


Prevention of information exchange network security violations in the light of Article 32 of the EU General Data Protection Regulation

Aboutaleb Koosha¹  | Hosein sadeghi²  | Mahdi Naser^{3*} 

1. Assistant Professor of University of Judicial Sciences and Administrative Services, Email: koosha1336@yahoo.com
2. Associate Professor, Faculty of Entrepreneurship, University of Tehran, Tehran, Iran, Email: hosadeghi@ut.ac.ir
3. Phd in Private Law, University of Judicial Sciences and Administrative Services, (Correspondant Author). mn.ujsasac0077@yahoo.com

Article Info	Abstract
<p>Article type: Scientific Article</p> <hr/> <p>Received: 2024/02/04</p> <p>Received in revised form: 2024/08/11</p> <p>Accepted: 2024/09/08</p> <hr/> <p>Keywords: <i>Security, Information exchange networks, Data, Controller, Data Subject, European Union.</i></p>	<p>In the criminal law of Iran, in the topic of "crimes" in paragraph (c) of Article 292 of the Islamic Penal Code approved in 1392, the mistake in person has been examined as an effective factor on the psychological element of the crime. In common law, there is also a mistake in the person in the topic of murder, and according to the view that "the target follows the bullet", they believe that this mistake has no effect on the intentionality of the crime committed on the victim of the unintentional crime. The question that is raised is that in Iranian law, is this mistake only limited to crimes against physical integrity or is it effective for other crimes, especially crimes against spiritual integrity? The findings of the research indicate that, contrary to the theory of transferred malice in common law, in Iranian law, a mistake in a person is effective in forming the absolute malice of intentional crimes as a kind of mistake in the subject of the victim (that is, a certain person). In such a way that the effect of the intended behavior on the unintended purpose, in principle, in terms of the lack of the subject's intention, causes the deterioration of the intentional psychological element. Except that in case of lack of intention, knowledge is a substitute for definite and certain intention. As a result, in crimes against the spiritual integrity of persons, according to Article 144 of the Islamic Penal Code approved in 2012, two assumptions can be considered; First, the fact that the perpetrator unintentionally made the unintended crime victim the subject of crimes against dignity or spiritual personality and also had no knowledge of the behavior. (Lack of intention and knowledge) Second, despite the lack of intention, the perpetrator knew or should have known that his behavior leading to a crime against the spiritual personality of the victim is unintentional. It is innocent, and it has no effect on the second hypothesis in terms of verifying the scientific, criminal and wrong element of psychology.</p>
<p>How To Cite</p>	<p>Koosha, A., Sadeghi, H., Naser, M., (2024). Prevention of information exchange network security violations in the light of Article 32 of the EU General Data Protection Regulation. <i>Journal of Judgment</i>, 23(3), 1-31. DOI: https://doi.com/10.22034/judg.2024.2022304.1279</p>
<p>DOI</p>	<p>10.22034/JUDG.2024.2022304.1279</p>
<p>Publisher</p>	<p>Publications of the Judiciary of Tehran Province </p>

پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات در پرتو ماده ۳۲ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا

ابوطالب کوشا^۱ | حسین صادقی^۲ | مهدی ناصر^{۳*}

۱. استادیار دانشکده حقوق قضایی، دانشگاه علوم قضایی و خدمات اداری. رایانامه: koosha1336@yahoo.com
۲. دانشیار دانشکده کارآفرینی، دانشگاه تهران. رایانامه: hosadeghi@ut.ac.ir
۳. دکترای حقوق خصوصی، دانشگاه علوم قضایی و خدمات اداری (نویسنده مسئول). رایانامه: mn.ujsasac0077@yahoo.com

اطلاعات مقاله	چکیده
نوع مقاله: علمی	پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات، امری است که همواره مورد توجه قانون گذاران بوده است. این موضوع از آن جهت اهمیت دارد که در عصر حاضر به عنوان عصر الکترونیک، نقض امنیت شبکه‌های تبادل اطلاعات منجر به نشست اطلاعات و ایجاد زمینه سوءاستفاده می‌گردد که سوء استفاده از اطلاعات شخصی افراد می‌تواند، گاه حتی اثرات مخرب بر امنیت زیستی یا ترور شخصیتی اتباع یک کشور را موجب گردد. نظام حقوقی اتحادیه اروپا در این زمینه دربردارنده مقررات مفصلی می‌باشد که از جمله آنها می‌توان به مقررات عمومی حفاظت از داده‌ها مصوب سال ۲۰۱۶ اشاره نمود. این مقررات دربردارنده قواعد مفصلی در زمینه حفظ و پیشگیری از نقض امنیت اطلاعات می‌باشد. سوال اصلی که این پژوهش به دنبال پاسخگویی به آن می‌باشد این است که ماده ۳۲ این مقررات دربردارنده چه سازوکارهایی در جهت پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات است؟ برای پاسخگویی به سوال فوق، پژوهش حاضر به روش اسنادی با ارائه مفاد ماده فوق الذکر و تحلیل بندهای آن، سازوکارهای تعیین شده در این ماده را در چهار دسته مستعارسازی و رمزگذاری داده‌های شخصی، اطمینان از محرمانه بودن، یکپارچگی، در دسترس بودن و انعطاف پذیری سیستم‌ها و خدمات پردازشی، خطرات (ریسک) مرتبط با پردازش اطلاعات و رعایت الزامات شکلی قرار داده و در قسمت نتیجه‌گیری نیز مبادرت به ارائه برخی توصیه‌های سیاستگذارانه از جمله نحوه اصلاح قوانین و مقررات مصوب در نظام حقوقی ایران، آگاهی بخشی به مردم از طریق رسانه‌های ارتباط جمعی و نظام مند نمودن اعطای مجوز به فعالیت شرکت‌های فراملی به عنوان نتایج حاصل از بررسی ماده ۳۲ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا نموده‌است.
تاریخ دریافت: ۱۴۰۳/۱۱/۱۶	
تاریخ بازنگری: ۱۴۰۳/۰۵/۲۱	
تاریخ پذیرش: ۱۴۰۳/۰۶/۱۸	
کلیدواژه: امنیت، شبکه‌های تبادل اطلاعات، داده‌پیام، موضوع داده، کنترل کننده، اتحادیه اروپا.	
استناد	کوشا، ابوطالب، صادقی، حسین، ناصر، مهدی (۱۴۰۳). پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات در پرتو ماده ۳۲ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا. نشریه قضاوت، (۳)، ۳۱-۱. DOI: https://doi.com/10.22034/judg.2024.2022304.1279
DOI	10.22034/JUDG.2024.2022304.1279
ناشر	انتشارات دادگستری کل استان تهران



مقدمه

شبکه‌های تبادل اطلاعات به کامپیوترهای متصل به هم که مبادرت به پردازش و به اشتراک گذاری اطلاعات می‌نمایند، اطلاق می‌گردد.^۱ یک شبکه متشکل از پنج جزء سخت افزار، نرم افزار، کاربران که متشکل از اشخاص موضوع داده-کنترل‌کنندگان و پردازندگان هستند، داده‌پیام‌های مورد تبادل و بسترهای ارتباطی می‌باشد. اشخاص موضوع داده در شبکه‌های تبادل اطلاعات، اشخاصی هستند که طی فرایند پردازش، اطلاعات آنها جمع‌آوری، تحلیل و ذخیره می‌گردد. کنترل‌کنندگان شبکه‌ها نیز اشخاصی هستند که مبادرت به مدیریت عملکرد و فرایند پردازش اطلاعات در یک شبکه می‌نمایند. در صورتی که این اشخاص مبادرت به اعطای فرایند پردازش به اشخاص ثالث و تعیین خط مشی پردازش به آنها کنند، اشخاص ثالث اصطلاحاً پردازندگان داده‌پیام‌ها در شبکه‌های تبادل اطلاعات تلقی می‌شوند.

آنچه در یک شبکه، مورد تبادل قرار می‌گیرد، داده‌پیام می‌باشد. داده‌پیام به تعبیر بند اول ماده ۲ قانون تجارت الکترونیکی، هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود. این مفهوم به دو نوع شخصی و غیرشخصی تقسیم بندی می‌شود. داده‌پیام‌های شخصی داده‌پیام‌هایی هستند که پردازش آنها منجر به شناسایی مستقیم یا غیرمستقیم اشخاص می‌گردند. اما داده‌پیام‌های غیرشخصی، خصوصیت بخصوصی نداشته و هر داده‌پیامی که در دسته داده‌پیام‌های غیرشخصی قرار نگیرند را شامل می‌گردند (van der Sloot, 2017, 20). آنچه در زمینه نقض امنیت شبکه در خصوص داده‌پیام‌ها تلقی می‌گردد، مربوط به داده‌پیام‌های شخصی می‌باشد. در حالی که داده‌پیام‌های غیرشخصی، اطلاعاتی هستند که در اختیار عموم افراد بوده و اساساً نقض امنیت داده در خصوص این اطلاعات مطرح نمی‌شود.

آنچه به عنوان معضل اصلی جوامع بشری در عصر حاضر به عنوان عصر الکترونیک مشاهده می‌گردد، نبود سازوکارهای صحیح پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات می‌باشد. به عبارت دیگر شبکه‌های تبادل اطلاعات به عنوان اصلی‌ترین مراکز ذخیره، جمع‌آوری، تحلیل و نگهداری اطلاعات، در معرض حمله‌های فراوان خارجی می‌باشند که عدم اتخاذ تدابیر لازم در جهت حفظ امنیت شبکه‌ها و اجزای آنها، موضوعی است که هر چند با توجه به برخورداری از ماهیتی فنی و اجرایی، در مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا مورد تصریح و تشریح قانون گذار این اتحادیه قرار گرفته است. به عبارت دیگر پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات،

1. Roy Winkelman, Director, What is a Network?, Florida Center for Instructional Technology College of Education, University of South Florida, <https://fcit.usf.edu/network/chap1/chap1.htm>, last visited 18/07/2023

به معنای پیشگیری از نقض تمامیت اجزای یک شبکه می باشد. این فرایند نیازمند بکارگیری اقدامات فنی مناسب در جهت تضمین امنیت شبکه می باشد. اقدامات فنی به هرگونه اقدامات گفته می شود که برای ایجاد سطح مناسبی از حفاظت از اجزای یک شبکه خصوصاً اطلاعات به کار گرفته می شوند (لطیف زاده و دیگران، ۱۴۰۲، ۲۵۳). اجرای این الزامات در یک شبکه بر عهده کلیه اجرای شبکه از جمله اشخاص موضوع داده، کنترل کنندگان و پردازندگان بوده و در صورتی که پردازنده ای به هر دلیل فرایند پردازش را به پردازنده دیگری محول نموده باشد، توسط پردازنده جدید نیز باید مورد توجه قرار گیرد. (همانجا) این الزامات در ماده ۳۲ مقررات عمومی حفاظت از داده ها مصوب سال ۲۰۱۶ اتحادیه اروپا^۱ مورد تصریح قرار گرفته اند. ماده ۳۲ مقرر می دارد:

۱. با در نظر گرفتن وضعیت فنی، هزینه های اجرا و ماهیت، دامنه، زمینه و اهداف پردازش و همچنین خطر احتمال و شدت متفاوت برای حقوق و آزادی های اشخاص حقیقی، کنترل کننده و پردازشگر باید اقدامات فنی و سازمانی مناسب را برای اطمینان از سطح امنیتی متناسب با خطر، از جمله موارد زیر اجرا کند:

- نام مستعار و رمزگذاری داده های شخصی؛
- توانایی اطمینان از محرمانه بودن، تمامیت، در دسترس بودن و انعطاف پذیری سیستم ها و خدمات پردازشی؛
- امکان بازیابی در دسترس بودن و دسترسی به داده های شخصی به موقع در صورت وقوع یک حادثه فیزیکی یا فنی؛
- فرآیندی برای آزمایش منظم، ارزیابی و ارزیابی اثربخشی اقدامات فنی و سازمانی برای اطمینان از امنیت پردازش؛

۲. در ارزیابی سطح مناسب امنیتی باید به ویژه خطراتی که از طریق پردازش به وجود می آیند، به ویژه ناشی از تخریب تصادفی یا غیرقانونی، از دست دادن، تغییر، افشای غیرمجاز، یا دسترسی به داده های شخصی منتقل شده، ذخیره شده یا به طور دیگری فرآوری شده در نظر گرفته شود

۳. پایبندی به مقررات شکلی مندرج در ماده ۴۰ یا سازوکار صدور گواهی نامه تأیید شده مندرج در ماده ۴۲ که می تواند به عنوان عنصری برای نشان دادن انطباق با الزامات مندرج در بنادول این ماده استفاده شود

۴. کنترل کننده و پردازشگر باید اقداماتی را انجام دهند تا اطمینان حاصل شود که هر شخص حقیقی که تحت اقتدار کنترل کننده یا پردازشگر که به داده های شخصی دسترسی دارد آنها

را پردازش نکند مگر به دستور یا درخواست کنترل‌کننده، بر اساس قانون اتحادیه اروپا یا هریک از کشورهای عضو باشد.

همانطور که ملاحظه می‌گردد، مفاد مقررات ماده ۳۲، الزامات مندرج در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات را در چهار دسته مستعارسازی و رمزگذاری داده‌های شخصی، اطمینان از محرمانه بودن، یکپارچگی، در دسترس بودن و انعطاف‌پذیری سیستم‌ها و خدمات پردازشی، خطرات (ریسک) مرتبط با پردازش اطلاعات و رعایت الزامات شکلی قرار داده که در گفتارهای چهارگانه این پژوهش مورد تحلیل و بررسی قرار خواهند گرفت. پژوهش حاضر در قسمت نتیجه‌گیری نیز مبادرت به ارائه برخی توصیه‌های سیاستگذارانه در جهت بهبود اجرای سازوکارهای بیان‌شده در متن تحقیق می‌نماید.

در بدایت امر یادآور می‌گردد که اگرچه در میان مقالات منتشر شده در نظام حقوقی ایران، پژوهش‌هایی پیرامون بررسی جنبه‌های حقوقی حفاظت از داده پیام‌های شخصی منتشر گردیده، اما هیچ‌کدام از پژوهش‌های منتشر شده، با محوریت پژوهش حاضر همپوشانی مطالب نداشته و این پژوهش در نوع خود یک پژوهش نوین تلقی می‌گردد.

در این زمینه فرحزادی و ناصر در مقاله حق بر تبادل داده‌های خصوصی و راه کارهای رفع چالش‌های آن در سازوکار عملکرد ابزارهای اینترنت اشیا به موضوع حق بر تبادل اطلاعات به عنوان یکی از حقوق اشخاص در فرایند پردازش اطلاعات شخصی آنها در سازوکار عملکرد ابزارهای اینترنت اشیا پرداخته‌اند. علاوه بر آن صادقی و ناصر در مقاله مطالعه تطبیقی سازوکار شناسایی قانون حاکم بر دعاوی ناشی از نقض مقررات حفاظت از داده‌های خصوصی و چالش‌های پیش رو در حقوق ایران و اتحادیه اروپا به موضوع تعارض قوانین و قانون حاکم بر نقض امنیت پردازش اطلاعات پرداخته‌اند. افراسیاب و ناصر نیز در مقاله چارچوب‌های حقوقی حفظ امنیت پردازش داده‌های خصوصی (مطالعه‌ای تطبیقی در حقوق ایران و اتحادیه اروپا) و فرحزادی، صادقی و ناصر در مقاله وظایف کنترل‌کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات به تبیین و تشریح وظایف کنترل‌کنندگان و پردازندگان در فرایند پردازش اطلاعات در شبکه‌های ارتباطی و پیشگیری از نقض امنیت فرایند پرداخته‌اند. مضاف بر آنچه بیان شد لطیف زاده، قبولی درافشان، محسنی و عابدی در مقالات تبیین اسباب مشروعیت پردازش داده شخصی از منظر حقوق اتحادیه اروپا و ایران، تعهدات پردازش‌کننده داده شخصی در اتحادیه اروپا و امکان سنجی پذیرش آن در حقوق ایران و حمایت از داده شخصی در حقوق اتحادیه اروپا و امکان سنجی آن در نظام حقوقی ایران به ترتیب به تشریح شرایط پردازش اطلاعات خصوصاً اخذ رضایت از موضوع داده، وظایف پردازندگان اطلاعات و تحلیل حقوق اشخاص موضوع داده در

فرایند پردازش اطلاعات اقدام کرده و انصاری و عطار در مقاله حمایت از داده‌ها در چین؛ مطالعه تطبیقی با رویکرد حمایت از داده‌ها در امریکا و اتحادیه اروپا نیز به صورت کلی به مقایسه نظام حاکم بر حمایت از داده‌ها در چین و اتحادیه اروپا و امریکا و شاخصه‌های هر یک پرداخته‌اند. آنچه در بررسی مقالات منتشره در این زمینه ملاحظه می‌گردد این است که مقالات منتشر شده در این زمینه دارای محوریت حقوق اشخاص و وظایف نهادهای فعال در پردازش اطلاعات شخصی افراد می‌باشند. این در حالی است که بررسی سازوکارهای حقوقی پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات مندرج در ماده ۳۲ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا موضوعی است که هم از جهت بعد پیشگیرانه، هم از جهت جزئی بودن بررسی یک ماده قانونی خاص و هم از جهت تبیین موضوع حول محوریت شبکه‌های تبادل اطلاعات این مقاله را به یک مقاله منحصر به فرد تبدیل می‌نماید.

۱. مستعارسازی و رمزگذاری داده‌های شخصی

یکی از راهکارهای پیشگیری از نقض امنیت داده‌پیام‌ها، ناشناس‌سازی آن‌ها می‌باشد. در فرایند ناشناس‌سازی اطلاعات، سه اصطلاح مهم با عنوان مستعارسازی^۱، ناشناس‌سازی^۲ و رمزگذاری^۳ وجود دارند. مستعارسازی اطلاعات به روشی برای پنهان کردن داده‌ها گفته می‌شود که در آن انتساب داده‌های شخصی به یک شخص خاص بدون وجود اطلاعات اضافی امکان پذیر نمی‌باشد.^۴ در مقابل ناشناس‌سازی به روشی اطلاق می‌گردد که در آن داده‌های شخصی به صورت بازگشت ناپذیر از قابلیت انتساب به یک شخص خاص جدا شده و به داده‌های کاملاً ناشناس تبدیل می‌شوند. رمزگذاری اطلاعات نیز به فرایند گفته می‌شود که در آن اطلاعات از طریق سازوکارهای فنی، از قابلیت پردازش خارج نموده و تنها با بکارگیری ابزارهایی که اصطلاحاً کلید نامیده می‌شوند، قابلیت پردازش را پیدا می‌کنند.

فرایند رمزگذاری اطلاعات به دو صورت متقارن^۵ و نامتقارن^۶ انجام می‌گیرد. گاه جهت افزایش امنیت اطلاعات، فرایند رمزگذاری به صورت ترکیبی از دو شق فوق انجام می‌شود که به آن رمزگذاری ترکیبی^۷ گفته می‌شود. وجه تمایز رمزنگاری متقارن و نامتقارن در وجود کلید مخفی

1. Pseudonymization

2. anonymization

3. encryption

4. Satori, Pseudonymisation: 9 Ways to Protect Your PII, <https://satoricyber.com/data-masking/pseudonymisation-9-ways-to-protect-your-pii/>, Last Visited 13/07/2023

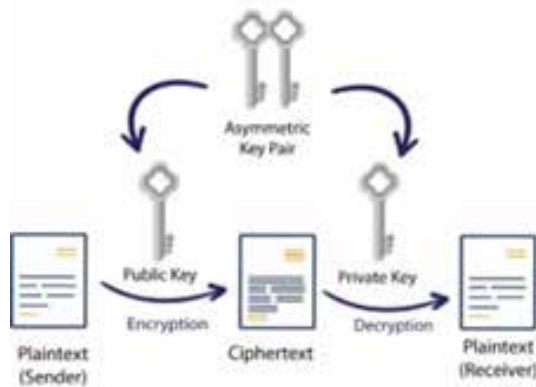
5. symmetric encryption

6. asymmetric encryption

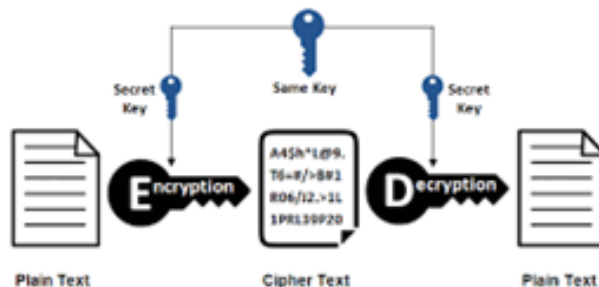
7. hybrid encryption

می‌باشد. به عبارت دیگر در رمزگذاری متقارن رمزگذاری اطلاعات با استفاده از کلید خصوصی که رمزگذار در اختیار دارد انجام شده و رمزگشایی اطلاعات نیز با استفاده از کلید عمومی که در اختیار مخاطب وجود دارد صورت می‌پذیرد. اما در رمزگذاری نامتقارن، جفت کلید مخفی در اختیار دو طرف وجود دارد که اگر هر عنصر بیگانه‌ای به کلیدهای عمومی و خصوصی دسترسی پیدا نماید، امکان رمزگشایی اطلاعات به جهت عدم دسترسی به کلیدهای مخفی در اختیار طرفین برای وی میسر نمی‌گردد.^۱ تصاویر ذیل گویای وجه تمایز دو رمزگذاری می‌باشند:

Asymmetric Encryption



Symmetric Encryption



وجه تمایز سه واژه مستعارسازی، ناشناس‌سازی و رمزگذاری این است که در فرایند رمزگذاری،

1. Ales Teska , Pseudonymization, Anonymization, Encryption ... what is the difference?, <https://teskalabs.com/blog/data-privacy-pseudonymization-anonymization-encryption>, Last visited 13/07/2023

اطلاعات رمزگذاری شده توسط شخص رمزگذارنده و فردی که مخاطب این اطلاعات بوده قابل رمزگشایی و پردازش می‌باشند. اما در فرایند مستعارسازی اطلاعات، تنها شخصی که مبادرت به مستعارسازی نموده است، از قابلیت ضمیمه اطلاعات دیگر جهت امکان انتساب این داده‌ها به موضوع داده برخوردار می‌باشد. به عبارت دیگر شخص دیگری جز مستعارساز، از نوع و ماهیت این اطلاعات اطلاع نداشته و بنابراین جز او فرد دیگری از قابلیت بازخوانی این اطلاعات برخوردار نیست. و اما در ناشناس‌سازی، اطلاعات شخصی بدون بازگشت به اطلاعات عمومی تبدیل شده و حتی شخصی که مبادرت به ناشناس‌سازی داده‌پیام‌ها نموده‌باشد نیز از این قابلیت بی‌بهره خواهد بود.^۱ در شکل زیر می‌توان به وجه تمایز مستعارسازی و ناشناس‌سازی اطلاعات به نحو مشخص‌تری پی برد:



بر اساس ماده ۲ قانون مدنی، جهل به قانون مدنی و طبق ماده ۱۵۵ قانون مجازات اسلامی، جهل به قانون کیفری رافع مسئولیت کیفری نیست جز در موارد موضوع ماده ۲۱۷ قانون مجازات اسلامی. به نظر نگارندگان، جهل به حکم مدنی که موضوع قانون با جمع بندی مطالب فوق می‌توان به این نتیجه رسید که دلیل اینکه قانون‌گذار اتحادیه اروپا از واژه‌های مستعارسازی یا رمزگذاری در ماده ۳۲ مقررات مصوب سال ۲۰۱۶ نام برده این است که اطلاعات شخصی پس از طی فرایند رمزگذاری و یا مستعارسازی، ماهیت خود را از دست نداده و همچنان داده‌های شخصی باقی می‌مانند. اما در فرایند ناشناس‌سازی، داده‌های شخصی ماهیت شخصی بودن خود را از دست داده و به داده‌های عمومی (غیرشخصی) تبدیل می‌شوند و در این صورت هیچ کدام از الزامات قانونی

1. Joshua Gresham , Is encrypted data personal data under the GDPR?, <https://iapp.org/news/a/is-encrypted-data-personal-data-under-the-gdpr/>, Last Visited 27/07/2023

مندرج در مقررات فوق‌الذکر در خصوص این نوع داده‌ها قابلیت اجرا نخواهد داشت. در نظام حقوقی اتحادیه اروپا بند پنجم ماده ۴ مقررات مصوب سال ۲۰۱۶، حاوی تعریف مستعارسازی اطلاعات می‌باشد. این بند مقرر می‌دارد:

«مستعارسازی» به معنای پردازش داده‌های شخصی به گونه‌ای است که دیگر نمی‌توان داده‌های شخصی را بدون استفاده از اطلاعات اضافی به یک موضوع خاص داده نسبت داد، مشروط بر اینکه این اطلاعات اضافی به طور جداگانه نگهداری شود و مشمول اقدامات فنی و سازمانی باشد تا اطمینان حاصل شود که داده‌های شخصی به یک شخص حقیقی شناسایی شده یا قابل شناسایی نسبت داده نمی‌شود.

در تعریف مندرج در ماده فوق‌الذکر، چند ویژگی برای مستعارسازی اطلاعات ذکر شده است. ویژگی اول همانطور که در مطالب فوق نیز بدان اشاره شد این است که عملیاتی بر روی اطلاعات صورت پذیرد که بدون استفاده از اطلاعات اضافی، امکان انتساب این داده‌ها به موضوع داده امکان پذیر نباشد. اما ویژگی مهم دیگر نگهداری اطلاعات اضافی به صورت جداگانه و با اقدامات فنی و سازمانی مناسب می‌باشد تا جز اشخاص صلاحیت دار، دیگران از امکان خارج نمودن اطلاعات از حالت مستعار برخوردار نباشند. به عنوان مثال می‌توان به داده‌های پزشکی و سلامت اشخاص اشاره نمود. امروزه سازمان‌های بهداشت و سلامت کشورها، برای حفظ امنیت داده‌های پزشکی حساس مردم، آن‌ها را مستعارسازی می‌نمایند. به عبارتی با تخصیص یک کد یا حرف به هر شخص و نگهداری لیست تطبیق کدهای اعطا شده با اسامی واقعی اشخاص در سامانه‌های امن، نسبت به مستعارسازی اطلاعات اقدام می‌کنند.^۱ این موضوع در اطلاعات شخصی مأمورین سازمان‌های اطلاعاتی نمود بیشتری دارد که معمولاً با اسامی مستعار یا کد در دستگاه‌های قضایی به وظایف خود در نقش یک ضابط اقدام می‌نمایند.

۲. توانایی اطمینان از محرمانه بودن، یکپارچگی، دردسترس بودن و انعطاف پذیری سیستم‌ها و خدمات پردازشی

برخلاف آنچه در متن ماده ۳۲ قید شده است، اطمینان از محرمانگی، یکپارچگی و دردسترس بودن و انعطاف‌پذیری سیستم‌ها و خدمات پردازشی به منزله اقدامات فنی و سازمانی تلقی نشده بلکه نیازمند به کارگیری زیرساخت‌های فنی می‌باشد تا اطمینان مذکور در خصوص سیستم‌ها و خدمات پردازشی یک سازمان حاصل گردد. از جمله این اقدامات می‌توان به موارد ذیل اشاره نمود:

- کنترل دسترسی: سیستم‌ها و خدمات پردازشی یک سازمان باید به نحوی طراحی شوند که

1. Thomas Zerdick, Pseudonymous data: processing personal data while mitigating risks, https://edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en, Last visited 31/07/2023

در محیطی جدا از محیط اداری آن سازمان قرار داشته و دسترسی به این اتاق به وسیله کارت کلیدها یا تراشه‌های مخصوصی که به افراد صلاحیت دار داده می‌شود، محدود گردد. علاوه بر آن اتاقی که سیستم‌ها در آن قرار دارند، الزاماً باید مجهز به هشدارهای امنیتی بوده تا در صورتی که افراد فاقد مجوز به هر دلیلی وارد محوطه سیستم‌ها شوند، نسبت به اعلام هشدار اقدام نماید.

- تعریف سطح دسترسی به کاربران جهت حفظ محرمانگی سیستم: نکته دومی که در قسمت دوم بند اول ماده ۳۲ بدان اشاره شده، اطمینان از محرمانگی سیستم‌ها می‌باشد. محرمانگی سیستم به معنای عدم دستیابی افراد فاقد صلاحیت به اجزای مختلف یک سیستم ارتباطی می‌باشد. بنابراین در صورتی که سازوکاری تعریف گردد تا هر شخص بر مبنای وظایف و اختیارات قانونی خود، از سطح دسترسی به اجزای مختلف یک سیستم بهره مند شود، می‌توان محرمانگی اجزای سیستم را حفظ نمود. این موضوع با تعریف نام کاربری مشخص برای هر شخص و تعریف سمت وی در یک سیستم میسر می‌گردد. امروز سازمان‌های مختلف نیز در سیستم‌های خود با تعریف سمت هر شخص، سطح دسترسی وی به اجزا و اطلاعات موجود در سیستم را تعیین نموده و کاربر تعریف شده بیش از مقدار تعریف شده از امکان دسترسی به سیستم برخوردار نیست. این امر تضمین کننده محرمانگی سایر اجرای یک سیستم خواهد بود.^۱

- امکان بازیابی اطلاعات جهت حفظ انعطاف پذیری سیستم: آنچه در یک سیستم ارتباطی اهمیت وافر دارد، توانایی بازیابی اطلاعاتی می‌باشد که ممکن است در اثر عملیات پردازش و یا به صورت سهوی پاک شده باشند. این موضوع می‌تواند تضمین کننده تمامیت اطلاعات ذخیره شده در یک سیستم نیز باشد. مهم‌ترین و موثرترین گام در این زمینه، تهیه نسخه پشتیبان از اطلاعات ذخیره شده در سیستم است که باید در هر بازه زمانی یا پس از انجام هر عملیات پردازش به طور کامل صورت پذیرد. در این صورت در مواقع حذف اطلاعات، امکان بازیابی آنها از طریق نسخه‌های پشتیبان موجود خواهد بود.^۲ در این فرایند تهیه نرم افزارهای ریکاوری اطلاعات یا استفاده از روش‌های بازیابی داده‌ها در داخل سامانه از کارکرد عملی برخوردار نیست.^۳ علت این موضوع نیز آن است که چون هاردهای ذخیره اطلاعات در سیستم‌ها دارای ظرفیت محدود می‌باشند که در هر بازه زمانی پاک

1. Data2.EU, Technical and organisational measures, <https://data2.eu/en/gdpr/what-technical-and-organisational-measures-do-we-need-to-take>, Last Visited 19/08/2023
2. Marie Prokopets, The Ultimate Manual To GDPR Article 32, <https://nira.com/gdpr-article-32/>, Last Visited 15/05/2023
3. Securiti, Article 32 Of The GDPR: Explained, <https://securiti.ai/blog/gdpr-article-32/>, Last Visited 12/03/2023

شده و نسخه جدید اطلاعات بر روی آن‌ها ذخیره می‌شوند، در عمل بازیابی اطلاعاتی که نسخه‌های جدید به صورت دوباره یا سه باره بر روی آن‌ها ذخیره شده باشند یا ممکن نبوده یا در صورت امکان با کیفیت بسیار ضعیف و دارای نقض صورت می‌گیرد. چرا که در عمل بازیابی اطلاعات عموماً بر روی آخرین لایه ذخیره شده در یک سامانه صورت می‌پذیرد.

۳. ارزیابی خطرات (ریسک) مرتبط با پردازش اطلاعات

ارزیابی خطرات مرتبط با پردازش اطلاعات، دیگر سازوکاری می‌باشد که در جهت تضمین امنیت اطلاعات کاربرد دارد. این موضوع از آن جهت مهم است که پیش بینی خطرات مرتبط با پردازش اطلاعات و به کارگیری اقدامات متناسب با نوع پردازش، می‌تواند از نقض امنیت اطلاعات در یک شبکه ارتباطی پیشگیری نماید. در این فرایند آنچه مهم است در نظر گرفتن حقوق موضوع داده، پیچیدگی پردازش داده‌ها، حساسیت موضوع و خسارات احتمالی نقض امنیت اطلاعات می‌باشد که درجه اهمیت این پروسه را نشان می‌دهد.^۱

به عبارت دیگر مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا، به گونه‌ای تنظیم شده‌اند که انجام پردازش اطلاعات را منوط به رعایت سطوح امنیتی متناسب با نوع داده و رعایت حقوق موضوع داده کرده‌اند. این موضوع از مواد ۸۵ الی ۸۹ این مقررات قابل برداشت می‌باشد.

مواد ۸۵ تا ۸۹ از مقررات مصوب سال ۲۰۱۶، دارای شرایطی برای پردازش برخی اطلاعات می‌باشند که پردازش آن‌ها ممکن است با خطراتی همراه باشد. ماده ۸۵ از این مقررات مرتبط با حق تقابلی آزادی بیان در مطبوعات و اطلاعات می‌باشد که انتشار اطلاعات در کشورهای عضو اتحادیه اروپا در رسانه‌های جمعی مانند تلویزیون، رادیو و ... را منوط به رعایت، حقوق موضوع داده، وظایف قانونی کنترل‌کنندگان و پردازندگان شبکه‌ها، سازوکار نظارت مقامات صلاحیت دار و ... نموده است. علت این موضوع آن است که انتشار اطلاعات در مطبوعات منجر به گسترش سریع داده‌ها در میان اقشار یک جامعه شده و عدم رعایت و توجه به الزامات امنیتی می‌تواند در صورت نقض، آثار زیان بار در سطح وسیعی ایجاد نماید. بنابراین وجود مفاهیم موسعی مانند «آزادی مطبوعات» مجوز این موضوع نمی‌باشد که کلیه الزامات قانونی تعیین شده در مقررات مصوب سال ۲۰۱۶ کنار گذاشته شوند و از این رو باید اصولی مانند به حداقل رساندن داده‌ها که در بردارنده نتیجه انتشار اطلاعات در حد «ضرورت» می‌باشد در شبکه‌های اجتماعی رعایت شود. (لطیف زاده و دیگران، ۱۴۰۱، ۱۵۹). در کنار این ماده، ماده ۸۶ از مقررات مصوب سال ۲۰۱۶، افشای اسناد دولتی را تنها تحت

1. Office of the Data Protection Ombudsman, Risk assessment and data protection planning, <https://tietosuojaja.fi/en/risk-assessment-and-data-protection-planning>, Last Visited 02/04/2023

ضوابط قانونی و نظارت مقامات صلاحیت دار حکومتی که اصطلاحاً مقام ناظر نامیده می‌شوند، امکان‌پذیر ساخته است. علت این موضوع، مرتبط بودن اسناد دولتی با اطلاعات ذخیره شده از کارکنان یا مشتریان ادارات و یا حتی تجهیزات موجود در یک اداره می‌باشد که می‌تواند پتانسیل نفرت یا کیفیت خدمات ارائه شده در یک سازمان را نشان دهد. از این رو اگر الزامات لازم در این زمینه حفظ نشود، ممکن است کمبودها و نیازمندی‌های یک سازمان یا نقاط ضعف موجود در سیستم ارائه خدمات یک کشور در شبکه‌های ارتباطی آن یا سایر شبکه‌های ارتباطی منتشر گردد. ماده ۸۷ نیز در کنار الزامات مقرر در این قانون، رعایت سایر الزامات مقرر در نظام حقوقی دیگر کشورها در زمینه پردازش اطلاعات شناسنامه ملی یا هر شناسه دیگری که به اتباع آن کشورها اختصاص یافته را ضروری تلقی نموده است. همانطور که می‌دانیم، این اطلاعات جزو داده‌های شخصی می‌باشند که پردازش آنها نیاز به برقراری سطح امنیتی مناسب داشته و هرچه سطح امنیت پردازش این اطلاعات افزایش یابد، امکان نقض امنیت آنها در فرایند پردازش نیز کاهش می‌یابد. علاوه بر آن هر کشور معمولاً متناسب با فرهنگ و امکانات و هنجارهای حاکم بر جامعه خود، الزامات امنیتی را برای پردازش چنین اطلاعاتی در نظر می‌گیرد که جمع این الزامات با الزامات مندرج در مقررات مصوب سال ۲۰۱۶، می‌تواند در بهبود امنیت پردازش این اطلاعات مؤثر باشد.

ماده ۸۸ از این مقررات نیز در بردارنده قواعدی در جهت پردازش اطلاعات استخدامی کارکنان دستگاه‌های اجرایی می‌باشد که پردازش این اطلاعات را منوط به رعایت کرامت انسانی و حقوق اساسی آنها نموده است. این موضوع از آن جهت اهمیت دارد که دستگاه‌های اجرایی در زمان استخدام نیروها، با انجام تحقیقات گسترده عموماً وارد حریم خصوصی اشخاص نیز شده و اطلاعات جامعی در ابعاد مختلف زندگی خصوصی اشخاص را جمع‌آوری و نگهداری می‌نمایند. هرگونه سوءاستفاده یا نشت این اطلاعات به بیرون از سازمان، می‌تواند اثرات مخربی بر زندگی شخصی یک فرد داشته باشد. بنابراین حفظ کرامت انسانی در پردازش این اطلاعات در تمامی ابعاد، موضوعی است که مدنظر قانون‌گذار اتحادیه اروپا در این ماده بوده است. در کنار این ماده، مقررات ماده ۸۹ نیز همانطور که پیشتر نیز توضیح داده شد، رعایت اصول پردازش اطلاعات خصوصاً اصل به حداقل رساندن داده‌ها و حقوق موضوع داده را در پردازش اطلاعات بر اساس اهداف مرتبط با منافع عمومی، اهداف تحقیقاتی و علمی و تاریخی اجباری نموده است. برای احراز و بررسی موارد فوق، آنچه در عمل باید اجرا گردد، طراحی فلوچارتی متشکل از مراحل پردازش اطلاعات و جدول سؤالات کلیدی می‌باشد که متناسب با نوع داده‌ها و پردازش

صورت گرفته، باید در دستور کار قرار گیرد.^۱ در حال حاضر فلوچارت بیان‌شده در ذیل در فرایند پردازش اطلاعات در نظام حقوقی اتحادیه اروپا کاربرد داشته و بکارگیری آن در نظام حقوقی ایران نیز می‌تواند در نظام مند نمودن فرایند پردازش اطلاعات و پیشگیری از نقض امنیت کاربران و داده‌های مورد پردازش کاربرد داشته باشد.

۱-۳. تعیین مرزهای عملیات پردازش و زمینه مربوط به آن

اولین مرحله در شروع فرایند پردازش اطلاعات و ارزیابی ریسک، تعیین مرزهای عملیات پردازش و زمینه مربوط به آن است. در انجام این کار، سازمان باید مراحل مختلف پردازش داده‌ها (جمع‌آوری، ذخیره‌سازی، تحلیل و استفاده، انتقال، حذف و غیره) و پارامترهای بعدی آنها را در نظر بگیرد. بر این مبنا توجه ویژه باید به این واقعیت معطوف شود که تجزیه و تحلیل صورت گرفته به یک عملیات پردازش خاص مربوط می‌شود. از این رو در صورتی که فرایند پردازش توسط سیستم از بیش از یک عملیات پردازش داده تشکیل شده باشد، تجزیه و تحلیل صورت گرفته باید برای هر عملیات پردازش ترتیب داده شود.

این موضوع اعم از آن است که پردازش اطلاعات بر روی داده‌های قرارگرفته در دسته‌های متفاوت داده‌ها از جمله بیومتریک، مذهبی، روانشناختی و... قرار گیرند یا نوع پردازش اطلاعات اعم از انتقال، استفاده، افشا و... مدنظر سازمان پردازش کننده باشند. انجام مرحله اول از پردازش اطلاعات در سازمان عموماً با تکمیل جدول ذیل که در بردارنده کلیه اطلاعات بیان‌شده برای شروع مرحله پردازش و ارزیابی ریسک می‌باشد، صورت می‌پذیرد:^۲

ردیف	عنوان اقدام	نوع و نحوه اقدام
۱	شرح عملیات پردازش	ذکر مشروع عنوان عملیات پردازش
۲	داده‌های شخصی مورد پردازش	نوع داده‌های شخصی که در عملیات پردازش، تحت پردازش قرار می‌گیرند
۳	اهداف پردازش	پردازش بر اساس چه اهدافی صورت می‌پذیرد

1. Enisa, Handbook on Security of Personal Data Processing, European Union Agency For Network and Information Security, online edition www.enisa.europa.eu, 2017, Last Visited 16/08/2023.

2. The European Union Agency for Cybersecurity, Evaluating the level of risk for a personal data processing operation, <https://www.enisa.europa.eu/risk-level-tool/risk>, Last Visited 02/04/2023.

۴	اشخاص موضوع داده	ذکر مشخصات و سمت اشخاص موضوع داده، به عنوان مثال نام و نام خانوادگی فرد چه بوده و در یک سازمان نقش کارمند، مشتری و... را بر عهده دارد.
۵	ابزارهای پردازش	فرایند پردازش اطلاعات توسط چه ابزارهایی و بر روی چه سخت افزار و نرم افزاری صورت می‌پذیرد. به عبارت دیگر آیا فرایند پردازش اطلاعات به صورت خودکار توسط سامانه شروع و اتمام می‌یابد یا در مراحل مختلف توسط ابزار یا ابزارهای خاصی صورت خواهد گرفت. علاوه بر آن پردازش اطلاعات در چه بستری صورت خواهد پذیرت. به عبارت دیگر پردازش اطلاعات در شبکه و سیستم‌های درون سازمانی صورت خواهد پذیرفت یا این اقدام در شبکه‌های عمومی مانند اینترنت انجام خواهد شد.
۶	پردازشگر اطلاعات	باید مشخصات و موقعیت مکانی پردازشگر اطلاعات و اینکه آیا پردازشگر در کشور متبوع موضوع داده یا کنترل‌کننده ساکن بوده یا مقر آن در کشور ثالثی می‌باشد، قید گردد. علاوه بر آن صرف نظر از مقر پردازنده، اطلاعات در کجا و کدام کشور و با چه نظام حقوقی و الزاماتی در پردازش اطلاعات تحت پردازش قرار خواهند گرفت.
۷	دریافت کنندگان داده‌های شخصی	پس از فرایند پردازش، چه شخص یا اشخاصی به داده‌های پردازش شده دسترسی داشته و به عبارتی این اطلاعات در اختیار چه افراد یا نهادهایی گذاشته خواهد شد.

۲-۳. ارزیابی تأثیر

مرحله دوم در فرایند ارزیابی ریسک پردازش اطلاعات، ارزیابی تأثیر می‌باشد. در این مرحله، کنترل‌کننده بر اساس اطلاعاتی که در جدول مرحله اول نهاده شده است، نسبت به ارزیابی تأثیر پردازش بر حقوق و آزادی‌های اساسی موضوع داده پرداخته و نتیجه حاصل را در چهار سطح تأثیر کم-متوسط-زیاد-خیلی زیاد به شرح جدول ذیل قرار می‌دهد. خاطر نشان می‌گردد حقوق و آزادی‌های موضوع داده تنها به حقوق وی در مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا محدود نشده و حقوق تعیین شده برای وی در مقررات داخلی کشور متبوع موضوع داده و سایر حقوق از جمله حقوق بشر، حقوق شهروندی و... او را نیز شامل می‌گردد. نکته قابل توجه این است که ارزیابی صورت گرفته در این مرحله به صورت نسبی بوده و ممکن است نتیجه آن در زمان‌ها و مکان‌های مختلف، متفاوت باشد؛ با این حال ملاک زمانی ارزیابی و تصمیم‌گیری برای پردازش اطلاعات خواهد بود.^۱

ردیف	سطح تأثیر	شرح ارزیابی
۱	کم	در این سطح از ارزیابی، سطح کمی از حقوق و آزادی‌های اساسی اشخاص مانند صرف وقت تحت الشعاع قرار می‌گیرند.
۲	متوسط	در این سطح برخی حقوق و آزادی‌های اساسی اشخاص تحت الشعاع قرار می‌گیرد و اشخاص را با مشکلاتی مانند تحمیل هزینه‌های اضافی، محرومیت از برخی خدمات متناسب با پردازش صورت گرفته در مورد اطلاعات، استرس، بیماری‌های جسمی و روحی غیرحادث مواجه می‌گرداند.
۳	زیاد	در این سطح، موضوع داده ممکن است با عواقب قابل توجهی در پردازش اطلاعات مواجه شود که تأثیر اساسی بر زندگی شخصی و اجتماعی وی داشته باشد. به عنوان مثال می‌توان به مصادیقی از جمله از دست دادن شغل، در معرض تعقیب قضایی قرار گرفتن، فرار گرفتن در وضعیت نامناسب سلامتی یا از دست دادن منابع مالی فراوان اشاره نمود.
۴	خیلی زیاد	در این سطح، افراد با پیامدهای مهم و یا حتی غیر قابل برگشتی مانند ناتوانی در کار، ایجاد بیماری‌های جسمی و روانی حاد و یا حتی مرگ مواجه می‌شوند.

برای تکمیل جدول فوق، کنترل‌کنندگان عموماً از سه شاخصه مهم دیگر که نشان دهنده سطح محرمانگی^۱، تمامیت^۲ و دردسترس بودن^۳ اطلاعات برای موضوع داده می‌باشد استفاده می‌کنند. این سه شاخصه در قالب جدولی طراحی می‌شود که با تکمیل شدن آن توسط موضوع داده، سه شاخصه بیان شده به دست آمده و بالاترین سطح ارائه شده به عنوان نتیجه نهایی ارزیابی قلمداد می‌شود.

ردیف	شاخصه	توضیحات	درجه (کم-متوسط-زیاد-خیلی زیاد)
۱	محرمانگی	افشای غیر مجاز داده‌های شخصی چه تأثیری بر روابط تجاری، زندگی فردی و اجتماعی شما می‌دهد. افشای غیر مجاز داده‌های شخصی می‌تواند تحت فرایندهای مختلفی همچون فقدان یا سرقت لپتاپ یا هر وسیله‌ای که اطلاعات در آن ذخیره شده یا ارسال اشتباه اطلاعات به گیرندگان غیر مجاز صورت پذیرد.	
۲	تمامیت	تغییر غیر مجاز داده‌های شخصی چه تأثیری بر روابط تجاری، زندگی فردی و اجتماعی شما می‌گذارد. تغییر غیر مجاز می‌تواند تغییر اطلاعات ذخیره شده در بانک سلامت یک کشور را شامل گردد.	
۳	دردسترس بودن	تخریب غیر مجاز یا از دست دادن دسترسی به داده‌های شخصی چه تأثیری بر روابط تجاری، زندگی شخصی و اجتماعی شما دارد. از دست دادن دسترسی به داده‌های شخصی می‌تواند مصادیقی مانند گم شدن فایل یا پرونده پرسنلی یا پزشکی یک شخص را از سرور سازمان مربوطه شامل شود که بیشتر نسبت به این اطلاعات نسخه پشتیبان تهیه نشده باشد.	

1. Confidentiality
2. Integrity
3. Availability

۳-۳. ارزیابی تهدیدات بالقوه

تهدید به هر شرایط یا رویدادی گفته می‌شود که می‌تواند بر امنیت داده‌های شخصی تأثیر منفی بگذارد. در این مرحله، هدف کنترل‌کننده یا پردازنده داده، درک تهدیدات مربوط به محیط کلی پردازش داده‌های شخصی (خارجی یا داخلی) و ارزیابی احتمال وجود یا عدم وجود تهدیدات بالقوه آن‌ها است. سطوح مختلف و انواع تهدیدات می‌توانند در شاخصه‌هایی همچون محرمانه بودن، تمامیت و در دسترس بودن داده‌های شخصی مورد بررسی قرار گیرند. در این فرایند سه سطح احتمال به شرح ذیل وجود دارد:

- کم: به معنای بعید بودن تحقق تهدید؛

- متوسط: امکان تحقق تهدید وجود دارد؛

- بالا: احتمال تحقق تهدید وجود دارد؛

ارزیابی تهدیدات بالقوه در شبکه‌های تبادل اطلاعات در اجزای این شبکه‌ها که شامل منابع فنی (نرم افزارها و سخت افزارها) می‌باشند، فرایندهای مربوط به پردازش داده‌های شخصی، اشخاص درگیر در عملیات پردازش و مقیاس پردازش به شرح مطالب آتی صورت می‌پذیرد:

ردیف	منابع فنی شبکه	فرایندهای مربوط به پردازش داده‌های شخصی	اشخاص درگیر در عملیات پردازش	مقیاس پردازش
۱	در این زمینه باید مشخص شود که آیا بخشی از پردازش اطلاعات از طریق اینترنت انجام می‌گیرد؟ علت طرح این موضوع از آن جهت است که هنگام خرید و فروش کالا از سایت‌های عرضه و فروش محصولات یا دانلود اطلاعات از پورتال‌های خبری الکترونیکی، تعهدی‌ات احتمالی مهاجمان آنلاین خارجی به ویژه زمانی که سرویس برای کلیه کاربران در دسترس باشد فراهم می‌باشد.	آیا نقش‌ها و مسئولیت‌های مربوط به پردازش داده‌های شخصی مبهم هستند یا به وضوح تعریف شده‌اند؟ به عنوان مثال کاربران بخش مالی تنها امکان وارد نمودن اطلاعات را برخوردار بوده و حق حذف یا اصلاح آنها را که در صلاحیت مدیران است ندارند. علاوه بر آن پرستاران تنها حق دسترسی به پرونده پزشکی بیمار را برخوردار بوده و تجویز موارد دارو و درج آن در پرونده در صلاحیت پزشک است. در صورتی که این وظایف به صورت دقیق و شفاف معین نشوند، دسترسی به داده‌های شخصی ممکن است کنترل نشده بوده و زمینه استفاده غیر مجاز از منابع شبکه و به خطر افتادن امنیت کلی سیستم فراهم گردد.	آیا پردازش داده‌های شخصی توسط تعداد مشخصی از کارمندان انجام می‌شود یا امکان دسترسی و پردازش برای افراد مختلف فراهم است؟ این موضوع از آن جهت دارای اهمیت می‌باشد که هرچه دسترسی به داده‌های شخصی برای تعداد بیشتری از کاربران فراهم شود، امکان نقض امنیت شبکه نیز بیشتر خواهد بود. از این رو دسترسی به شبکه باید الزاماً توسط اشخاصی که با داده‌ها سر و کار دارند انجام گیرد. چالش موجود زمانی اتفاق می‌افتد که به عنوان مثال منشی یک پزشک، با نام کاربری و رمز وی، به اطلاعاتی که سطح دسترسی آن برای یک پزشک فراهم شده، دست می‌یابد، یا در مراجع انتظامی نام کاربری و رمز رئیس کلانتری گاها در اختیار سربازان قرار می‌گیرد که تحت هیچ کدام از تدابیر گزینشی و حفاظتی قرار نگرفته‌اند.	آیا قسمت‌های خصوصی از شبکه مستعد حملات سایبری یا نقض امنیت می‌باشند؟ در صورتی که در گذشته بخش‌های خصوصی از شبکه تحت نقض امنیتی قرار گرفته باشند، باید اقدامات لازم در جهت رفع خلاءهای امنیتی در این قسمت‌ها بیش از پیش و بیش از سایر قسمت‌ها مدنظر قرار گیرد.
۲	آیا امکان دسترسی به یک سیستم پردازش داده‌های شخصی داخلی از طریق اینترنت (به عنوان مثال برای کاربران خاص یا گروه‌هایی از کاربران) وجود دارد؟ به عبارت دیگر آیا امکان دسترسی از راه دور به شبکه برای مدیران یا برخی کارکنان یک سازمان فراهم شده است؟ علت طرح این موضوع این است که در حالی که امکان دسترسی به شبکه خارج از محیط سازمان برای برخی افراد فراهم شده باشد، احتمال سوءاستفاده یا نشت اطلاعات به خارج از سازمان افزایش می‌یابد.	آیا مصادیق استفاده قابل قبول از شبکه، سیستم و منابع فیزیکی در سازمان مشخص شده یا به وضوح تعریف نشده است؟ به عنوان مثال آیا کارکنان یک سازمان حق استفاده از ایمیل سازمانی برای فعالیت شخصی را خواهند داشت. این موضوع از آن جهت دارای اهمیت است که عدم تعیین مشخص مرزهای استفاده از امکانات سازمانی گاه می‌تواند منجر به تعلق برخی اقدامات شخصی کاربران به عنوان تهدیدات امنیتی از سوی مراجع حفاظتی شناخته شود.	آیا بخشی یا تمام عملیات پردازش توسط پردازنده (شخص ثالث) انجام می‌گیرد؟ به عنوان مثال ممکن است سیستم فناوری اطلاعات یک مدرسه خصوصی توسط یک مرکز داده خارجی پشتیبانی شود یا اطلاعات ذخیره شده در سیستم یک شرکت وابسته خارجی در درون یک کشور، به شرکت مادر که خارج از آن کشور قرار دارد ارسال شوند. اهمیت این موضوع از آن جهت است که در صورت انجام فرایند پردازش توسط اشخاص ثالث، سازمان ممکن است تا حدی کنترل این داده‌ها را از دست بدهد.	ایجاد حملات سایبری یا نقض امنیت اطلاعات در چه بازه‌های زمانی رخ داده است؟ بررسی بازه‌های زمانی نقض امنیت اطلاعات یا به طور کلی شبکه موجود، به عنوان مثال در زمان تعطیلات آخر هفته یا فصل تابستان می‌تواند معیارهای مناسبی در تشخیص علل نقض امنیت و رفع مشکل به سازمان مربوطه بدهد.

۳	<p>آیا سیستم پردازش داده‌های شخصی شبکه سازمان، به سیستم سازمان دیگر متصل می‌باشد؟ به عنوان مثال سیستم یک کتابفروشی الکترونیکی به سیستم پشتیبانی پرداخت آنلاین متصل باشد یا سیستم مالی یک کلینیک پزشکی به سیستم بیمه برای تأیید وضعیت بیمه بیماران متصل باشد. علت طرح این موضوع آن است که با وجود اتصال میان سامانه‌ها، هرگونه تهدید صورت گرفته برای یکی از سامانه‌ها می‌تواند سامانه متصل به آن را نیز تحت الشعاع قرار دهد.</p>	<p>آیا مرزهای دسترسی به شبکه پردازش اطلاعات تنها محدود به سخت افزارهای سازمانی می‌باشد یا سخت افزارهای شخصی کارکنان دستگاه را نیز دربرمی‌گیرد. به عنوان مثال آیا کارکنان یک اداره حق اتصال لبتاب شخصی خود را به شبکه سازمان برخوردارند؟ این موضوع از دو جهت دارای اهمیت است. جهت اول امکان نشست با افشای اطلاعات درون سامانه‌های یک سازمان بوده و جهت دوم امکان انتقال ویروس و انواع بدافزار و تروجان و... به سامانه‌های داخلی یک شرکت را شامل می‌گردد.</p>	<p>آیا تعهدات افراد درگیر در فرایند پردازش به طور واضح مشخص شده‌است؟ به عنوان مثال آیا دستورالعمل‌هایی مبنی بر مسئولیت و تعهدات اشخاصی که در پردازش درگیر هستند در یک سازمان وجود دارد و علاوه بر آن برای نمونه میان تعهدات اشخاصی که داده‌های شخصی دسته‌های خاص (موضوع ماده ۹ مقررات مصوب ۲۰۱۶) و سایر داده‌های شخصی را پردازش می‌کنند تفاوت در نظر گرفته شده‌است؟</p>	<p>آیا در گذشته، کاربران شبکه گزارشاتی مبنی بر نقض امنیت شبکه ازسوی عوامل مشخص یا نامشخص به سازمان داده‌اند؟ به عنوان مثال گزارشاتی حاکی از ورود به حساب کاربری اشخاص در سایت‌های عرضه و فروش محصولات یا سازمان‌های دولتی به مقامات صلاحیت دار واصل شده‌است؟ آیا در این زمینه بولتن‌های امنیتی جهت نگهداری آرشيو سوابق گزارشات واصله طراحی شده‌اند؟</p>
۴	<p>آیا افراد غیرمجاز می‌توانند به راحتی به محیط پردازش داده‌ها دسترسی داشته باشند؟ به عنوان مثال آیا شرکت یک اتاق کامپیوتر اختصاصی برای مدیریت سیستم فناوری اطلاعات سازمان برای پردازش اطلاعات دارد یا در صورتی که فرایند پردازش و ذخیره سازی اطلاعات در بیرون از سازمان صورت می‌پذیرد، اقدامات امنیتی مناسبی در این زمینه رخ داده است؟ این موضوع از آن جهت دارای اهمیت می‌باشد که علاوه بر نرم افزارها، سخت افزارها و محیط فیزیکی نگهداری آنها نیز دارای اهمیت بوده و دسترسی غیر مجاز به سخت افزارهای شبکه نیز می‌تواند زمینه خرابکاری و سوءاستفاده را فراهم نماید.</p>	<p>آیا کارکنان مجاز به انتقال، ذخیره یا پردازش اطلاعات شخصی در خارج از محوطه سازمان هستند؟ در صورتی که امکان این موضوع فراهم شده باشد می‌توان از دو جنبه به موضوع نگریست، اول اینکه این اقدامات توسط سخت افزارهای شخصی کاربران صورت می‌پذیرد یا از طریق سخت افزارهای اختصاصی که سازمان در اختیار کاربران گذاشته است؟ در صورتی که توسط سخت افزارهای شخصی کارکنان امکان پذیر باشد، طبیعتاً چالش‌های بیان شده در کادر قبلی ازجمله افشا و دسترسی غیر مجاز و ورود بدافزارها به شبکه می‌تواند مطرح شود. علاوه بر آن در صورتی که این اقدام توسط سخت افزارهای اختصاصی داده شده به کارکنان صورت پذیرد، باید محدوده استفاده و اینکه امکان اتصال این سخت افزارها به شبکه‌های دیگر ازجمله اینترنت با استفاده از وای فای وجود خواهد داشت یا خیر</p>	<p>آیا پرسنل درگیر با فرایند پردازش اطلاعات با تعهدات قانونی خود در قبال کل مجموعه آشنایی دارند؟ آیا الزامات امنیتی که در برخورد با اطلاعات در یک سازمان در نظر گرفته شده‌اند، به کارکنان آموزش داده شده یا ابلاغ گردیده‌اند؟ این موضوع از آن جهت دارای اهمیت است که در صورتی که اشخاص از مسئولیت‌های حقوقی خود به طور کامل مطلع باشند، عملاً حساسیت بیشتری در اقدامات خود در نظر گرفته که این موضوع می‌تواند از نقض امنیت داده‌ها و کل شبکه پیشگیری نماید.</p>	<p>گستره عملیات پردازش اطلاعات به چه حجمی از افراد مربوط می‌شود؟ به عنوان مثال آیا پردازش اطلاعات در خصوص وضعیت عملکرد یک بیمار جهت شناسایی یک مشکل در گونه سفیدپوستان یک کشور صورت گرفته یا تنها در جهت درمان آن شخص بخصوص انجام شده‌است؟ این موضوع از آن جهت اهمیت دارد که نوع و حجم داده‌ها و گستره پردازش می‌تواند نمود بخش اهمیت پردازش و مخاطب حملات سایبری قرار گرفتن باشد.</p>

<p>آیا اقدامات حفاظتی متناسب با نوع پردازش صورت گرفته در یک سازمان پیاده سازی شده‌اند؟ به عبارت دیگر در صورتی که پردازش اطلاعات بر روی دسته‌های مختلفی از داده‌ها رخ دهد، متناسب با هر دسته، اقدام حفاظتی بخصوص نیز در نظر گرفته شده‌است یا خیر؟</p>	<p>آیا افراد درگیر در فرایند پردازش اطلاعات، در رعایت الزامات حفاظتی و امنیتی کوتاهی می‌کنند؟ عدم رعایت الزامات حفاظتی، معمولاً به عنوان یکی از علل نقض امنیت شبکه به شمار می‌رود که رعایت آن از سوی کاربران شبکه و پردازندگان می‌تواند از ایجاد نقض در شبکه پیشگیری کند.</p>	<p>درفرایند پردازش اطلاعات شخصی، اقدامات مبتنی بر ثبت و نظارت به چه نحوی انجام خواهد شد؟ به عبارت دیگر زمان‌های ورود و خروج از شبکه و دفعات دسترسی به شبکه و پرونده‌های آن به چه نحوی صورت می‌پذیرد. این موضوع هم می‌تواند از جهت روانی با توجه به ثبت ورود و خروج و میزان دسترسی یک کاربر از نقض امنیت اطلاعات جلوگیری نماید و همچنین در صورت نقض امکان شناسایی عامل نفوذی و برخورد و پیشگیری از موارد نقض بعدی را فراهم نماید.</p>	<p>۵ آیا سیستم پردازش اطلاعات شخصی در یک سازمان با استفاده از پروتکل‌های از پیش تعیین شده کار کرده و نگهداری اطلاعات بر مبنای دستورالعمل‌های از پیش تعیین شده صورت می‌گیرد؟ این موضوع از آن جهت دارای اهمیت است که وجود پروتکل‌های از پیش تعیین شده که مراحل ارزیابی خود را سپری و نقاط ضعف آنها بررسی شده باشد، می‌تواند در زمینه بهبود امنیت پردازش اطلاعات کاربرد داشته باشد.</p>
--	---	--	--

۳-۴. ارزیابی خطر

پس از ارزیابی تأثیر و تهدیدات بالقوه می‌توان به شرح فرمول ذیل از طریق ضرب نتایج حاصل از ارزیابی هریک از دو شاخصه بیان شده، نسبت به ارزیابی خطر در فرایند پردازش اطلاعات اقدام نمود.



۴. رعایت الزامات شکلی

مقررات مصوب سال ۲۰۱۶، در ماده ۴۰ کشورهای عضو را موظف به تنظیم مقررات داخلی در جهت بهبود اجرای مقررات مصوب سال ۲۰۱۶ و رفع خلاءهای این قانون که در هر نظام حقوقی مطابق با هنجارهای حاکم بر آن نظام ممکن است پدید آید، نموده‌است.

۴-۱. تنظیم گری مقررات

بنداول از این ماده کشورهای عضو و مقامات نظارتی را ملزم به تدوین مقررات در جهت اجرای صحیح مقررات مصوب سال ۲۰۱۶ نموده و بند دوم از این ماده ضرورت توجه به مفاهیمی مانند پردازش منصفانه و شفاف اطلاعات، منافع مشروع کنترل‌کنندگان، جمع‌آوری داده‌های شخصی،

مستعارسازی داده‌های شخصی، اطلاعات ارائه شده به عموم مردم، حقوق موضوع داده، نحوه حمایت از کودکان و سازوکار پردازش اطلاعات آنها، اخذ رضایت از موضوع داده، وظایف اطلاع رسانی و سازوکار تبادل اطلاعات کرده است.

نکته قابل توجه در مقررات این ماده این می‌باشد که مفاد بند سوم از این ماده، به جهت اهمیتی که فرایند پردازش داده‌های شخصی دارد، در خصوص آیین نامه‌ها و سایر مقرراتی که بر مبنای بندهای پنجم و نهم از این ماده به تصویب می‌رسند، در خصوص اتخاذ تدابیر امنیتی و الزامات مبتنی بر تبادل فراملی اطلاعات، حتی کنترل‌کنندگان و پردازندگان که مشمول مقررات این قانون نباشند را مشمول مقررات فوق‌الذکر نموده است.

مقررات بند چهارم این ماده نیز نظارت بر حسن اجرای مواد مقررات مصوب سال ۲۰۱۶ را بر عهده مقام ناظری تعیین نموده است که بر مبنای مواد ۳۷-۳۹ و ۵۱-۵۹ این مقررات تعیین و حدود وظایف آن در مواد مرقوم، تعیین شده است. علاوه بر آن این ماده مقرر داشته حدود وظایف و اختیارات مقام ناظر، نافذ اختیارات دیگر مقامات صلاحیت دار حکومتی در نظارت بر حسن اجرای این مقررات نمی‌باشد.

بنظر می‌رسد، تدبیر در مفاد مواد ۳۷-۳۹ و ۵۱-۵۹ مقررات مصوب سال ۲۰۱۶ این موضوع را احاله می‌نماید که وظایف و اختیارات مقام ناظر، همانطور که از نام آن پیداست تنها در بعد پیشگیری از نقض امنیت اطلاعات، انعقاد و اجرای صحیح قراردادها و انجام صحیح وظایف اشخاص درگیر در فرایند پردازش اطلاعات بوده و در صورتی که نقضی صورت گرفته باشد، این مقام تنها وظیفه اعلام موضوع به مراجع قضایی و پیگیری امر ناحیه آن مقامات را برخوردار باشد. از این رو وظیفه پیشگیرانه و نظارتی وی، تداخلی با وظیفه برخورد و مقابله با ناقضان مقررات را نخواهد داشت. بندهای پنجم و ششم این مقررات نیز، تصویب آیین نامه‌ها و دستورالعمل‌های داخلی هر کشور عضو اتحادیه اروپا را منوط به تأیید مفاد مقررات فوق و تطبیق و تأیید عدم مغایرت آنها با مقررات مصوب سال ۲۰۱۶ توسط مقام ناظر نموده است. علاوه بر آن، این مقام در صورتی که موضوعی وجهه بین‌المللی داشته و به عبارتی مقرر مصوب در یک کشور، مربوط به فعالیت‌های پردازشی در چند کشور بوده و نظام حقوقی کشورهای مختلف را درگیر نماید، با ارائه نظریه مشورتی، مراتب را به هیئت مقرر در بندهای هفتم این ماده اطلاع داده و پس از جمع‌آوری نظرات و دیدگاه‌ها و مراتب موجود، هیئت مطابق با مفاد بندهای هشتم این ماده وضعیت حادث را بنظر کمیسیون مقرر در بندهای این ماده اطلاع می‌دهد. کمیسیون نیز پس از بررسی دیدگاه‌ها و مراتب، می‌تواند تصویب نماید که مقررات مصوب داخلی در یکی از کشورهای عضو اتحادیه، دارای اعتبار در سطح کشورهای اتحادیه اروپا باشد.

۴-۲. وظایف و اختیارات مرجع نظارتی

مراجع نظارتی مقرر در مقررات مصوب سال ۲۰۱۶، به دو دسته تقسیم می‌شوند که وظایف و اختیارات آنها ابتدائاً در مواد ۳۷-۳۹ و پس از آن در مواد ۵۱-۵۹ مقرر شده است. مقاماتی که بر مبنای مقررات مواد ۳۷-۳۹ مشخص می‌شوند اصطلاحاً «Data Protection Officer» نامیده شده و مقاماتی که بر مبنای مقررات مواد ۵۱-۵۹ معین می‌شوند اصطلاحاً «Supervisory Authority» نامیده می‌شوند. اگرچه این دو مقام، در واقع دارای وظایف و مسئولیت‌های مشابه در نظارت بر فرایند پردازش اطلاعات یا انعقاد قراردادهای منعقد می‌ان پردازنده و کنترل‌کننده یا کنترل‌کننده و موضوع داده می‌باشند، اما دارای تفاوت‌هایی هستند که در مطالب آتی بدان اشاره خواهد شد.

نکته قابل توجه نقش کلیدی این اشخاص در پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات می‌باشد. به عبارت دیگر با توجه به اینکه وظیفه این اشخاص مراقبت از اجرای مقررات قانونی در انجام پردازش اطلاعات یا رعایت حقوق موضوع داده در فرایند پردازش یا اجرای وظایف کنترل‌کننده و پردازنده می‌باشد، عملاً تدابیر امنیتی در فرایند تبادل اطلاعات در یک شبکه ارتباطی حفظ شده و از نقض امنیت پیشگیری می‌گردد. ضمن اینکه بر فرض نقض امنیتی صورت گرفته باشد، این مقام امکان ارجاع موضوع به مراجع قضایی و انتظامی و پیشگیری از نقض بیشتر یا چند باره امنیت شبکه را برخوردار خواهد بود. از این رو می‌توان نقض این مقام در حفظ امنیت و پیشگیری از نقض امنیت در شبکه‌های تبادل اطلاعات را نقشی کلیدی دانست. اینک به بررسی وظایف و اختیارات این مقامات در فرایند پردازش اطلاعات در شبکه‌های ارتباطی اقدام خواهیم کرد.

۴-۲-۱. وظایف و اختیارات افسر حفاظت از اطلاعات

افسر حفاظت از اطلاعات، مقامی است که بر مبنای مواد ۳۷-۳۹ مقررات مصوب سال ۲۰۱۶ انتخاب شده و وظایف و مسئولیت‌های وی در این مقررات ذکر شده است. با ملاحظه متن ماده ۳۷ مقررات مصوب سال ۲۰۱۶ می‌توان به نتایج ذیل رسید. بر اساس قسمت اول از بند اول این ماده، مقام ناظر معین شده به عنوان افسر حفاظت از اطلاعات، شخصی منصوب از جانب کنترل‌کننده و پردازنده بوده و وظایف وی سوای وظیفه نظارتی مقامات قضایی می‌باشد. با این حال بنظر می‌رسد انتصاب مقام ناظر توسط مقامات قضایی در راستای وظایف نظارت قضایی خود، امری خلاف مقررات قانون نبوده اما مقام منصوب از ناحیه دستگاه قضایی، دارای وظایف و اختیاراتی خواهد بود که توسط مقام نصب‌کننده به وی اعطا شده و وظایف و اختیارات وی ارتباطی با آنچه در مقررات ماده ۳۷ این قانون ذکر شده ندارد.^۱

1. Personal Data Protection Commission, Data Protection Officers, <https://www.pdpc.gov.sg/overview-of-pdpc/data-protection/business-owner/data-protection-officers>, Last Visited 22/07/2023

ثانیاً، انتصاب افسر حفاظت از اطلاعات تنها به اقدامات صورت گرفته توسط پردازنده و کنترل‌کننده در «مقیاس بزرگ» محدود شده و در فعالیتهای پردازندگی در مقیاس کوچک نیازی به انتصاب افسر حفاظت از اطلاعات وجود ندارد. البته این موضوع به معنای ایجاد ممنوعیت در انتصاب وی در فعالیتهای پردازشی کوچک تلقی نمی‌گردد. این موضوع از اهداف تصویب این مقررات قابل برداشت است. چرا که همانطور که ماده ۴۰ مقررات مصوب سال ۲۰۱۶ مورد تصریح قرار داد، هدف اصلی از تصویب این مقررات افزایش ضریب امنیت پردازش اطلاعات و پیشگیری از نقض امنیت فعالیتهای پردازشی خواهد بود. از این رو در صورتی که کنترل‌کننده و پردازنده نسبت به انتصاب چنین مقامی در هر فعالیتی اقدام نمایند، مانعی وجود نخواهد داشت.

نکته قابل توجه امکان انتصاب این افسر از سوی پردازنده و کنترل‌کننده به صورت توامان می‌باشد (Hintze, 2018, 4). اما سؤال موجود این است که چرا با توجه به اینکه پردازنده تحت راهنمایی و دستورات صادره از سوی کنترل‌کننده مبادرت به انجام وظیفه می‌نماید، قانون این شخص را نیز موظف به انتصاب مقام حفاظت از اطلاعات نموده است؟ آیا پردازنده در انتخاب مقام فوق‌الذکر می‌تواند آزادانه اقدام کند یا باید معیارهای بخصوصی را نیز مدنظر قرار دهد؟

برای پاسخ به سؤال اول می‌توان مجدداً به مقررات ماده ۴۰ قانون فوق‌الذکر توجه نمود که در بردارنده اهمیت پردازش اطلاعات و امنیت این پروسه می‌باشد. از این رو در صورتی که کنترل‌کننده که وظیفه شروع و ارائه نظارت بر عملکرد پردازنده را بر عهده دارد، به وظیفه خود در قبال تعیین مقام حفاظت از داده‌ها عمل نکند، پردازنده باید نسبت به این مهم اقدام نماید. از آنجا که به طور کلی پردازنده در طول تصمیمات و دستورات صادره از سوی کنترل‌کننده اقدام می‌کند، در زمینه انتصاب مأمور حفاظت از داده‌ها نیز باید، وظیفه پردازنده را در طول وظیفه کنترل‌کننده حساب نمود. از این رو پردازنده در صورتی می‌تواند نسبت به انتصاب مأمور حفاظت از داده‌ها اقدام نماید، که چنین امری از سوی کنترل‌کننده صورت نگرفته باشد.

بعلاوه، وی در انتخاب مأمور حفاظت از داده‌ها تنها مقررات ماده ۳۷ و شرایط مقرر در مواد ۳۸-۳۹ را در نظر خواهد گرفت. با این حال چون این شخص تحت تدابیر و دستورات کنترل‌کننده اقدام می‌کند، اگر کنترل‌کننده شرایط دیگری نیز برای پردازنده معین نموده باشد، در انتخاب مقام حفاظت از داده‌ها به این شرایط نیز باید توجه نماید. البته شرایط تعیین شده از سوی کنترل‌کننده نباید مغایر با مقررات مواد ۳۷-۳۹ قانون فوق‌الذکر باشد.

نکته دیگر این است که برای تشخیص بزرگ و کوچک بودن فرایند پردازش، معیاری در مقررات مصوب سال ۲۰۱۶ معین نشده است و بر این مبنا می‌توان نتیجه‌گیری نمود که این موضوع امری نسبی بوده و بنظر نگارنده توجه به اثرات پردازش می‌تواند نشان‌دهنده مقیاس آن باشد. از این

رو در صورتی که اثرات پردازش، قشر کثیری از جامعه را تحت الشعاع قرار دهد، این امر می‌تواند پردازش در مقیاس بزرگ و در صورتی که محدود به شخص یا اشخاصی از یک گروه کوچک باشد، پردازش در مقیاس کوچک تلقی می‌گردد. بر این مبنا برخلاف نظر برخی که جمع‌آوری داده‌های کاربران توسط یک سایت فروش و عرضه محصولات برای ارائه پیشنهادات مبتنی بر سلاقی هر مراجعه‌کننده (لطیف زاده و دیگران، پیشین، ۱۴۰۲، ۲۵۳) یا پردازش داده‌های شخصی توسط شرکت‌های تبلیغاتی برای ارسال تبلیغات به مشتریان (همانجا) را پردازش در مقیاس بزرگ محسوب نموده‌اند، این نوع اقدامات به منزله فعالیت‌های پردازشی در مقیاس بزرگ محسوب نمی‌شوند. برعکس در صورتی که داده‌های حاصل از بررسی DNA قومیت خاصی از اقشار یک جامعه مانند سیاهپوستان، برای بررسی مقاومت بدن آنها در برابر بیماری بخصوصی مورد پردازش قرار گرفته و در قیاس این پردازش با داده‌های جمع‌آوری شده از سفیدپوستان، داروی خاصی تولید گردد، می‌توان این اقدامات را به عنوان فعالیت‌های پردازشی در مقیاس بزرگ محسوب نمود. در کنار معیار بیان‌شده، بنظر برخی دیگر می‌توان از طریق معیارهای دیگری نیز مقیاس بزرگ فعالیت‌های پردازشی را شناسایی نمود. معیارهای موجود به قرار ذیل هستند:^۱

- تعداد موضوع داده درگیر در فرایند چه به عنوان گروهی خاص یا نسبتی از یک جمعیت
- حجم داده‌های مورد پردازش
- مدت پردازش
- گستره جغرافیایی پردازش

در بررسی معیارهای فوق سوالی که به ذهن می‌رسد این است که تعداد اشخاص موضوع داده یا حجم داده‌های مورد پردازش یا مدت پردازش، برای یک عملیات پردازش ملاک می‌باشند یا در صورتی که تعدادی عملیات پردازش مرتبط با هم انجام گرفته باشند، همه آنها را شامل می‌شوند؟ به عنوان مثال در سایت‌های عرضه و فروش محصولات، اگرچه در خصوص هر کاربری که وارد سایت می‌شود، یک عملیات پردازش با بررسی تعداد محدودی از داده‌ها در مدت زمان چند دقیقه حضور وی در سایت صورت می‌پذیرد، اما در طول روز این اقدامات برای تعداد بسیار زیادی از اشخاص با داده‌های انبوه و مدت زمانی طولانی انجام می‌شود. اگر ملاک همان عملیات پردازش بر روی یک نفر باشد، طبیعتاً نمی‌توان این اقدامات را دارای گستره وسیع محسوب نمود اما در صورتی که مجموع اقدامات پردازشی در کل شبکه ملاک عمل باشد، تشخیص مقیاس بزرگ برای این موضوع دور از ذهن نخواهد بود. بنظر می‌رسد همانطور که در معیار مدنظر نگارنده نیز بیان

1. GDPR.eu, Everything you need to know about the GPDR Data Protection Officer (DPO), <https://gdpr.eu/data-protection-officer/>, Last Visited 28/02/2023

گردید، در این خصوص ملاک تشخیص، اقدامات صورت گرفته بر روی هر موضوع داده خواهد بود مگر اینکه ماهیت اقدامات، تعداد بیشتری از اشخاص موضوع داده را در برگیرد. ثالثاً مقررات بندهای دوم و سوم ماده ۳۷ امکان انتخاب یک افسر حفاظت از اطلاعات را برای چند کنترل کننده و پردازنده صرف نظر از اینکه این اشخاص جزو اشخاص حقوقی عمومی باشد یا خیر معین نموده است. اما شرط لازم برای این موضوع، در دسترس بودن افسر حفاظت از اطلاعات برای کلیه پردازندگان و کنترل کنندگانی می باشد که نسبت به انتصاب وی اقدام کرده اند. مضاف بر آنچه بیان شده به حکم بنا ششم از این ماده، انتخاب افسر فوق الذکر لزوماً از میان اشخاص خارج از کارکنان پردازنده یا کنترل کننده فراهم نبوده و اگرچه این مقامات می توانند با کنترل کنندگان و پردازندگان با اخذ قرارداد، شروع به همکاری نمایند، اما انتخاب آنها از میان کارکنان پردازندگان و کنترل کنندگان فاقد ایراد قانونی خواهد بود.

نکته قابل توجه دیگر این است که این مقام تنها به بالاترین مقام منصوب کننده وی پاسخگو بوده و گزارشات خود را باید به آن شخص اعطا نماید. (بند سوم ماده ۳۸) از این رو سایر اشخاص نه حق و نه اختیار اخذ گزارش از مقام حفاظت از داده ها در یک فرایند پردازشی را خواهند داشت. در مقابل این افسر برای انجام وظایف خود حق هرگونه جستجو در اقدامات صورت گرفته در فرایند پردازش را برخوردار خواهد بود.^۱ سوالی که در این زمینه می توان بیان داشت این است که آیا مقام مذکور تنها باید یک شخص حقیقی بوده یا اشخاص حقوقی نیز می توانند به این مقام منصوب شوند؟ تدبر در مقررات مواد ۳۸ و ۳۹ نشان می دهد که شرایط تعیین شده در قانون برای انتصاب وی، شرایط حاکم خاصه اشخاص حقیقی نبوده و اشخاص حقوقی نیز به شرط برخورداری از الزامات مندرج در مواد ۳۸-۳۹ امکان انتخاب به مقام فوق الذکر را خواهند داشت.^۲ رابعاً مقررات بند پنجم ماده ۳۷، وجود شرایط دانش و تخصص در افسر حفاظت از اطلاعات را جزو شرایط اساسی انتخاب وی جهت انجام وظایف ماده ۳۹ محسوب نموده است. مواد ۳۹ مقررات مصوب سال ۲۰۱۶ ماده مقرر می دارد:

۱. افسر حفاظت از داده ها باید حداقل وظایف زیر را داشته باشد:

- اطلاع رسانی و توصیه به کنترل کننده یا پردازنده و کارکنانی که تعهدات خود را طبق این مقررات و سایر مقررات حفاظت از داده های اتحادیه یا کشورهای عضو انجام می دهند

1. National Privacy Commission, APPOINTING A DATA PROTECTION OFFICER, <https://privacy.gov.ph/appointing-a-data-protection-officer/>, Last Visited 04/05/2023

2. GDPR, What is a GDPR Data Protection Officer and who needs to appoint one?, <https://www.gdpreu.org/the-regulation/key-concepts/data-protection-officer/>, Last Visited 04/08/2023

- نظارت بر انطباق با این مقررات، سایر مقررات حفاظت از داده‌های اتحادیه یا کشورهای عضو و سیاست‌های کنترل‌کننده یا پردازنده در رابطه با حفاظت از داده‌های شخصی، از جمله واگذاری مسئولیت‌ها، افزایش آگاهی و آموزش کارکنان درگیر در عملیات پردازش، و ممیزی‌های مرتبط

- ارائه مشاوره در صورت درخواست در مورد ارزیابی تأثیر حفاظت از داده‌ها و نظارت بر عملکرد آن طبق ماده ۳۵

- همکاری با مقام ناظر

- به عنوان نقطه تماس مقام ناظر در مورد مسائل مربوط به پردازش، از جمله مشاوره قبلی که در ماده ۳۶ اشاره شده است، عمل کند و در صورت لزوم در مورد هر موضوع دیگری مشورت کند

۲. افسر حفاظت از داده‌ها باید در اجرای وظایف خود با در نظر گرفتن ماهیت، دامنه، زمینه و اهداف پردازش، خطرات مربوط به عملیات پردازش را در نظر بگیرد.

با بررسی مفاد بند پنجم ماده ۳۷ و مقررات ماده ۳۸ می‌توان به این نتیجه رسید که ذکر عنوان ماده ۳۹ در بند پنجم ماده ۳۷، ناشی از مسامحه قانون‌گذار اتحادیه اروپا و تاکید آن مقام بر مطلق وظایف افسر حفاظت از اطلاعات می‌باشد. از این رو می‌توان بیان داشت که وظایف مقرر در ماده ۳۹، تنها وظایف افسر حفاظت از اطلاعات نبوده و وجود دانش و تخصص به عنوان شرط انتخاب وی در ماده ۳۷، علاوه بر ماده ۳۹، ناظر بر وظایف مندرج در ماده ۳۸ نیز خواهد بود. در این زمینه بندهای پنجم این ماده افسر حفاظت از اطلاعات را ملزم به محرمانگی فرایند پردازش و حفظ رازداری و بند ششم نیز عدم انجام اقداماتی که با منافع کنترل‌کننده و پردازنده در تعارض باشد، نموده است. نکته قابل توجه این است که وظایف مندرج در مواد ۳۸ و ۳۹ مقررات مصوب سال ۲۰۱۶، وظایف انحصاری مقام منصوب شده نبوده و کنترل‌کننده یا پردازنده که نسبت به انتصاب این مقام اقدام می‌کنند، از امکان تعیین وظایف بیشتر برای وی نیز برخوردار و این مقام ملزم به رعایت آنها خواهد بود. البته این اقدامات نیز تا جایی جریان دارد که با مقررات مواد ۳۸ و ۳۹ تعارضی نداشته باشند.

در خصوص تعارض منافع مندرج در بند ششم ماده ۳۸ نیز می‌توان بیان داشت که این واژه دارای معنایی بسیط بوده و می‌توان دو نوع تفسیر از آن ارائه نمود. تفسیر اول که از دیدگاه نگارنده ناشی می‌شود بر این مبنا استوار است که تعارض منافع میان کنترل‌کننده و پردازنده و اقدامات انجام شده از سوی مقام منصوب نباید وجود داشته باشد. به عنوان مثال در صورتی که شخصی به عنوان افسر حفاظت از اطلاعات توسط پردازنده یا کنترل‌کننده‌ای منصوب شود، در صورتی قابلیت انعقاد قرارداد با کنترل‌کننده دیگر جهت نظارت بر فرایند پردازش در محلی دیگر را خواهد داشت

که منافع مقام منصوب کننده اول وی تحت الشعاع قرار نگیرد. علاوه بر آن الزامات دیگر از جمله دسترسی که در ماده ۳۷ این قانون برای شخص مذکور معین شده نیز رعایت شود. اما تفسیر دوم که از دیدگاه برخی دیگر ناشی می‌شود از عدم تعارض میان وظایف افسر حفاظت از اطلاعات با مقررات قانونی حکایت دارد. به عنوان مثال ماده ۳۰ مقررات مصوب سال ۲۰۱۶ کنترل کننده و پردازنده را موظف به حفظ سوابق پردازشی نموده است. در صورتی که این اشخاص، وظیفه بیان شده را جزو وظایف افسر حفاظت از اطلاعات قرار دهند، این موضوع با وظایف ذاتی آن شخص در تعارض نبوده و بنابراین امکان انجام آن توسط فرد بیان شده نیز موجود است. اما در صورتی که وظیفه تعیین اهداف پردازش جزو وظایف وی تعریف شود، با توجه به اینکه وی مسئول نظارت بر اجرای مقررات مصوب سال ۲۰۱۶ بوده و تعیین اهداف پردازش، با وظایف نظارتی او در تعارض می‌باشد، نمی‌توان چنین وظیفه‌ای را برای او در نظر گرفت (لطیف زاده و دیگران، پیشین، ۱۴۰۲، ۲۶۲).

۴-۲-۲. وظایف و اختیارات مقام صلاحیت دار نظارتی

مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا، علاوه بر اختصاص موادی بر تعیین افسر حفاظت از اطلاعات، در مواد ۵۱-۵۹ موادی را به تعیین مقامات نظارتی دولتی نیز بر فرایند پردازش اطلاعات و حدود اختیارات آنها اختصاص داده است. وجود این مقامات در کنار افسر حفاظت از اطلاعات می‌تواند یکی از سازوکارهای مهم نظارت و پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات به دلایل بیان شده در مطالب پیشین در باب افسر حفاظت از اطلاعات تلقی گردد.

ماده ۵۱ از مقررات مصوب سال ۲۰۱۶ مقرر می‌دارد که هر یک از کشورهای عضو اتحادیه اروپا باید یک یا چند مقام دولتی مستقل را برای نظارت بر فرایند پردازش اطلاعات، صیانت از حقوق موضوع داده و تبادل آزاد اطلاعات در کشور خود منصوب نمایند. این مقامات باید با یکدیگر و مقامات سایر کشورهای عضو در ارتباط بوده و همکاری‌های لازم را با کمیسیون مقرر در ماده ۴۰ مقررات مصوب سال ۲۰۱۶ نیز داشته باشند. علاوه بر آن در صورت انتخاب مقامات متعدد نظارتی، هر کشور باید یکی از این مقامات را به عنوان ارشد انتخاب نماید تا نحوه و چگونگی نظارت بر فرایند پردازش اطلاعات در محدوده سرزمینی آن کشور تحت نظارت و تصمیم‌گیری آن مقام صورت پذیرد.

مقامات نظارتی تعیین شده به حکم ماده ۵۲ در انجام وظایف خود مستقل بوده و حق انجام اقدامات مغایر یا انتخاب شغل مغایر با وظایف نظارتی خود را نخواهند داشت. علاوه بر آن کشورهای عضو اتحادیه اروپا موظف می‌باشند کلیه امکانات فنی و مالی و زیرساختی لازم را جهت

انجام وظیفه در اختیار این مقامات قرار داده و بندششم ماده فوق‌الذکر حتی امکان تعیین بخشی از بودجه عمومی کشور را به عنوان بودجه سالانه در این زمینه پیش بینی نموده است. هر یک از مقامات نظارتی باید بر مبنای خط مشی که مجلس یا دولت یا سازمان منصوب کننده برای آنها تعیین می‌کند، (بنداول ماده ۵۳) نسبت به انجام وظایف خود اقدام نماید. انتخاب هر عضو باید بر مبنای معیارهای مشخصی از جمله تجربه، مهارت، دانش و... بوده (بنددوم ماده ۵۳) و در صورت انقضای مدت مسئولیت، استعفا، یا بازنشستگی اجباری (بندسوم ماده ۵۳) یا سوءرفتار جدی (بندچهارم ماده ۵۳)، به پایان می‌رسد.

سوالی که در بدایت امر بنظر می‌رسد این است که معیار تعیین سوءرفتار جدی برای برکناری مقامات نظارتی مقرر در ماده ۵۱ مقررات مصوب سال ۲۰۱۶ چه می‌باشد؟ در این زمینه اظهار نظر شده است که سوءرفتار به «رفتاری اطلاق می‌گردد که مشتمل بر نقض تعهدات قانونی یا قراردادی تحمیل شده بر شخص» باشد. از این رو در صورتی که رفتاری دارای آثار مخرب بیش از حد متوسط مورد انتظار باشد، می‌تواند به عنوان سوءرفتار جدی تلقی گردد.^۱ از جمله این مصادیق می‌توان به انتقال عمدی اطلاعات، بی توجهی به استانداردهای تعیین شده، عدم ارائه گزارش جامع و مانع به مقام مسئول در موارد مقتضی، عملکرد مداوم ضعیف و اشتباهاتی که باعث ضررهای مالی یا معنوی از جمله آسیب رساندن به شهرت گردد، اشاره نمود.^۲

هر یک از مقامات نظارتی تعیین شده در کشور حوزه فعالیت خود، صلاحیت رسیدگی داشته و امکان فعالیت در کشور دیگری را نخواهند داشت. (بنداول ماده ۵۵) علاوه بر آن، این مقامات نیز همانند افسر حفاظت از اطلاعات، امکان دخالت در نظارت مراجع قضایی و اعمال حاکمیت و اختیارات آن مقامات را ندارند (بندسوم ماده ۵۵).

اما آنچه در این زمینه باید مدنظر قرار گیرد، اعمال صلاحیت مقامات نظارتی در فرایند تبادل فراملی اطلاعات خواهد بود که با توجه به وجود عنصر خارجی به نحو باید صورت پذیرد؟ به عنوان مثال در صورتی که پردازنده دارای تابعیت کشوری غیر از کشوری که مبادرت به نصب مقام نظارتی نموده باشد، نحوه نظارت بر اقدامات پردازنده توسط مقام مزبور به چه نحوی خواهد بود؟ برای پاسخ به این سؤال باید به ماده ۶۰ مقررات مصوب سال ۲۰۱۶ توجه نمود.

بندهای اول ماده مذکور، مقامات نظارتی که کشورها را ملزم به همکاری با یکدیگر نموده و در صورتی که اقدامی نظارتی باید در کشوری غیر از کشور مقام نظارتی اول موجود باشد، این

1. Care Quality Commission, Serious misconduct or mismanagement, <https://www.cqc.org.uk/guidance-providers/regulations-enforcement/serious-misconduct-or-mismanagement>, Last Visited 24/08/2023
2. LegalVision, Employee Ordinary Misconduct vs Serious and Gross Misconduct in the UK, <https://legalvision.co.uk/employment/ordinary-gross-misconduct/>, Last Visited 05/06/2023

مقام به قید فوریت مراتب را باید به مقام نظارتی که هدف اطلاع داده (بندسوم ماده ۶۰) و با ارائه خط مش و نحوه عملکرد، مقام نظارتی کشور هدف نیز باید نسبت به انجام وظایف اقدام نماید. آنچه در بررسی مقررات ماده ۶۰ بنظر می‌رسد این است که در مواردی که انجام فرایند نظارت در کشوری غیر از کشور حوزه صلاحیت مقام نظارتی انجام گرفته و این مقام نسبت به ارائه سازوکارهای نظارتی به مقام نظارتی کشور هدف اقدام کند، مقام نظارتی مذکور باید طبق دستورالعمل‌های واصله نسبت به انجام نظارت و همکاری اقدام نموده و این موضوع استثنایی بر وظایف و خط مش تعیین شده برای وی توسط مجاس یا دولت منصوب کننده او خواهد بود. بنظر می‌رسد عدم اطلاع به موقع اقدامات از سوی مقام ناظر اول به مقام ناظر کشور هدف، بر مبنای ماده ۵۳ مقررات مصوب سال ۲۰۱۶، به منزله سوء رفتار جدی تلقی شده و حتی امکان برکناری وی را نیز فراهم آورد.

نکته آخر در این زمینه وظایف و اختیارات مقام نظارتی می‌باشد که در مواد ۵۷ و ۵۸ مقررات مصوب سال ۲۰۱۶ پیش بینی شده است. به طور کلی می‌توان وظایف مقام نظارتی مندرج در ماده ۵۷ را در سه دسته نظارتی، آموزشی و تقنینی تقسیم نمود. بر مبنای ماده مقام مذکور از وظیفه نظارت بر نحوه پردازش اطلاعات، آموزش، افزایش آگاهی عمومی و ارائه مشاوره به موضوع داده و کنترل کنندگان شبکه‌های تبادل اطلاعات و پردازندگان اطلاعات و همچنین تصویب و ابلاغ دستورالعمل‌های مختلف در زمینه چگونگی عملکرد نهادهای فعال در حوزه پردازش اطلاعات و صدور گواهینامه‌ها و مجوزهای لازم برخوردار خواهد بود. این مقام بر مبنای مفاد ماده ۵۸ از این مقررات، حق هرگونه ارسسی و درخواست اطلاعات از کلیه اشخاص درگیر در فرایند پردازش اطلاعات را داشته و اشخاص مذکور الزاماً باید با این مقامات همکاری‌های لازم را داشته باشند. از جمله اختیارات ذکر شده در ماده ۵۸ می‌توان به درخواست ارائه اطلاعات در ارتباط با اختیارات پردازنده و کنترل کننده، محل استقرار پردازنده و کنترل کننده و همچنین ابزارها و تجهیزات آنها، تأیید یا اصلاح گواهینامه‌های صادر شده در باب تبادل فراملی اطلاعات و...، صدور دستور مبنی بر شروع یا توقف فرایند پردازش در زمان مشخص، اعمال محدودیت در انجام پردازش اشاره نمود.

نتیجه گیری

پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات نیازمند سازوکارهایی است که برخی از آنها در ماده ۳۲ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا با عنوان مستعارسازی و رمزگذاری داده‌های شخصی، اطمینان از محرمانه بودن، یکپارچگی، در دسترس بودن و انعطاف پذیری سیستم‌ها

و خدمات پردازشی، خطرات (ریسک) مرتبط با پردازش اطلاعات و رعایت الزامات شکلی پیش بینی شده است. هریک از سازوکارهای بیان شده در فوق به صورت مفصل در متن این پژوهش مورد بررسی قرار گرفته‌اند. این سازوکارها در عین کارایی و ضرورت بکارگیری در نظام حقوقی ایران نیازمند برخی زیرساخت‌ها می‌باشند که بیان برخی توصیه‌های سیاستگذارانه به شرح ذیل در این خصوص ایجاب می‌گردد:

۱- اصلاح قوانین و مقررات مصوب در کشور ایران: متأسفانه در بررسی قوانین و مقررات موجود در حقوق ایران ملاحظه می‌شود که قوانین و مقررات بخصوصی در جهت پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات در این کشور وجود نداشته و تنها دو ماده ۵۸ و ۵۹ قانون تجارت الکترونیکی به سازوکار پردازش داده‌پیام‌های شخصی پرداخته‌اند. این در حالی است که نظام حقوقی اتحادیه اروپا با تصویب مقررات مصوب سال ۲۰۱۶ خود، قواعد مفصلی در این زمینه به پیش بینی نموده که می‌تواند به عنوان مبنایی جهت اصلاح قوانین مصوب در ایران تلقی گردد.

۲- آگاهی بخشی به مردم: در کنار اصلاح قوانین موجود، آگاهی بخشی به مردم از طریق وسائل ارتباط جمعی مانند تلویزیون یا رادیو و اطلاع رسانی در خصوص حقوق قانونی خود و سازوکار پیشگیری از نقض اطلاعات شخصی یا شبکه‌های تبادل اطلاعاتی که در آن فعالیت دارند، باید در دستور کار دولت قرار گیرد.

۳- نظام‌مند نمودن اعطای مجوز به فعالیت شرکت‌های فراملی: متأسفانه رویه‌ای که در کشور ایران حاکم می‌باشد این است که متأسفانه رویکردهای شدیددی در فیلترینگ شبکه‌های ارتباطی و قطع دسترسی کاربران به این نوع شبکه‌ها در میان نهادهای دولتی حاکم است. در حالی که این موضوع می‌تواند با سازوکار اعطای مجوز فعالیت و تأسیس نمایندگی این شرکت‌ها در ایران و همچنین نظارت بهتر بر سازوکار تبادل اطلاعات به نحو مطلوبی حل و فصل شود. چرا که در عصر حاضر، فیلترینگ شبکه‌های تبادل اطلاعات تنها منجر به استفاده کاربران از پروکسی یا انواع فیلتر شکن و بی اثر نمودن آثار اقدامات صورت گرفته شود.

نکته پایانی که لازم است بدان اشاره گردد این است که آنچه در این پژوهش مورد تحلیل و بررسی قرار گرفت، تبیین راهکارهایی در جهت پیشگیری از نقض امنیت شبکه‌های تبادل اطلاعات و همچنین اجزای آنها بوده است. اما سوال اینجاست که آیا در صورت نقض امنیت شبکه، راهکارهایی در جهت حل غیرقضایی اختلافات و اعمال ضمانت اجراهای صحیح و قانونی می‌تواند مورد پیش بینی و در دستور کار قرار گیرد؟ این امر، موضوعی است که می‌تواند محل انجام پژوهش‌های متعاقب از سوی سایر پژوهشگران قرار گرفته و با توجه به راهکارهای

ارائه شده در نظام حقوقی اتحادیه اروپا خصوصا مفاد مواد ۷۷-۸۴ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا، گام‌های اولیه در راستای انجام هرچه بهتر سیاست‌گذاری‌های تقنینی و بهره‌مندی از تجربیات نظامات حقوقی کشورهای توسعه یافته جهت رفع خلاءهای تقنینی موجود در نظام حقوقی ایران برداشته شود.

منابع

الف) منابع فارسی

۱. لطیف زاده، مهدیه، قبولی درافشان، سیدمحمد مهدی، محسنی، سعید، عابدی، محمد، (۱۴۰۲)، تعهدات پردازش کننده داده شخصی در اتحادیه اروپا و امکان سنجی پذیرش آن در حقوق ایران، فصلنامه آموزه‌های فقه مدنی، دوره ۱۶، شماره ۲۷، صص ۲۴۵-۲۸۶
۲. لطیف زاده، مهدیه، (۱۴۰۱)، رفع تقابل بین حق آزادی بیان و اطلاعات با حق بر داده‌های شخصی در رسانه‌ها از منظر حقوق اتحادیه اروپا و نظام حقوقی ایران، فصلنامه پژوهش‌های ارتباطی، دوره ۲۹، شماره ۱۱۱، صص ۱۵۳-۱۷۳.

ب) منابع خارجی

3. Aepd, (Last visited 13/07/2023), Risk Management and Impact Assessment in the Processing of Personal Data, Online Edition: <https://www.aepd.es/es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf>, pp 1-160
4. Ales Teska , (Last visited 13/07/2023), Pseudonymization, Anonymization, Encryption ... what is the difference?, <https://teskalabs.com/blog/data-privacy-pseudonymization-anonymization-encryption>,
5. Care Quality Commission, (Last Visited 24/08/2023), Serious misconduct or mismanagement, <https://www.cqc.org.uk/guidance-providers/regulations-enforcement/serious-misconduct-or-mismanagement>,
6. Data2.EU, (Last Visited 19/08/2023), Technical and organisational measures, <https://data2.eu/en/gdpr/what-technical-and-organisational-measures-do-we-need-to-take>
7. Data Protection Commission, (Last Visited 18/07/2023), Risk based approach, <https://www.dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach>
8. Enisa, (Last Visited 16/08/2023), Handbook on Security of Personal Data Processing, European Union Agency For Network and Information Security, online edition www.enisa.europa.eu
9. GDPR.eu, (Last Visited 28/02/2023), Everything you need to know about the GPDR Data Protection Officer (DPO), <https://gdpr.eu/data-protection-officer/>.
10. GDPR, (Last Visited 04/08/2023), What is a GDPR Data Protection Officer and who needs to appoint one?, <https://www.gdpreu.org/the-regulation/key-concepts/data-protection-officer/>.
11. Hintze, Mike, (2018), "Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR", Journal of Internet Law (Wolters Kluwer), <https://ssrn.com/=3192721>
12. Intersoft Consulting, (Last visited 04/07/2023), General Data Protection Regulation (GDPR), <https://gdpr-info.eu/art-40-gdpr/>
13. Joshua Gresham , (Last Visited 27/07/2023), Is encrypted data personal data under the GDPR?, <https://iapp.org/news/a/is-encrypted-data-personal-data-under-the-gdpr/>
14. LegalVision, (Last Visited 05/06/2023), Employee Ordinary Misconduct vs Serious and Gross Misconduct in the UK, <https://legalvision.co.uk/employment/ordinary-gross-misconduct/>

15. Marie Prokopets, (Last Visited 15/05/2023), The Ultimate Manual To GDPR Article 32, <https://nira.com/gdpr-article-32/>
16. National Privacy Commission, (Last Visited 04/05/2023), APPOINTING A DATA PROTECTION OFFICER, <https://privacy.gov.ph/appointing-a-data-protection-officer/>
17. Office of the Data Protection Ombudsman, (Last Visited 02/04/2023), Risk assessment and data protection planning, <https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning>,
18. Personal Data Protection Commission, (Last Visited 22/07/2023), Data Protection Officers, <https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers>,
19. Roy Winkelman, (Last visited 18/07/2023), Director, What is a Network?, Florida Center for Instructional Technology College of Education, University of South Florida, <https://fcit.usf.edu/network/chap1/chap1.htm>,
20. Satori, (Last Visited 13/07/2023), Pseudonymisation: 9 Ways to Protect Your PII, <https://satoricyber.com/data-masking/pseudonymisation-9-ways-to-protect-your-pii/>
21. Securiti, (Last Visited 12/03/2023), Article 32 Of The GDPR: Explained, <https://securiti.ai/blog/gdpr-article-32/>
22. The European Union Agency for Cybersecurity, (Last Visited 02/04/2023), Evaluating the level of risk for a personal data processing operation, <https://www.enisa.europa.eu/risk-level-tool/risk>
23. Thomas Zerdick, (Last visited 31/07/2023), Pseudonymous data: processing personal data while mitigating risks, https://edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en.
24. van der Sloot, Bart, (2017) '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, pp 18-34.