوق و منافع دیگران نیز مجاز است. هرگونه تخفیف یا محدودیت باید با منشور اروپایی حقوق بشر مطابقت داشته باشد، به اصل حقوق و آزادی‌های موردنظر احترام گذاشته و لازم و متناسب باشد (EUAFR v.2, 2020: 54).

شواهد نشان می‌دهد که به‌طور تقریبی همه مقامات حفاظت از داده‌های اتحادیه اروپا[۴] رهنمودهای مربوط به بیماری همه‌گیر را صادر کرده‌اند.[۵] این بیانیه‌ها مجدداً تأیید می‌کنند که حقوق بهداشتی و حفاظت از اطلاعات شخصی دست‌به‌دست هم می‌دهند و با یکدیگر تعارضی ندارند. آن‌ها همچنین تأکید می‌کنند که هر اقدامی که موجب نقض حقوق زندگی خصوصی و حفاظت از داده‌ها شود، باید قانونی، لازم و متناسب باشد (EUAFR v.1, 2020: 41).

---

1. EU Committee on Bioethics (DH-BIO). (2020, April 14). DH-BIO statement on human rights considerations relevant to the COVID-19 pandemic. Council of Europe. https://rm.coe.int/09000016809e2785

2. European Data Protection Board. (2020, June 3). Statement on restrictions on data subject rights in connection to the state of emergency in member states. https://edpb.europa.eu/our-work-tools/our-documents/other/statement-restrictions-data-subject-rights-connection-state_en

3 . ePrivacy

4. DPA

۵. برای مشاهده رهنمودهای مقامات حفاظت از داده‌ها در کشورهای مختلف رجوع کنید به مجله Coronavirus pandemic in the EU - fundamental rights implications - bulletin 1 صفحات ۴۴ الی ۴۶.

مؤسسه حقوقی اروپا (ELI) که موسسه‌ای غیرانتفاعی برای مطالعه، پژوهش ارائه دستورالعمل‌ها و توصیه‌نامه‌هایی برای یکپارچه‌سازی قواعد حقوقی اتحادیه اروپا است، در ۱۵ اصل توصیه‌هایی قانونی برای کشورهای عضو اتحادیه اروپا، در راستای مقابله با بیماری همه‌گیر کووید-۱۹ بیان می‌کند: یا در اصل ۶ با عنوان «حریم خصوصی و حفاظت از داده‌ها» بیان می‌کند:

۱- دولت‌ها باید اطمینان حاصل کنند که مقامات دولتی و کارفرمایان، مطابق با مقررات عمومی حفاظت از داده‌ها، سایر قوانین و مقررات حفاظت از داده‌ها و منشور حقوق اساسی اتحادیه اروپا، مجاز به پردازش داده‌های شخصی (ازجمله داده‌های مخابراتی)، تا آنجا که برای کاهش COVID-19 لازم است، هستند. بااین‌حال، چنین پردازشی باید به حداقل برسد و تا جای ممکن بجای پردازش داده‌ها در سطح وسیع، راه‌حل‌های مصداقی مطابق با اصل تناسب ترجیح داده شوند.

۲- پردازش داده‌های حساس، مانند داده‌های بهداشتی یا به‌ویژه انواع پردازش‌های سرزده و بدون اطلاع قبلی، مانند استفاده از ردیابی جغرافیایی و پیگیری جغرافیایی، باید برای تأیید به مقامات حفاظت از داده ارسال شود و کد منبع هرگونه برنامه باید حداقل برای طیف وسیعی از سازمان‌های غیردولتی مستقل برای بررسی فاش شود. استفاده از چنین برنامه‌هایی باید براساس رضایت آزادانه یا درصورت اجباری بودن، براساس یک عمل پارلمانی باشد که شرایط را مطابق با قانون مربوطه به‌وضوح مشخص کند. همه اقدامات انجام‌شده توسط دولت‌ها باید از روش اروپایی پیروی کنند، به‌ویژه در مورد برنامه‌های تلفن همراه.

۳- در هر صورت، داده‌های جمع‌آوری‌شده بر اساس چنین اقدامات خارق‌العاده‌ای باید پس از پایان بحران COVID-19 کاملاً ناشناس یا پاک شوند و هر نرم‌افزاری که اجازه جمع‌آوری داده‌ها را داشته باشد باید غیرفعال شود. این اقدامات باید بدون آسیب زدن به داده‌ها انجام شوند، مانند ماده ۸۹ GDPR، با ضمانت‌های مناسب (European Law Institute, 2020: 5).

بنابراین به‌طور اجمالی اصول کلی حفاظت از داده‌ها که به‌طور خاص در بحران کووید-۱۹ باید رعایت شوند، عبارت‌اند از:

- محدود بودن جمع‌آوری و پردازش داده‌ها برای تحقق هدف مشخص و به حداقل رساندن جمع‌آوری و پردازش داده‌ها برای تحقق اهداف مشروع: جمع‌آوری، استفاده، به اشتراک‌گذاری، ذخیره‌سازی و سایر پردازش‌های داده‌های بهداشتی باید محدود به موارد ضروری برای مبارزه با ویروس باشد. همه‌گیری بهانه‌ای برای جمع‌آوری اطلاعات گسترده و غیرضروری نیست.

- محدودیت دسترسی و امنیت داده‌ها: دسترسی به داده‌های بهداشتی فقط به افرادی که برای انجام درمان، تحقیق و یا در غیر این صورت رفع بحران به اطلاعات نیاز دارند محدود می‌شود. اطلاعات باید به‌صورت ایمن و در یک پایگاه داده جداگانه ذخیره شود.
- نگهداری داده‌ها و تحقیقات آینده: داده‌های پردازش‌شده در پاسخ به بحران باید فقط برای مدت‌زمان بحران نگهداری شوند. پس‌ازآن، بیشتر داده‌های بهداشتی پاک می‌شود، اگرچه برخی از اطلاعات غیرقابل‌شناسایی را می‌توان برای اهداف تاریخی و تحقیقاتی نگهداری کرد. این اطلاعات باید در دسترس باشد و برای این اهداف عمومی استفاده شود.
- داده‌های بهداشتی نباید فروخته شوند: تحت هیچ شرایطی نباید داده‌های بهداشتی فروخته یا به اشخاص ثالثی که به مصالح عمومی کار نمی‌کنند منتقل شود (Access Now, 2020: 9).

علاوه بر بیانیه‌هایی که به‌طورکلی و عام ناظر بر حفاظت از داده‌ها رهنمودهایی ارائه داده بود، نهادهای مرتبط، رهنمودها و بیانیه‌های مختلفی در حفاظت از داده‌ها به‌صورت موضوعی و تخصصی نیز صادر کرده‌اند. برنامه‌های ردیابی تماس فقط یکی از فن‌آوری‌هایی است که توسط دولت‌ها و شرکت‌ها برای مهار همه‌گیر استفاده می‌شود. نقشه راه مشترک اروپا همچنین پردازش داده‌های کلی و ناشناس از شبکه‌های اجتماعی و اپراتورهای شبکه تلفن همراه را به‌عنوان بخشی از راه‌حل برای جلوگیری از همه‌گیری پذیرفته است. این پردازش می‌تواند الگوها و روندهای تحرک اجتماعی را نشان دهد و می‌تواند برای پیش‌بینی‌های ریاضی شیوع ویروس مفید باشد. ابزارهای دیگری که داده‌های کاربران را پردازش می‌کنند عبارت‌اند از: برنامه‌های خود اظهاری بهداشت و وب‌سایت‌هایی که مشاوره و ارتباط با مقامات بهداشتی را ارائه می‌دهند، که ممکن است شامل انتقال داده‌های بیومتریک باشد. دسترسی به مکان و داده‌های ترافیکی افراد برای ردیابی افراد در قرنطینه؛ استفاده از هواپیماهای بدون سرنشین برای نظارت بر اقدامات فاصله‌گذاری فیزیکی و دوربین‌های حرارتی، به‌ویژه برای نظارت بر دمای کارکنان در محل کار (EUAFR v.2, 2020: 41).

این ابزارها همچنین مسائل مربوط به حفظ حریم خصوصی و حفاظت از داده‌ها را مطرح می‌کنند. برای مثال، در اسپانیا، برنامه‌های خودارزیابی نگرانی‌هایی را در مورد امکان افشای موقعیت جغرافیایی کاربر و جمع‌آوری داده‌های شخصی مانند شماره تلفن‌های همراه ایجاد می‌کنند. اداره حفاظت از داده‌های اسپانیا با تأکید بر اینکه بحران COVID-19 نباید منجربه تعلیق حقوق حفاظت از داده شود، اصولی را که این برنامه‌ها باید رعایت کنند، ارائه داد. در کرواسی، کارشناسان موضوعات مرتبط با اشتراک اجباری شماره تلفن همراه کاربران و عدم شفافیت در دسترسی به حقوق، دوره‌های ذخیره‌سازی، پردازش داده‌های به اشتراک گذاشته‌شده و اهداف پردازش را برجسته کردند. کمیسر فدرال

آلمان برای حفاظت از داده‌ها بر لزوم تعیین اهداف پردازش داده‌ها و سایر اصول حفاظت از داده‌ها، مانند دوره‌های ذخیره‌سازی، تأکید کرد. کارشناسان فنی همچنین نگرانی‌های خود را در مورد این برنامه ابراز داشتند مقامات بهداشتی سوئد پس از ابراز نگرانی مقامات و کارشناسان، ابزاری را برای نقشه‌برداری از افراد با علائم COVID-19 متوقف کردند (EUAFR v.2, 2020: 54).

اتحادیه اروپا حتی در این زمینه توصیه‌نامه‌هایی تصویب کرده است به‌عنوان‌مثال: «توصیه کمیسیون 2020/518 (EU) از ۸ آوریل ۲۰۲۰ در مورد یک جعبه‌ابزار مشترک در اتحادیه، برای استفاده از فن‌آوری و داده‌ها برای مبارزه و خروج از بحران COVID-19، به‌ویژه در مورد برنامه‌های تلفن همراه و استفاده از داده‌های جابه‌جایی ناشناس»[1].

۳-۲. حفاظت از داده در بحران همه‌گیری کووید-۱۹ در ایران

در طی همه‌گیری، ممکن است برخی حقوق اساسی شهروندان با یکدیگر پیدا کنند، برای مثال اولویت حق بر سلامتی برجسته‌تر شود و با حقوق مرتبط با حفاظت از داده‌ها تعارض پیدا کند. اما انتظار می‌رود که حقوق اساسی متعارض، در برابر یکدیگر متعادل شوند. اما نکته اساسی این است که آیا نتیجه متعادل‌سازی بین حق بر سلامتی و حق حریم خصوصی باید محدودیت مورد دوم باشد؟ اگر چنین است، آیا این محدودیت ازنظر زمانی موقت، متناسب و محدود می‌باشد؟ البته ایجاد نقطه تعادل جدید زمانی مطرح می‌شود که اصل تعارض حقوق در شرایط اضطراری را بپذیریم که خود محل مناقشه است.

در نظام حقوقی ایران که مطابق با اصل چهارم قانون اساسی مطابق بر موازین شرع می‌باشد، تزاحم میان حریم خصوصی با حق بر سلامتی را می‌توان با مراجعه به قواعد فقهی برطرف کرد. با دلالت یابی از حکومت قاعده لاضرر بر قاعده سلطنت این تزاحم برطرف و حدود تحدید حریم خصوصی مشخص می‌شود. قاعده تسلیط یکی از مبانی اصلی حمایت از حریم خصوصی در اسلام است (حسینی و برزویی، ۱۳۹۶: ۱۲۰). مطابق با قاعده تسلیط هر شخصی بر اموال خود تسلط کامل دارد و می‌تواند در آن هر نوع تصرف حقوقی و مادی انجام دهد (انصاری، ۱۳۷۴: ۳۲۰). از طرفی قاعده لاضرر، دلالت بر نفی ضرر مادی و معنوی به دیگران و نفی حکم ضرری دارد در فقه شیعه قاعده لاضرر بر قاعده تسلیط حکومت دارد، به این معنا که در مقام تزاحم، قاعده تسلیط و حقوق مالکانه محدود می‌شود و مانع ضرر به دیگری می‌شود (محقق داماد، ۱۳۷۸: ۱۵۴). در خوانش امام خمینی (ره) از اصل لاضرر، ابعاد حکومتی آن برجسته شده است و حاکم می‌تواند در مواردی که ضرری عمومی به جامعه وارد می‌شود، مداخله کرده و مانع از آن شود (خمینی، ۱۳۸۵: ۶۳)،

1. www.data.europa.eu/eli/reco/2020/518/oj

برای نمونه در بحران همه گیری ویروس کووید-۱۹، حاکم جامعه می‌تواند برای جلوگیری حداکثری از آسیب های این همه گیری، محدودیت‌هایی را وضع کند. صیانت از حریم خصوصی در همه‌گیری کووید-۱۹، ممکن است در برخی از موارد منجربه آسیب رسیدن به سلامت عمومی جامعه شود، بنابراین در حد ضرورت و با رویکرد مضیق می‌توان حریم خصوصی افراد را به نفع سلامت عمومی جامعه، محدود کرد.

تزاحم میان حق‌ها و نظم عمومی امری انکارناپذیر است. مسئله نظم عمومی ایجاب می‌کند که برخی محدودیت‌ها در حد الزامات مربوط به نظم عمومی به‌صورت مقید و البته متناسب برای آزادی وجود داشته باشد. به این ترتیب که اگر تزاحم نظم عمومی و آزادی‌های مشروع رخ داد، گام اول یافتن راهکاری برای تضمین نظم عمومی بدون تحدید و سلب و آزادی‌های مشروع است، البته در هیچ حالتی وفق اصل نهم قانون اساسی امکان سلب وجود ندارد، ولی امکان تحدید بر اساس قاعده تناسب - «ما ابیح للضروره یقدر بقدرها» - به‌قدر ضرورت وجود دارد (بحرانی، ۱۴۱۹: ۴۳۴).

با وجود اینکه به‌موجب اصل نهم از قانون اساسی سلب آزادی‌های مشروع مردم منع شده است، اما تزاحم حق‌ها و آزادی‌ها با نظم عمومی رویدادی انکارناپذیر است. پذیرش وضعیت اضطراری در بسیاری از کشورها مبین این تزاحم می‌باشد (غمامی و نیکونهاد، ۱۳۹۷: ۱۲۹). اصل هفتادونهم قانون اساسی با شرایطی اجازه محدود کردن آزادی ملت را به مجلس داده است. اما بیان این نکته ضروری می‌باشد که با توجه به اصول مختلف قانون اساسی نمی‌توان صلاحیت محدود کردن آزادی‌های مردم را محدود به مصوبات مجلس شورای اسلامی‌دانست؛ چراکه به موجب بند «۳» اصل یکصد و هفتادوششم، می‌توان یکی از صلاحیت‌های شورای عالی امنیت ملی را ایجاد محدودیت نسبت به آزادی‌های مردم در جهت حفظ امنیت داخلی یا خارجی کشور دانست. درنتیجه مرجع صالح برای وضع این محدودیت‌ها تنها مجلس شورای اسلامی نیست. علاوه بر این موارد، با عنایت به جایگاه و مفهوم ولایت مطلقه فقیه در اصل پنجاه وهفتم باید پذیرفت که ولی فقیه نیز صلاحیت ایجاد چنین محدودیت‌هایی را درچارچوب موازین شریعت دارد.[1] البته این اصول که استثنا بر اصل نهم قانون اساسی هستند و در نظام‌های مردم سالار باید به‌صورت کاملاً دقیق تفسیر شوند.

امکان و حدود محدودیت حریم خصوصی، براساس استدلال های پیش گفته باید براساس تفسیری دقیق تبیین شود؛ چراکه نخست براساس اصول نهم و هفتادونهم قانون اساسی، اصل رعایت کامل حریم خصوصی افراد است و در شرایط عادی حتی مجلس شورای اسلامی نیز نمی‌تواند حقوق و آزادی های مشروع را محدود کند، دوماً اقتضای استثنا بودن شرایط اضطراری در اصل هفتادونهم،

1. www.vasael.ir/0001qu

محدودیت حداکثری از حیث زمانی و دامنه استثنائات را به‌همراه دارد. سوماً در اصول فقه شیعی تخصیص اکثر، یا به‌عبارت دیگر غلبه استثنا بر قاعده، امری قبیح است و هرچه یک قاعده استثنا بیشتری داشته باشد، قبیح‌تر می‌باشد (عراقی، ۱۴۱۷: ۱۶۷)؛ بنابراین باید تا جای ممکن قاعده اصلی که رعایت حریم خصوصی افراد است، مورد توجه قرار گیرد و در مواردی‌که هیچ راهکار آسان یا دشواری برای جمع میان صیانت از سلامت عمومی و حفظ حریم خصوصی وجود ندارد، اقدام به محدودیت حریم خصوصی کرد.

در بحران همه گیری ویروس Covid-19 در جمهوری اسلامی ایران، ستاد ملی مقابله با کرونا ذیل شورای عالی امنیت ملی و در اوایل اسفندماه ۱۳۹۸ ایجاد شد که مسئول عالی مقابله با همه گیری کووید-۱۹ است. این ستاد تصمیمات مختلفی داشته است که در مبارزه با همه گیری کووید-۱۹ به واسطه حفظ سلامت عمومی، به محدودیت حق‌ها و آزادی‌های شهروندان منجر شده است، مانند مصوبات ناظر بر محدودیت‌های تردد برون مرزی، محدودیت‌های تردد بین شهری و محدودیت‌های تردد شبانه درون‌شهری که در جلسات مختلف ستاد ملی مقابله با بیماری کرونا تصویب و تمدید شده است.[۱] حمایت از خانوارها در زمینه اجاره املاک ساختمانی که منجربه محدودیت حقوق و آزادی‌های مؤجر می‌شود[۲]، تعویق یک ماهه در صدور گواهینامه عدم پرداخت و برگشت چک که منجربه محدودیت حقوق طلبکاران می‌شود.[۳] تمام مصوبات مذکور می‌تواند حقوق و آزادی‌های عده از شهروندان را محدود کند، اما برخی مصوبات این ستاد اثر قابل‌توجهی بر محدودیت حریم خصوصی و حفاظت از داده‌ها دارد، ازجمله مصوبه جلسه ۵۹ ستاد مقابله با کرونا که کنترل بیشتر تردد در مبادی ورودی کشور، ورود ایمن مسافران ایرانی به کشور (که نیازمند معاینات پزشکی یا بررسی سوابق پزشکی است) و ردیابی ویروس جهش یافته در جهان و کشورهای همسایه را شامل می‌شود.

جمهوری اسلامی ایران، پس از چین، از نخستین کشورهایی بود که به‌صورت جدی با بحران همه‌گیری کووید-۱۹ در جهان مواجه شد. اما تاکنون سندی از جنس قوانین، مقررات، بیانیه رسمی یا دستورالعملی در خصوص الزامات حفاظت از داده‌ها در جریان بحران همه‌گیری کووید-۱۹ در ایران منتشرنشده است. دلیل عمده عدم ایجاد چنین سندی در کشور، عدم وجود نظام حقوقی

---

۱. محدودیت های ناظر بر تردد در مصوبات مختلف ستاد ملی مقابله با کرونا، مورد اشاره قرار گرفته است ازجمله در مصوبات جلسات ۸۱، ۵۹، ۵۰ و سایر جلسات. قابل‌مشاهده در سایت www.coronomy.ir

۲. مصوبه جلسه ۷۲ ستاد ملی مقابله با کرونا

۳. مصوبه جلسه ۷۱ ستاد ملی مقابله با کرونا

منسجم حفاظت از داده‌ها و حریم خصوصی در کشور می‌باشد. بنابراین دور از ذهن است، دولتی که در ارتباط با شرایط عادی در موضوعی قانون‌گذاری و قاعده گذاری حقوقی نکرده است، در ارتباط با شرایط بحران و شرایط اضطراری در آن موضوع قاعده گذاری کرده باشد. از طرف دیگر دلیل دیگری که می‌توان برای عدم ایجاد چنین سندی در ایران ذکر کرد، بیان این واقعیت است که در مقابله با بحران همه‌گیر کووید-۱۹ راهکارهای مبتنی بر فناوری اطلاعات و پردازش داده، نسبت به سایر کشورها، در ایران به‌صورت جدی استفاده نشده است و اگر هم استفاده شده باشد، به‌صورت عمومی اعلام و شفاف‌سازی نشده است. بنابراین در بررسی وضعیت حفاظت از داده در بحران کووید-۱۹ در ایران به علت عدم وجود سند رسمی در این حوزه به‌ناچار به تحلیل اخبار و مصاحبه‌های مقامات مسئول اکتفا می‌شود.

اخیراً اقداماتی از سوی دولت در بهره‌گیری از ظرفیت فناوری اطلاعات و ارتباطات برای پیشگیری و مهار همه‌گیری کووید-۱۹ شروع‌شده است (آذرماه ۱۳۹۹). برای مثال در جلسه مشترک وزیر ارتباطات و فناوری اطلاعات و وزیر بهداشت، درمان و آموزش پزشکی مصوب شد تا کمیته فناوری اطلاعات ذیل ستاد ملی مبارزه با کووید-۱۹ فعالیت خود را آغاز کند.

همچنین در ۱۳۹۹/۸/۱، معاون وزیر بهداشت در نشست تلویزیونی بیان کرد: «باید افراد مبتلابه ویروس کووید-۱۹ را زود پیدا کرده و اطرافیان آن‌ها را هم شناسایی کنیم و اگر این فرد جایی رفته و برگشته، باید ردیابی شده و افراد را پیدا کنیم که به همین منظور با هماهنگی وزارت ارتباطات، ردیابی هوشمند از این هفته اجرا می‌شود.» در ادامه وی افزود: «آزمایشگاه‌های کشور به یکدیگر متصل شده‌اند. آزمایشگاه‌های خصوصی و دولتی که آزمون کووید-۱۹ انجام می‌دهند، جواب آزمون در پرونده الکترونیک او ثبت‌شده و به روز و مراقب سلامت مشاهده می‌کند که چه کسانی مبتلا شده‌اند».[1]

در تاریخ ۱۳۹۹/۸/۱ زالی، فرمانده ستاد مقابله با بیماری کووید-۱۹ در تهران، بیان کرد: «طی توافق صورت گرفته، ردیابی و غربال‌گری افرادی که تستشان مثبت شده و همراهانشان با استفاده از ظرفیت وزارت ارتباطات انجام خواهد شد. پایلوت این طرح انجام‌شده و تاکنون ۴۹ هزار بیمار براساس محل سکونت ردیابی شده‌اند. طبق آمار مرحله نخست، تراکم بیماران در شرق، جنوب شرقی و مرکز استان وجود دارد و این الگو در موج اول، دوم و سوم تکرار شده است».[2]

حسن روحانی رئیس‌جمهور وقت، در جلسه هیئت دولت در تاریخ ۱۳۹۹/۸/۱، بیان کرد ره‌گیری هوشمند و ایجاد محدودیت‌های هدفمند برای کسانی‌که دوران قرنطینه را سپری می‌کنند، ضروری

1. www.donya-e-eqtesad.com/fa/tiny/news-3704472
2. www.irna.ir/news/84085633/

است.[1] علیرضا رئیسی معاون بهداشت وزیر بهداشت در جلسه ستاد ملی مقابله با کووید-۱۹ در تاریخ ۱۳۹۹/۸/۱۳ نتایج تکان‌دهنده یک ردیابی الکترونیکی ۱۵ هزار بیمار مثبت کووید-۱۹ را ارائه کرد و گفت: «نزدیک به ۲۰ درصد مبتلایان مطلقاً قرنطینه را رعایت نکرده‌اند».[2]

با رصد اظهارات مقامات در این موضوع مشخص می‌شود اقداماتی برای بهره‌گیری از فناوری اطلاعات و ارتباطات در مقابله با بحران کووید-۱۹ در سطح حاکمیتی وجود دارد، اما متأسفانه به علت عدم شفافیت و نبود زیرساخت و الزام قانونی امکان رصد و تحلیل وضعیت حفاظت از داده‌ها در این حوزه میسور نیست.

در بخش غیردولتی نیز اقداماتی در راستای مقابله با ویروس کووید-۱۹ صورت پذیرفته است. برجسته‌ترین اقدام، راه‌اندازی نرم‌افزار «ماسک» توسط گروهی در دانشگاه شریف با رویکردی غیرانتفاعی می‌باشد که علاوه‌بر اطلاع‌رسانی نکات بهداشتی، از امکانات دیگری مانند خوداظهاری سلامت، ره‌گیری تماس و نقشه انتشار ویروس کووید-۱۹ برخوردار می‌باشد. این نرم‌افزار در صفحه اینترنتی خود اقدام به انتشار سیاست حریم خصوصی خود کرده است. در این صفحه بیان شده است که توسعه‌دهندگان ماسک تعهد می‌دهند که داده‌های کاربران را تنها برای کنترل شیوع کووید-۱۹ استفاده کنند و هم چنین تعهد به محرمانه بودن داده‌ها و صیانت از آن‌ها را بیان کرده‌اند. هم‌چنین بیان شده است که این نرم‌افزار تنها به داده‌هایی که خود کاربر اجازه بدهد، دسترسی دارد. هم‌چنین کمیته‌ای متشکل از نمایندگان تعدادی از نهادهای تخصصی علمی، مدنی و مستقل کشور بر رعایت اصول حفاظت از داده‌ها در این نرم‌افزار نظارت می‌کنند. هم‌چنین در این صفحه بیان شده است مالکین نرم افزار، حتی اجازه استفاده از اطلاعات بی‌هویت شده کاربران برای مقاصد علمی را هم نمی‌دهد. توسعه‌دهندگان تلاش خواهند کرد تا در نخستین فرصت بی‌فایده شدن اطلاعات کاربران از حیث مبارزه با کووید-۱۹، آن‌ها را حذف کند. هم‌چنین درصورت صدور دستور قانونی از سوی مراجع قضایی، توسعه‌دهندگان موظف به ارائه اطلاعات کاربران به دادگاه خواهند بود.[3] توسعه‌دهندگان ماسک با وجود عدم الزام قانونی در کشور، اقدام به اعلام تعهدات داوطلبانه در رعایت قواعد حفاظت از داده‌های کاربران کردند که از نظر حقوقی این اقدامات را برای آن‌ها الزام‌آور می‌کند.

---

1. www.president.ir/fa/117901
2. www.yjc.ir/00VfRu
3. www.mask.ir/privacy.html

نتیجه‌گیری

بحران‌ها و شرایط اضطراری یکی از محک‌های کارامدی نظام‌های حقوقی در موضوعات مختلف است. تاکنون، بحران همه‌گیری ویروس کووید-۱۹ جدی‌ترین محک برای نظام‌های حقوقی حفاظت از داده‌ها محسوب می‌شود. نظام حفاظت از داده‌ها در اتحادیه اروپا که براساس مقررات GDPR بنا شده است، به خوبی توانست تعادلی بین حقوق مرتبط با حفاظت از داده و حریم خصوصی با کنترل همه‌گیری و مبارزه با بحران کووید-۱۹، ایجاد کند. نهادهای مختلف حفاظت از داده‌های در اتحادیه اروپا در مواجهه با بحران کووید-۱۹ اقدام به صدور بیانیه‌ها و دستورالعمل‌هایی برای حفاظت از داده‌ها به‌صورت عام و به‌صورت خاص در حوزه‌های مشخصی مثل، نرم‌افزارهای رهگیری تماس، آموزش مجازی، حفاظت از داده‌های کارکنان شرکت‌ها، حفاظت از داده‌ها در خوداظهاری سلامت و موضوعات متنوعی کرده‌اند. این اقدامات منجربه قاعده مند کردن و منظم کردن حفاظت از داده‌ها در بحران همه‌گیری شده است و موجب شد که نتوان به بهانه حفظ سلامت عمومی، حریم خصوصی و الزامات حفاظت از داده‌ها را نقض کرد. در همین زمینه، پروژه‌های ایجابی مختلفی برای انطباق‌پذیری روش‌های تکنولوژیک مقابله با کووید-۱۹ با الزامات حفاظت از داده‌ها تعریف شده است. ازجمله فناوری Apple/Google ENS و پروژه PEPP-PT. در واقع در اتحادیه اروپا نظام حقوقی به‌صورت کاملاً پویا با بحران همه‌گیری ویروس کووید-۱۹ مواجه شد و قوانین خود در حوزه حفاظت از داده را در موضوعات و پروژه‌های مختلف تطبیق و تعمیم داده است.

نظام حقوقی ایران خلأ جدی قانونی در زمینه حفاظت از داده‌ها دارد که مشکلات عدیده‌ای ازجمله نقض حریم خصوصی و تهدیدات امنیت سایبری برای کاربران در سطح ملی ایجاد کرده است و به‌سبب عدم وجود قانون، بی نظمی در این حوزه حاکم می‌باشد و اقدامات چارچوب حقوقی مشخصی ندارد. از طرفی عدم توجه به قانون‌مند کردن حفاظت از داده‌ها، علاوه‌بر خسارت‌های مهمی که در بُعد داخلی دارد، ممکن است مشکلات مختلفی در آینده برای تعاملات تجاری و اقتصادی بین‌المللی کشور ایجاد کند. بنابراین قاعده‌مند کردن حریم خصوصی و حفاظت از داده‌ها از طریق تقنین یکی از اولویت‌های اجتناب‌ناپذیر کشور در برنامه بلندمدت، با درنظر گرفتن الزامات شرعی و بومی می‌باشد.

اما در مواجهه با بحران کووید-۱۹ نظام حقوقی ایران تدبیری برای برقراری تعادل میان حفاظت از داده‌ها و حریم خصوصی با حق بر سلامتی و ایجاد شرایط اضطراری درنظر نگرفته است. پیشنهاد می‌شود در وهله نخست توجه بیشتری به راه‌کارهای فناوری‌محور برای مقابله با بحران کووید-۱۹

صورت پذیرد، ازجمله نرم‌افزارهای ردیابی تماس و ایجاد قرنطینه هوشمند. در گام بعد نهادهای مسئول برنامه موقتی در رعایت الزامات حفاظت از داده‌ها و رعایت حریم خصوصی شهروندان در بحران کووید-۱۹ تدارک ببینند. به‌طور خاص پیشنهاد می‌شود کمیته فناوری اطلاعات ستاد ملی مقابله با کووید-۱۹، دستورالعملی در حفظ حریم خصوصی و حفاظت از داده‌ها برای نهادهای دولتی و خصوصی تهیه و ابلاغ کند.

منابع

فارسی

- انصاری، شیخ مرتضی (۱۳۷۴)، **فرائد الاصول (الرسائل)**، قم: انتشارات مصطفوی.
- بحرانی، احمد بن صالح (۱۴۱۹)، **الرسائل الاحمدیه**، جلد دوم، قم: دارالمصطفی لاحیاء التراث.
- بخشی‌پور، معصومه (۱۳۹۹)، **جایگاه ضعیف ایران در حفاظت از اطلاعات کاربران**، بازیابی از سایت خبرگزاری مهر: https://www.mehrnews.com/xS5hS
- جلیلی, میترا (۱۳۹۷)، **با اجرای قانون «حفاظت از اطلاعات عمومی» (GDPR) حریم خصوصی در اروپا امن‌تر می‌شود**، بازیابی از روزنامه ایران:
https://www.irannewspaper.ir/newspaper/item/469092
- حسینی، مهدی؛ برزویی، محمدرضا (۱۳۹۶)، «مبانی و مولفه های فقهی حمایت از حریم خصوصی افراد در فضای مجازی»، **دوفصلنامه مطالعات حقوق بشر اسلامی**، سال ششم، شماره سیزدهم، صفحات ۱۱۵-۱۳۷.
- خمینی، روح الله (۱۳۸۵)، **رسائل**، قم: مؤسسه اسماعیلیان.
- عراقی، ضیاء الدین (۱۴۱۷)، **نهایة الأفکار**، جلد چهارم، قم: مؤسسه نشر اسلامی.
- غمامی، سید محمد مهدی و نیکونهاد، حامد (۱۳۹۷)، **شرح قانون اساسی؛ فصل اول: اصول کلی**، تهران: پژوهشکده شورای نگهبان.
- قربان‌نیا، ناصر (۱۳۸۶)، «تعلیق اجرای حقوق بشر در شرایط اضطراری»، **مجله حقوق اسلامی**، سال سوم، شماره ۱۲، ۳۷-۶۲.
- کرمی، رضا؛ شریفی طرازکوهی، حسین (۱۳۹۷)، «آزادی رسانه و وضعیت اضطراری در نظام حقوق بشر پس ازیازدهم سپتامبر»، **جستارهای سیاسی معاصر**، سال نهم، شماره دوم، صفحات ۱۶۱-۱۸۶.
- محسنی، فرید (۱۳۹۴). **حریم خصوصی اطلاعات: مطالعه کیفری در حقوق ایران، ایالات‌متحده آمریکا و فقه امامیه**، تهران: انتشارات دانشگاه امام صادق (ع).
- محقق داماد، مصطفی (۱۳۷۸)، **قواعد فقه**. تهران: مرکز نشر علوم اسلامی تهران.
- نوری، محمد علی؛ نخجوانی، رضا (۱۳۹۰)، **حقوق تجارت الکترونیک**. تهران: گنج دانش.
- وزارت ارتباطات و فناوری اطلاعات. (۱۳۹۷/۵/۶)، **لایحه «صیانت و حفاظت از داده‌های شخصی» رونمایی شد**، بازیابی از سایت وزارت ارتباطات و فناوری اطلاعات:
https://www.ict.gov.ir/fa/newsagency/21691/

انگلیسی

- Bock, K., Kühne, C. R., Mühlhoff, R., Ost, M. R., Pohle, J., & Rehak, R. (2020), Data Protection Impact Assessment for the Corona App. Available at SSRN 3588172.
- Bradford, L. R., Aboy, M., & Liddell, K. (2020), COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes. Journal of Law and the Biosciences.
- Council of Europe (2020), Joint statement on the right to data protection in the context of the COVID-19 pandemic, 30 March 2020.
- EC, European Commission. (2012), Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the

Processing of Personal Data and on the Free movement of Such Data (General Data Protection Regulation). Brussels: European Commission.

- EU Committee on Bioethics (DH-BIO), (2020), DH-BIO statement on human rights considerations relevant to the COVID-19 pandemic. Council of Europe. https://rm.coe.int/09000016809e2785
- European Data Protection Board. (2020), Statement on restrictions on data subject rights in connection to the state of emergency in member states. https://edpb.europa.eu/our-work-tools/our-documents/other/statement-restrictions-data-subject-rights-connection-state_en
- European Data Protection Board (2020), Statement on the processing of personal data in the context of the COVID-19 outbreak, 19 March 2020.
- European Law Institute. (2020, May). ELI PRINCIPLES FOR THE COVID-19 CRISIS. ISBN: 978-3-9504549-4-9. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_for_the_COVID-19_Crisis.pdf
- European Union Agency for Fundamental Rights. (2020), Coronavirus pandemic in the EU - fundamental rights implications - bulletin 1 (No. 1). Publications Office of the European Union. https://doi.org/10.2811/009602
- European Union Agency for Fundamental Rights. (2020, April). Coronavirus pandemic in the EU - Fundamental Rights Implications - bulletin 2 (No. 2). Publications Office of the European Union. https://doi.org/10.2811/441998
- Global Privacy Assembly (2020), Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic.
- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (2020), European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf. P.5.
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. (2020), European Data Protection Board.https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en
- Karmer J. F., Hoar S. B. (2017), GDPR, part I: history of European Data Protection law, Lewis Brisbois law firm. Retrieved From. https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European _Data_Protection_Law
- Kittichaisaree, K. (2017), Public international law of cyberspace (Vol. 32).,Cham: Springer.
- Privacy and data protection in the age of COVID-19. (2020), Deloitte Touche Tohmatsu Limited. https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf
- Raul, A. C. (Ed.). (2020). The privacy, data protection and cybersecurity law review. Law Business Research Limited.
- Regulation, E. G. D. P. (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) 2016. OJ L, 119(1).

- Simmons, D. (2019), 10 Countries with GDPR-like Data Privacy Laws. Retrieved From. https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws
- Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. (2020, March 16). European Data Protection Board. https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en#:%7E:text=COVID%2D19%20outbreak-,Statement%20by%20the%20EDPB%20Chair%20on%20the%20processing%20of%20personal,of%20the%20COVID%2D19%20outbreak&text=Andrea%20Jelinek%2C%20Chair%20of%20the,fight%20against%20the%20coronavirus%20pandemic.
- UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available at: https://www.refworld.org/docid/453883f922.html
- Office of the High Commissioner for Human Rights of United Nations, & International Bar Association. (2003), Human Rights In The Administration Of Justice: A Manual On Human Rights For Judges, Presecutors And Lawyers (No. 9). New York and Geneva: United Nations.