

تاریخ دریافت: ۹۸/۱۱/۲۰

تاریخ پذیرش: ۹۹/۰۳/۱۷

نوع مقاله: پژوهشی

بررسی حقوقی رگولاتوری‌های حمایت از داده

نوشته

داود زارعیان *

فائزه واحد **

چکیده

با پیشرفت‌های بشری و افزایش سطح آگاهی اشخاص درباره حقوق اولیه خود، توجه به حفظ و نگهداری از داده‌های شخصی افزایش یافته است. اما در عین حال، زندگی در دنیایی که شکل جدیدی از ارتباطات را رقم می‌زند، بسترهای تحول‌یافته و مختلفی را برای نقض این حق به وجود می‌آورد. اگرچه قوانین و مقررات مربوط به حمایت از داده‌های شخصی و حفظ حریم خصوصی تلاش می‌کنند تا دایره شمول قواعد مذکور را با تحولات بشری منطبق سازند، اما اشکال جدید نقض حق، نیازمند بررسی‌های بیشتر و کارآمدتری است. چالش اصلی زمانی مطرح می‌شود که علاوه بر ظهور اشکال جدید نقض حریم خصوصی، ارتباطات گسترده و فراملی دایره نقض حق را گسترش داده و نیاز به اصولی را آشکار می‌سازد که جامع تمام تعاریف از حریم خصوصی باشد. بر همین اساس، ضروری است نهادی مستقل و حقوقی وجود داشته باشد تا با نظارت صحیح بر نحوه اجرای قواعد حمایت از داده، از نقض این حق جلوگیری کند؛ موضوعی که در بیشتر کشورهای دنیا مورد توجه قرار گرفته، ولیکن در نظام حقوقی ایران مغفول مانده است. لذا در این پژوهش نمونه‌های مشابه مورد مطالعه قرار گرفته و وضعیت ایران در مقایسه با آن‌ها بررسی و راهکار مناسب برای برطرف کردن این خلأ ارائه شده است.

کلیدواژه: رگولاتوری، داده، حمایت از داده، حریم خصوصی، اتحادیه اروپا، حقوق بشر، نظام حقوقی.

انقلاب ارتباطات و اطلاعات، به سرعت نظام‌های قانونی، اقتصاد، فرهنگ و سیاست جهان را دستخوش دگرگونی کرده است. در عصر حاضر، دسترسی به داده‌ها نوعی قدرت محسوب می‌شود و لذا توانایی تنظیم و نظارت بر این داده‌ها نیز رمز قدرت به شمار می‌آید. بررسی تحول‌های صورت گرفته در نظام حقوقی کشورهای پیشرو در زمینه صنعت فناوری اطلاعات و ارتباطات، نشان می‌دهد این کشورها به دنبال توسعه فناوری‌های اطلاعاتی و شکل‌گیری کسب و کارهای مبتنی بر داده، به سبب پیدایش چالش‌ها و مخاطرات گسترده‌ای در این زمینه، یک نهاد رسمی به عنوان "متولی داده" تشکیل داده‌اند. چراکه، کلان داده‌های به دست آمده از محتوای تولید کاربر در شبکه‌های اجتماعی، حاوی اطلاعات ارزشمندی است که تحلیل کمی و کیفی آن‌ها می‌تواند منجر به استخراج رفتار مصرف کننده و تأثیر آن بر فعالیت‌های تجاری شود (میربها، ۱۳۹۸: ۱۴۲). مسئولیت نهادهای متولی داده، تنظیم و نظارت بر حوزه داده، بر اساس قوانین و مقررات حمایت از داده است.

نتایج بررسی اسناد بالادستی و رویه‌های اجرایی کشور ایران، مؤید این مطلب است که در نظام حقوقی ایران، قانون جامعی در خصوص حمایت از داده‌ها وجود ندارد و بالطبع، نهادی هم متولی رسمی داده در کشور نیست. این امر، باعث شده تا علیرغم رشد فناوری‌های نوین، بسترهای قانونی مرتبط با حقوق داده در نظام حقوقی کشور تشکیل نشود؛ در نتیجه، رشد کسب و کارهای مبتنی بر داده نیز در ایران، به کندی صورت خواهد گرفت. بر همین اساس، بهره‌برداری مبتکرانه از ارزش سرمایه‌ای داده‌ها، مستلزم تصویب یک قانون جامع و متناسب با فناوری‌های نوین و همچنین وجود یک نهاد رسمی با نام رگولاتوری، به عنوان مجری این قانون، تنظیم کننده و ناظر بر حوزه حمایت از داده است. لذا می‌بایست در یک پژوهش کاربردی نخست ضرورت وجود چنین قانون و نهادی مورد واکاوی قرار گیرد و سپس پیشنهادهای لازم برای ارائه یک قانون جامع و مانع ارائه شود.

به عبارت دیگر، مسئله اصلی که ضرورت این پژوهش را بیش از پیش آشکار می‌سازد، وضعیت موجود کشور ایران، در مقایسه با سایر کشورهای جهان در زمینه ساز و کارهای قانونی و حقوقی پدیده‌ای تحت عنوان داده و اهمیت آن در گسترش کسب و کارهای جدید است. از آنجایی که میزان پیشرفت فناوری و وضعیت حقوقی و مقررات‌گذاری کشور ایران، در این زمینه بسیار عقب‌تر از سایر کشورها است، باید در این خصوص پژوهش‌های بیشتری، برای نیل به ساز و کار حقوقی مناسب انجام گیرد. موضوعی که از نظر پژوهشگران حقوقی مغفول مانده و تاکنون پژوهش کاربردی مؤثری در این زمینه صورت نگرفته است. چراکه اکثر حقوقدانان در شاخه‌های کلاسیک حقوق فعالیت می‌کنند و پژوهشگران حوزه فناوری نیز فاقد دانش حقوقی مناسب برای پرداختن به چنین موضوع‌هایی هستند. از این رو، این پژوهش به عنوان یک پژوهش میان‌رشته‌ای (حقوق،

فناوری، ارتباطات و اطلاعات) می‌تواند برای فعالان حوزه فناوری و حقوقدانان قابل استفاده باشد. در این پژوهش، ابتدا نتایج مطالعات تطبیقی صورت گرفته در خصوص نهاد متولی داده در چند کشور ارائه شده، سپس با توجه به دستاوردهای مطالعات تطبیقی و همچنین وضعیت موجود کشور، پیشنهادهایی در خصوص ایجاد یا تعیین نهاد متولی داده در نظام حقوقی ایران ارائه می‌شود. در نهایت موضوع رگولاتوری حمایت از داده، در پیش‌نویس حمایت از داده وزارت ارتباطات مورد بررسی قرار خواهد گرفت.

مطالعه تطبیقی

از نقطه نظر تاریخی، شکل‌گیری نهادهای حمایت از داده را به طور گسترده، باید وام‌دار دستورالعمل ۱۹۹۵ اتحادیه اروپا با عنوان "حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده‌ها"^۲ دانست. اگرچه قبل از این دستورالعمل نیز کشورهای نظیر فرانسه از قانون حمایت از داده و به تبع آن، نهاد حمایت از داده برخوردار بودند، اما با تصویب این دستورالعمل توسط اتحادیه اروپا و الزام کشورها به رعایت آن، این امر فراگیری بیشتری یافت. در توضیح بیشتر باید گفت، یکی از اهداف اتحادیه اروپا هماهنگ ساختن مقررات کشورهای عضو است. آن‌ها موظف‌اند قوانین داخلی خود را، در صورت تعارض با قواعد اتحادیه اروپا، تغییر دهند و با اصول اتحادیه منطبق سازند و در صورت خلأ قانونی، با تصویب قانونی جدید این خلأ را برطرف کنند. از این رو و بر اساس دستورالعمل ۱۹۹۵، اتحادیه اروپا با عنوان "حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده‌ها"، تمام کشورهای عضو را ملزم به تصویب قانونی در حمایت از داده‌های شخصی کرده است. یکی از موارد مهمی که در قوانین حمایت از داده باید مورد توجه قرار گیرد، در نظر گرفتن نهادی، جهت نظارت بر اجرای صحیح قانون مذکور است. از طرف دیگر، این نهاد که معمولاً نهاد عمومی و دارای استقلال کامل است، این اطمینان را به اشخاص می‌دهد که سطح بالایی از حمایت در خصوص داده‌های شخصی در کشور آنها در جریان است.

بر اساس همین ضرورت، طبق ماده ۲۹^۳ دستورالعمل "حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده‌ها" مصوب ۱۹۹۵، کارگروهی^۴ برای حمایت از اشخاص در زمینه پردازش اطلاعات شخصی تشکیل شد. بر اساس قسمت الف از بند ۱ این ماده^۵، این کارگروه ملزم بود به هرگونه سؤالی در زمینه چگونگی اجرای این دستورالعمل پاسخ دهد و تمام تلاش خود را، جهت هماهنگی کشورهای عضو با این دستورالعمل به کار گیرد. همچنین این کارگروه بایستی گزارش‌های دوره‌ای خود را، راجع به وضعیت سایر کشورها در زمینه حمایت از داده‌های شخصی تهیه کرده و در صورت ضرورت اصلاح مصوبه‌های موجود را به کمیسیون اتحادیه اروپا ارائه می‌کرد (Article 29 working party archives 1997-2016). کمیسیون اروپایی اتحادیه

اروپا در سال ۲۰۱۲، دستورالعمل حمایت از داده‌های شخصی مصوب ۱۹۹۵ خود را بازنگری و اصلاحیه‌ای را در این خصوص تصویب کرد. این اصلاحیه که در سال ۲۰۱۶ اجرایی و از سال ۲۰۱۸ لازم‌الاجرا شده، دربرگیرنده مقررات کلی حمایت از داده‌ها و مسائل مربوط به سیاستگذاری و بخش مربوط به موضوع‌های کیفی است. این اصلاحیه شامل مهم‌ترین و بنیادی‌ترین حقوق شهروندان حوزه اتحادیه اروپا در عصر دیجیتال بوده و شامل کلیه فعالان این حوزه می‌شود. بر اساس این اصلاحیه که به طور خلاصه "مقررات عمومی حمایت از داده ۶" نامیده می‌شود، هیئت نظارت بر دادرسی اروپا ((The European Data Protection Board (EDPB) جایگزین کارگروه ماده ۲۹ خواهد شد. این هیئت، یک نهاد مستقل اروپایی است که در جهت تطابق قوانین حمایت از داده در سراسر اتحادیه اروپا و ارتقاء همکاری بین مقامات حمایت از داده در این اتحادیه فعالیت می‌کند. (Carticle 29 working party)

در ادامه، به برخی از مهم‌ترین نهادهای حمایت از داده در اتحادیه اروپا اشاره می‌شود. شایان ذکر است به دلیل اهمیت بالای اتحادیه اروپا در تبادل داده و سطح بالای حمایت از داده در این منطقه، کشورهای خارج از این اتحادیه نیز به صورت داوطلبانه خود را ملزم به رعایت مقررات این حوزه کرده و قوانین حمایت از داده خود را با "مقررات عمومی حمایت از داده" هماهنگ ساخته‌اند. از این رو، ابتدا به دو کشور فرانسه (داخل در اتحادیه) و کره جنوبی (خارج از اتحادیه) به طور مفصل پرداخته شده و سپس چند کشور دیگر مورد اشاره قرار خواهند گرفت.

فرانسه

در کشور فرانسه، کمیسیون ملی انفورماتیک و آزادی^۷ متولی داده مسئول تضمین و اجرای قانون حمایت از داده این کشور است. این کمیسیون یک مقام اداری مستقل بوده و استقلال آن از طریق ترکیب آن تضمین شده است. (CNLI)

این کمیسیون ۱۷ عضو دارد که توسط مجامع و حوزه‌های تخصصی که به آن تعلق دارند، انتخاب می‌شوند. رییس کمیسیون نیز از بین اعضای آن انتخاب می‌شود.

ترکیب اعضا به این شرح است:

- چهار نماینده مجلس (دو عضو مجلس شورای ملی و دو عضو مجلس سنا)؛
- دو نماینده از اعضای شورای اقتصادی اجتماعی محیط زیست فرانسه؛
- شش نماینده از حوزه‌های قضایی (دو عضو شورای دولتی، دو عضو دیوان عالی کشور، دو عضو دیوان محاسبات)؛
- پنج شخصیت عمومی (یک نفر به انتخاب رییس مجلس شورای ملی و یک نفر به انتخاب مجلس سنا، سه نفر به انتخاب هیئت دولت فرانسه).

اعضا برای پنج سال انتخاب شده، هفته‌ای یکبار جلسه عمومی تشکیل می‌دهند و صورت جلسه‌ها و پیش‌نویس مقرراتی را که دولت فرستاده، ارزیابی می‌کنند. همچنین تجزیه و تحلیل عواقب ورود فناوری‌های نوین و تأثیر آن بر زندگی شخصی از دیگر وظایف این کمیسیون در جلسه‌های هفتگی است. (Ibid) به منظور بررسی دقیق‌تر، وظایف و اختیارات این کمیسیون تشریح می‌شود:

۱. اطلاع‌رسانی و آموزش

یکی از وظایف اولیه کمیسیون که در بند یک ماده ۱۱ قانون حمایت از داده^۸ این کشور آمده است، آگاه کردن اشخاص از حقوق ذکرشده آنها در قانون حمایت از داده‌های شخصی فرانسه است؛ این وظیفه با اطلاع‌رسانی به شهروندان و کنترل‌کننده‌های داده انجام می‌پذیرد. بر همین اساس در سال ۲۰۱۳، کمیسیون حدود ۱۲۵ هزار تماس تلفنی برای دریافت مشاوره یا اطلاعات بیشتر داشته است. گفتنی است، کمیسیون این وظیفه خود را با شرکت در کنفرانس‌ها، سمینارها و کارگاه‌های آموزشی با موضوع‌هایی نظیر اطلاع‌رسانی به شهروندان اجرایی می‌کند.

۲. رگولاتوری و ارائه توصیه

از آنجایی که یکی از مهم‌ترین مراحل در چرخه حیات داده، مرحله پردازش داده است، قانون حمایت از داده‌های شخصی، ابزارهای مختلفی را برای نظارت بر این مرحله در اختیار کمیسیون قرار داده که رگولاتوری به معنای صدور مجوز و یا ارائه نظر و توصیه از جمله آنهاست. بر این اساس باید گفت به طور کلی، قانون حمایت از داده‌های شخصی در خصوص پردازش داده‌های شخصی توسط کنترل‌کننده داده، چهار وضعیت را پیش‌بینی کرده است که عبارت‌اند از:

۲-۱. داده‌هایی که ممنوعیت دارند

مطابق بخش نخست ماده ۸ قانون حمایت از داده‌های شخصی «جمع‌آوری و پردازش داده‌هایی که به‌طور مستقیم یا غیرمستقیم، ریشه‌های نژادی و قومی، نظرهای سیاسی، فلسفی، مذهبی یا وابستگی اشخاص به اتحادیه تجاری را نشان می‌دهد، یا اینکه مربوط به سلامت و زندگی جنسی افراد باشد»^۹ ممنوع است؛ اما بر اساس بخش دوم این ماده، در مواردی پردازش چنین داده‌هایی مجاز شمرده شده است. این موارد را می‌توان به شرح زیر بیان کرد:

الف. پردازشی که صاحب داده رضایت صریح خود را اعلام کند، به‌استثنای مواردی که قانون تصریح کند که رضایت صاحب داده در پردازش تأثیری ندارد.

ب. درجایی که صاحب داده، به دلیل عدم اهلیت قانونی یا نبود امکان فیزیکی قادر به رضایت دادن نیست و پردازش داده برای حمایت از حیات بشر ضروری و لازم است.

ج. پردازش را، یک انجمن یا هر نهاد غیرانتفاعی مذهبی، فلسفی، سیاسی یا تجاری انجام دهد که این شرایط را داشته باشد:

- تنها برای داده‌هایی که با هدف آن انجمن یا نهاد مرتبط باشد.
 - پردازش تنها مربوط به اعضای این انجمن یا نهاد باشد و در صورت لزوم مربوط به افرادی باشد که ارتباط منظمی با آن نهاد در زمینه فعالیت‌هایشان دارند.
 - پردازش تنها در رابطه با داده‌ای صورت گیرد که به اشخاص ثالث منتقل نمی‌شود، به استثنای مواردی که صاحبان داده به صراحت رضایت خود را در مورد چنین انتقالی اعلام کنند.
 - د. پردازش مربوط به داده‌ای باشد که صاحب داده آن را علنی ساخته و در دسترس عموم قرار داده باشد.
 - ه. پردازشی که برای طرح، اعمال یا دفاع از یک دعوای قانونی (Legal Claim) ضروری باشد.
 - و. پردازشی که با اهداف پیشگیری، تشخیص پزشکی، ارائه مراقبت‌های بهداشتی یا درمانی، یا برای مدیریت خدمات درمانی باشد و یک عضو حرفه پزشکی یا شخصی که به موجب وظایفش ملزم و متعهد به رازداری است، آن را انجام دهد.
 - ز. پردازشی که برای تحقیق‌های پزشکی و با رعایت سایر مقررات این قانون صورت گیرد.
- (French Data protection AC)

۲-۲. داده‌هایی که پردازش آن‌ها نیازمند اطلاع به کمیسیون است

به موجب ماده ۲۲ این قانون، انجام پردازش خودکار داده باید به اطلاع کمیسیون برسد.^{۱۰} همچنین به موجب ماده ۲۳، اطلاع‌رسانی (Notification) از مهم‌ترین تعهدهای قانونی پردازش‌کنندگان داده است. این تعهد از طریق اطلاعیه الکترونیکی که به کمیسیون ارسال می‌شود، انجام می‌پذیرد. در مقابل کمیسیون موظف است بدون تأخیر، تأییدیه دریافت اطلاعیه را برای متقاضی پردازش ارسال کند. بدیهی است، این تأییدیه نیز به صورت الکترونیکی ارسال می‌شود. با این حال، به موجب بند ۲ ماده ۲۲ در دو مورد پردازش داده نیازمند رعایت تشریفاتمانند اطلاع‌رسانی یا کسب مجوز نیست که عبارت‌اند از:

- پردازشی که باهدف ثبت (Register) اطلاعات عمومی است و علاوه بر اینکه نفع مشروعی برای تمامی شهروندان دارد، برای تمامی آنها قابل دسترسی باشد.
- پردازشی که توسط یک انجمن یا هر نهاد غیرانتفاعی مذهبی، فلسفی، سیاسی یا تجاری انجام شود که دارای شرایط مذکور باشند. (Ibid)

۲-۳. داده‌هایی که پردازش آن‌ها نیازمند کسب مجوز از کمیسیون است

- ماده ۲۵ قانون مذکور، پردازش در این موارد را منوط به کسب مجوز از کمیسیون کرده است:
- پردازش خودکار یا غیر خودکاری که مؤسسه ملی مطالعات آماری و اقتصادی

(National Institute of Economic studies (INSE)) یا یکی از سرویس‌های آماری وزارتخانه‌ها^{۱۱} انجام دهد و مربوط به رعایت تعهدها، هماهنگی و رازداری و متعاقب نظر شورای ملی برای اطلاعات آماری ((National Council for Statistical in for mation (CNIS)) باشد.

- پردازش خودکار داده‌های مربوط به ژنتیک، مگر اینکه به وسیله پزشکان یا زیست‌شناسان صورت گرفته و برای پیشگیری، تشخیص یا درمان پزشکی ضروری باشد.
- پردازش خودکار یا غیر خودکار داده‌های مربوط به جرائم، مجازات‌ها یا اقدام‌های امنیتی به‌استثنای مواردی که توسط نمایندگان دادگستری (Representatives justice) صورت می‌گیرد.
- پردازش خودکاری که با توجه به ماهیت، میزان اهمیت و هدف پردازش، صاحب داده را از حق دسترسی به داده‌های خود محروم سازد.
- پردازش خودکاری که هدف آن از ترکیب داده‌ها و اطلاعات یک یا چند مؤسسه عمومی ارائه خدمات عمومی باشد که در راستای منافع عمومی فعالیت می‌کنند.
- پردازش داده‌هایی که دربرگیرنده شماره ملی اشخاص حقیقی^{۱۲} بوده و امکان کسب رضایت از آن‌ها وجود نداشته باشد.
- پردازش خودکار داده‌هایی که دربرگیرنده ارزیابی مشکل‌های اجتماعی اشخاص باشد.
- پردازش خودکار داده‌های بیومتریک (زیست‌سنجشی) که برای احراز هویت یک شخص ضروری است.

شایان ذکر است که کمیسیون موظف است نظر خود را در خصوص امکان صدور مجوز برای پردازش داده‌های مذکور ظرف مدت دو ماه از تاریخ دریافت تقاضا اعلام کند. این مدت با تصمیم رییس کمیسیون قابل تمدید بوده و در صورت انقضای مدت و عدم اعلام نظر کمیسیون، درخواست رددشه تلقی خواهد شد. (French Data protection Act)

۲-۴. داده‌هایی که پردازش آن‌ها نیازمند کسب نظر از کمیسیون است

بر اساس مواد ۲۶ و ۲۷ قانون حمایت از داده‌های شخصی، چنین داده‌هایی قابل تقسیم به دو دسته هستند: الف. داده‌هایی که پردازش آن‌ها با صدور حکم وزیر یا وزرای ذی‌صلاح پس از اعلام نظر کمیسیون^{۱۳} امکان‌پذیر است. که این داده‌ها عبارت‌اند از:

- داده‌های مربوط به امنیت دولتی، امنیت عمومی و دفاع.
- داده‌هایی که هدف از پردازش آن‌ها پیشگیری، تحقیق، اثبات جرم، محاکمه مجرم، اجرای احکام کیفری یا اقدام‌های امنیتی باشد.
- داده‌هایی که به‌طور مستقیم یا غیرمستقیم، ریشه‌های نژادی و قومی، نظرهای سیاسی، فلسفی، مذهبی یا وابستگی اشخاص به اتحادیه تجاری را نشان می‌دهد یا اینکه مربوط به سلامت و زندگی جنسی اشخاص باشد.

ب. داده‌هایی که پردازش آن‌ها با حکم شورای دولتی فرانسه (Council of State/ conseil d'Etat) پس از اعلام نظر کمیسیون امکان‌پذیر است که این داده‌ها عبارت‌اند از:

- داده‌های مربوط به شناسایی هویت اشخاص که از سوی مؤسسه‌های دولتی یا خصوصی ارائه دهنده خدمات عمومی پردازش می‌شوند.
- داده‌های بیومتریک (زیست‌سنجشی) که دولت برای شناسایی یا احراز هویت اشخاص پردازش می‌کند.

در نهایت در خصوص وظیفه رگولاتوری و ارائه توصیه کمیسیون باید به این نکته اشاره کرد که مطابق قسمت b بند ۲ ماده ۱۱، کمیسیون اختیار وضع استانداردهای مربوط به پردازش داده را نیز در اختیار دارد، همچنین می‌تواند نظرهای رسمی خود را در مورد پیش‌نویس قوانین مربوط به حمایت از داده به دولت ارائه کند. (French Data protection Act)

۳. حمایت از حقوق شهروندان

هر فردی که در اعمال حقوق حمایت از داده خود با مشکلاتی مواجه شده باشد، می‌تواند به کمیسیون مراجعه کرده و شکایت کند. کمیسیون، به موجب قسمت c بند ۲ ماده ۱۱ قانون حمایت از داده‌های شخصی، ملزم شده است که کلیه ادعاها، درخواست‌ها و شکایت‌های مربوط به پردازش داده شخصی را دریافت و متقاضی آن‌ها را از اقدام‌های صورت گرفته در این مورد مطلع کند.^{۱۵} در سال ۲۰۱۳، کمیسیون تعداد ۵۶۴۰ شکایت را که شامل موارد زیر بود دریافت کرد:

- اعتبار (Reputation) الکترونیکی (درخواست برای پاک کردن داده در اینترنت)؛
 - تجارت (درخواست‌هایی برای متوقف کردن تبلیغات از طریق ایمیل)؛
 - منابع انسانی (ساز و کارهای نظارتی مانند نظارت ویدئویی یا تعیین محل جغرافیایی وسایل نقلیه)؛
 - بانک‌ها و وام‌ها (اعتراض به ثبت نام‌هایشان در فایل‌های بانک فرانسه).
- بر همین اساس کمیسیون در وب‌گاه خود یک سرویس شکایت بر خط را، برای رسیدگی به شکایاتی مانند پاک کردن داده شخصی در اینترنت، مخالفت با دریافت تبلیغات از طریق ایمیل، به‌روزرسانی صحت داده شخصی و مواردی از این قبیل ایجاد کرده است. (Ibid)

۴. بازرسی

به موجب ماده ۴۴ قانون حمایت از داده‌های شخصی، بازرسی، یکی از مهم‌ترین ابزارهای کمیسیون برای نظارت بر حسن اجرای این قانون است.^{۱۶} بر همین اساس اعضای کمیسیون و مأموران آن با مجوز کمیسیون، اختیار دارند تا مکان‌ها، تجهیزات و ساختمان‌های پردازش‌کنندگان داده را از ساعت شش صبح تا نه شب بازرسی کنند. بدیهی است این نظارت، تنها شامل مکان‌های عمومی شده و مکان‌های خصوصی را در بر نمی‌گیرد. شایان ذکر است که در هر مورد بازرسی میدانی،

دادستان عمومی بخش مورد بازرسی، باید در جریان قرار گیرد. همچنین ضروری است مأموران کمیسیون در صورت کشف جرم، دادستانی را همراه با دلایل و مدارک مطلع سازند. در صورت ممانعت پردازش‌کنندگان داده از ورود و بازرسی مأموران کمیسیون، عدم ارائه اطلاعات مورد نیاز مأموران، تخریب یا نابودی اطلاعات و یا فریب مأموران، به مجازات حبس و جزای نقدی تا ۱۵ هزار یورو محکوم خواهند شد.

در نهایت، باید به این نکته اشاره شود که مطابق قانون حمایت از داده‌های شخصی فرانسه، کمیسیون می‌تواند به شرکت‌هایی که سطح بالایی از حمایت را رعایت می‌کنند، گواهینامه (Certification) اعطاء کند که از یک طرف نشان‌دهنده شاخص اعتماد در محصول‌ها، سرویس‌ها و کیفیت مطلوب آن‌ها در حمایت از داده‌ها است و از طرف دیگر، دارنده را از مزیت رقابتی به نسبت سایر رقبا برخوردار می‌کند. گفتنی است کمیسیون در سال ۲۰۱۲، به منظور تقویت مأموریت خود در خصوص فناوری‌ها و سرویس‌های جدید، کمیته‌ای تحت عنوان کمیته آینده‌نگر (Prospective Committee) را ایجاد کرده که به مطالعه و بررسی فناوری‌ها و سرویس‌های جدید می‌پردازد. (Ibid)

۵. تعیین ضمانت اجراهای اداری

کمیسیون، یک کمیته ویژه (The Restricted Committee) مرکب از یک رییس و پنج عضو دارد که به وسیله کمیسیون و از بین اعضای آن انتخاب می‌شوند. کمیته ویژه، به موجب ماده ۱۷ قانون حمایت از داده‌های شخصی، صلاحیت وضع مجازات‌های اداری را علیه هر کنترل‌کننده داده‌ای دارد که مقررات قانون مذکور را رعایت نکند.

آیین رسیدگی این کمیته، مطابق قانون مزبور بدین صورت است که کمیته بعد از دریافت شکایت، جلسه‌ای با طرفین دعوا تشکیل می‌دهد که بعد از جلسه ممکن است به کنترل‌کننده داده، به دلیل رعایت نکردن تعهدهای مقرر در این قانون اخطار بدهد، چنین اخطاری نوعی مجازات اداری محسوب می‌شود. همچنین رییس کمیسیون این اختیار را دارد که یک دستور رسمی به کنترل‌کننده داده جهت رعایت مقررات این قانون و توقف رعایت نکردن آن با تعیین یک مهلت زمانی مشخص بدهد. در صورت ضرورت، این مهلت ممکن است تا پنج روز هم تعیین شود. اگر کنترل‌کننده داده مطابق با اخطار داده‌شده عمل کند، رییس کمیسیون ختم رسیدگی را اعلام می‌کند؛ در غیر این صورت، کمیته ممکن است مجازات‌های زیر را پس از جلسه با طرفین بر کنترل‌کننده داده وضع کند:

۱. وضع جریمه مالی، به جز در مواردی که دولت پردازش را انجام می‌دهد؛

۲. دستور توقف پردازش؛

۳. لغو مجوز پردازش.

در مواردی که پردازش و یا استفاده از داده‌های پردازش‌شده منجر به نقض حقوق و آزادی‌های

کاربران شود، کمیته می‌تواند بعد از شنیدن اظهارات طرفین و در صورت حکم شورای دولتی یکی از این اقدام‌ها را انجام دهد:

۱. صدور اخطار؛
۲. دستور توقف موقت پردازش داده‌ها حداکثر برای سه ماه، به شرطی که پردازش با هدف امنیت عمومی، مسائل سیاسی یا کیفری نبوده باشد.
۳. دستور به غیر قابل استفاده شدن برخی داده‌های پردازش شده حداکثر برای سه ماه به شرطی که پردازش با هدف امنیت عمومی، مسائل سیاسی یا کیفری نبوده باشد.
۴. در صورتی که پردازش با هدف امنیت عمومی، مسائل سیاسی یا کیفری بوده، به نخست‌وزیری اطلاع داده می‌شود تا اقدام‌های ضروری را برای جلوگیری از ادامه نقض انجام دهد. گفتنی است کمیته این اختیار را دارد که دستور انتشار ضمانت اجراهای وضع شده را در مجله‌ها، روزنامه‌ها یا سایر رسانه‌ها برای شناساندن متخلفان و با هزینه آن‌ها صادر کند. (*Ibid*)

کره جنوبی

کره جنوبی در ۳۰ سپتامبر ۲۰۱۱، بر اساس دستورالعمل ۱۹۹۵ اتحادیه اروپا، "قانون حمایت از داده‌های شخصی (Personal Information Protection ACT)" خود را تصویب کرد. بر اساس این قانون، دفتر ریاست جمهوری، موظف به ایجاد کمیسیونی تحت عنوان کمیسیون حمایت از داده ((Personal Information Protection Commission (PIPC)) است که ملزم است مستقل از دولت، مسئولیت حمایت از اطلاعات را بر عهده بگیرد. (Status of PIPC)

در خصوص ساختار و ترکیب این کمیسیون، باید گفت که مطابق ماده ۷ قانون حمایت از داده‌های شخصی، اعضای آن نباید از پانزده عضو بیشتر شود. این کمیسیون شامل یک رییس و یک عضو موظف (Standing Commissioner) است که رییس کمیسیون را باید رییس‌جمهور و از میان افراد غیردولتی انتخاب کند. شایان ذکر است اعضای این کمیسیون را رییس‌جمهور از میان اشخاص مطرح شده در قسمت ذیل انتخاب می‌کند:

- پنج عضو از بین نامزدهای مطرح شده توسط مجلس شورای ملی؛
 - پنج عضو از بین نامزدهای مطرح شده توسط رییس دیوان عالی کشور؛
- مابقی اشخاص نیز تا سقف پانزده نفر، از گروه‌های ذیل توسط مجلس یا رییس دیوان عالی کشور نامزد می‌شوند:

- افراد توصیه شده توسط سازمان‌های مدنی مرتبط با حریم خصوصی یا حمایت از مصرف‌کننده؛
- افراد توصیه شده توسط انجمن‌های صنفی پردازشگر داده‌های شخصی؛
- دیگر افرادی که دارای دانش و تجربه آکادمیک و دانشگاهی مرتبط با داده‌های شخصی هستند.

(Personal Information Protection Act)

مدت عضویت در این کمیسیون سه سال بوده و تنها برای یک دوره دیگر قابل تمدید است. جلسه‌ها نیز با حضور اکثریت اعضاء رسمیت یافته و تصمیم‌گیری با نظر موافق اکثریت اعضای حاضر صورت می‌گیرد. در خصوص وظایف و اختیارات این کمیسیون باید ذکر شود که به موجب ماده ۸ قانون حمایت از داده‌های شخصی وظایف و عملکردهای کمیسیون عبارت‌اند از:

۱. برنامه‌ریزی و مدیریت

در بخش برنامه‌ریزی و مدیریت، این کمیسیون هر سه سال یک‌بار، برنامه‌ای را به‌عنوان چارچوب ملی حمایت از داده‌ها و به منظور اطمینان از حمایت مؤثر از داده‌ها و ارتقای سطح حمایت از داده‌ها در این کشور تدوین می‌کند. همچنین سیاست‌های دولت را از طریق مشارکت در برنامه‌های اجرایی بخش‌های دولتی از منظر هماهنگ بودن این سیاست‌ها با اصول حمایت از داده، بررسی و مدیریت می‌کند.

۲. ارزیابی لوایح قانونی

در بخش ارزیابی لوایح قانونی، این کمیسیون ارزیابی می‌کند که آیا لوایح قانونی تدوین شده، مطابق با اصول حمایت از داده‌های این کشور هست یا خیر. همچنین این کمیسیون در صورت لزوم به نهادهای تدوین‌کننده لوایح قانونی، توصیه‌های لازم را ارائه می‌کند تا این لوایح با توجه به قوانین و مقررات حمایت از داده تغییر یافته و منطبق شوند.

۳. نظارت

این کمیسیون نظارت می‌کند که آیا اقدام‌های کنترل‌کننده‌های داده، در بخش‌های عمومی یا خصوصی مطابق با قانون حمایت از داده‌های این کشور است یا خیر. علاوه بر این، کمیسیون می‌تواند در صورت نقض قانون حمایت از داده، حسب مورد، پیشنهاد تعلیق یا اقدام اصلاحی را از طریق سازمان‌های قانون اساسی، سازمان‌های دولتی مرکزی و دولت‌های محلی توصیه کند.

۴. حل اختلاف

کمیسیون، به عنوان یک نهاد میانجی، در صورت بروز اختلاف میان شهروندان و ارجاع آن به این کمیسیون، به اختلاف‌ها رسیدگی می‌کند و در خصوص جبران خسارت‌های ناشی از نقض قانون حمایت از داده تصمیم می‌گیرد.

۵. بازبینی

در بخش بازبینی، کمیسیون به اعلام نظر در خصوص مواردی می‌پردازد که در آن‌ها قانون حمایت از داده

تفسیر و اجرا شده است؛ تا مطمئن شود این موارد با قانون حمایت از داده مطابقت دارند. همچنین این کمیسیون، نظرهای نهادهای دولتی را، در مورد پردازش اطلاعات هماهنگ می‌کند. (*Ibid*)

وظایف و اختیارات این کمیسیون را به طور خلاصه می‌توان ذیل ده دسته بدین شرح بیان کرد:
 ۱. اجرای طرح اساسی حمایت از داده (Data Protection Basic Draft): وزارت امنیت و اجرای سیاست‌های دولت کره جنوبی (Minister of Public Administration and Security) هر سه سال یکبار پس از مشورت با رئیس طرح اساسی حمایت از داده را تهیه و آن را برای اجرا به کمیسیون ارائه می‌کند. طرح اساسی مزبور دربرگیرنده موارد زیر است:

- اهداف اساسی و دستورالعمل‌های در نظر گرفته شده برای حمایت از داده؛
- بهبود و ارتقاء سیستم‌ها و قوانین مربوط به حمایت از داده؛
- اقدام‌های لازم برای جلوگیری از نقض حریم خصوصی؛
- نحوه تسهیل خودتنظیمی (Self-regulation) برای حمایت از داده؛
- چگونگی فعال کردن آموزش و روابط عمومی برای حمایت از داده؛
- آموزش و تعلیم متخصصان در حمایت از داده؛
- مسائل ضروری دیگر در راستای حمایت از داده.

۲. امور و مسائل مربوط به سیاست‌ها، سیستم‌ها و مقررات‌گذاری مربوط به حمایت از داده؛

۳. امور و مسائل مربوط به هماهنگی مواضع اتخاذ شده توسط مؤسسه‌های عمومی در رابطه با حمایت از اطلاعات؛

۴. مسائل مربوط به تفسیر و بهره‌برداری از قوانین و مقررات مربوط به حمایت از داده؛

۵. وظیفه مربوط به استفاده و ارائه داده مقرر در ماده ۱۸ (این ماده ارائه و استفاده از داده را در مواردی منوط به نظر کمیسیون کرده است که این ماده در بندهای بعدی به طور مفصل توضیح داده خواهد شد)؛

۶. ارائه نظرهای خود در خصوص گزارش ارزیابی اثرات حریم خصوصی به وزیر امنیت و اجرای سیاست‌های دولت؛

۷. ارائه نظرها و پیشنهادها خود به وزیر امنیت و اجرای سیاست‌های دولتی به درخواست وزارت مربوطه؛

۸. پیشنهاد انجام اقدام‌های اصلاحی در خصوص نقض قانون حمایت از داده‌ها به دیارتمان مرکزی اداری، دولت‌های محلی، مجمع ملی، دادگاه قانون اساسی و کمیسیون انتخابات ملی طبق ماده ۶۴؛

۹. تهیه و ارائه گزارش سالانه به مجمع ملی (National Assembly)؛

۱۰. مسائل ارجاع شده به کمیسیون از سوی رئیس جمهور، شخص رئیس کمیسیون یا بیشتر از دو کمیسیونر، در رابطه با حمایت از داده و وظایف دیگری که در این قانون یا قوانین دیگر ذکر شده است.

همان‌طور که از وظایف کمیسیون حمایت از داده‌های شخصی استنباط می‌شود، این نهاد بیشتر دارای نقش نظارتی و تشریفاتی است و قدرت مقررات‌گذاری و اجرایی چندانی ندارد. در این قانون حتی اختیار وضع دستورالعمل‌های مربوط به حمایت از داده‌ها، با وزیر امنیت و اجرای سیاست‌های دولت است. همچنین در این قانون بر ترویج و حمایت از خودتنظیمی تأکید فراوانی شده و ماده ۱۳ قانون مزبور وزیر امنیت و اجرای سیاست‌های دولت را به انجام اقدام‌هایی به شرح زیر در جهت ترویج خودتنظیمی ملزم کرده است:

- آموزش و تعلیم کاربران؛
 - تشویق و پشتیبانی حمایت از داده در نهادها و مؤسسات مربوطه؛
 - معرفی و استفاده از سیستم نشان حریم خصوصی^{۱۷}؛
 - حمایت از تشکیل و اجرای قواعد خودتنظیمی توسط پردازشگران اطلاعات خصوصی.
- قانون مزبور برخی محدودیت‌ها را بر پردازش داده شخصی به شرح زیر مقرر کرده است:
- محدودیت پردازش داده‌های حساس مانند ایدئولوژی، عقیده، طرز فکر سیاسی، سلامت، اطلاعات جنسی و ...؛
 - محدودیت نصب و راه‌اندازی دستگاه‌های پردازش داده تصویری؛
 - محدودیت انتقال داده متعاقب انتقال داده‌های مرتبط با کسب و کار
 - محدودیت پردازش به صورتی که هویت یک فرد مطابق با قوانین و مقررات معلوم باشد. (*Ibid*)
- در ماده ۱۸ این قانون محدودیت‌هایی برای استفاده و ارائه اطلاعات شخصی^{۱۸} آمده است. این محدودیت‌ها عبارت‌اند از:
- الف. پردازشگر اطلاعات شخصی نباید از اطلاعات شخصی فراتر از محدوده تصریح شده‌اش (هدف اصلی پردازش) استفاده کند، همچنین نباید آن اطلاعات را به شخص ثالث غیرمجاز ارائه کند، مگر در موارد ذیل:
۱. چنانچه "رضایت تکمیلی" (Additional consent) را از موضوع داده کسب کرده باشد. لازم به توضیح است که در این مورد، پردازشگر اطلاعات علاوه بر اخذ رضایت تکمیلی از موضوع داده، ملزم است موارد زیر را به وی اطلاع دهد:

- هویت دریافت‌کننده اطلاعات شخصی (The recipient of personal information)؛
- هدف استفاده دریافت‌کننده از اطلاعات شخصی (The purpose of use of personal information)؛
- مشخصات اطلاعات شخصی مورد استفاده یا ارائه‌شده به دریافت‌کننده اطلاعات (Particulars of personal information to be used or provided)؛
- مدت‌زمان حفظ و استفاده از اطلاعات شخصی (The period when personal information is retained and used)
- اطلاع‌رسانی به موضوع داده مبنی بر امکان رد رضایت و ضررهای ناشی از این رد^{۱۹}.

۲. چنانچه در آن مورد مقررۀ قانونی خاصی در اسناد بالادستی وجود داشته باشد.
 ۳. چنانچه استفاده یا جمع‌آوری اطلاعات شخصی، به‌صراحت برای حمایت از خطر قریب‌الوقوع، حیات، جسم یا منافع اقتصادی موضوع داده یا شخص ثالثی ضروری باشد و موضوع داده یا نماینده قانونی‌اش در وضعیت مناسبی برای بیان قصد یا رضایت خود نباشند، یا رضایت قبلی با توجه به ناشناخته بودن آدرس، قابل اتخاذ نباشد.
 ۴. چنانچه اطلاعات شخصی به شیوه‌ای که هویت افراد ناشناخته باشد، حفظ یا نگهداری شده و پردازش آن‌ها لزوماً برای تحقق اهداف تحقیق‌های آماری و آموزشی و مواردی از این قبیل باشد.
 ۵. چنانچه فعالیت پردازشگر، به منظور اعمال صلاحیت مجاز خود بدون استفاده از اطلاعات شخصی غیرممکن باشد. در این مورد امکان استفاده پردازشگر از اطلاعات شخصی به منظور انجام وظایف قانونی آن، منوط به مشورت و تصمیم کمیسیون است.
 ۶. چنانچه استفاده از اطلاعات شخصی، به منظور اجرای یک معاهده یا کنوانسیون بین‌المللی به یک کشور خارجی یا سازمان‌های بین‌المللی ضروری باشد.
 ۷. چنانچه این امر برای تحقیق جرائم، صدور کیفرخواست و محاکمه ضروری باشد.
 ۸. چنانچه این امر برای دادگاه در رسیدگی به پرونده ضروری باشد.
 ۹. چنانچه برای مجازات، اجرای مراقبت و بازداشت لازم باشد.
- ب. چنانچه یک نهاد عمومی از اطلاعات شخصی برای هدفی به غیر از آنچه در نظر گرفته شده استفاده یا آن را به شخص ثالث ارائه می‌کند، نهاد عمومی باید زمینه‌های قانونی برای چنین امری، هدف، دامنه و دیگر موضوع‌های لازم را در روزنامه رسمی یا وب‌گاه رسمی خود اعلام کند.
- ج. زمانی که پردازشگر، اطلاعات شخصی را به یک شخص ثالث مجاز، برای هدف قانونی دیگری به موجب قوانین و مقررات ارائه می‌کند، پردازشگر باید از گیرنده اطلاعات درخواست کند که هدف و روش استفاده خود را از داده‌ها محدود کند و همچنین تدابیر حفاظتی لازم برای تضمین امنیت اطلاعات را به کار گیرد. در این مورد، شخص ثالث موظف است که کلیه تدابیر و اقدام‌های لازم را برای تضمین امنیت اطلاعات به کار گیرد.
- لازم به توضیح است که در این قانون، آیین میانجیگری به عنوان ساز و کاری برای حل و فصل اختلاف‌های مربوط به اطلاعات در نظر گرفته شده است. در ماده ۴۰ قانون مزبور، ایجاد کمیته حل اختلاف‌های مربوط به داده‌های شخصی (Personal Information Dispute Mediation Committee)، برای میانجیگری در اختلاف‌های مربوط به داده پیش‌بینی شده است. به موجب این ماده، وزیر امنیت و اجرای سیاست‌های دولت (The Minister Of Public Administration And Security)، اعضای کمیته را که بیشتر از بیست عضو نخواهد داشت از میان اشخاص زیر انتخاب می‌کند:
- مأموران دولتی متعلق به کالج مأموران عالی‌رتبه دولتی از دپارتمان‌های اداری مرکزی یا مؤسسه‌های مسئول حمایت از داده، یا اشخاصی که در موقعیت‌های مربوطه در بخش

دولتی سازمان‌های مربوطه کار کرده یا در حال حاضر فعالیت می‌کنند و از تجربه‌های کاری در زمینه حمایت از داده برخوردارند.

- اشخاصی که به‌عنوان استادان مربوطه یا موقعیت‌های بالاتر در دانشگاه‌ها یا در مؤسسه‌های تحقیقاتی شناخته‌شده در حال حاضر فعالیت می‌کنند یا فعالیت کرده‌اند.
- اشخاصی که به‌عنوان قاضی، دادستان عمومی، یا وکیل مدافع در حال حاضر فعالیت می‌کنند یا فعالیت کرده‌اند.
- اشخاص توصیه‌شده به وسیله سازمان‌های مدنی مرتبط با حمایت از داده یا گروه‌های مصرف‌کننده.
- اشخاصی که به‌عنوان مأموران ارشد برای انجمن‌های صنفی متشکل از پردازشگرهای داده‌های شخصی در حال حاضر فعالیت می‌کنند یا فعالیت کرده‌اند.

رئیس کمیته مزبور را وزیر امنیت و اجرای سیاست‌های دولت، از بین اعضای کمیته به‌استثنای مأموران دولتی تعیین می‌کند. مدت عضویت در این کمیته دو سال است که برای یک دوره دیگر نیز قابل تمدید است. کمیته در صورت ضرورت، می‌تواند یک پنل کوچک‌تر مرکب از پنج عضو یا کمتر تشکیل دهد که اعتبار تصمیم‌های این پنل مانند تصمیم خود کمیته است. شایان‌ذکر است که جلسه‌های کمیته یا این پنل با حضور اکثریت اعضای آن‌ها رسمیت می‌یابد و تصمیم‌گیری با نظر موافق اکثریت آرای حاضر اتخاذ می‌شود.

آیین رسیدگی در کمیته مزبور، به موجب ماده ۴۳ قانون حمایت از داده‌های شخصی بدین صورت است که هر شخصی می‌تواند درخواست میانجیگری اختلاف را به کمیته تحویل دهد. کمیته موظف است درخواست را دریافت کند و آن را به طرف مقابل دعوا اطلاع دهد. پس از دریافت درخواست، کمیته از طرفین تقاضا می‌کند تا دلایل خود را ارائه کنند و طرفین ملزم به تبعیت از این درخواست هستند. کمیته موضوع را بررسی و نسخه اولیه میانجیگری را ظرف ۶۰ روز از تاریخ دریافت درخواست میانجیگری تهیه می‌کند، کمیته می‌تواند در موارد ضروری مهلت مزبور را تمدید کند. همچنین کمیته قبل از میانجیگری می‌تواند مبادرت به برقراری سازش بین طرفین کند. (Personal Information Protection Act)

کمیته می‌تواند تصمیم‌های زیر را در نسخه اولیه میانجیگری ارائه کند:

- تعلیق فعالیت‌های احتمالی مربوط به نقض داده‌های خصوصی جهت بررسی و تحقیق بیشتر؛
 - جبران خسارت‌ها و ضرر و زیان‌های وارده؛
 - هر اقدام ضروری برای جلوگیری از تکرار مجدد چنین نقض‌های یکسان یا مشابه.
- پس از تهیه پیش‌نویس میانجیگری، کمیته بدون تأخیر پیش‌نویس میانجیگری را به طرفین دعوا ارائه می‌کند. هر طرفی که پیش‌نویس مربوطه به او ارائه یا تسلیم شده است، پذیرش یا رد پیش‌نویس میانجیگری را، به کمیته در طول ۱۵ روز از تاریخ دریافت اطلاع خواهد داد، بدون چنین اطلاعی میانجیگری رد شده تلقی می‌شود.

اگر طرفین نسخه اولیه میانجیگری را که کمیته تهیه کرده بپذیرند، کمیته بی‌درنگ میانجیگری را مکتوب و به امضا و تأیید رئیس کمیته و طرفین اختلاف می‌رساند. لازم به توضیح است که میانجیگری توافق‌شده، تأثیر مشابهی مانند سازش قبل از دادگاه را خواهد داشت. چنانچه کمیته تشخیص دهد که طرح دعوا از نظر ماهیت نادرست و یا اینکه درخواست مزبور ناعادلانه است، می‌تواند میانجیگری را رد کند؛ در این صورت دلایل رد میانجیگری را به اطلاع متقاضی می‌رساند. طرح دعوا در دادگاه، هنگامی که دعوا در کمیته در حال بررسی است، موجب تعلیق رسیدگی به وسیله کمیته خواهد شد. همچنین دولت یا دولت‌های محلی، سازمان‌ها و مؤسسه‌های حمایت از داده و نیز پردازشگران داده‌های شخصی، ممکن است درخواست میانجیگری را در کمیته مطرح کنند که در این حالت، این نوع میانجیگری، میانجیگری جمعی نامیده می‌شود. (*Ibid*)

نهادهای حمایت از داده در کشورهای مختلف

همان‌طور که گفته شد، در ادامه به نمونه‌هایی از نهادهای حمایت از داده در کشورهای اروپایی و سپس به یک نمونه از کشورهای غیراروپایی اشاره می‌شود. لزوم بررسی کشورهای غیراروپایی از آنجایی است که در حوزه اتحادیه اروپا سطح بالایی از حمایت از داده در جریان است و همان‌طور که اشاره شد، امکان تبادل داده با کشورهای اروپایی در صورتی مجاز است که کشور خارج از حوزه اتحادیه اروپا نیز همان میزان حمایت از داده را داشته باشد، به همین جهت کشورهای دیگر نیز به صورت داوطلبانه قانون حمایت از داده خود را منطبق با GDPR تصویب کرده‌اند تا امکان تبادل داده را با کشورهای اروپایی داشته باشند.

کرواسی

کشور کرواسی عضو اتحادیه اروپا است و به تبعیت از دستورالعمل ۱۹۹۵ اتحادیه، قانون حمایت از داده‌های شخصی (The Act on personal data protection) را در سال ۲۰۰۳ تصویب کرده است. این کشور، همگام با به روزرسانی دستورالعمل ۱۹۹۵ و تصویب مقررات عمومی حمایت از داده (GDPR)، خود را ارتقا داده است. در این کشور آژانس کروات حمایت از داده (Croatia personal Data protection Agency) مسئول اجرای درست این قانون، نظارت و رسیدگی به شکایت‌ها را بر عهده دارد. (About the agency)

این آژانس، یک شخصیت حقوقی مستقل داشته و در برابر مجلس کروات پاسخگو است. ساختار اجرایی و شیوه عمل این آژانس بر اساس اساسنامه‌ای است که به تصویب مجلس رسیده است. مدیر آژانس، با پیشنهاد دولت و تأیید مجلس انتخاب می‌شود. علاوه بر مدیر، آژانس یک معاون مدیر هم دارد که شیوه انتخاب او همانند مدیر است. مدیر و معاون باید شهروند کرواسی بوده و علاوه بر تحصیلات دانشگاهی، حداقل ده سال سابقه کار مرتبط داشته باشند. مدت عضویت مدیر و معاون چهار سال بوده و امکان تصویب مجدد بلامانع است. این آژانس مشمول قانون حقوق

و تعهدات کارمندان دولت بوده و حقوق و دستمزد مدیر و معاون همانند حقوق و دستمزد یک مدیر و معاون دستگاه اجرایی است. (Promulgating The Act On Personal Data Protection)

دانمارک

کشور دانمارک عضو اتحادیه اروپا است و به تبعیت از دستورالعمل ۱۹۹۵ اتحادیه، قانون پردازش داده‌های شخصی (The Act on Processing of Personal Data) را در سال ۲۰۰۰ تصویب کرده است. بدیهی است با توجه به عضویت دانمارک در اتحادیه اروپا، قانون پردازش داده‌های شخصی مصوب سال ۲۰۰۰، همگام با تصویب مقررات عمومی حمایت از داده (GDPR) اتحادیه، مورد بازنگری قرار گرفته و سال ۲۰۱۸ مقررات تکمیلی حمایت از داده‌های شخصی به تصویب رسیده است. مسئولیت حفاظت و نظارت بر تمامی مواد این قانون بر عهده آژانس دانمارکی حمایت از داده (Danish data protection Agency) است. این آژانس متشکل از یک شورا و یک دبیرخانه است. مسئولیت تهیه گزارش روزانه و اطلاع به رییس از وظایف دبیرخانه است. اعضای شورا را وزیر دادگستری انتخاب می‌کند، رییس آن باید قاضی باشد، شش عضو اصلی و شش عضو علی‌البدل نیز دارد. اعضا برای چهار سال انتخاب می‌شوند. این آژانس استقلال کامل دارد و باید مقررات و شیوه اجرایی خود را بر مبنای تقسیم کار بین شورا و دبیرخانه تقسیم کند. (The Data Protection Act)

فنلاند

کشور فنلاند عضو اتحادیه اروپا بوده و به تبعیت از دستورالعمل ۱۹۹۵ اتحادیه، قانون فنلاندی داده‌های شخصی (The Finnish Personal Data Act) را در سال ۱۹۹۹، تصویب کرده است. پارلمان این کشور در نوامبر سال ۲۰۱۸، قانون جدید حمایت از داده را، به تبعیت مقررات عمومی حمایت از داده اتحادیه اروپا (GDPR) به تصویب رساند و قانون سال ۱۹۹۹ را منسوخ کرد (Parliament of Finland approves new Data Protection Act). در این کشور، نهاد آمبودزمان حمایت از داده‌ها (The Data Protection Ombudsman) مسئول حمایت و نظارت بر اجرای صحیح قانون است. این نهاد یک دفتر مستقل دارد که در ارتباط با وزارت دادگستری است. اعضای این نهاد ۲۰ نفرند و رییس آن‌ها را شورای دولتی برای پنج سال انتخاب می‌کند. از آنجایی که انتخاب مجدد رییس بلاشکال است، رییس این نهاد از سال ۱۹۹۷ تاکنون تغییر نکرده است. (Data protection is a success factor, available)

ایتالیا

کشور ایتالیا عضو اتحادیه اروپا است و به تبعیت از دستورالعمل ۱۹۹۵ اتحادیه، قانون حریم خصوصی (The Privacy Code) را در سال ۲۰۰۳، تصویب کرده است. مقام حمایت از داده‌ها

(The data protection authority) حافظ این قانون است. این مقام دارای استقلال بوده و چهار عضو دارد که برای هفت سال توسط رییس مجلس انتخاب می‌شوند. این اعضا به ترتیب دارای عناوین رییس، معاون و عضو (دو نفر) هستند. این مقام در حال حاضر ۱۲۵ کارمند دارد.

هلند

کشور هلند عضو اتحادیه اروپا است و به تبعیت از دستورالعمل ۱۹۹۵ اتحادیه، قانون حمایت از داده‌های شخصی (The Act on the Protection of Personal Data) را در سال ۲۰۰۰ تصویب کرده است. این قانون مطابق با مقررات عمومی حمایت از داده (GDPR) در سال ۲۰۱۸ اصلاح شده است. (Data Protection Code - Legislative Decree no. 196/2003). بر اساس این قانون، مقام هلندی حمایت از داده‌ها (Dutch Data protection Authority) مسئول نظارت بر این قانون است. این مقام متشکل از کمیسیونی است که یک رییس و دو عضو دارد. هر سه این اعضا پس از نامزدی، توسط فرمان سلطنتی و تصویب وزیر دادگستری و عدلیه منصوب می‌شوند. مدت ریاست شش سال و مدت حضور دو عضو دیگر چهار سال بوده و انتخاب دوباره آنها تنها برای یک دوره بلامانع است.

آرژانتین

قانون حمایت از داده‌های شخصی به شماره ۲۵,۳۲۶ (Personal Data Protection Law Number 25,326 (The PDPL)) مصوب اکتبر ۲۰۰۰، سطح بسیار گسترده‌ای از حمایت از داده‌های اشخاص را در آرژانتین فراهم آورده است. از آنجایی که این قانون بسیاری از اصول دستورالعمل ۱۹۹۵ اتحادیه اروپا را به رسمیت شناخته است، این اتحادیه در ۳۰ ژوئن ۲۰۰۳ اعلام کرد سطح قابل قبولی از حمایت از داده طبق دستورالعمل مذکور در کشور آرژانتین مورد حمایت است. بنابراین محدودیت خاصی در انتقال داده‌های شخصی شهروندان اروپایی به این کشور وجود ندارد و جریان آزاد اطلاعات از آرژانتین به اتحادیه اروپا نیز مجاز است. (Data protection in Argentina)

آژانس حمایت از داده‌های شخصی (Argentine Personal Data Protection Agency) مسئول حفاظت از این قانون است. این آژانس با حفظ استقلال، به عنوان سازمان غیرمتمرکز در چارچوب وزارت عدلیه و حقوق بشر فعالیت می‌کند. مدیر این آژانس با پیشنهاد دولت و تصویب مجلس سنا، برای یک دوره چهارساله انتخاب می‌شود. (<http://www.jus.gov.ar/datos-personales.aspx>)

تحلیل نهاد متولی داده در نظام حقوقی ایران

همان‌طور که در ابتدا مطرح شد، نظام حقوقی ایران فاقد قانونی جامع در خصوص حریم خصوصی و حمایت از داده است و به طریق اولی متولی رسمی داده نیز در کشور وجود ندارد. لذا با توجه به توسعه فناوری‌های مبتنی بر داده و اهمیت روزافزون داده‌ها به عنوان سرمایه هر کشور، ضروری است در نظام حقوقی ایران نیز قانونی جامع

در زمینه حمایت از داده‌ها تصویب و متولی اجرا و نظارت بر آن نیز به موجب قانون مجلس ایجاد یا تعیین شود.

وضعیت موجود ایران از منظر قوانین و مقررات در خصوص متولی داده

لازم به توضیح است با توجه به نبود متن قانونی منسجم و یکپارچه در این موضوع، کشور با خلأ جدی در این زمینه مواجه است. لذا ضروری است، هر یک از نهادهای مسئول در این حوزه که در ادامه مورد اشاره قرار خواهند گرفت، با توجه محدوده وظایف و صلاحیت‌های خود، جهت رفع این خلأ اساسی در کشور گام بردارند.

مراجع	نام نهاد یا سازمان	ماده قانونی مرتبط
مراجع سیاستگذاری و تقنینی	مجمع تشخیص مصلحت نظام	بند ۱ اصل ۱۱۰ قانون اساسی؛ «تعیین سیاست‌های کلی نظام جمهوری اسلامی ایران» (منبع ۱)
	مجلس شورای اسلامی *	اصل ۷۱ قانون اساسی: «مجلس شورای اسلامی در عموم مسائل در حدود مقرر در قانون اساسی می‌تواند قانون وضع کند.» (منبع ۲)
	شورای عالی فضای مجازی	«تدوین سیاست‌ها و تصویب مقررات کلان مورد نیاز فضای مجازی کشور از جمله توافق‌نامه‌های درجه و سطح خدمات، حمایت از حقوق کاربران فضای مجازی و تنظیم روابط فعالان فضای مجازی در چارچوب مصوبات شورای عالی.» (منبع ۳)
	کمیسیون تنظیم مقررات ارتباطات **	سیاستگذاری، تدوین و تصویب مقررات در حوزه ارتباطات و فناوری اطلاعات (منبع ۴)
مراجع نظارتی و اجرا ***	وزارت ارتباطات و فناوری اطلاعات	قانون اهداف و وظایف وزارت ارتباطات و فناوری اطلاعات: بند ک. «تدوین و پیشنهاد استانداردهای ملی مربوط به ارتباطات و فناوری اطلاعات در کشور به مراجع ذیربط.» بند ف. «حفاظت و حراست و عدم ضبط و افشای انواع مراسلات و امانات پستی و همچنین مکالمات تلفنی و مبادلات شبکه اطلاع‌رسانی و اطلاعات مربوط به اشخاص حقیقی و حقوقی طبق قانون.» (منبع ۵)
	سازمان تنظیم مقررات و ارتباطات رادیویی	بند ۹، ماده ۶ اساسنامه با موضوع وظایف و اختیارات سازمان: «حمایت از حقوق استفاده‌کنندگان خدمات پستی، مخابراتی و فناوری اطلاعات و نظارت مستمر بر اعمال صحیح آن‌ها، تدوین و پیشنهاد دستورالعمل‌های لازم به منظور تنظیم روابط ارائه‌کنندگان خدمات پستی، مخابراتی و فناوری اطلاعات و پیشنهاد اصلاح قوانین پستی، مخابراتی و ارتباطی به مراجع ذیصلاح قانونی.» (منبع ۶)
	کارگروه تعیین مصادیق محتوای مجرمانه	ماده ۲۲ قانون جرایم رایانه‌ای؛ «مسئولیت نظارت بر فضای مجازی و پالایش تارنماهای حاوی محتوای مجرمانه.»
مراجع قضایی	سازمان فناوری اطلاعات	ماده ۲ اساسنامه؛ «مدیریت، حمایت و ساماندهی امور مربوط به امنیت فضای تبادل اطلاعات، نرم‌افزار و سخت‌افزار، بالابردن آمادگی الکترونیک، توسعه اینترنت، توسعه فناوری اطلاعات و کاربردهای آن در کشور.» بند ۱۱ ماده ۷ اساسنامه: «ایجاد، توسعه، نگهداری و بهره‌برداری از مراکز داده ملی اینترنتی به منظور میزبانی و حفظ داده‌های حساس دولتی.» (منبع ۷)
	قوه قضاییه	اصل ۱۵۶ قانون اساسی: «رسیدگی و صدور حکم در مورد تظلمات، تعدیات، شکایات، حل و فصل دعاوی و رفع خصومات و اخذ تصمیم و اقدام لازم.»
	کارگروه تعیین مصادیق محتوای مجرمانه	ماده ۲۲ قانون جرایم رایانه‌ای؛ «رسیدگی به شکایات مردمی.»

منبع ۱: قانون اساسی جمهوری اسلامی ایران. منبع ۲: همان. منبع ۳: وظایف و اختیارات شورای عالی فضای مجازی. منبع ۴: کمیسیون تنظیم مقررات ارتباطات. منبع ۵: قانون تجارت الکترونیک. منبع ۶: اساسنامه سازمان تنظیم مقررات و ارتباطات رادیویی. منبع ۷: اساسنامه سازمان فناوری اطلاعات.

* گفتنی است در سال ۱۳۸۴ و در اواخر دولت هشتم "لایحه مربوط به حفظ حریم خصوصی" تقدیم مجلس شد، که حرکتی رو به جلو و بسیار مثبت بود. مجلس شورای اسلامی و مرکز پژوهش‌های مجلس نیز از این لایحه استقبال خوبی داشتند؛ اما متأسفانه قبل از رسیدگی و تصویب آن، در فروردین سال ۱۳۸۵ دولت جدید (دولت نهم)، آن را پس گرفت. از آن زمان، نه مجلس و نه دولت‌های بعدی این موضوع را پیگیری نکردند. این لایحه در ۷ سرفصل، به "حریم خصوصی جسمانی"، "حریم خصوصی اماکن و منازل"، "حریم خصوصی در محل کار"، "حریم خصوصی اطلاعات"، "اطلاعات شخصی در فعالیت‌های رسانه‌ای"، "حریم خصوصی ارتباطات" و "مسئولیت‌های ناشی از نقض حریم خصوصی" پرداخته بود. بدیهی است به علت عدم تصویب این لایحه، موارد ذکر شده در آن مورد حمایت قانونگذار نخواهد بود و از منوط اعتبار ساقط است، پس نمی‌توان گفت این نهاد نقش خود را در این موضوع به سرانجام رسانده است. در نتیجه، کشور همچنان با خلأ بزرگی نداشتن قانون حمایت از حریم خصوصی مواجه است.

** در خصوص صلاحیت کمیسیون تنظیم مقررات ارتباطات در وضع مقررات لازم در موضوع حریم خصوصی و امنیت داده باید گفت، قانونگذاری وظیفه اولیه و اصلی مجلس شورای اسلامی است، این نهاد به طور عام نمی‌تواند در زمینه حریم خصوصی وارد شود. اما از آنجایی که، حفظ حقوق کاربران در حوزه فناوری اطلاعات و ارتباطات یکی از شاخه‌هایی است که کمیسیون صلاحیت مداخله دارد، در صورت ضرورت می‌تواند الزام‌های فنی حفظ حریم خصوصی کاربران را، با وضع مصوبه‌ای به بازیگران این حوزه بار کند.

*** با توجه به توضیح‌های ارائه شده و انطباق آن با مراجع نظارتی و اجرایی حریم خصوصی، باید گفت بدیهی است نبود متن قانونی منسجم در این موضوع به معنای نبود نهاد نظارتی و اجرایی نیز هست. توضیح بیشتر آنکه یکی از موارد مهمی که در قوانین حریم خصوصی باید مورد توجه قرار گیرد، در نظر گرفتن نهادی به جهت نظارت بر اجرای صحیح قانون مذکور است. از طرف دیگر، مراجع نظارتی و اجرا، که معمولاً نهادی عمومی و دارای استقلال کامل است، به اشخاص این اطمینان را می‌دهد که سطح بالایی از حمایت از حریم خصوصی در کشور جریان دارد. بر اساس همین ضرورت و مطابق آنچه گفته شد، در تمام کشورهای که قانون حریم خصوصی دارند، نهاد حمایت از آن نیز ایجاد شده است. این در حالی است که با وجود اهمیت بالایی که این موضوع دارد، در ایران نادیده گرفته شده و قانون و نهادی برای حمایت از حریم خصوصی در نظر گرفته نشده است. اما سؤال اصلی اینجاست که در صورت تصویب چنین قانونی، کدام یک از نهادهای موجود در کشور، صلاحیت بر عهده گرفتن چنین مسئولیتی را دارد؟ و یا اینکه ضروری است یک نهاد جدید، با ساختار و تشکیلاتی منحصر به خود ایجاد شود؟ هرچند پاسخ به دو سؤال مذکور بسیار مهم است اما به همان اندازه نیز سختی و پیچیدگی دارد. چراکه می‌توان به هر دو سؤال پاسخ مثبت داد، یعنی می‌توانیم بگوییم که سازمان‌های موجود صلاحیت دارند و هم می‌توانیم سازمان

جدیدی برای حمایت از داده ایجاد کنیم. در نتیجه در حال حاضر نمی‌توان پاسخ قطعی به آن‌ها داد و تنها می‌توان به طور کلی، نقش نهادهای نظارتی و اجرایی را در حوزه حریم خصوصی کلان داده‌ها، منطبق با مقررات پراکنده در صورت وجود سازمان شناسایی قرار کرد.

نقدی بر لایحه حمایت از داده و حریم خصوصی در فضای مجازی

بر اساس اهمیت ویژه داده در دنیای امروز، به همت سازمان فناوری اطلاعات ایران و پژوهشگاه قوه قضاییه و دانشگاه علم و فرهنگ "لایحه حمایت از داده و حریم خصوصی در فضای مجازی" تدوین شده است. این لایحه، یکی از مهم‌ترین لوایح در خصوص حفظ حریم خصوصی و صیانت از داده‌ها و اطلاعات کاربران در حوزه فضای سایبر است.

در باب چهارم این پیش‌نویس، با عنوان "تنظیم و نظارت بر پردازش داده‌های شخص"، چهار رکن (کمیسیون صیانت و حفاظت از داده‌های شخصی، هیئت نظارت، کارگروه‌های تخصصی و دبیرخانه اجرایی کمیسیون)، مسئولیت نظارت بر پردازش داده‌های شخصی را بر عهده گرفته‌اند که معادل نهادهای حمایت از داده در سایر کشورهاست. اعضای کمیسیون صیانت و حفاظت از داده‌های شخصی در ماده ۴۰ به این نحو تعریف شده است:

«کمیسیون از اعضای ذیل تشکیل می‌شود:

۱) وزیر ارتباطات و فناوری اطلاعات به عنوان رئیس کمیسیون؛

۲) وزیر اطلاعات؛

۳) وزیر کشور؛

۴) وزیر دادگستری؛

۵) وزیر فرهنگ و ارشاد اسلامی؛

۶) وزیر اقتصاد و امور دارایی؛

۷) دبیر شورای عالی و رئیس مرکز ملی فضای مجازی؛

۸) معاون پیشگیری از وقوع جرم قوه قضائیه؛

۹) رییس کمیسیون اصل نودم مجلس شورای اسلامی؛

۱۰) دادستان کل کشور؛ و

۱۱) دبیر شورای اجرایی فناوری اطلاعات به عنوان دبیر کمیسیون.»

مطابق تبصره این ماده، به تشخیص رییس کمیسیون، جلسه‌ها در سطح اعضا یا معاونان ذیربط آنها با دعوتنامه رسمی تشکیل و احکام عضویت نمایندگان اعضا از سوی رییس کمیسیون صادر می‌شود. مطابق ماده ۴۷ و ۴۸، کارگروه‌های تخصصی، متشکل از نمایندگان نهادهای متولی امور حاکمیتی مرتبط با صیانت و حفاظت از داده‌های شخصی هستند که به وظایف مقرر در این قانون می‌پردازند و در نخستین جلسه کمیسیون، آیین‌نامه تشکیل کارگروه‌ها به تصویب می‌رسد که شامل

بخش‌ها و حیطه کار آن‌ها، ریاست، دبیر و محل دبیرخانه، اعضاء، تکالیف و مأموریت‌ها، چگونگی اداره و رسمیت یافتن جلسه‌ها و مصوبه‌ها، تعامل کارگروه‌ها، گزارش به کمیسیون و سایر مراجع صلاحیت‌دار است.

در باب این بخش از این لایحه ذکر نکات زیر ضروری است:

۱. تنظیم و نظارت باید بر کنترل‌کننده و پردازشگر صورت گیرد، نه فقط پردازش داده‌های شخصی؛
 ۲. در نظر گرفتن چهار رکن یعنی کمیسیون، هیأت نظارت، کارگروه تخصصی و دبیرخانه اجرایی، سبب پیچیده شدن فرایند تنظیم و نظارت و افزایش ساز و کار اداری خواهد شد.
 ۳. ساز و کار اجرایی هر یک از مراجع به مصوبات بعدی ارجاع داده شده است، که سبب افزایش مقررات لازم‌الاجرا شده و دوباره ساز و کار اجرایی قانون را با اختلال روبه‌رو خواهد کرد.
 ۴. اعطای صلاحیت، برای حل و فصل اختلافات، بین کارگروه‌های تخصصی و هیأت نظارت و سایر نهادهای حاکمیتی، در تناقض با صلاحیت‌های دیوان عدالت اداری است.
 ۵. کارگروه‌های تخصصی که نمایندگان نهادهای متولی امور حاکمیتی معرفی شده‌اند، واضح نیست؛ متولی امور حاکمیتی چه نهادهایی هستند؟
- از این رو، پیشنهاد می‌شود یک کمیسیون برای نظارت بر اجرای صحیح این لایحه و به تبع آن کنترل‌کنندگان و پردازشگران تشکیل شود و وظایف، صلاحیت‌ها و اختیارات نهاد مذکور بدون ارجاع به مصوبه‌های بعدی در متن خود لایحه پیش‌بینی شود تا ساز و کارهای اداری پیچیده در مسیر حمایت و صیانت از داده‌های شخصی وجود نداشته باشد.

نتیجه‌گیری

بررسی تحول‌های صورت‌گرفته در نظام حقوقی کشورهای پیشرو، در زمینه صنعت فناوری اطلاعات و ارتباطات، حاکی از آن است که این کشورها، به دنبال توسعه فناوری‌های اطلاعاتی و شکل‌گیری کسب و کارهای مبتنی بر داده، به سبب پیدایش چالش‌ها و مخاطرات گسترده‌ای در این زمینه، یک نهاد رسمی به عنوان "متولی داده" تشکیل داده‌اند. مسئولیت این نهادها، تنظیم و نظارت بر این حوزه، بر اساس قوانین و مقررات حمایت از داده است.

حال آنکه نتایج بررسی اسناد بالادستی و رویه‌های اجرایی کشور، مؤید این مطلب است که در نظام حقوقی ایران، قانون جامعی در خصوص حفاظت از داده‌ها وجود ندارد و بالطبع، نهادی هم متولی رسمی داده در کشور نیست. این امر باعث شده تا علیرغم رشد فناوری‌های نوین، بسترهای قانونی مرتبط با حقوق داده در نظام حقوقی کشور تشکیل نشود. در نتیجه، رشد کسب و کارهای مبتنی بر داده نیز در ایران به‌کندی صورت خواهد گرفت؛ لذا با توجه به اینکه بهره‌برداری مبتکرانه از ارزش سرمایه‌ای داده‌ها مستلزم تصویب یک قانون جامع و متناسب با فناوری‌های نوین و

همچنین وجود یک نهاد رسمی، به‌عنوان مجری این قانون، تنظیم‌کننده و ناظر بر این حوزه است، پیشنهاد می‌شود که در نظام حقوقی ایران نیز قانون جامعی در خصوص حمایت از داده تصویب شود؛ همچنین یک نهاد، به‌عنوان متولی رسمی داده در کشور ایجاد یا از میان نهادهای موجود ضمن اعطای این اختیار از طریق اصلاح و به‌روزرسانی قوانین و مقررات مربوط نهاد متولی داده تعیین شود.

در مقام جمع‌بندی، با توجه ساختار نهاد متولی حمایت از داده و همچنین وظایف و اختیارات آن در کشورهای مورد بررسی، می‌توان دو ویژگی زیر را از مهم‌ترین ویژگی‌های نهادهای متولی داده در نظر گرفت:

۱. نهاد متولی داده باید یک نهاد مستقل فراقوه‌ای یا فراسازمانی باشد؛ چراکه موضوع داده منحصر به حوزه فناوری ارتباطات و اطلاعات (فاوا) نبوده و در سایر حوزه‌ها نظیر سلامت، آموزش، امور قضایی و غیره نیز موضوعیت دارد. لذا به منظور لازم‌الاجرا شدن استانداردها و مصوبه‌های این نهاد توسط سایر نهادهای حاکمیتی، لازم است که این نهاد به‌صورت فراقوه‌ای تشکیل شود و ترکیب آن متشکل از نمایندگان قوا و سازمان‌های ذی‌صلاح باشد.

نکته در خور توجه، در ترکیب نهاد متولی داده، حضور شخصیت‌های عمومی با دانش و تخصص آکادمیک یا اشخاص معرفی شده از طرف سازمان‌های مدنی یا انجمن‌های صنفی در آن است، که حضور این دسته از اشخاص ضمن تضمین استقلال این نهاد، موجب پر کردن خلأهای موجود میان دولت و مردم، جبران نقایص بازار و دولت و درنهایت به عنوان ضربه‌گیری در مقابل این دو است. ۲. نهاد متولی داده، اختیار قانونگذاری در حوزه داده را ندارد و تنها متولی اجرا و نظارت بر قانون حمایت از داده مصوب پارلمان است.

در نهایت، باید گفت امید است ساختار قانونی کشور ایران، به‌ویژه لایحه "حمایت از داده و حریم خصوصی در فضای مجازی" با توجه به تجارب جهانی مورد بررسی و بازنگری عمیق‌تری قرار گیرد.

پی‌نوشت‌ها

۱. دکتر کاظم معتمدنژاد در کتاب جامعه اطلاعاتی خود از معادل "سازمان نظم‌دهی ارتباطات" و وزارت ارتباطات و اطلاعات کشور از معادل "سازمان تنظیم مقررات و اطلاعات" برای واژه رگولاتوری استفاده کرده‌اند. اما در این مقاله همانطور که در مقدمه مورد اشاره قرار خواهد گرفت، منظور از رگولاتوری، نهاد متولی داده جهت تنظیم‌گری و نظارت بر حوزه داده بر اساس قوانین و مقررات حمایت از داده است که به علت عدم تعیین معادل فارسی مناسب، از همان واژه رگولاتوری استفاده شده است.

2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

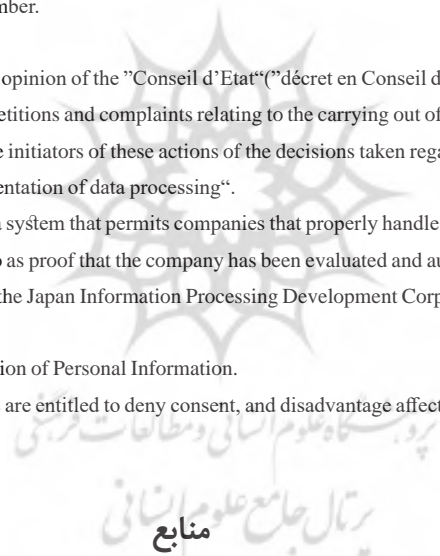
3. Working Party on the Protection of Individuals with regard to the Processing of Personal Data.

4. Working party (WP29)

5. examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures.
6. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016³ 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)
7. The Commission Nationale De l'Informatique Et Des Libertés
8. "It shall inform all data subjects and data controllers of their rights and duties"....
9. "The collection and processing of personal data that reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or which concern their health or sexual life, is prohibited".
10. "Automatic processing of personal data must be notified to the CNIL"....

۱۱. مطابق با قانون شماره ۵۱-۷۱۱، ۷ ژوئن ۱۹۵۱.

12. NIR (Registration Number of Natural Persons In The National Register For the Identification of Individuals, I.E. Social Security Number.
13. Opinion of the CNIL.
14. by a decree subject to a prior opinion of the "Conseil d'Etat" ("décret en Conseil d'Etat").
15. "(c) it shall receive claims, petitions and complaints relating to the carrying out of the processing of personal data and inform the initiators of these actions of the decisions taken regarding them".
16. "Supervision of the implementation of data processing".
17. The privacy mark system is a system that permits companies that properly handle personal information to use the privacy mark logo as proof that the company has been evaluated and authorized by third-party organizations such as the Japan Information Processing Development Corporation (JIPDEC) or its designated institutions.
18. Limitation to Use and Provision of Personal Information.
19. The fact, which data subjects are entitled to deny consent, and disadvantage affected resultantly from the denial of consent.



منابع

- اساسنامه سازمان تنظیم مقررات و ارتباطات رادیویی، قابل دسترسی در: <https://www.cra.ir/statute>
- اساسنامه سازمان فناوری اطلاعات، قابل دسترسی در: <https://www.ito.gov.ir/statute>
- قانون اساسی جمهوری اسلامی ایران، قابل دسترسی در: https://rc.majlis.ir/fa/content/iran_constitution
- قانون تجارت الکترونیک، قابل دسترسی در: <http://rc.majlis.ir/fa/law/show/93997>
- کمیسیون تنظیم مقررات ارتباطات، قابل دسترسی در: <https://www.cra.ir/commission>
- میربها، فاطمه (۱۳۹۸)، "کاربرد محتوای تولید کاربر در بازاریابی"، فصلنامه رسانه، سال سی ام، شماره ۴.
- وظایف و اختیارات شورای عالی فضای مجازی، قابل دسترسی در: http://www.majazi.ir/general_content/76437
- وظایف - اختیارات - مرکز ملی - فضای - مجازی.html?html=محتوای - عمومی

- About the Agency, available at: <https://azop.hr/about-agency/>
- About the Danish Data Protection Agency, available at: <https://www.datatilsynet.dk/english/about-us/>
- Article 29 working party archives 1997 – 2016, available at: https://ec.europa.eu/justice/article-29/documentation/index_en.htm
- CNIL, available at: <https://www.cnil.fr/en/node/287>
- Data Protection Code - Legislative Decree no. 196/2003, available at: https://www.garanteprivacy.it/web/guest/home_en/italian-legislation¹
- Data protection in Argentina: overview, available at: <http://www.ebv.com.ar/images/publicaciones/trdatap.pdf>
- Data protection is a success factor, available at: <https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman>
- French Data Protection Act, available at: <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>
- <http://www.jus.gob.ar/datos-personales.aspx>
- Parliament of Finland approves new Data Protection Act, available at: <https://www.roschier.com/news-and-media/parliament-finland-approves-new-data-protection-act>
- Personal Information Protection Act, available at: <http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf>
- Promulgating The Act on Personal Data Protection, available at: http://www.ceecprivacy.org/doc/law_croatia.pdf
- Status of PIPC, available at: <http://www.pipc.go.kr/cmt/english/introduction/status.do>
- The Data Protection Act, available at: <https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf>

