وظایف کنترل‌کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات

علی‌اکبر فرحزادی[1]، حسین صادقی[2]، مهدی ناصر[3]

دریافت: ۱۴۰۱/۰۸/۲۵ پذیرش: ۱۴۰۱/۱۲/۰۲

چکیده

در دنیای کنونی، پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات نیازمند سازوکارهایی در جهت حفظ تمامیت و امنیت اجرای شبکه است. ازجمله اجزای شبکه، اشخاص موضوع داده و داده‌پیام‌های مورد تبادل می‌باشند. در این فرایند مدیران شبکه‌های تبادل اطلاعات و پردازندگان داده‌پیام‌ها که اصطلاحاً کنترل‌کننده و پردازنده نامیده می‌شوند، دارای وظایفی هستند. پژوهش حاضر به دنبال پاسخ به وظایف اشخاص مذکور در زمینه پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات چه خواهد بود. بدین ترتیب، پژوهش حاضر به روش اسنادی بامطالعه مقررات حاکم بر نظام حقوقی اتحادیه اروپا و تطبیق این مقررات در حقوق ایران، وظایف این اشخاص را در انجام اقدامات مناسب در اجرای صحیح و قانونی پردازش اطلاعات، وظایف در قبال اطلاع‌رسانی به اشخاص موضوع داده (اخذ رضایت وی جهت پردازش، اعلام دلایل رد درخواست او، رفع محدودیت از پردازش، اقدامات حفاظتی در تبادل فراملی اطلاعات، حقوق موضوع داده، اقدامات صورت گرفته در فرایند پردازش اطلاعات، وجود خطر در پردازش)، سایر کنترل‌کنندگان و پردازندگان (در اعلام مراتب حذف یا ایجاد محدودیت در پردازش) و مقامات نظارتی (در همکاری و اطلاع‌رسانی) انجام کرده است..

واژگان کلیدی: کنترل‌کنندگان، پردازندگان، شبکه‌های تبادل اطلاعات، حقوق اتحادیه اروپا.

[1] دانشیار دانشگاه علوم قضایی و خدمات اداری، تهران، ایران، farahzadi@ujsas.ac.ir

[2] دانشیار دانشگاه تهران، تهران، ایران، hosadeghi@ut.ac.ir

[3] دانشجوی دکترای حقوق خصوصی دانشگاه علوم قضایی و خدمات اداری، تهران، ایران، Mn.ujsasac0077@yahoo.com

مقدمه

شبکه تبادل اطلاعات به مجموعه کامپیوترهای متصل‌به‌هم اطلاق می‌گردد که در یک بستر مبادرت به تبادل داده‌پیام‌های الکترونیکی می‌کنند. تبادل داده‌پیام‌های الکترونیکی زمانی می‌تواند ثمربخش بوده و اهداف حاصل از تبادل را محقق سازد که امنیت شبکه مورداستفاده حفظ گردد. «امنیت» در شبکه‌های ارتباطی به معنای به‌کارگیری سازوکارهایی در راستای حفظ تمامیت نرم‌افزارها، سخت‌افزارها، اشخاص موضوع داده که اطلاعات آن‌ها تحت جمع‌آوری و پردازش قرار می‌گیرند، دستگاه‌های ارتباطی و داده‌پیام‌های مورد تبادل در آن‌ها به‌عنوان اجزای شبکه است.

در این میان، سازوکارهای مختلفی در حوزه فناوری اطلاعات مانند به‌کارگیری دستگاه‌های امنیتی مانند فایروال‌ها و نرم‌افزارهای ضدویروس، تنظیمات امنیتی در روتر یا سیستم‌عامل دستگاه‌های رمزگذاری داده برای داده‌های حساس، پشتیبان گیری از داده‌ها ازجمله استفاده از پشتیبان گیری خارج از سایت، محدود کردن دسترسی به زیرساخت‌های شبکه فقط به افراد مجاز و موارد مشابه وجود دارند که می‌توانند این امنیت را حفظ کنند؛ اما حلقه مفقوده این پروسه که در پژوهش‌های دیگر نیز کمتر بدان پرداخته‌شده عدم تحلیل سازوکارهای حقوقی در حفظ «امنیت» شبکه در جمع‌آوری و تبادل اطلاعات است.

داده‌پیام به هر نمادی از واقعه، اطلاعات یا مفهوم که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود، اطلاق می‌گردد.[1] داده‌پیام‌های الکترونیکی به دو دسته داده پیام شخصی و غیرشخصی تقسیم می‌شوند «داده پیام شخصی به اطلاعاتی گفته می‌شود که به صورت مستقیم یا غیرمستقیم زمینه شناسایی اشخاص حقیقی را فراهم می‌آورند» (van der Sloot, 2017,18). اهمیت این نوع اطلاعات ازآنجا نمایان می‌گردد که انجام وظایف نهادهای دولتی و غیردولتی درگرو پردازش این نوع اطلاعات بوده و داده‌پیام‌های غیرشخصی عموماً کاربردی در زمینه پردازش اطلاعات ندارند.

[1] ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲

پردازش به تعبیر بند دوم از ماده ۴ مقررات مصوب ۲۰۱۶ «به عملیاتی ازجمله جمع‌آوری، ضبط، سازمان‌دهی، ساختاربندی، ذخیره‌سازی، سازگاری یا تغییر، بازیابی، مشاوره، استفاده، افشای از طریق تبادل، انتشار یا استفاده دیگر، تراز یا ترکیب، محدودیت، پاک یا اصلاح کردن و تخریب داده اطلاق می‌گردد که از طریق وسایل خودکار یا غیر خودکار بر روی داده‌پیام‌ها انجام می‌شود» (Intersoft Consulting, 2023).

در نظام حقوقی ایران نیز، بند دوم از ماده ۲ طرح حمایت و حفاظت از داده و اطلاعات شخصی واصل‌شده به مجلس شورای اسلامی در تاریخ ۱۳۹۹/۰۷/۱۲ نیز بابیان تعریفی مشابه با آنچه در نظام حقوقی اتحادیه اروپا قیدشده، مقرر می‌دارد «پردازش هرگونه عملیات دستی یا خودکار برداده‌ها و اطلاعات شخصی، از قبیل ایجاد، ثبت، دریافت، گردآوری، نگهداری، جداسازی، تغییر، تجزیه‌وتحلیل، طبقه‌بندی، ساختاربندی، تطبیق، ذخیره‌سازی، اشتراک‌گذاری، فرستادن، توزیع و عرضه، انتشار و در دسترس قراردادن و پاک کردن آن‌ها است».

همانطورکه در تعاریف مذکور مشاهده می‌گردد، گستردگی مصادیق مندرج در تعریف پردازش در مقررات مصوب ۲۰۱۶ و طرح فوق‌الذکر، منجر شده است تا تقریباً تمامی اعمال انجام‌شده بر روی داده‌پیام‌ها توسط اشخاص حقیقی یا حقوقی قابلیت ذکر، ذیل عنوان پردازش داده داشته باشند. پردازش اطلاعات در شبکه‌های ارتباطی نیازمند برخی الزامات و سازوکارها است تا با پیشگیری از نقض امنیت اطلاعات به‌عنوان یکی از اجزای شبکه، امکان حفظ امنیت شبکه ارتباطی نیز فراهم گردد.

در این میان اشخاص فعال در فرایند پردازش اطلاعات در یک شبکه ارتباطی همواره وظایفی در قبال داده‌پیام‌های مورد پردازش دارند. درصورتی‌که این اشخاص مبادرت به رعایت مقررات قانونی و انجام وظایف از پیش تعیین‌شده نمایند، می‌توان از نقض امنیت اطلاعات در شبکه پیشگیری نمود. نظام حقوقی اتحادیه اروپا با تصویب قانون مصوب سال ۲۰۱۶ خود، مقررات مفصلی در باب وظایف کنترل‌کنندگان شبکه‌های ارتباطی و پردازندگان اطلاعات در شبکه‌ها پیش‌بینی نموده است. این در حالی است که نظام حقوقی ایران فاقد مقرره‌ای لازم‌الاجرا در این زمینه است.

به‌عبارت‌دیگر معضل و مشکل اصلی که پژوهش حاضر به دنبال رفع خلأهای آن در نظام حقوقی ایران است، تهی بودن این نظام از برخی سازوکارهای پیشگیرانه در جهت تعیین وظایف اشخاصی که مدیریت شبکه‌های تبادل اطلاعات و پشتیبانی و پردازش داده‌پیام‌ها را بر عهده‌دارند، است. این موضوع به‌صورت مفصل در مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا پیش‌بینی‌شده است. مطالعه این مقررات و همچنین تبیین سازوکارهای موجود در این نظام می‌تواند گام‌های اولیه و مناسبی در جهت رفع خلأهای تقنینی در نظام حقوقی ایران سنجیده شود.

البته این موضوع نیز بدیهی است که صرف پیش‌بینی برخی سازوکارها در یک نظام خارجی نمی‌تواند مبنایی صرف بر تغییر و اصلاح قوانین در نظام اسلامی کشور ایران باشد؛ اما بیان راهکارهای پیش‌بینی‌شده در نظامات توسعه‌یافته می‌تواند به‌منزله گام‌هایی در جهت معرفی راهکارهای اندیشیده شده در نظامات دیگر و تحلیل و بررسی آن‌ها در کشور ایران تلقی گردد. امری که هدف اصلی این پژوهش را به خود اختصاص داده است.

در زمینه نوآوری پژوهش حاضر نیز می‌توان بیان داشت، پژوهش‌های انجام‌شده در حفظ امنیت شبکه‌های تبادل اطلاعات ازجمله امنیت شبکه: چالش‌ها و راهکار (چاپ‌شده در فصلنامه پژوهشنامه پردازش و مدیریت اطلاعات)، نقش سیستم‌های بیومتریک در امنیت شبکه (چاپ‌شده در فصلنامه علوم و فناوری دریا)، مروری بر امنیت شبکه‌های مخابراتی مورداستفاده در شبکه‌های توزیع برق (چاپ‌شده در فصلنامه محاسبات نرم)، عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان‌های استان سیستان و بلوچستان و اولویت‌بندی آن‌ها (چاپ‌شده در فصلنامه پژوهش‌های مدیریت عمومی)، برنامه‌ریزی و بهره‌برداری منابع اکتیو و راکتیو مقید به امنیت ولتاژ در شبکه توزیع هوشمند قابل بازآرایی (فصلنامه مهندسی و مدیریت انرژی) همگی به سازوکارهای فنی در جهت حفظ امنیت شبکه‌های تبادل اطلاعات پرداخته‌اند که خارج از محوریت پژوهش حاضر است.

علاوه بر آن در میان پژوهش‌های حقوقی نیز پژوهشی که به‌صورت مستقل مبادرت به بررسی سازوکارهای حقوقی پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات بپردازد، تاکنون صورت نگرفته و در برخی پژوهش‌ها ازجمله رفع تقابل بین

حق آزادی بیان و اطلاعات با حق برداده های شخصی در رسانه‌ها از منظر حقوق اتحادیه اروپا و نظام حقوقی ایران (چاپ‌شده در فصلنامه پژوهش‌های ارتباطی) نیز محوریت بحث اگرچه مرتبط با رسانه‌ها و شبکه‌های ارتباطی است اما نویسنده مقاله فوق، به بررسی تزاحمات میان حق آزادی بیان و حق برداده های شخصی به‌عنوان دو حق اساسی اشخاص پرداخته است که ارتباطی به پژوهش حاضر ندارد. ازاین‌رو این پژوهش در محوریت خود یک تحقیق نوین است.

بابیان مطالب فوق اینک نوبت به تبیین مطالب اصلی این پژوهش می‌رسد. ازآنجاکه واژگانی مانند کنترل‌کننده و پردازنده در ادبیات حقوقی، مفاهیمی نو تلقی می‌شوند، دستیابی به اهداف پژوهش در بدایت امر نیازمند تحلیل حقوقی این مفاهیم است. ازاین‌رو گفتار اول این پژوهش به مفهوم شناسی کنترل‌کننده و پردازنده در شبکه‌های تبادل اطلاعات اختصاص‌یافته و پس از تبیین این مفاهیم در گفتار دوم نسبت به تحلیل وظایف این اشخاص در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات اقدام خواهد شد.

۱- مفهوم شناسی کنترل‌کننده و پردازنده

طرح مباحث اصلی پژوهش در باب وظایف کنترل‌کنندگان و پردازندگان در شبکه‌های تبادل اطلاعات در وهله اول نیازمند آشنایی با مفهوم این واژگان است؛ بنابراین گفتار اول از پژوهش حاضر به تبیین مفهوم قانونی دو واژه کنترل‌کننده و پردازنده اختصاص‌یافته است.

۱-۱- کنترل‌کننده

کنترل‌کننده به تعبیر بند هفتم از ماده ۴ مقررات مصوب سال ۲۰۱۶ «به معنای شخص حقیقی یا حقوقی، مقام عمومی، سازمان یا نهاد دیگری است که به‌تنهایی یا مشترکاً با دیگران، اهداف و ابزار پردازش داده‌های شخصی را تعیین می‌کند. در مواردی که اهداف و ابزار چنین پردازشی توسط قانون اتحادیه یا کشور عضو تعیین‌شده است، کنترل‌کننده یا معیارهای خاص برای تعیین آن ممکن است توسط قانون اتحادیه یا کشور عضو پیش‌بینی شود».

در کنار مقررات مصوب سال ۲۰۱۶، طرح حمایت و حفاظت از داده‌های شخصی سال ۱۴۰۰ ایران نیز در بند پ از ماده ۲ خود از کنترل‌کننده به واژه کنترل‌گر تعبیر و بیان داشته که «کنترل‌گر شخصی است که همه یا بخشی از هدف، سازوکار، شرایط، ویژگی‌ها و ابزارهای یک یا چند عملیات پردازش داده‌ها و اطلاعات شخصی در اختیار پردازش گر را تعیین می‌کند. مصوبات و تصمیمات مراجع صلاحیت‌دار در امور تنظیم گری، نظارت، ضابطیت و دادرسی درباره پردازش داده‌ها و اطلاعات شخصی، جز در مواردی که جنبه فردی دارد، کنترل گری به شمار نمی‌آید».

نکته اول در بررسی مقررات فوق این است که خط مش و به عبارتی «مدیریت یک شبکه ارتباطی بر عهده کنترل‌کننده است». این شخص می‌تواند یک شخص حقیقی یا شخص حقوقی دولتی یا غیردولتی باشد که تصمیم‌گیری در خصوص پردازش اطلاعات و چگونگی و دلیل پردازش بر عهده وی است (احمدوند و جهانشاهی، ۱۴۰۲، ۱۰۸). اگرچه در بدایت امر مقررات بیان‌شده در فوق میان کنترل‌کننده و پردازنده قائل به تفاوت شده و در ظاهر فرایند پردازش اطلاعات را در صلاحیت پردازنده قرارداده‌اند، اما به نظر می‌رسد، این موضوع مانع از جمع سمت پردازنده و کنترل‌کننده در یک شخص نخواهد بود.

اگرچه نص بند هفتم ماده ۴ مقررات مصوب ۲۰۱۶، تعیین خط مش و اهداف عملکرد یک شبکه تبادل اطلاعات را در اختیار کنترل‌کننده قرارداده که به‌تنهایی یا با کمک دیگر اشخاص حقیقی یا حقوقی امکان تعیین آن‌ها را دارد، اما درهرحال «مجری و مسئول در قبال اقدامات صورت گرفته در یک شبکه کنترل‌کننده خواهد بود»(Iron Montain,2023).

مضافاً اینکه ماده فوق‌الذکر، علیرغم ارائه تعریف و سازوکار شناسایی کنترل‌کننده در نظام حقوقی اتحادیه اروپا، امکان تعیین شرایط شناسایی کنترل‌کننده را به‌نظام داخلی کشورهای عضو نیز اعطا نموده و می‌توان نتیجه‌گیری نمود که مقررات بند هفتم از ماده ۴ علی‌رغم تصریح در یک قانون آمره، دارای وجه تکمیلی بودن می‌باشند.

نکته مهمی که باید بدان توجه نمود این است که قسمت دوم از بند پ ماده ۲ طرح حمایت و حفاظت از داده‌های شخصی ایران، با تصریح به عبارت «مصوبات مراجع

صلاحیت‌دار» این موضوع را به ذهن احاله می‌نماید که کنترل‌کنندگان در شبکه‌های تبادل اطلاعات الزاماً اشخاص حقوقی بوده و امکان اطلاق این واژه به یک شخص حقیقی در نظام حقوقی ایران وجود ندارد؛ اما به نظر نگارنده، این موضوع را باید ناشی از مسامحه و ناظر به مورد غالب دانست. چراکه واژه «شخص» در صدر ماده هم شامل اشخاص حقیقی و هم شامل اشخاص حقوقی شده و لزومی ندارد، تعیین خط مش برای یک شبکه تبادل اطلاعات حتماً توسط یک مرجع رسمی دولتی یا غیردولتی صورت پذیرد. ازاین‌رو در نظام حقوقی ایران نیز می‌توان کنترل‌کننده را شخص حقیقی یا حقوقی قلمداد نمود.

نکته دیگری که می‌توان بدان اشاره نمود، اصطلاح «کنترل‌کنندگان مشترک» است. این اصطلاح در ماده ۲۶ از مقررات مصوب سال ۲۰۱۶ تصریح‌شده و کنترل‌کنندگانی که به‌طور مشترک اهداف، دستورالعمل‌ها و ابزارهای پردازش را فراهم می‌آورند، در وظایف و مسئولیت‌ها نیز همسان در نظر گرفته است. در این زمینه تفاوتی وجود ندارد که کنترل‌کنندگان حتماً اشخاص حقیقی یا حقوقی بوده و در یک فرایند پردازش اطلاعات در یک شبکه ممکن است کنترل‌کنندگان مشترک اشخاص حقیقی و حقوقی در کنار یکدیگر باشند.

«البته صرف همکاری در پردازش داده‌ها، لزوماً اشخاص را به کنترل‌کنندگان مشترک تبدیل نمی‌کند، بلکه باید حتماً این اشخاص دارای اهداف و خط مش مشترک در یک فرایند باشند»(لطیف زاده، ۱۴۰۲، ۲۴۹)؛

به‌عنوان‌مثال درصورتی‌که چند شرکت خودروسازی با طراحی یک سایت در خصوص نحوه جمع‌آوری اطلاعات مشتریان خود توافق نمایند، می‌توان آن‌ها را به‌عنوان کنترل‌کنندگان مشترک در نظر گرفت.

۱-۲- پردازنده

بند هشتم از ماده ۴ مقررات مصوب سال ۲۰۱۶ در خصوص پردازنده بیان می‌دارد: «پردازنده به معنای یک شخص حقیقی یا حقوقی، مقام عمومی، سازمان یا نهاد دیگری است که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند». در کنار آن بندت ماده ۲ طرح حمایت و حفاظت از داده‌های شخصی نیز با تعبیر پردازنده به

پردازشگر، بیان می‌دارد که «پردازش گر شخص مأذون کنترل‌گر در پردازش است. در صورت نبود کنترل‌گر یا عدم امکان اتصاف پردازش به آن، پردازش گر به‌عنوان کنترل‌گر نیز شناخته می‌شود».

در خصوص پردازنده باید بیان داشت، به‌تصریح بند هشتم ماده ۴ مقررات مصوب سال ۲۰۱۶، پردازنده یک شخص حقیقی یا حقوقی دولتی یا غیردولتی است که نسبت به پردازش اطلاعات با سازوکار تعیین‌شده توسط کنترل‌کننده اقدام می‌کند؛ بنابراین وجه تمایز اصلی میان کنترل‌کننده و پردازنده این است که پردازنده همواره مجری است نه سیاست‌گذار؛ بنابراین درصورتی‌که شخصی علاوه بر اجرا، از صلاحیت سیاست‌گذاری نیز برخوردار باشد، به‌تصریح بندت ماده ۲ طرح حمایت و حفاظت از داده‌های شخصی، عنوان کنترل‌کننده را نیز خواهد داشت. اثر این موضوع در شناسایی مسئولیت آن در فرایند پردازش اطلاعات در یک شبکه ارتباطی نمایان می‌گردد.

برای تشخیص عنوان کنترل‌کننده از پردازنده می‌توان به دو مثال ذیل توجه نمود. یک سایت فروش و عرضه محصولات مانند آمازون را در نظر بگیرید. هنگام ورود به سایت و خرید محصول، اطلاعات شخصی ازجمله نام و نام خانوادگی و آدرس و... خریدار پس از خرید کالا از این سایت جمع‌آوری و پس از پرداخت هزینه توسط خریدار، به اپراتور انبار جهت تخصیص کالا و ارسال به مقصد اعلام می‌گردد، یا در سراچه‌هایی مانند هِین آنلاین، خرید اشتراک و درخواست اطلاعات هویتی برای ایجاد کاربری توسط سامانه یا یک اپراتور آنلاین که وظیفه پشتیبانی از سایت را بر عهده دارد صورت پذیرفته و پس از ایجاد حساب کاربری و پرداخت هزینه، امکان دانلود مقدار مشخصی مقاله توسط اپراتور برای کاربر فراهم می‌گردد.

در مثال اول وظیفه جمع‌آوری و ارسال اطلاعات جهت تخصیص فلان کالا و ارسال به مقصد توسط اپراتور سایت صورت پذیرفته و به عبارتی ارائه دستور جهت تخصیص کالا یا ارائه خدمات توسط اپراتور صورت می‌پذیرد. ازاین‌رو اپراتور نقش کنترل‌کننده در این شبکه را برخوردار است.

«در مقابل شخص یا سامانه‌ای که در انبار، اطلاعات واصله را پردازش و نسبت به ارسال کالا به مقصد اقدام می‌کند، پردازنده تلقی می‌گردد»(Clarip,2023) ؛ اما در مثال دوم، با توجه به اینکه فرایند جمع‌آوری و پردازش اطلاعات توأمان توسط یک

شخص صورت می‌پذیرد، عنوان کنترل‌کننده و پردازنده در یک شخص جمع شده و آن شخص دارای وظایف و مسئولیت‌های کنترل‌کننده و پردازنده خواهد بود.

۲-وظایف کنترل‌کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات

بابیان تعریف کنترل‌کننده و پردازنده در گفتار پیشین، در گفتار حاضر نسبت به تبیین وظایف این اشخاص در فرایند پردازش اطلاعات شبکه‌های ارتباطی اقدام خواهد شد.

۲-۱- انجام اقدامات مناسب در اجرای صحیح و قانونی پردازش اطلاعات

همان‌طور که بیان گردید، فرایند پردازش اطلاعات توسط یا تحت نظارت و دستورات صادره از سوی کنترل‌کننده صورت می‌پذیرد. ازاین‌رو درصورتی‌که کنترل‌کننده در اعطای پردازش اطلاعات به پردازشگر، وظایفی ازجمله اعتبارسنجی او را بر عهده دارد. اعتبارسنجی پردازشگر با دریافت تضمین کافی در انجام پردازش قانونی و عدم نقض امنیت اطلاعات در دسترس صورت می‌پذیرد؛

بنابراین یکی از معیارهای انتخاب پردازشگر در پردازش اطلاعات می‌تواند کیفیت و کمیت تضمین ارائه‌شده توسط وی باشد. این موضوع در بند اول از ماده ۲۸ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا مورد تصریح قرارگرفته است. این بند مقرر می‌دارد:

در مواردی که قرار است پردازش از طرف یک کنترل‌کننده انجام شود، کنترل‌کننده باید فقط از پردازشگرهایی استفاده کند که تضمین‌های کافی برای اجرای اقدامات فنی و سازمانی مناسب را ارائه می‌دهند، به‌گونه‌ای که پردازش الزامات این آیین‌نامه را برآورده و حمایت از حقوق موضوع داده‌ها را تضمین کند.

در بررسی مفاد این بند می‌توان به نکاتی دست‌یافت. نکته اول این است که وجود عبارت «فقط از پردازشگرهایی استفاده کند» مفید این معنا است که کنترل‌کننده موظف به اخذ تضمین از پردازشگری که فرایند پردازش اطلاعات را به وی می‌سپرد بوده و اعطای فرایند پردازش به پردازشگری که نسبت به ارائه تضمین اقدام نکند، ممنوع است.

نکته دوم این است که پردازشگر باید نسبت به ارائه «تضمین کافی» به کنترل‌کننده

اقدام نماید؛ اما سؤال اینجاست که کفایت تضمین داده‌شده بر چه معنایی باید سنجیده شده و مرجع تشخیص این کفایت چه کسی خواهد بود؟ برای پاسخ به این سؤال باید بیان داشت، ازآنجاکه در کلیه فرایند پردازش اطلاعات، مسئولیت حقوقی نقض امنیت اطلاعات و کاربران آن‌ها بر عهده کنترل‌کننده است، اصولاً تعیین میزان کفایت تضمین نیز برای حفظ امنیت شبکه بر عهده کنترل‌کننده خواهد بود. معیار کفایت نیز به نظر نگارنده به میزانی است که کنترل‌کننده از حفظ امنیت اطلاعات یا جبران خسارات وارده در صورت نقض، اطمینان حاصل نماید.

نکته سوم این است که اخذ تضمین از پردازنده به‌منزله شرط لازم در اعطای فرایند پردازش به وی محسوب اما شرط کافی محسوب نمی‌گردد. در این راستا کنترل‌کننده علاوه بر ارائه دستورالعمل‌های حفاظتی در چگونگی اجرای حفاظت از اطلاعات، باید به‌طور مستمر، عملکرد پردازنده را تحت نظر داشته و جزئیات اقدامات وی را تحت رصد قرار دهد (لطیف زاده، پیشین،۲۵۱). در این صورت حتی در فرضی که امنیت برخی داده‌پیام‌ها نقض گردد، می‌توان با شناخت چالش به وجود آمده و حل آن، از نقض امنیت دیگر داده‌پیام‌ها پیشگیری نمود.

نکته آخر این است که «اعطای فرایند پردازش اطلاعات به پردازنده، باید تحت انعقاد قرارداد کتبی صورت پذیرد»(EUR-Lex,2016,49). اگرچه در هر نظام حقوقی توافقات اشخاص می‌تواند در قالب کتبی یا شفاهی به قرارداد تبدیل شود، اما حساسیت موضوع و وجود شرایطی مانند اخذ تضمین کافی موجب می‌گردد تا امکان انعقاد قرارداد شفاهی در این موضوع وجود نداشته باشد. چراکه طرفین باید در قرارداد خود میزان و نوع تضمین اخذشده از سوی پردازنده را درج نمایند تا در صورت وقوع اختلاف یا اقدام پردازشگر برخلاف دستورات داده‌شده، امکان جبران خسارت وجود داشته باشد. علاوه بر آن دستورالعمل‌های اولیه جهت شروع فرایند پردازش نیز می‌تواند ازجمله شروط قرارداد مذکور تلقی گردد تا امکان استناد به مسئولیت قراردادی پردازنده بیش‌ازپیش فراهم باشد.

۲-۲- انجام وظایف مرتبط با اطلاع‌رسانی

یکی از وظایف مهم کنترل‌کننده در فرایند پردازش اطلاعات، اطلاع‌رسانی است. این وظیفه دارای سه شق اطلاع‌رسانی به موضوع داده، اطلاع‌رسانی به مقامات صلاحیت‌دار نظارتی و اطلاع‌رسانی به سایر کنترل‌کنندگان است. درصورتی‌که کنترل‌کننده در انجام این مهم کوتاهی نماید، مسئولیت‌های حقوقی مندرج در مواد ۷۷-۸۴ مقررات مصوب سال ۲۰۱۶ شامل حال وی خواهد شد.

۲-۲-۱- وظایف مرتبط با اطلاع‌رسانی به موضوع داده

وظایف مرتبط با اطلاع‌رسانی به موضوع داده در مواد ۶، ۹، ۱۲، ۱۵، ۱۷، ۱۸، ۲۴ و ۳۴ مورد تصریح قانون‌گذار اتحادیه اروپا قرارگرفته است که ذیلاً به تبیین هر یک اقدام می‌گردد.

۲-۲-۱-۱- وظیفه مرتبط با اطلاع‌رسانی در خصوص اخذ رضایت موضوع داده

بنا بر تصریح بند اول ماده ۶ مقررات مصوب سال ۲۰۱۶، یکی از شرایط اصلی در پردازش اطلاعات، اخذ موافقت یا رضایت موضوع داده است. برای این کار کنترل‌کننده موظف به اطلاع‌رسانی شرایط و اهداف پردازش اطلاعات به موضوع داده و اخذ رضایت وی است. درصورتی‌که به هر نحو رضایت موضوع داده در پردازش اطلاعات شخصی وی اخذ نگردد و پردازش بر اساس دیگر معافیت‌های قانونی مندرج در ماده ۶ همان قانون (ازجمله ضرورت پردازش برای حفظ منافع عمومی یا اعمال اختیارات رسمی)، تجویز نگردد، مسئولیت‌های حقوقی شامل حال کنترل‌کننده خواهد بود.

اما سؤال موجود این است که نحوه اطلاع‌رسانی به موضوع داده چطور خواهد بود؟ آیا این موضوع باید به‌صورت رسمی صورت پذیرد یا به‌صورت غیررسمی نیز امکان‌پذیر خواهد بود؟ آیا این موضوع باید به‌صورت کتبی صورت پذیرد یا به‌صورت غیر کتبی و شفاهی نیز امکان‌پذیر خواهد بود؟

برای پاسخ به این سؤال می‌توان به مطالب پیشین مطرح‌شده در موضوع انعقاد قرارداد توجه نمود و بیان داشت که در اینجا نیز حساسیت موضوع ایجاب می‌نماید که فرایند اطلاع‌رسانی به وی به‌صورت کتبی صورت پذیرد. چه‌بسا موضوع داده بنا بر ضروریاتی

تمایل به اعتراض به نحوه پردازش یا تعیین برخی قیود داشته باشد که می‌تواند در پاسخ به اطلاع‌رسانی صورت گرفته، از این امر استفاده کند؛ اما در این فرایند، ضرورتی به اطلاع‌رسانی رسمی به موضوع داده موجود نبوده و اطلاع‌رسانی به هر شکل کتبی می‌تواند مفید شرط مقرر باشد. «چراکه مهم در این زمینه اعلام قصد به موضوع داده بوده و نوع اعلام قصد، تأثیری در آثار حقوقی آن ندارد» (مستفاد از خادمی کوشا، ۱۳۹۷، ۲۱۰-۲۱۱).

حق اطلاع‌رسانی جهت اخذ رضایت از موضوع داده در نظام حقوقی ایران به‌صورت مصرح در مقررات مصوب مورداشاره قرار نگرفته است؛ اما مقررات ماده ۳۳ طرح حمایت و حفاظت از داده و اطلاعات شخصی، دربردارنده احکامی در این زمینه است. این ماده دربردارنده وظایف کنترل‌کننده در قبال اشخاص موضوع داده است که در ده بند دربردارنده اهداف پردازش، نوع و نحوه پردازش، هویت و نحوه فعالیت کنترل‌کنندگان و پردازش کنندگان، موقعیت پردازش، منابع پردازش و پایگاه‌های اطلاعاتی موجود، ویژگی‌های فنی پردازش، گواهی‌های اخذشده از مراجع صلاحی دار، سطح ایمنی پردازش، حقوق موضوع داده در پردازش اطلاعات و وجود یا عدم وجود و شرایط ناظر ویژه پردازش، است.

نکته قابل‌توجه این است که در مقررات این طرح، انجام پردازش باید جز در موارد استثنا مسبوق بر اخذ رضایت از موضوع داده بوده و اخذ رضایت صریح از موضوع داده نیز نیازمند ذکر تمامی جزئیات مقرر در ماده ۳۳ طرح خواهد بود.

۲-۲-۱-۲- وظیفه مرتبط با اطلاع‌رسانی دلایل رد درخواست موضوع داده

مطابق با مفاد بند سوم ماده ۱۲ مقررات مصوب سال ۲۰۱۶ درصورتی‌که موضوع داده به هر دلیلی درخواستی از کنترل‌کننده در باب نوع و نحوه پردازش اطلاعات خود داشته باشد، کنترل‌کننده موظف انجام یا رد و اعلام دلایل به موضوع داده خواهد بود. بند سوم از ماده ۱۲ مقرر می‌دارد:

باید دلایل منطقی مبنی بر عدم اجرای درخواست‌های موضوع داده به‌صورت دقیق به وی اطلاع داده‌شده و وی از چگونگی امکان اعتراض به تصمیم خود، آگاه گردد.

این بند دربردارنده چند شق است. شق اول بر ضرورت اطلاع‌رسانی به موضوع داده

تأکید دارد. خاطرنشان می‌گردد که این وظیفه تنها محدود به کنترل‌کننده نبوده و پردازنده اطلاعات نیز از این وظیفه برخوردار است. اگرچه بیشتر درخواست‌های ارائه‌شده توسط موضوع داده به کنترل‌کننده صورت گرفته و اصولاً موضوع داده، طرف حساب با پردازنده اطلاعات نیست، اما این موضوع مانع از طرح درخواست از پردازنده نخواهد بود. در این صورت اگر درخواست ارائه‌شده، صراحتاً با دستورالعمل‌هایی که کنترل‌کننده به پردازنده ارائه داده در تعارض باشد، پردازنده الزاماً باید نسبت به رد درخواست اقدام و مراتب را به‌ضمیمه دلایل رد به موضوع داده اعلام کند.

شق دوم از این بند بر اطلاع‌رسانی چگونگی اعتراض به موضوع داده حکایت دارد. مطابق با این بند، تنها اعلام رد و دلایل رد درخواست به موضوع داده کفایت ننموده و کنترل‌کننده یا پردازنده حسب مورد وظیفه اعلام چگونگی و مرجع صلاحیت‌دار جهت اعتراض را نیز بر عهده خواهند داشت.

۲-۲-۱-۳- وظیفه مرتبط با اطلاع‌رسانی رفع محدودیت از پردازش

دیگر وظیفه کنترل‌کننده و پردازنده در قبال موضوع داده، وظیفه مرتبط با اطلاع‌رسانی رفع محدودیت از پردازش موضوع‌بند سوم ماده ۱۸ مقررات مصوب سال ۲۰۱۶ است. این بند مقرر می‌دارد:

> موضوع داده‌ای که طبق بند ۱ محدودیت پردازش اخذ کرده است، باید قبل از رفع محدودیت پردازش، توسط کنترل‌کننده مطلع گردد.

یکی از حقوق موضوع داده ایجاد محدودیت در پردازش اطلاعات است که در ماده ۱۸ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا مورد تصریح قرارگرفته است؛ بنابراین درصورتی‌که به هر نحو، کنترل‌کننده نسبت به رفع محدودیت اقدام و پردازش اطلاعات را از سر گیرد، باید این امر را به موضوع داده اطلاع‌رسانی نماید. عدم انجام این کار می‌تواند به‌منزله اقدام به پردازش غیرقانونی اطلاعات تلقی گردد.

سؤالی که می‌تواند مطرح شود این است که درصورتی‌که کنترل‌کننده نسبت به این امر اقدام ننموده و دستور اقدام به پردازش اطلاعات را برای پردازنده صادر نماید، آیا پردازنده موظف به بررسی اطلاع‌رسانی صورت گرفته به موضوع داده خواهد بود؟ آیا وظیفه‌ای در باب اطلاع‌رسانی متوجه پردازنده است؟ برای پاسخ به سؤال فوق باید

بیان داشت که پردازنده تنها موظف به انجام دستورات واصله از کنترل‌کننده بوده و به نیابت از وی تنها نسبت به پردازش اقدام می‌کند؛ بنابراین وی مسئولیتی در باب اطلاع‌رسانی یا عدم اطلاع‌رسانی به موضوع داده نخواهد داشت.

اما درصورتی‌که وی مطلع از عدم اطلاع‌رسانی کنترل‌کننده به موضوع داده شود، به نظر نمی‌رسد نمی‌توان نافی مسئولیت قانونی او در اعلام امر به کنترل‌کننده یا اطلاع‌رسانی به موضوع داده شد. چراکه اطلاع‌رسانی حکمی آمره در مقررات مصوب سال ۲۰۱۶ بوده و پردازنده نیز به نیابت از کنترل‌کننده مبادرت به امر پردازش می‌نماید و ازآنجاکه عدم اطلاع‌رسانی منجر به غیرقانونی شدن فرایند پردازش می‌گردد، علم به عدم انجام‌وظیفه قانونی می‌تواند منجر به مسئولیت پردازنده در جبران خسارات نیز گردد. بااین‌حال توجه به اطلاق ماده، تنها این وظیفه را بر عهده کنترل‌کننده قرارداده و اگر اظهارنظری در باب نص این ماده صورت گرفته و مطلقاً پردازنده را از این امر مبری نماید، نمی‌تواند محل اشکال واقع شود.

اگرچه مفاد این اصل به‌صورت مصرح در قوانین مصوب ایران پیش‌بینی‌نشده است، اما با توجه به مفاد ماده ۳۸ طرح حمایت و حفاظت از داده و اطلاعات شخصی که کنترل‌کنندگان و پردازش گران را به‌طور مطلق ملزم به پاسخگویی کامل در برابر اشخاص موضوع داده نموده است، می‌توان به‌ضرورت پاسخگویی کنترل‌کننده در رفع محدودیت از پردازش اطلاعات که توسط شخص موضوع داده ایجادشده، پی برد.

۲-۲-۱-۴- وظیفه مرتبط با اطلاع‌رسانی اقدامات حفاظتی در تبادل فراملی اطلاعات

مطابق با مفاد بند دوم از ماده ۱۵ مقررات مصوب سال ۲۰۱۶ درصورتی‌که اطلاعات شخصی موضوع داده، محل تبادل فراملی جهت پردازش واقع گردد، وی محق بر اطلاع از اقدامات حفاظتی صورت گرفته مطابق با مفاد ماده ۴۵ همان قانون خواهد بود. بند دوم از ماده ۱۵ مقرر می‌دارد:

> هنگامی‌که داده‌های شخصی به کشور ثالث یا سازمان بین‌المللی منتقل می‌شود، اشخاص موضوع داده این حق را خواهند داشت که طبق ماده ۴۶ مربوط به انتقال، از اقدامات حفاظتی مناسب مطلع شوند

وظیفه اطلاع‌رسانی در فرایند تبادل فراملی اطلاعات جزو وظایف کنترل‌کننده بوده و پردازنده اطلاعات وظیفه‌ای در باب اطلاع‌رسانی بر عهده ندارد. مگر اینکه مطابق با استدلالاتی که در بند پیشین در خصوص علم پردازنده به عدم اطلاع‌رسانی ذکر شد، در آن حالت وی را موظف به اقدام قانونی نماییم.

اما سؤالی که در این خصوص مطرح می‌شود این است که با توجه به اینکه مقررات نظام حقوقی اتحادیه اروپا، کنترل‌کننده را موظف به انجام چنین امری نموده است، درصورتی‌که کنترل‌کننده دارای تابعیت کشوری غیر از کشورهای اتحادیه اروپا مانند ایران بوده که چنین وظیفه‌ای را برای وی نشناخته باشد و یا برعکس کنترل‌کننده دارای تابعیت یکی از کشورهای عضو اتحادیه اروپا بوده ولی موضوع داده در کشوری ثالث مانند ایران ساکن و تابعیت داشته باشد تکلیف چیست؟

در کنار آن اگر پردازنده نیز دارای تابعیت کشوری ثالث غیر از کشورهای عضو اتحادیه اروپا را داشته و خود را موظف به رعایت مقررات نظام حقوقی اتحادیه اروپا ندانسته و حتی در کشور متبوع خود مقرراتی معارض با آنچه در نظام حقوقی اتحادیه اروپا موجود است، تصویب‌شده باشد، تکلیف چه خواهد بود؟ این موضوع نیازمند توجه به پدیده تعارض قوانین است[1].

۲-۲-۱-۵- وظیفه مرتبط با اطلاع‌رسانی حقوق موضوع داده به وی

بند چهارم ماده ۲۱ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا پا کنترل‌کننده را موظف به اعلام وجود حق اعتراض به موضوع داده در صورت مشاهده اقدامات خلاف قانون در پردازش اطلاعات، در حداکثر اولین ارتباط صورت گرفته با وی به‌صورت واضح نموده است. این بند مقرر می‌دارد:

> حداکثر در زمان اولین ارتباط با موضوع داده، حق موضوع‌بندهای ۱ و ۲ به‌صراحت به اطلاع موضوع داده خواهد رسید و باید به‌وضوح و جدا از هرگونه اطلاعات دیگر ارائه شود.

۱ جهت مطالعه سازوکار رفع تعارض قوانین در فرایند پردازش اطلاعات شبکه‌های ارتباطی، رک به مقاله‌ای از همین نویسندگان با عنوان: مطالعه تطبیقی سازوکار شناسایی قانون حاکم بر دعاوی ناشی از نقض مقررات حفاظت از داده های خصوصی و چالش های پیش رو در حقوق ایران و اتحادیه اروپا ، فصلنامه اندیشه‌های حقوق عمومی، دوره ۱۰، شماره ۲ پیاپی ۱۹، بهار و تابستان ۱۴۰۰، صص ۴۵-۵۸

سؤالی که می‌توان در این بند در نظر گرفت این است که آیا می‌توان با تفسیر موسع از مقررات این بند، وظیفه کنترل‌کننده به اعلام سایر حقوق قانونی موضوع داده (ازجمله حق حذف اطلاعات، حق دسترسی به اطلاعات و...) که در مواد ۱۵-۲۰ مقررات مصوب سال ۲۰۱۶ مورد تصریح قرارگرفته است، به وی را ثابت دانست یا باید مقررات این ماده را تنها در محدوده حق اعتراض تفسیر نمود؟

پاسخ به این سؤال می‌تواند از دو منظر مطرح شود. دیدگاه اول بر ضرورت تفسیر مضیق از مقررات این ماده و عدم تصریح قانون‌گذار بر ضرورت اعلام دیگر حقوق به موضوع داده استوار است؛ اما دیدگاه دوم که به نظر صحیح‌تر می‌رسد بر حمایتی بودن مقررات این قانون تأکید دارد؛ به‌عبارت‌دیگر اگرچه مقررات این ماده تنها بر ضرورت اعلام حق اعتراض به موضوع داده تأکید دارد، اما حمایتی بودن مفاد آن ایجاب می‌نماید که کنترل‌کننده دیگر حقوق موضوع داده را نیز به وی اعلام نماید. ازاین‌رو عدم تصریح قانون‌گذار را نه بر نفی موضوع بلکه باید بر مسامحه تفسیر نمود. در همین راستا قسمت دوم از بند دوم ماده ۱۳ همان قانون نیز بر ضرورت اعلام سایر حقوق قانونی موضوع داده به وی اقدام نموده است. مفاد این ماده در مطالب آتی ذکرشده است.

نکته دیگر این است که این وظیفه در بند «خ» ماده ۳۳ طرح حمایت و حفاظت از داده و اطلاعات شخصی نیز مورد تصریح ارائه‌کنندگان طرح قرارگرفته است. این بند مقرر می‌دارد که کنترل‌کننده یا پردازنده موظف است اطلاعات مرتبط با حقوق اشخاص موضوع داده نسبت به پردازش داده‌ها و اطلاعات شخصی‌شان و چگونگی استیفای آن‌ها را به موضوع داده اطلاع دهند. نکته مهم در مقررات این بند آن است که آنچه مدنظر ارائه‌کنندگان این طرح بوده نه‌فقط اعلام حقوق موضوع داده بلکه نحوه استیفای آن‌ها نیز است؛ بنابراین درصورتی‌که نحوه استیفای حقوق به موضوع داده اطلاع داده نشود، به‌منزله عدم اجرای مقررات این بند خواهد بود.

اما سؤال موجود این است که اطلاع‌رسانی قید شده در این بند باید به چه نحوی صورت پذیرد؟ آیا باید با تمام جزئیات توسط کنترل‌کننده به موضوع داده ارائه‌شده یا بیان آن به‌صورت کلی نیز کفایت می‌کند؟

اهمیت طرح این سؤال می‌تواند در شناسایی انجام یا عدم انجام وظایف قانونی کنترل‌کننده و مسئولیت‌های حقوقی وی مؤثر باشد. به نظر نگارنده تأکید بر نحوه استیفای حقوق توسط ارائه‌دهندگان طرح، نشان از اهمیت بالای آن در دیدگاه آن‌ها داشته و اصولاً برای تحقق اهداف لازم در ارائه اطلاعات فوق، اطلاع‌رسانی در این زمینه باید به‌صورت تفصیلی و با جزئیات صورت پذیرد.

۲-۲-۱-۶- وظیفه مرتبط با اطلاع‌رسانی اقدامات صورت گرفته در فرایند پردازش اطلاعات

دیگر وظیفه مهم کنترل‌کننده وظیفه مرتبط با اطلاع‌رسانی اقدامات صورت گرفته بر روی اطلاعت در فرایند پردازش است. این وظیفه در ماده ۱۳ مقررات مصوب سال ۲۰۱۶ مورد تصریح قرارگرفته است.

بر مبنای مفاد بند اول ماده ۱۳، کنترل‌کننده موظف است در هنگام جمع‌آوری اطلاعات، مشخصات هویتی خود و اشخاص ناظر بر فرایند پردازش اطلاعات، اهداف و مبنای قانونی پردازش، منافع مشروع خود و اشخاص ثالث و همچنین مشخصات اشخاصی که اطلاعات در دسترس آن‌ها قرار می‌گیرد، دوره پردازش و حقوق موضوع داده را در اختیار وی قرار دهد. علاوه بر آن درصورتی‌که نسبت به هر یک از موارد فوق تغییری ایجادشده و به‌عنوان‌مثال، داده‌ها را به غیر اهدافی که برای موضوع داده معین نموده، پردازش نماید، باید پیش از پردازش نسبت به اعلام مجدد امر به موضوع داده اقدام کند.

نکته دیگر این است که طبق مقررات ماده ۱۴ این قانون نیز حتی در فرایند جمع‌آوری اطلاعات، داده‌ای از موضوع داده به دست نیامده باشد نیز کنترل‌کننده را موظف به اعلام مراتب اطلاعات هویتی کنترل‌کننده، اهداف و مبانی پردازش، افرادی که اطلاعات شخصی در صورت جمع‌آوری در اختیار آن‌ها قرار می‌گرفت و نیز دسته‌های داده‌های شخصی موردنظر نموده است؛

اما سؤالی که به ذهن می‌رسد این است که ارائه این اطلاعات به اشخاص موضوع داده پس از شروع فرایند پردازش (همان‌طور که بیان شد جمع‌آوری یکی از شقوق پردازش اطلاعات است) چه اثری در حفظ حقوق موضوع داده دارد؛

به‌عبارت‌دیگر ذکر عبارت «درصورتی‌که داده‌های شخصی از موضوع داده به دست نیامده باشد...» در ماده ۱۴ افاده این معنا را می‌کند که ممکن است فرایند اخذ رضایت مقرر در ماده ۶، از موضوع داده مسبوق بر شروع فرایند پردازش باشد. این چالش با تدبر در صدر بند اول ماده ۱۳ نیز با امعان نظر از عبارت «باید درزمانی که داده‌های شخصی به دست می‌آید...» قابل‌برداشت است؛ به‌عبارت‌دیگر قانون‌گذار در ماده ۱۳، شروع فرایند پردازش اطلاعات را تجویز و پس از دستیابی و در هنگام جمع‌آوری اطلاعات، ارائه مفاد بندهای ماده فوق‌الذکر را به موضوع داده الزامی نموده است.

برای حل این چالش تنها راه ممکن ارائه این پاسخ است که در جمع مقررات مواد ۱۳-۱۴ و ۶ این قانون، ارائه اطلاعات مندرج دربندهای مواد ۱۳-۱۴ را به فرایند پردازش اطلاعات دربندهای دیگر ماده ۶ جز بند اول که ضرورت اخذ رضایت را مورد تصریح قرارداده نسبت دهیم؛

به‌عبارت‌دیگر کنترل‌کننده تنها در حالتی موظف به ارائه اطلاعات مندرج دربندهای مواد ۱۳ و ۱۴ پس از شروع فرایند پردازش به موضوع داده است که پردازش در راستای انجام تعهد قانونی کنترل‌کننده (بند دوم ماده ۶)، منافع حیاتی موضوع داده یا شخص ثالث (بند سوم ماده ۶)، نفع عمومی یا اعمال اختیارات رسمی (بند چهارم ماده ۶) و اهداف مشروع (بند پنجم ماده ۶) صورت پذیرفته و ارائه این اطلاعات در خصوص مفاد بند اول که اخذ رضایت موضوع داده است باید پیش از شروع فرایند پردازش صورت پذیرد.

۲-۲-۱-۶- وظیفه مرتبط با اطلاع‌رسانی وجود خطر به موضوع داده

وظیفه دیگر مقرر در مقررات مصوب سال ۲۰۱۶ اطلاع‌رسانی در مواردی است که نقض امنیت اطلاعات صورت گرفته و این نقض دربردارنده خطر بالا برای حقوق و آزادی‌های اشخاص حقیقی باشد. این موضوع در ماده ۳۴ مقررات فوق‌الذکر معین‌شده است.

مقررات ماده ۳۴، مبین اطلاع‌رسانی به موضوع داده پس از نقض امنیت اطلاعات وی است. نقض امنیت عموماً زمانی اتفاق می‌افتد که سازمان مسئول دچار یک حادثه

امنیتی شده و این امر نقض محرمانگی و دسترس قرار گرفتن اطلاعات را منجر گردد. به‌عنوان‌مثال می‌توان به «نشت اطلاعات بیماران یک بیمارستان از سایت این مجموعه و یا حتی به‌صورت فیزیکی توسط یکی از عوامل این سازمان اشاره نمود» (European Commission,2023).

این موضوع ازآن‌جهت در حوزه پیشگیری اهمیت دارد که اعلام نقض یک دسته از اطلاعات به موضوع داده می‌تواند از نقض بعدی یا سایر اطلاعات پیشگیری نماید؛ بنابراین پس از نقض، در صورتی کنترل‌کننده وظیفه اطلاع‌رسانی فوری و حداکثر طرف ۷۲ ساعت به موضوع داده را خواهد داشت که نقض منجر به خطر بالا برای حقوق و آزادی‌های شخصی اشخاص حقیقی باشد؛ بنابراین وجود خطر تنها برای موضوع داده متصور نبوده و درصورتی‌که برای اشخاص ثالث نیز دارای خطر باشد، وظیفه اطلاع‌رسانی کنترل‌کننده ثابت می‌گردد.

«فرایند اطلاع‌رسانی در این زمینه دارای سه جنبه زبان مورداستفاده، جزئیات لازم برای اعلام و نحوه برقراری ارتباط خواهد بود»(ISMS,2023). در این راستا بند دوم ماده ۳۴ بیان می‌دارد که زبان مورداستفاده باید واضح و روشن بوده و دربردارنده اطلاعات مفاد قسمت‌های ب، ج و د بند ۳ ماده ۳۳ این قانون باشد. قسمت‌های ب و ج و د بند سوم ماده ۳۳ مقرر می‌دارند:

- نام و مشخصات تماس افسر حفاظت از داده‌ها یا سایر نقاط تماس را که می‌توان اطلاعات بیشتری را در آنجا به دست آورد، در میان گذاشته شوند
- شرح عواقب احتمالی نقض داده‌های شخصی
- شرح اقدامات انجام‌شده یا پیشنهادشده توسط کنترل‌کننده برای رسیدگی به نقض داده‌های شخصی، ازجمله، در صورت لزوم، اقداماتی برای کاهش اثرات نامطلوب احتمالی

بااین‌حال بند سوم ماده ۳۴، استثنائاتی را برای اطلاع‌رسانی به موضوع داده در موارد وقوع نقض پیش‌بینی نموده است که شامل انجام اقدامات مناسب فنی و حفاظتی در مقابله با نقض صورت گرفته و پیشگیری از نقض‌های متعاقب است. علاوه بر آن درصورتی‌که اعلام موضوع به موضوع داده منجر به تلاش نامتناسب کنترل‌کننده باشد، باید به روش ارتباطات عمومی موضوع به اطلاع عموم جامعه برسد.

به نظر می‌رسد موضوع بیان‌شده در خصوص تلاش نامتناسب می‌تواند در فرضی تحقق یابد که دسترسی به موضوع داده مشقت‌بار بوده و بر این مبنا کنترل‌کننده تصمیم بگیرد تا از طریق وسایل ارتباط‌جمعی مانند تلویزیون و رادیو یا اطلاع‌رسانی در شبکه‌های اجتماعی موضوع را به اطلاع اشخاص برساند.

۲-۲-۲- وظایف مرتبط با اطلاع‌رسانی به سایر کنترل‌کنندگان

وظیفه دیگر مقررشده برای کنترل‌کننده در مقررات مصوب سال ۲۰۱۶، اعلام حذف اطلاعات شخصی موضوع داده به سایر کنترل‌کنندگان موضوع‌بند ب ماده ۱۷ همان قانون است. این بند مقرر می‌دارد:

> درصورتی‌که کنترل‌کننده داده‌های شخصی را عمومی کرده است و طبق بند ۱ موظف به پاک کردن داده‌های شخصی است، کنترل‌کننده با در نظر گرفتن فناوری موجود و هزینه‌های پیاده‌سازی، اقدامات معقولی را انجام می‌دهد، ازجمله اقدامات فنی تا به کنترل‌کنندگانی که در حال پردازش داده‌های شخصی هستند اطلاع دهد که موضوع داده‌ها درخواست پاک کردن هرگونه پیوند به یا کپی یا تکرار آن داده‌های شخصی توسط کنترل‌کنندگان را داشته است.

مفاد این بند به حالتی اشاره دارد که موضوع داده از حق پاک کردن اطلاعات خود استفاده نموده و به هر طریق ممکن، کنترل‌کننده را از این امر مطلع نماید. در این صورت کنترل‌کننده موظف خواهد بود نه‌تنها نسبت به حذف اطلاعات موضوع داده از سامانه‌های خود اقدام نماید، بلکه درصورتی‌که اطلاعات را در اختیار کنترل‌کنندگان دیگر نیز قرارداده باشد، نسبت به اطلاع‌رسانی به آن‌ها نیز اقدام کند.

«چراکه مفاد حق پاک کردن اطلاعات موضوع داده زمانی تکمیل می‌شود که اطلاعات وی از دسترس کلیه کنترل‌کنندگان و پردازندگان پاک شود» (Mittal, 2017, 68)[1].

[1] نقل‌شده در لطیف زاده (۲)، ۹۸۹

علاوه بر این ماده، ماده ۱۹ مقررات فوق‌الذکر نیز دربردارنده احکامی مشابه و حتی وسیع‌تر از ماده ۱۷ بوده و کنترل‌کنندگان را موظف به اعلام مراتب به کلیه اشخاص ثالثی که اطلاعات در دسترس آن‌ها است، نموده است. این اشخاص می‌توانند پردازندگان اطلاعات یا هر شخص حقیقی یا حقوقی دیگر باشند؛

اما نکته‌ای که باید بدان توجه نمود این است که حق بر حذف اطلاعات، مرتبط با داده‌پیام‌های شخصی است و این موضوع ارتباطی به افشا یا عدم افشای این اطلاعات ندارد؛ بنابراین نمی‌توان استدلال نمود که چون این اطلاعات عمومی شده‌اند، حق بر حذف اطلاعات شامل آن‌ها نمی‌گردد.

البته ثمره این موضوع صرف‌نظر از هزینه‌های بالایی که می‌تواند برای کنترل‌کننده در حذف کلیه اطلاعات در دسترس اشخاص ثالث تحمیل نماید، این است که صرف اطلاع‌رسانی توسط کنترل‌کننده می‌تواند نافی مسئولیت‌های بعدی وی از نقض امنیت این اطلاعات یا سوءاستفاده از آن‌ها با تبادل فراملی و در دسترس قرار گرفتن این اطلاعات توسط بیگانگان باشد.

۲-۲-۳- وظایف مرتبط با اطلاع‌رسانی و همکاری با مراجع صلاحیت‌دار نظارتی

آخرین وظیفه‌ای که برای کنترل‌کنندگان و پردازندگان در فرایند پردازش اطلاعات مقررشده است، وظیفه اطلاع‌رسانی و همکاری با مراجع صلاحیت‌دار نظارت بر امر پردازش اطلاعات است. این وظیفه در مقررات مواد ۳۱ و ۳۳ مقررات مصوب سال ۲۰۱۶ مورد تصریح قرارگرفته است.

بر مبنای ماده ۳۱ این مقررات کنترل‌کننده و پردازشگر و در صورت لزوم، نمایندگان آن‌ها باید در صورت درخواست با مقام ناظر در انجام وظایف خود همکاری کنند. علاوه بر آن تعهد به اطلاع‌رسانی به مراجع نظارتی، تعهدی است که حسب مفاد ماده ۳۳ مقررات مصوب سال ۲۰۱۶، پس از نقض امنیت اطلاعات در یک شبکه ارتباطی رخ می‌دهد. علت این موضوع ورود مراجع نظارتی به بحث، شناسایی عوامل مخل و پیشگیری از نقض بیشتر امنیت داده‌پیام‌های دیگر است.

در این میان بنا بربند دوم از ماده ۳۳، پردازنده مکلف به اعلام موارد نقض به کنترل‌کننده است و پس‌ازآن به‌حکم بند اول این ماده کنترل‌کننده حداکثر ظرف ۷۲

ساعت باید مراتب را به مراجع صلاحیت‌دار نظارتی اعلام نماید. نکته قابل‌توجه در خصوص این بند، وجود واژه «در صورت امکان» است که «در صورت وجود دلایل موجه، امکان تمدید این مهلت را برای کنترل‌کننده فراهم کرده است» (Cynet,2023).

بااین‌حال تمدید مهلت باید همراه با ذکر دلایل تمدید باشد. عدم انجام وظایف مقرر در بند اول ماده ۳۳ یا عدم درج مندرجات مقرر در بند دوم ماده ۳۳ علیرغم اعلام، می‌تواند «منجر به جریمه‌های سنگین ازجمله جریمه ده میلیون یورویی یا دو درصد درآمد سالانه برای کنترل‌کننده شود»(Accountability,2023).

اما سؤال موجود این است که منظور قانون‌گذار از واژه نقض در این ماده چه است. برای پاسخ به این سؤال می‌توان بیان داشت که «مفهوم نقض در این ماده مفهومی بسیط بوده و می‌تواند تمامی شقوق نقض امنیت داده‌پیام‌ها را شامل گردد.

ازاین‌رو هرگونه تغییر، دسترسی، انتقال، تخریب، افشا و... صورت گرفته بر روی داده‌پیام‌ها که خارج از موازین قانونی یا قراردادی میان کنترل‌کننده و پردازنده یا کنترل‌کننده و موضوع داده صورت گرفته باشد، به‌منزله نقض امنیت داده‌پیام تلقی خواهد شد»(Infoseg Insights,2023).

سؤالی دیگری که باید مدنظر قرارداد این است که جایگاه واژه «تأخیر بی‌مورد» در صدر بند اول ماده ۳۳ چه بوده و چه تأثیری بر مدت‌زمان اعلام نقض امنیت داده‌پیام‌ها به مقام نظارتی خواهد داشت. برای تفسیر این واژه باید به مفاد دستورالعمل شماره ۸۷ مقررات مصوب سال ۲۰۱۶ توجه نمود. این دستورالعمل مقرر می‌دارد که «عواملی مانند «ماهیت، اهمیت نقض داده‌های شخصی، عواقب و اثرات منفی آن بر موضوع داده» باید در فوریت اعلام مراتب به مقام نظارتی تأثیرگذار باشد» (Reini,2019,18).[1]

[1] نقل‌شده در لطیف زاده، پیشین، ص ۲۵۷

ازاین‌رو ممکن است در مواقع ضروری با توجه به نوع و دسته حساس داده‌های شخصی مانند اطلاعات بیومتریک اشخاص، ضرورت اعلام فوری و قبل از حداکثر زمان مقرر در ماده ۳۳ ایجاب و عدم انجام این اقدام توسط کنترل‌کننده به‌منزله نقض مفاد ماده ۳۳ مقررات مصوب سال ۲۰۱۶ باشد.

نتیجه‌گیری

همان‌طور که بیان شد، شبکه‌های تبادل اطلاعات به‌عنوان شریان‌های اصلی جمع‌آوری و پردازش اطلاعات در یک کشور تلقی می‌شوند. ازاین‌رو به‌کارگیری سازوکارهایی در جهت حفظ امنیت و پیشگیری از نقض امنیت این شبکه‌ها ازجمله هر ضروریات در نظام حقوقی و سیاسی است.

ازجمله مهم‌ترین اجرای یک شبکه کاربران شبکه و داده‌پیام‌های مورد تبادل می‌باشند. سازوکارهای بیان‌شده در این پژوهش نیز حول محوریت حفظ امنیت این دو جزء شکل‌گرفته‌اند.

اگرچه در این زمینه سازوکارهای فنی نیز می‌توانند به نحوی مطلوب در جهت افزایش امنیت و پیشگیری از نقض امنیت شبکه به کار گرفته شوند، اما محوریت پژوهش در زمینه سازوکارهای حقوقی است. پژوهش حاضر بامطالعه تحلیلی جدیدترین قانون مصوب در نظام حقوقی اتحادیه اروپا (مقررات مصوب سال ۲۰۱۶ این اتحادیه) و تطبیق این مفاهیم با نظام حقوقی ایران، سازوکارهای حقوقی این مهم را در اجرای برخی وظایف از سوی مدیران شبکه‌های تبادل اطلاعات و پردازندگان اطلاعات که اصطلاحاً کنترل‌کننده و پردازنده نامیده می‌شوند، تقسیم‌بندی نموده است.

وظایف کنترل‌کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات در انجام اقدامات مناسب در اجرای صحیح و قانونی پردازش اطلاعات، اطلاع‌رسانی در خصوص اخذ رضایت موضوع داده، اطلاع‌رسانی دلایل رد درخواست موضوع داده، اطلاع‌رسانی رفع محدودیت از پردازش، اطلاع‌رسانی اقدامات حفاظتی در تبادل فراملی اطلاعات، اطلاع‌رسانی حقوق موضوع داده به وی، اطلاع‌رسانی اقدامات

صورت گرفته در فرایند پردازش اطلاعات، اطلاع‌رسانی وجود خطر به موضوع داده، اطلاع‌رسانی به سایر کنترل‌کنندگان در حذف و ایجاد محدودیت در پردازش و اطلاع‌رسانی و همکاری با مراجع صلاحیت‌دار نظارتی، دسته‌بندی می‌شوند.

با توجه به اینکه مقررات عمومی حفاظت از اطلاعات اتحادیه اروپا مصوب سال ۲۰۱۶، دربردارنده مقررات مفصلی در این زمینه است، این مقررات می‌توانند به‌عنوان منبعی جهت تدوین و اصلاح مقررات لازم در این زمینه در نظام حقوقی ایران نیز تلقی شوند.

چراکه در نظام حقوقی ایران مقررات بخصوصی در زمینه پیش‌بینی وظایف کنترل‌کنندگان و پردازندگان در قوانین مصوب وجود نداشته و آنچه در متن این پژوهش در خصوص مواد طرح حمایت و حفاظت از داده و اطلاعات شخصی قید شد، مربوط به طرحی است که علیرغم برخورداری از برخی مقررات در این زمینه، هنوز به مرحله تصویب و لازم‌الاجرا درآمدن در نظام حقوقی ایران نرسیده است.

ازاین‌رو در وهله اول نیاز به عزم مجلس قانون‌گذاری در تصویب مقرره‌ای جامع مطابق با مقتضیات و هنجارهای حاکم بر جامعه ایرانی در زمینه حفظ امنیت شبکه‌های تبادل اطلاعات و اجزای آن‌ها است.

نکته قابل‌توجه این است که با توجه به اینکه گستره حاکمیتی کشورها، قوانین و مصوبات مصوب در آن کشور را برای اتباع خود صرف‌نظر از محل سکونت آن‌ها در داخل یا خارج از آن کشور به رسمیت شناخته و همچنین محدوده اجرای این قوانین را در خصوص اتباع خارجی که محدوده سرزمینی این کشور ساکن می‌باشند، قرار می‌دهد. بااین‌حال گاه در اجرای مقررات موصوف، تعارضاتی میان قوانین کشورها پیش می‌آید که در این زمینه باید به قواعد حل تعارض متناسب با هر نوع نظام حقوقی توجه نمود.

در کنار آن باید سیاست‌گذاران، مقررات مصوب را به نحوی به آگاهی و اطلاع مردم برسانند که همگان با زبان ساده قوانین از حقوق قانونی خود و وظایف اشخاص درگیر در فرایند پردازش اطلاعات در شبکه‌های ارتباطی مطلع شوند.

این موضوع می‌تواند در دو اقدام به مرحله اجرایی درآید. اقدام اول تولید برنامه‌های

آموزشی در شبکه‌های ارتباط‌جمعی ازجمله تلویزیون یا رادیو یا کلیپ‌های آموزشی در شبکه‌های اجتماعی داخلی است.

علاوه بر آن ملزم نمودن کنترل‌کنندگان سایت‌های اینترنتی برای ایجاد آیکونی که نشان‌دهنده کلیه وظایف آن‌ها و حقوق کاربران سایت بوده و در هنگام ورود کاربر به سایت نسبت به ارائه اطلاعات فوق به آن شخص اقدام نماید، می‌تواند در آگاهی بخشی به افراد نقش مؤثر داشته باشد.

علاوه بر آن ارسال پیامک‌های آموزشی به شماره تلفن همراه اشخاص دیگر راهکاری است که در این زمینه پیش‌بینی می‌شود. آخرین توصیه، فراهم نمودن فرایند اعطای مجوز به فعالیت کنترل‌کنندگان خارجی شبکه‌های تبادل اطلاعات در کشور ایران است.

در دیدگاه نگارنده فراهم نمودن امکان نظارت بر شبکه‌های تبادل اطلاعات کاری بس مفیدتر از فیلترینگ آن‌ها است. چراکه در عصر حاضر تولید فیلترشکن‌های متعدد عملاً امکان نظارت بر شبکه‌های فیلتر شده را از میان می‌برد و به نظر می‌رسد راهکارهایی جایگزین در این زمینه در جهت بهبود فعالیت این شرکت‌ها در کشور ایران باید در دستور کار قرار گیرد.

نکته آخر در این زمینه آن است که اگرچه پژوهش حاضر مبادرت به تحلیل و بررسی وظایف کنترل‌کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات نموده است، اما اجرای هر چه‌بهتر این فرایند نیازمند بررسی ضمانت اجراهای موجود در این زمینه چه در بعد مدنی و چه کیفری مطابق با هنجارهای اخلاقی، اجتماعی و فرهنگی هر دو نظام، دادگاه صالح در رسیدگی به دعاوی ناشی از این اقدامات خصوصاً در مواردی که یکی از اشخاص درگیر دارای تابعیت کشوری خارجی بوده و یا یکی از اشخاص جزو اشخاص حقوقی حوزه حقوق عمومی و یک شرکت دولتی خارجی تلقی گردد، است.

علاوه بر آن نکته قابل ضرورت بررسی صلاحیت‌های نظارتی مقامات دولتی و غیردولتی در نظارت بر فرایند پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات و انجام صحیح وظایف کنترل‌کنندگان و پردازندگان است.

اگرچه در نظام حقوقی اتحادیه اروپا مقامات صلاحیت‌دار نظارتی در این زمینه

پیش‌بینی‌شده و در برخی مواد مقررات مصوب سال ۲۰۱۶ نیز کنترل‌کنندگان موظف به تعیین اشخاصی موسوم به افسران حفاظت از اطلاعات در نظارت بر فرایند پردازش‌شده‌اند، اما کشور ایران خالی از چنین سازوکارهایی است که این موضوع نیز می‌تواند به‌عنوان یکی از موضوعات پیشنهادی پژوهش‌های آتی موردتوجه قرار گیرد.

منابع

۱. احمدوند، بهناز، جهانشاهی، آرتین، **بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی ایران و اتحادیه اروپا**، فصلنامه پژوهش‌های حقوق تطبیقی، دوره ۲۷، شماره ۱، بهار ۱۴۰۲، صص ۱۰۵-۱۳۲.

۲. خادمی کوشا، محمدعلی، **شرط قصد و ابراز صریح آن در قرارداد الکترونیکی از منظر فقه اسلامی**، فصلنامه اقتصاد اسلامی، دوره ۱۸، شماره ۷۰، ۱۳۹۷، صص ۲۰۵-۲۲۴.

۳. لطیف زاده، مهدیه، قبولی درافشان، سیدمحمد مهدی، محسنی، سعید، عابدی، محمد؛ (۲) **حمایت از دادۀ شخصی در حقوق اتحادیۀ اروپا و امکان‌سنجی آن در نظام حقوقی ایران**، فصلنامه مطالعات حقوق عمومی، دوره ۵۳، شماره ۲، ۱۴۰۲، صص ۹۸۱-۱۰۰۵.

۴. لطیف زاده، مهدیه، قبولی درافشان، سیدمحمد مهدی، محسنی، سعید، عابدی، محمد، **تعهدات پردازش کننده داده شخصی در اتحادیه اروپا و امکان‌سنجی پذیرش آن در حقوق ایران**، فصلنامه آموزه‌های فقه مدنی، دوره ۱۶، شماره ۲۷، ۱۴۰۲، صص ۲۴۵-۲۸۶.

۵. صادقی، حسین، ناصر، مهدی، **مطالعه تطبیقی سازوکار شناسایی قانون حاکم بر دعاوی ناشی از نقض مقررات حفاظت از داده های خصوصی و چالش های پیش رو در حقوق ایران و اتحادیه اروپا** ، فصلنامه اندیشه‌های حقوق عمومی، دوره ۱۰، شماره ۲ پیاپی ۱۹، ۱۴۰۰، صص ۴۵-۵۸.

6. Accountability, **security and breach notification** | Personal data breaches and notification, https://www.twobirds.com/-/media/pdfs/gdpr-pdfs/42--guide-to-the-gdpr--personal-data-breaches-and-notification.pdf, Last Visited 28/07/2023.

7. Clarip, Clarity in privacy, **Differences between a GDPR Data Controller** vs. Data Processor,

https://www.clarip.com/data-privacy/gdpr-data-controller-vs-processor-differences/, Last Visited 24/07/2023.

8. Cynet, **GDPR Data Breach Notifications: Everything You Need to Know**, https://www.cynet.com/cynet-for-compliance/gdpr-data-breach-notifications-everything-you-need-to-know/, Last Visited 28/07/2023.
9. Datatilsynet, **Data controller and processor**, https://www .datatilsynet.dk/english/fundamental-concepts-/data-controller-and-processor, Last Visited 24/07/2023.
10. EUR-Lex, 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 – GDPR), Official Journal of the European Union, L 119, https://eur-lex.europa.eu/legal content/EN/TXT/PDF /?uri=CELEX:32016R0679&from=EN,2016.
11. European Commission, **What is a data breach and what do we have to do in case of a data breach?** https://commission. europa. eu/law/law-topic/data-protection /reform/rules- business -and -organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en, Last visited 27/07/2023.
12. Infoseg Insights, **What Constitutes a GDPR Data Breach?** Definition & Meaning, https://sectigostore.com/blog/what-constitutes-a-gdpr-data-breach-definition-meaning/, Last Visited 28/07/2023
13. Intersoft Consulting, **General Data Protection Regulation (GDPR)**, https://gdpr-info.eu/art-40-gdpr/, last visited 18/07/2023
14. Iron Montain, **Data Processor vs. Data Controller**, https://www.ironmountain.com/resources/general-

articles/d/ data-processor-vs-data-controller, Last Visited 24/07/2023

15. ISMS.online, **How to Demonstrate Compliance With GDPR** Article 34, https://www.isms.online/general-data-protection-regulation-gdpr/gdpr-article-34-compliance/, Last visited 27/07/2023.
16. Mittal, Sandeep, "**Old Wine with a New Label: Rights of Data Subjects Under GDPR**", SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2992042, 2017, pp 67-71.
17. Reini, Pasi, **GDPR implementation, Case: Headpower Oy**, Master's thesis, University of Transport and Communications,https://www.theseus.fi/bitstream/handle/10024/166514/Reini_k7696_thesis_versio4.1.pdf?sequence=2, 2019.
18. Van der Sloot, Bart, '**Do Privacy and Data Protection Rules Apply to Legal Persons and Should They? A Proposal for a Two-tiered System**', Computer Law and Security Review, Volume 13, Issue 8, 2017, pp 18-34.

Duties of controllers and processors in preventing security violations of information exchange networks

Aliakbar Farahzadi[۱], Hossein Sadeghi[۲], Mehdi Nasser[۳]

Received:2022/11/16 Accepted: 2023/02/21

Abstract

In today's world, preventing security breaches of information exchange networks requires mechanisms to maintain the integrity and security of network implementation. Among the components of the network, individuals are the subject of data and data messages to be exchanged. In this process, managers of information exchange networks and processors of data messages, which are called controllers and processors, have duties. What will the present research look for in answering the duties of the mentioned persons in the field of preventing security violations of information exchange networks. In this way, the present research, by studying the regulations governing the legal system of the European Union and the application of these regulations in the laws of Iran, has determined the duties of these persons in carrying out appropriate measures in the correct and legal implementation of information processing, the duties of notifying the subject persons through a documentary method. His consent to processing, announcing the reasons for rejecting his request, removing restrictions on processing, protective measures in the transnational exchange of information, the rights of the data subject, measures taken in the process of information processing, the existence of risk in processing), other controllers and processors (in announcing the deletion or creating restrictions on processing) and supervisory authorities (in cooperation and notification) has done.

Keywords: controllers, processors, information exchange networks, EU law.

[1] Associate Professor, University of Judicial Sciences and Administrative Services, Tehran, Iran, farahzadi@ujsas.ac.ir
[2] Associate Professor, University of Tehran, Tehran, Iran, hosadeghi@ut.ac.ir
[3] PhD student in private law, University of Judicial Sciences and Administrative Services, Tehran, Iran, Mn.ujsasac0077@yahoo.com