Justice Administration of Tehran Province

Jadgment

https://www.Gazavat.org

Online ISSN: 1735-1227

Volum:23 Issue:115

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

Aboutaleb Koosha[1] | Hosein sadeghi[2] | 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

Article type:
Research Article

Received:
2024/02/04
Received in revised form:
2024/08/11
Accepted:
2024/09/08

Keywords:
Security, Information exchange networks, Data, Controller, Data Subject, European Union.

Abstract

Prevention of security violations of information exchange networks is something that has always been the concern of legislators. This issue is important because in today's era, as an electronic era, breaching the security of information exchange networks leads to information leakage and creating grounds for abuse, which misuse of people's personal information can, sometimes even have destructive effects on biological security or cause the personal assassination of the nationals of a country. The legal system of the European Union in this field includes detailed regulations, among which we can refer to the General Data Protection Regulations approved in 2016. These regulations contain detailed rules in the field of maintaining and preventing information security violations. The main question that this research seeks to answer is, what mechanisms does Article 32 of these regulations contain in order to prevent security violations of information exchange networks? In order to answer the above question, the present research, in a documentary way, by presenting the provisions of the above-mentioned article and analyzing its clauses, the mechanisms determined in this article in the four categories of anonymizing and encrypting personal data, ensuring confidentiality, integrity, availability, and flexibility. processing systems and services, risks (risk) related to information processing and compliance with formal requirements, and in the conclusion part, he tried to provide some policy recommendations, including how to amend the laws and regulations approved in Iran's legal system, informing the people through Mass communication media and systematizing the granting of licenses to the activities of transnational companies as the results of the review of Article 32 of the European Union regulations approved in 2016.

How To Site	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. *Journal of Judgment*,23(3), 1-24. DOI: https://doi.com/10.22034/judg.2024.2022304.1279
DOI	http//doi.org/10.22034/judg.2024.2022304.1279
Publisher	University of Tehran Press

فصلنامه قضاوت

https://www.Gazavat.org

آموزش دادگستری استان تهران

شاپا چاپی: ۱۲۲۷-۱۷۳۵

دوره : ۲۳ شماره ۱۱۵

پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات در پرتو ماده ۳۲ مقررات عمومی حفاظت از داده‌های اتحادیه‌اروپا

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

نوع مقاله: علمی- تخصصی

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، اتحادیه‌اروپا.

چکیده

پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات، 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 شبکه های تبادل اطلاعات منجر به نشت اطلاعات و ایجاد زمینه سوءاستفاده می گردد که سوء استفاده از اطلاعات شخصی افراد می تواند، گاه حتی اثرات مخرب بر امنیت زیستی یا ترور شخصیتی اتباع یک کشور را موجب گردد. نظام حقوقی اتحادیه‌اروپا در این زمینه دربردارنده مقررات مفصلی می باشد که از جمله آنها می توان به مقررات عمومی حفاظت از داده ها مصوب سال ۲۰۱۶ اشاره نمود. این مقررات دربردارنده قواعد مفصلی در زمینه حفظ و پیشگیری از نقض امنیت اطلاعات می باشد. سوال اصلی که این پژوهش به دنبال پاسخگویی به آن می باشد 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 بند های آن، سازوکارهای تعیین شده در این ماده را در چهار دسته مستعارسازی و رمزگذاری داده‌های شخصی، اطمینان از محرمانه بودن، یکپارچگی، دردسترس‌بودن و انعطاف پذیری سیستم‌ها و خدمات‌پردازشی، خطرات (ریسک) مرتبط با پردازش اطلاعات و رعایت الزامات شکلی قرار داده و در قسمت نتیجه گیری نیز مبادرت به ارائه برخی توصیه های سیاستگذارانه از جمله نحوه اصلاح قوانین و مقررات مصوب در نظام حقوقی ایران، آگاهی بخشی به مردم از طریق رسانه های ارتباط جمعی و نظام مند نمودن اعطای مجوز به فعالیت شرکت های فراملی به عنوان نتایج حاصل از بررسی ماده ۳۲ مقررات مصوب سال ۲۰۱۶ اتحادیه اروپا نموده‌است.

استناد کوشا، ابوطالب، صادقی، حسین، ناصر، مهدی (۱۴۰۳). پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات در پرتو ماده ۳۲ مقررات عمومی حفاظت از داده‌های اتحادیه‌اروپا . نشریهٔ قضاوت، ۲۳(۳)، ۱-۲۴.
DOI: https://doi.com/10.22034/judg.2024.2022304.1279

DOI https://doi.com/10.22034/judg.2024.2022304.1279

ناشر انتشارات دادگستری کل استان تهران

مقدمه

شبکه‌های‌تبادل‌اطلاعات به کامپیوترهای متصل به هم که مبادرت‌به پردازش و به اشتراک گذاری اطلاعات می‌نمایند، اطلاق می‌گردد.[1] یک‌شبکه متشکل از پنج جزء سخت افزار، نرم افزار، کاربران که متشکل از اشخاص موضوع‌داده-کنترل‌کنندگان و پردازندگان هستند، داده‌پیام‌های مورد تبادل و بسترهای ارتباطی می‌باشد. اشخاص موضوع‌داده در شبکه‌های‌تبادل‌اطلاعات، اشخاصی هستند که طی فرایندپردازش، اطلاعات آنها جمع‌آوری، تحلیل و ذخیره می‌گردد. کنترل‌کنندگان شبکه‌ها نیز اشخاصی هستند که مبادرت‌به مدیریت عملکرد و فرایندپردازش‌اطلاعات در یک‌شبکه می‌نمایند. در صورتی که این اشخاص مبادرت‌به اعطای فرایندپردازش به اشخاص ثالث و تعیین خط مش پردازش به آنها کنند، اشخاص ثالث اصطلاحاً پردازندگان داده‌پیام‌ها در شبکه‌های‌تبادل‌اطلاعات تلقی می‌شوند.

آنچه در یک‌شبکه، مورد تبادل قرار می‌گیرد، داده‌پیام می‌باشد. داده‌پیام به تعبیر بنداول ماده ۲ قانون تجارت الکترونیکی، هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسائل 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 نقض‌امنیت‌شبکه در خصوص داده‌پیام‌ها تلقی می‌گردد، مربوط به داده‌پیام‌های شخصی می‌باشد. چرا که این نوع داده‌پیام‌ها می‌باشند که دربردارنده طبقه بندی دسترسی بده و اشخاص عادی امکان دسترسی به آنها را ندارند. در حالی که داده‌پیام‌های غیرشخصی، اطلاعاتی هستند که در اختیار عموم افراد بوده و اساساً نقض‌امنیت داده در خصوص این اطلاعات مطرح نمی‌شود.

آنچه به عنوان معضل اصلی جوامع بشری در عصر حاضر به عنوان عصر الکترونیک مشاهده می گردد، نبود سازوکار های صحیح پیشگیری از نقض امنیت شبکه های تبادل اطلاعات می باشد. به عبارت دیگر شبکه های تبادل اطلاعات به عنوان اصلی ترین مراکز ذخیره، جمع آوری، تحلیل و نگهداری اطلاعات، در معرض هجمه های فراوان خارجی می باشند که عدم اتخاذ تدابیر لازم در جهت حفظ امنیت شبکه ها و اجزای آنها، موضوعی است که هرچند 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 نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات، به معنای پیشگیری از نقض تمامیت اجزای یک‌شبکه می‌باشد. این فرایند نیازمند بکارگیری اقدامات فنی مناسب در جهت تضمین امنیت شبکه می‌باشد. اقدامات فنی به هرگونه اقدامات گفته می‌شود که برای ایجاد سطح مناسبی از حفاظت از اجزای یک‌شبکه خصوصاً اطلاعات به کار گرفته می‌شوند (لطیف زاده و دیگران، ۱۴۰۲، ۲۵۳). اجرای این الزامات در یک‌شبکه بر عهده کلیه اجرای شبکه ازجمله اشخاص موضوع‌داده، کنترل‌کنندگان و پردازندگان بوده و در صورتی که پردازنده‌ای به هر دلیل فرایندپردازش را به پردازنده دیگری محول نموده‌باشد، توسط پردازنده جدید نیز باید مورد توجه قرار گیرد. (همانجا) این الزامات در ماده ۳۲ مقررات عمومی حفاظت از داده‌ها مصوب سال ۲۰۱۶ اتحادیه‌اروپا[2] مورد تصریح قرار گرفته‌اند. ماده ۳۲ مقرر می‌دارد:

---

[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

[2] General Data Protection Regulation

۱- با درنظر گرفتن وضعیت فنی، هزینه‌های اجرا و ماهیت، دامنه، زمینه و اهداف پردازش و همچنین خطر احتمال و شدت متفاوت برای حقوق و آزادی‌های اشخاص حقیقی، کنترل‌کننده و پردازشگر باید اقدامات فنی و سازمانی مناسب را برای اطمینان از سطح امنیتی متناسب با خطر، ازجمله موارد زیر اجرا کند:

- نام مستعار و رمزگذاری داده‌های‌شخصی
- توانایی اطمینان از محرمانه‌بودن، تمامیت، دردسترس‌بودن و انعطاف‌پذیری سیستم‌ها و خدمات‌پردازشی
- امکان بازیابی دردسترس‌بودن و دسترسی به داده‌های‌شخصی 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 امنیت‌پردازش

۲- در ارزیابی سطح مناسب امنیتی باید به ویژه خطراتی که از طریق پردازش به وجود می‌آیند، به ویژه ناشی از تخریب تصادفی یا غیرقانونی، از دست دادن، تغییر، افشای غیرمجاز، یا دسترسی به داده‌های‌شخصی منتقل شده، ذخیره‌شده یا به‌طور دیگری فرآوری شده درنظر گرفته شود

۳- پایبندی به مقررات شکلی مندرج در ماده ۴۰ یا سازوکار صدور گواهینامه تأیید شده مندرج در ماده ۴۲ که می‌تواند به عنوان عنصری برای نشان دادن انطباق با الزامات مندرج در بنداول این ماده استفاده شود

۴- کنترل‌کننده و پردازشگر باید اقداماتی را انجام دهند تا اطمینان حاصل شود که هر شخص حقیقی که تحت اقتدار کنترل‌کننده یا پردازشگر که به داده‌های‌شخصی دسترسی دارد آنها را پردازش نکند مگر به دستور یا درخواست کنترل‌کننده، بر اساس قانون اتحادیه‌اروپا یا هریک از کشورهای‌عضو باشد.

همانطور که ملاحظه می‌گردد، مفاد مقررات ماده ۳۲، الزامات مندرج در پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات را در چهار دسته مستعارسازی و رمزگذاری داده‌های‌شخصی ، اطمینان از محرمانه‌بودن، یکپارچگی، دردسترس‌بودن و انعطاف‌پذیری سیستم‌ها و خدمات‌پردازشی، خطرات (ریسک) مرتبط با پردازش‌اطلاعات و رعایت الزامات شکلی قرار داده که در گفتارهای چهارگانه این پژوهش مورد تحلیل و بررسی قرار خواهند گرفت. پژوهش حاضر در قسمت نتیجه گیری نیز مبادرت‌به ارائه برخی توصیه‌های سیاستگذارانه در جهت بهبود اجرای سازوکارهای بیان‌شده در متن تحقیق می‌نماید.

در بدایت امر یادآور می گردد که اگرچه در میان مقالات منتشر شده در نظام حقوقی ایران، پژوهش هایی پیرامون بررسی جنبه های حقوقی حفاظت از داده پیام های شخصی منتشر گردیده، اما هیچ کدام از پژوهش های منتشر شده، با محوریت پژوهش حاضر همپوشانی مطالب نداشته و این پژوهش در نوع خود یک پژوهش نوین تلقی می گردد.

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 کنترل کنندگان و پردازندگان در پیشگیری از نقض امنیت شبکه‌های

تبادل اطلاعات به تبیین و تشریح وظایف کنترل کنندگان 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 پردازش کننده 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 آمریکا و شاخصه‌های هر یک پرداخته‌اند.

آنچه در بررسی مقالات منتشره در این زمینه ملاحظه می گردد این است که مقالات منتشر شده در این زمینه دارای محوریت حقوق اشخاص و وظایف نهادهای فعال در پردازش اطلاعات شخصی افراد می باشند. این در حالی است که بررسی سازوکارهای حقوقی پیشگیری از نقض امنیت شبکه های 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 شبکه های تبادل اطلاعات این مقاله را به یک مقاله منحصر به فرد تبدیل می نماید.

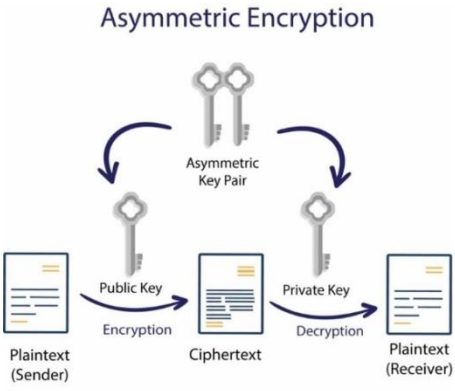
۱- مستعارسازی و رمزگذاری داده‌های‌شخصی

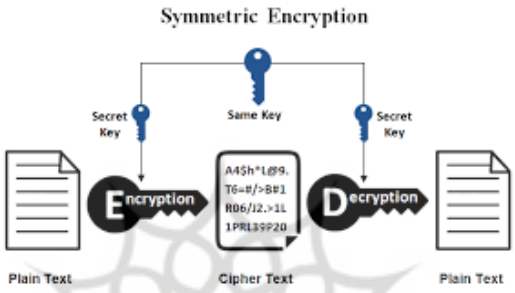
یکی از راهکارهای پیشگیری از نقض‌امنیت داده‌پیام‌ها، ناشناس‌سازی آن‌ها می‌باشد. درفرایند ناشناس‌سازی اطلاعات، سه اصطلاح مهم با عنوان مستعارسازی[۳]، ناشناس‌سازی[۴] و رمزگذاری[۵] وجود دارند. مستعارسازی اطلاعات به روشی برای پنهان کردن داده‌ها گفته می‌شود که در آن انتساب داده‌های‌شخصی به یک شخص خاص بدون وجود اطلاعات اضافی امکان پذیر نمی‌باشد.[۶] در مقابل ناشناس‌سازی به روشی اطلاق می گردد که در آن داده‌های‌شخصی به صورت بازگشت ناپذیر از قابلیت انتساب به یک شخص خاص جدا شده و به داده‌های کاملاً ناشناس تبدیل می‌شوند. رمزگذاری‌اطلاعات 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 می کنند.

فرایند رمزگذاری‌اطلاعات به دو صورت متقارن[۷] و نامتقارن[۸] انجام می گیرد. گاه جهت افزایش امنیت‌اطلاعات، فرایند رمزگذاری به صورت ترکیبی از دو شق فوق انجام می‌شود که به آن رمزگذاری ترکیبی[۹] گفته می‌شود. وجه تمایز رمزنگاری متقارن و نامتقارن در وجود کلید مخفی می‌باشد. به‌عبارت‌دیگر در رمزگذاری متقارن رمزگذاری‌اطلاعات 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

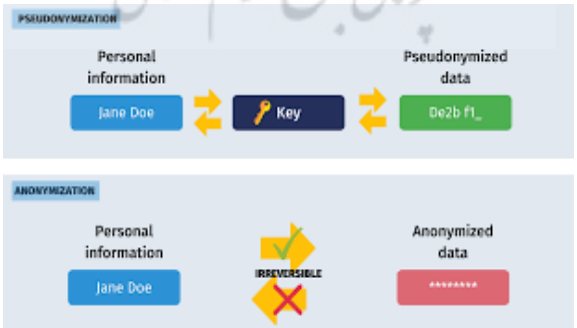
[3] Pseudonymization
[4] anonymization
[5] encryption
[6] Satori, Pseudonymisation: 9 Ways to Protect Your PII, https://satoricyber.com/data-masking/pseudonymisation-9-ways-to-protect-your-pii/, Last Visited 13/07/2023
[7] symmetric encryption
[8] asymmetric encryption
[9] hybrid encryption

دسترسی به کلیدهای مخفی در اختیار طرفین برای وی میسر نمی‌گردد.[10] تصاویر ذیل گویای وجه تمایز دو رمزگذاری می‌باشند:





وجه تمایز سه واژه مستعارسازی، ناشناس‌سازی و رمزگذاری این‌است که درفرایند رمزگذاری، اطلاعات رمزگذاری شده توسط شخص رمزگذارنده و فردی که مخاطب این اطلاعات بوده قابل رمزگشایی و پردازش می‌باشند. اما درفرایند مستعارسازی اطلاعات، تنها شخصی که مبادرت‌به مستعارسازی نموده‌است، از قابلیت ضمیمه اطلاعات دیگر جهت امکان انتساب این داده‌ها به موضوع‌داده برخوردار می‌باشد. به‌عبارت‌دیگر 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، اطلاعات‌شخصی بدون بازگشت به اطلاعات عمومی تبدیل شده و حتی شخصی که مبادرت‌به ناشناس‌سازی داده‌پیام‌ها نموده‌باشد نیز از این قابلیت بی بهره خواهدبود.[11] در شکل زیر می‌توان‌به وجه تمایز مستعارسازی و ناشناس‌سازی اطلاعات به نحو مشخص‌تری پی برد:



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

[11] 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

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 می‌توان‌به این نتیجه رسید که دلیل اینکه قانون گذار اتحادیه‌اروپا از واژه‌های مستعارسازی یا رمزگذاری در ماده ۳۲ مقررات‌مصوب‌سال۲۰۱۶ نام برده این‌است که اطلاعات‌شخصی پس از طی فرایند رمزگذاری و یا مستعارسازی، ماهیت خود را از دست نداده و همچنان داده‌های‌شخصی باقی می‌مانند. اما درفرایند ناشناس‌سازی، داده‌های‌شخصی ماهیت شخصی بودن خود را از دست داده و به داده‌های عمومی(غیرشخصی) تبدیل می‌شوند و در این صورت هیچ کدام از الزمات قانونی مندرج در مقررات فوق الذکر در خصوص این نوع داده‌ها قابلیت اجرا نخواهد داشت.

در نظام‌حقوقی‌اتحادیه‌اروپا بندپنجم ماده ۴ مقررات‌مصوب‌سال۲۰۱۶، حاوی تعریف مستعارسازی اطلاعات می‌باشد. این بند مقرر می‌دارد:

> «مستعارسازی» به معنای پردازش‌داده‌های‌شخصی به گونه‌ای است که دیگر نمی‌توان داده‌های‌شخصی 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 داده‌های‌شخصی به یک شخص حقیقی شناسایی شده یا قابل شناسایی نسبت داده نمی‌شود.

در تعریف مندرج در ماده فوق‌الذکر، چند ویژگی برای مستعارسازی اطلاعات ذکر شده‌است. ویژگی اول همانطور که در مطالب فوق نیز بدان اشاره شد این‌است که عملیاتی بر روی اطلاعات صورت پذیرد که بدون استفاده از اطلاعات اضافی، امکان انتسای این داده‌ها به موضوع‌داده 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 می‌توان‌به داده‌های پزشکی و سلامت اشخاص اشاره‌نمود. 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.[۱۲] این موضوع در اطلاعات‌شخصی مأمورین سازمان‌های اطلاعاتی نمود بیشتری دارد که معمولاً با اسامی مستعار یا کد در دستگاه‌های قضایی به وظایف ضابطیت اقدام می‌نمایند.

۲- توانایی اطمینان از محرمانه‌بودن، یکپارچگی، دردسترس‌بودن و انعطاف‌پذیری سیستم‌ها و خدمات‌پردازشی

برخلاف آنچه در متن ماده ۳۲ قید شده‌است، اطمینان از محرمانگی، یکپارچگی و دردسترس‌بودن و انعطاف‌پذیری سیستم‌ها و خدمات‌پردازشی به منزله اقدامات فنی و سازمانی تلقی نشده بلکه نیازمند به کارگیری زیرساخت‌های فنی می‌باشد تا اطمینان مذکور در خصوص سیستم‌ها و خدمات‌پردازشی یک سازمان حاصل گردد. ازجمله این اقدامات می‌توان‌به موارد ذیل اشاره‌نمود:

- کنترل دسترسی: سیستم‌ها و خدمات‌پردازشی یک سازمان باید به نحوی طراحی شوند که در محیطی جدا از محیط اداری آن سازمان قرار داشته و دسترسی به این اتاق به وسیله کارت کلیدها یا تراشه‌های مخصوصی که به

[12] 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

افراد صلاحیت دار داده می‌شود، محدود گردد. علاوه‌برآن 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 بنداول 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 وظایف‌واختیارات 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 خواهدبود.[۱۳]
- امکان بازیابی اطلاعات جهت حفظ انعطاف‌پذیری سیستم: آنچه در یک سیستم ارتباطی اهمیت وافر دارد، توانایی بازیابی اطلاعاتی می‌باشد که ممکن‌است در اثر عملیات‌پردازش 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 عملیات‌پردازش به طور کامل صورت پذیرد. در این صورت در مواقع حذف اطلاعات، امکان بازیابی آنها از طریق نسخه‌های پشتیبان موجود خواهدبود.[۱۴] در این فرایند تهیه نرم افزارهای ریکاوری اطلاعات یا از روش‌های بازیابی داده‌ها در داخل سامانه از کارکرد عملی برخوردار نیست.[۱۵] علت این موضوع نیز آن است که چون هاردهای ذخیره اطلاعات در سیستم‌ها دارای ظرفیت محدود می‌باشند که در هر بازه زمانی پاک 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 پردازش‌اطلاعات

ارزیابی خطرات مرتبط با پردازش‌اطلاعات، دیگر سازوکاری می‌باشد که در جهت تضمین امنیت‌اطلاعات کاربرد دارد. این موضوع از آن جهت مهم است که پیش بینی خطرات مرتبط با پردازش‌اطلاعات و به کارگیری اقدامات متناسب با نوع پردازش، می‌تواند از نقض‌امنیت‌اطلاعات در یک‌شبکه ارتباطی پیشگیری نماید. در این فرایند آنچه مهم است درنظرگرفتن

[13] 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

[14] Marie Prokopets, The Ultimate Manual To GDPR Article 32, https://nira.com/gdpr-article-32/, Last Visited 15/05/2023

[15] Securiti, Article 32 Of The GDPR: Explained, https://securiti.ai/blog/gdpr-article-32/, Last Visited 12/03/2023

حقوق‌موضوع‌داده، پیچیدگی پردازش‌داده‌ها، حساسیت موضوع و خسارات احتمالی نقض‌امنیت‌اطلاعات می‌باشد که درجه اهمیت این پروسه را نشان می‌دهد.[16]

به‌عبارت‌دیگر مقررات‌مصوب‌سال۲۰۱۶ اتحادیه‌اروپا، به گونه‌ای تنظیم شده‌اند که انجام پردازش‌اطلاعات را منوط به رعایت سطوح امنیتی متناسب با نوع داده و رعایت حقوق‌موضوع‌داده کرده‌اند. این موضوع از مواد ۸۵ الی ۸۹ این مقررات قابل برداشت می‌باشد.

مواد ۸۵ تا ۸۹ از مقررات‌مصوب‌سال۲۰۱۶، دارای شرایطی برای پردازش برخی اطلاعات می‌باشند که پردازش آنها ممکن‌است با خطراتی همراه باشد. ماده ۸۵ از این مقررات مرتبط با حق تقابل آزادی بیان در مطبوعات و اطلاعات می‌باشد که انتشار اطلاعات در کشورهای‌عضواتحادیه‌اروپا در رسانه‌های جمعی مانند تلویزیون، رادیو و ... را منوط به رعایت، حقوق‌موضوع‌داده، وظایف قانونی کنترل‌کنندگان و پردازندگان شبکه‌ها، سازوکار نظارت مقامات صلاحیت دار و ... نموده‌است. 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 تعیین‌شده در مقررات‌مصوب‌سال۲۰۱۶ کنار گذاشته شوند و از این رو باید اصولی مانند به حداقل رساندن داده‌ها که دربردارنده 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 مقررات‌مصوب‌سال۲۰۱۶، افشای اسناد دولتی را تنها تحت ضوابط قانونی و نظارت مقامات صلاحیت دار حکومتی که اصطلاحاً مقام ناظر نامیده می‌شوند، امکان پذیر ساخته است. علت این موضوع، مرتبط بودن اسناد دولتی با اطلاعات ذخیره شده از کارکنان یا مشتریان ادارات و یاحتی تجهیزات موجود در یک اداره می‌باشد که می‌تواند پتانسیل نفرات یا کیفیت خدمات ارائه شده در یک سازمان را نشان دهد. از این رو اگر الزامات لازم در این زمینه حفظ نشود، ممکن‌است 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 نظام‌حقوقی دیگر کشورها در زمینه پردازش‌اطلاعات شناسنامه ملی یا هر شناسه دیگری که به اتباع آن کشورها اختصاص یافته را ضروری تلقی نموده‌است. همانطور که می دانیم، این اطلاعات جزو داده‌های‌شخصی می‌باشند که پردازش آنها نیاز به برقراری سطح امنیتی مناسب داشته و هرچه سطح امنیت‌پردازش این اطلاعات افزایش یابد، امکان نقض‌امنیت آنها درفرایندپردازش نیز کاهش می‌یابد. علاوه‌برآن هر کشور معمولاً متناسب با فرهنگ و امکانات و هنجارهای حاکم بر جامعه خود، الزامات امنیتی را برای پردازش چنین اطلاعاتی درنظر می‌گیرد که جمع این الزامات با الزامات مندرج در مقررات‌مصوب‌سال۲۰۱۶، می‌تواند در بهبود امنیت‌پردازش این اطلاعات مؤثر باشد.

ماده ۸۸ از این مقررات نیز دربردارنده قواعدی در جهت پردازش‌اطلاعات استخدامی کارکنان دستگاه‌های اجرایی می‌باشد که پردازش این اطلاعات را منوط به رعایت کرامت انسانی و حقوق اساسی آنها نموده‌است. 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 داشته‌باشد. بنابراین حفظ

[16] Office of the Data Protection Ombudsman, Risk assessment and data protection planning, https://tietosuoja.fi/en/risk-assessment-and-data-protection-planning, Last Visited 02/04/2023

کرامت انسانی در پردازش این اطلاعات در تمامی ابعاد، موضوعی است که مد نظر قانون گذار اتحادیه‌اروپا در این ماده بوده است. در کنار این ماده، مقررات ماده ۸۹ نیز همانطور که پیشتر نیز توضیح داده شد، رعایت اصول پردازش‌اطلاعات خصوصاً اصل به حداقل رساندن داده‌ها و حقوق‌موضوع‌داده را در پردازش‌اطلاعات بر اساس اهداف مرتبط با منافع عمومی، اهداف تحقیقاتی و علمی و تاریخی اجباری نموده‌است.

برای احراز و بررسی موارد فوق، آنچه در عمل باید اجرا گردد، طراحی فلوچارتی متشکل از مراحل پردازش‌اطلاعات و جدول سؤالات کلیدی می‌باشد که متناسب با نوع داده‌ها و پردازش صورت گرفته، باید در دستور کار قرار گیرد.[۱۷] در حال حاضر فلوچارت بیان‌شده در ذیل درفرایندپردازش‌اطلاعات در نظام‌حقوقی‌اتحادیه‌اروپا کاربرد داشته و بکارگیری آن در نظام‌حقوقی ایران نیز می‌تواند در نظام مند نمودن فرایندپردازش‌اطلاعات و پیشگیری از نقض‌امنیت کاربران و داده‌های مورد پردازش کاربرد داشته‌باشد.

۳-۱. تعیین مرزهای عملیات‌پردازش و زمینه مربوط به آن

اولین مرحله در شروع فرایندپردازش‌اطلاعات و ارزیابی ریسک، تعیین مرزهای عملیات‌پردازش و زمینه مربوط به آن است. در انجام این کار، سازمان باید مراحل مختلف پردازش‌داده‌ها (جمع‌آوری، ذخیره سازی، تحلیل و استفاده، انتقال، حذف و غیره) و پارامترهای بعدی آنها را درنظر بگیرد. بر این مبنا توجه ویژه باید به این واقعیت معطوف شود که تجزیه و تحلیل صورت گرفته به یک عملیات‌پردازش خاص مربوط می‌شود. از این رو در صورتی که فرایندپردازش توسط سیستم از بیش از یک عملیات‌پردازش داده تشکیل شده باشد، تجزیه و تحلیل صورت گرفته باید برای هر عملیات‌پردازش ترتیب داده شود. این موضوع اعم از آن است که پردازش‌اطلاعات بر روی داده‌های قرارگرفته در دسته‌های متفاوت داده‌ها ازجمله بیومتریک، مذهبی، روانشناختی و... قرار گیرند یا نوع پردازش‌اطلاعات اعم از انتقال، استفاده، افشاو ... مدنظر سازمان پردازش کننده باشند. انجام مرحله اول از پردازش‌اطلاعات در سازمان عموماً با تکمیل جدول ذیل که در بردارنده کلیه اطلاعات بیان‌شده برای شروع مرحله پردازش و ارزیابی ریسک می‌باشد، صورت می‌پذیرد:[۱۸]

ردیف	عنوان اقدام	نوع و نحوه اقدام
۱	**شرح عملیات‌پردازش**	ذکر مشروع عنوان عملیات‌پردازش
۲	**داده‌های‌شخصی مورد پردازش**	نوع داده‌های‌شخصی که در عملیات‌پردازش، تحت پردازش قرار می‌گیرند.
۳	**اهداف پردازش**	پردازش بر اساس چه اهدافی صورت می‌پذیرد
٤	**اشخاص موضوع‌داده**	ذکر مشخصات و سمت اشخاص موضوع‌داده، به عنوان مثال نام و نام خانوادگی فرد چه بوده و در یک سازمان نقش کارمند، مشتری و... را بر عهده دارد.
٥	**ابزارهای پردازش**	فرایندپردازش‌اطلاعات توسط چه ابزارهایی و بر روی چه سخت افزار و نرم افزاری صورت می‌پذیرد. به‌عبارت‌دیگر آیا فرایندپردازش‌اطلاعات به صورت خودکار توسط سامانه شروع و اتمام می‌یابد یا در مراحل مختلف توسط ابزار یا ابزارهای خاصی صورت خواهد گرفت. علاوه‌برآن پردازش‌اطلاعات در چه بستری صورت خواهد پذیرت. به‌عبارت‌دیگر پردازش‌اطلاعات در شبکه و سیستم‌های درون سازمانی صورت خواهد پذیرفت یا این اقدام در شبکه‌های عمومی مانند اینترنت انجام خواهد شد.
٦	**پردازشگر اطلاعات**	باید مشخصات و موقعیت مکانی پردازشگر اطلاعات و اینکه آیا پردازشگر در کشور متبوع موضوع‌داده یا کنترل‌کننده ساکن بوده یا مقر آن در کشور ثالثی می‌باشد، قید گردد. علاوه‌برآن صرف نظر از مقر پردازنده،

[17] 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

[18] 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

		اطلاعات در کجا و کدام کشور و با چه نظام‌حقوقی و الزاماتی در پردازش‌اطلاعات تحت پردازش قرار خواهند گرفت.
۷	**دریافت کنندگان داده‌های‌شخصی**	پس از فرایندپردازش، چه شخص یا اشخاصی به داده‌های پردازش شده دسترسی داشته و به عبارتی این اطلاعات در اختیار چه افراد یا نهادهایی گذاشته خواهد شد.

۳-۲. ارزیابی تأثیر

مرحله دوم درفرایند ارزیابی ریسک پردازش‌اطلاعات، ارزیابی تأثیر می‌باشد. در این مرحله، کنترل‌کننده بر اساس اطلاعاتی که در جدول مرحله اول نهاده شده‌است، نسبت به ارزیابی تأثیر پردازش بر حقوق و آزادی‌های اساسی موضوع‌داده 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 موضوع‌داده تنها به حقوق وی در مقررات‌مصوب‌سال۲۰۱۶ اتحادیه‌اروپا محدود نشده و حقوق تعیین‌شده برای وی در مقررات داخلی کشور متبوع موضوع‌داده و سایر حقوق ازجمله حقوق بشر، حقوق شهروندی و... او را نیز شامل می‌گردد. نکته‌قابل‌توجه این‌است که ارزیابی صورت گرفته در این مرحله به صورت نسبی بوده و ممکن‌است نتیجه آن در زمان‌ها و مکان‌های مختلف، متفاوت باشد؛ با این حال ملاک زمانی ارزیابی و تصمیم گیری برای پردازش‌اطلاعات خواهدبود.[19]

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 غیرحاد مواجه می‌گرداند.
۳	**زیاد**	در این سطح، موضوع‌داده ممکن‌است با عواقب قابل توجهی در پردازش‌اطلاعات مواجه شود که تأثیر اساسی بر زندگی شخصی و اجتماعی وی داشته‌باشد. به عنوان مثال می‌توان‌به مصادیقی ازجمله از دست دادن شغل، در معرض تعقیب قضایی قرار گرفتن، قرار گرفتن در وضعیت نامناسب سلامتی یا از دست دادن منابع مالی فراوان اشاره‌نمود.
٤	**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[20]، تمامیت[21] و دردسترس‌بودن[22] اطلاعات برای موضوع‌داده می‌باشد استفاده می‌کنند. این سه شاخصه در قالب جدولی طراحی می‌شود که با تکمیل شدن آن توسط موضوع‌داده، سه شاخصه بیان‌شده به دست آمده و بالاترین سطح ارائه شده به عنوان نتیجه نهایی ارزیابی قلمداد می‌شود.

[19] Enisa, Op.cit, p2
[20] Confidentiality
[21] Integrity
[22] Availability

ردیف	شاخصه	توضیحات	درجه (کم-متوسط-زیاد-خیلی زیاد)
۱	**محرمانگی**	افشای غیر مجاز داده‌های‌شخصی چه تاثیری بر روابط تجاری، زندگی فردی و اجتماعی شما می‌دهد. افشای غیرمجاز داده‌های‌شخصی می‌تواند تحت فرایندهای مختلفی همچون فقدانی یا سرقت لبتاب یا هر وسیله‌ای که اطلاعات در آن ذخیره شده یا ارسال اشتباه اطلاعات به گیرندگان غیر مجاز صورت پذیرد.	
۲	**تمامیت**	تغییر غیرمجاز داده‌های‌شخصی چه تاثیری 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	**دردسترس‌بودن**	تخریب غیرمجاز یا از دست دادن دسترسی به داده‌های‌شخصی چه تاثیری بر روابط تجاری، زندگی شخصی و اجتماعی شما دارد. از دست دادن دسترسی به داده‌های‌شخصی می‌تواند مصادیقی مانند گم شدن فایل یا پرونده پرسنلی یا پزشکی یک شخص را از سرور سازمان مربوطه شامل شود که پیشتر نسبت به این اطلاعات نسخه پشتیبان تهیه نشده باشد.	

۳-۳. ارزیابی تهدیدات بالقوه

تهدید به هر شرایط یا رویدادی گفته می‌شود که می‌تواند بر امنیت داده‌های‌شخصی تأثیر منفی بگذارد. در این مرحله، هدف کنترل‌کننده یا پردازنده داده، درک تهدیدات مربوط به محیط کلی پردازش‌داده‌های‌شخصی (خارجی یا داخلی) و ارزیابی احتمال وجود یا عدم وجود تهدیدات بالقوه آن‌ها است. سطوح مختلف و انواع تهدیدات می‌توانند در شاخصه‌هایی همچون محرمانه‌بودن، تمامیت و دردسترس‌بودن داده‌های‌شخصی 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 وجد دارد
- بالا: احتمال تحقق تهدید وجود دارد

ارزیابی تهدیدات بالقوه در شبکه‌های‌تبادل‌اطلاعات در اجزای این شبکه‌ها که شامل منابع فنی (نرم افزارها و سخت افزارها) می‌باشند، فرایندهای مربوط به پردازش‌داده‌های‌شخصی، اشخاص درگیر در عملیات‌پردازش و مقیاس پردازش به شرح مطالب آتی صورت می‌پذیرد[۲۳]:

[23] Aepd, 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, p35

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، تعهدیدات 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. علاوه‌برآن 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 خواهدبود. از این رو دسترسی به شبکه باید الزاماً توسط اشخاصی که با داده‌ها سر و کار دارند انجام گیرد. چالش موجود عموماً زمانی اتفاق می افتد 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 بخصوصی از شبکه مستعد حملات سایبری یا نقض‌امنیت می‌باشند؟ در صورتی که در گذشته بخش‌های بخصوصی از شبکه تحت نقض امنیتی قرار گرفته باشند، باید اقدامات لازم در جهت رفع خلاء های امنیتی در این قسمت‌ها بیش از پیش و بیش از سایر قسمت‌ها مدنظر قرار گیرد.
۲	آیا امکان دسترسی به یک سیستم پردازش‌داده‌های‌شخصی داخلی از طریق اینترنت (به عنوان مثال برای کاربران خاص یا گروه‌هایی از کاربران) وجود دارد؟ به‌عبارت‌دیگر آیا امکان دسترسی از راه دور به شبکه برای مدیران یا برخی کارکنان	آیا مصادیق استفاده قابل قبول از شبکه، سیستم و منابع فیزیکی در سازمان مشخص شده یا به وضوح تعریف نشده‌است؟ 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	آیا بخشی یا تمام عملیات پردازش توسط پردازنده (شخص ثالث) انجام می‌گیرد؟ به عنوان مثال ممکن‌است سیستم فناوری اطلاعات یک مدرسه خصوصی توسط یک مرکز داده خارجی پشتیبانی شود یا اطلاعات ذخیره شده در	ایجاد حملات سایبری یا نقض‌امنیت‌اطلاعات در چه بازه‌های زمانی رخ داده است؟ بررسی بازه‌های زمانی نقض امنیت‌اطلاعات یا به طور کلی شبکه موجود، به عنوان مثال در زمان تعطیلات آخر هفته یا فصل تابستان می‌تواند معیارهای مناسبی در تشخیص

	یک سازمان فراهم شده‌است؟ علت طرح این موضوع این‌است که در حالتی 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.	مشخص مرزهای استفاده از امکانات سازمانی گاه می‌تواند منجر به تلقی برخی اقدامات شخصی کاربران به عنوان تهدیدات امنیتی ازسوی مراجع حفاظتی شناخته شود.	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 فرایندپردازش، توسط اشخاص ثالث، سازمان ممکن‌است تا حدی کنترل این داده‌ها را از دست بدهد.	علل نقض‌امنیت و رفع مشکل به سازمان مربوطه بدهد.
۳	آیا سیستم پردازش‌داده‌های 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.	آیا مرزهای دسترسی به شبکه پردازش‌اطلاعات تنها محدود به سخت افزارهای سازمانی می‌باشد یا سخت افزارهای شخصی کارکنان دستگاه را نیز دربرمی گیرد. 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 نشت یا 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 می گردد.	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 علاوه‌برآن برای نمونه میان تعهدات اشخاصی که داده‌های‌شخصی دسته‌های خاص (موضوع ماده ۹ مقررات‌مصوب ۲۰۱۶) و سایر داده‌های‌شخصی را پردازش می‌کنند تفاوت درنظر گرفته شده‌است؟	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 آرشیو سوابق گزارشات واصله طراحی شده‌اند؟
٤	آیا افراد غیرمجاز می‌توانند به راحتی به محیط پردازش‌داده‌ها دسترسی داشته باشند؟ به عنوان مثال آیا شرکت یک اتاق کامپیوتر اختصاری برای مدیریت سیستم فناوری اطلاعات سازمان برای پردازش‌اطلاعات دارد یا در صورتی که فرایندپردازش و ذخیره سازی اطلاعات در بیرون از سازمان صورت می‌پذیرد، اقدامات امنیتی مناسبی در این زمینه رخ داده	آیا کارکنان مجاز به انتقال، ذخیره یا پردازش‌اطلاعات‌شخصی 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	آیا پرسنل درگیر با فرایندپردازش‌اطلاعات با تعهدات قانونی خود در قبال کل مجموعه آشنایی دارند؟ آیا الزامات امنیتی که در برخورد با اطلاعات در یک سازمان درنظر 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	گستره عملیات‌پردازش‌اطلاعات به چه حجمی از افراد مربوط می‌شود؟ به عنوان مثال آیا پردازش‌اطلاعات در خصوص وضیت 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

	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.	پذیر باشد، طبیعتاً چالش‌های بیان‌شده در کادر قبلی ازجمله افشا و دسترسی غیر مجاز و ورود بدافزارها به شبکه می‌تواند مطرح شود. علاوه‌برآن 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	مطلع باشند، عملاً حساسیت بیشتری در اقدامات خود درنظر گرفته که این موضوع می‌تواند از نقض امنیت داده‌ها و کل شبکه پیشگیری نماید.	پردازش می‌تواند نمود بخش اهمیت پردازش و مخاطب حملات سایبری قرار گرفتن باشد.
۵	آیا سیستم پردازش اطلاعات شخصی در یک سازمان با استفاده از پروتکل‌های از پیش تعیین‌شده کار کرده و نگهداری اطلاعات بر مبنای دستورالعمل‌های از پیش تعیین‌شده صورت می‌گیرد؟ این موضوع از آن جهت دارای اهمیت است که وجود پروتکل‌های از پیش تعیین‌شده که مراحل ارزیابی خود را سپری و نقاط ضعف آنها بررسی شده باشد، می‌تواند در زمینه بهبود امنیت پردازش اطلاعات کاربرد داشته‌باشد.	درفرایندپردازش اطلاعات شخصی، اقدامات مبتنی بر ثبت و نظارت به چه نحوی انجام خواهد شد؟ به‌عبارت‌دیگر 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.	آیا افراد درگیر درفرایند 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 ازسوی کاربران شبکه و پردازندگان می‌تواند از ایجاد نقض در شبکه پیشگیری کند.	آیا اقدامات حفاظتی متناسب با نوع پردازش صورت گرفته در یک سازمان پیاده سازی شده‌اند؟ به‌عبارت‌دیگر در صورتی که پردازش اطلاعات بر روی دسته‌های مختلفی از داده‌ها رخ دهد، متناسب با هر دسته، اقدام حفاظتی بخصوص نیز درنظر گرفته شده‌است یا خیر؟

۳-٤. ارزیابی خطر

پس از ارزیابی تأثیر و تهدیدات باالقوه می‌توان‌به شرح فرمول ذیل از طریق ضرب نتایج حاصل از ارزیابی هریک از دو شاخصه بیان‌شده، نسبت به ارزیابی خطر درفرایندپردازش اطلاعات اقدام نمود.

٤- رعایت الزامات شکلی

مقررات‌مصوب‌سال۲۰۱۶، در ماده ۴۰ کشورهای‌عضو را موظف به تنظیم مقررات داخلی در جهت بهبود اجرای مقررات‌مصوب‌سال۲۰۱۶ و رفع خلاء های این قانون که در هر نظام‌حقوقی مطابق با هنجارهای حاکم بر آن نظام ممکن‌است پدید آید، نموده‌است.

٤-۱. تنظیم گری مقررات

بنداول از این ماده کشورهای‌عضو و مقامات نظارتی را ملزم به تدوین مقررات در جهت اجرای صحیح مقررات‌مصوب‌سال۲۰۱۶ نموده و بنددوم از این ماده ضرورت توجه به مفاهیمی مانند پردازش منصفانه و شفاف اطلاعات، منافع مشروع کنترل‌کنندگان، جمع‌آوری داده‌های‌شخصی، مستعارسازی داده‌های‌شخصی، اطلاعات ارائه شده به عموم مردم، حقوق‌موضوع‌داده، نحوه حمایت از کودکان و سازوکار پردازش‌اطلاعات آنها، اخذ رضایت از موضوع‌داده، وظایف اطلاع رسانی و سازوکار تبادل‌اطلاعات کرده است.

نکته قابل توجه در مقررات این ماده این می‌باشد که مفاد بند سوم از این ماده، به جهت اهمیتی که فرایندپردازش‌داده‌های‌شخصی 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 پردازندگانی که مشمول مقررات این قانون نباشند را مشمول مقررات فوق‌الذکر نموده‌است.

مقررات بندچهارم این ماده نیز نظارت بر حسن اجرای مواد مقررات‌مصوب‌سال۲۰۱۶ را بر عهده مقام ناظری تعیین نموده‌است که بر مبنای مواد ۳۷-۳۹ و ۵۱-۵۹ این مقررات تعیین و حدود وظایف آن در مواد مرقوم، تعیین‌شده‌است. علاوه‌برآن این ماده مقرر داشته حدود وظایف‌واختیارات مقام ناظر، نافی اختیارات دیگر مقامات صلاحیت دار حکومتی در نظارت بر حسن اجرای این مقررات نمی‌باشد.

بنظر می‌رسد، تدبر در مفاد مواد ۳۷-۳۹ و ۵۱-۵۹ مقررات‌مصوب‌سال۲۰۱۶ این موضوع را احاله می‌نماید که وظایف‌واختیارات مقام ناظر، همانطور که از نام آن پیداست تنها در بعد پیشگیری از نقض‌امنیت‌اطلاعات، انعقاد و اجرای صحیح قراردادها و انجام صحیح وظایف اشخاص درگیر درفرایندپردازش‌اطلاعات 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 برخودار 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 عضواتحادیه‌اروپا را منوط به تأیید مفاد مقررات فوق و تطبیق و تأیید عدم مغایرت آنها با مقررات‌مصوب‌سال۲۰۱۶ توسط مقام ناظر نموده‌است. علاوه‌برآن، این مقام در صورتی که موضوعی وجهه بین المللی داشته و به عبارتی مقرره مصوب در یک کشور، مربوط به فعالیت‌های‌پردازشی در چند کشور بوده و نظام‌حقوقی کشورهای مختلف را درگیر نماید، با ارائه نظریه مشورتی، مراتب را به هیئت مقرر در بندهفتم این ماده اطلاع داده و پس از جمع‌آوری نظرات و دیدگاه‌ها و مراتب موجود، هیئت مطابق با مفاد بندهشتم این ماده وضعیت حادث را بنظر کمیسیون مقرر در بندنهم این ماده اطلاع می‌دهد. کمیسیون نیز پس از بررسی دیدگاه‌ها و مراتب، می‌تواند تصویب نماید که مقررات‌مصوب داخلی در یکی از کشورهای‌عضو اتحادیه، دارای اعتبار در سطح کشورهای اتحادیه‌اروپا باشد.

٤-٢. وظایف‌واختیارات مرجع نظارتی

مراجع نظارتی مقرر در مقررات‌مصوب‌سال۲۰۱۶، به دو دسته تقسیم می‌شوند که وظایف‌واختیارات آنها ابتدائا در مواد ۳۷-۳۹ و پس از آن در مواد ۵۱-۵۹ مقرر شده‌است. مقاماتی که بر مبنای مقررات‌مواد ۳۷-۳۹ مشخص می‌شوند اصطلاحاً « Data Protection Officer» نامیده شده و مقاماتی که بر مبنای مقررات‌مواد ۵۱-۵۹ معین می‌شوند اصطلاحاً « Supervisory Authority» نامیده می‌شوند. اگرچه این دو مقام، در واقع دارای وظایف و مسئولیت‌های مشابه در نظارت بر فرایندپردازش‌اطلاعات یا انعقاد قراردادهای منعقده میان پردازنده و کنترل‌کننده یا کنترل‌کننده و موضوع‌داده می‌باشند، اما دارای تفاوت‌هایی هستند که در مطالب آتی بدان اشاره خواهد شد.

نکته‌قابل‌توجه نقش کلیدی این اشخاص در پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات می‌باشد. به‌عبارت‌دیگر با توجه به اینکه وظیفه این اشخاص مراقبت از اجرای مقررات قانونی در انجام پردازش‌اطلاعات یا رعایت حقوق‌موضوع‌داده درفرایندپردازش یا اجرای وظایف کنترل‌کننده و پردازنده می‌باشد، عملاً تدابیر امنیتی درفرایند تبادل‌اطلاعات در یک‌شبکه ارتباطی حفظ شده و از نقض‌امنیت پیشگیری می‌گردد. ضمن اینکه بر فرض نقض‌امنیتی 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 خواهدبود. از این رو می‌توان نقض این مقام در حفظ امنیت و پیشگیری از نقض‌امنیت در شبکه‌های‌تبادل‌اطلاعات را نقشی کلیدی دانست. اینک به بررسی وظایف‌واختیارات این مقامات درفرایندپردازش‌اطلاعات در شبکه‌های ارتباطی اقدام خواهیم کرد.

٤-٢-١. وظایف‌واختیارات افسر حفاظت‌ازاطلاعات

افسر حفاظت‌ازاطلاعات، مقامی است که بر مبنای مواد ۳۷-۳۹ مقررات‌مصوب‌سال۲۰۱۶ انتخاب شده و وظایف و مسئولیت‌های وی در این مقررات ذکر شده‌است. با ملاحظه متن ماده ۳۷ مقررات‌مصوب‌سال۲۰۱۶ می‌توان‌به نتایج ذیل رسید. بر اساس قسمت اول از بنداول این ماده، مقام ناظر معین شده به عنوان افسر حفاظت‌ازاطلاعات، 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 وظایف‌واختیاراتی خواهدبود که توسط مقام نصب کننده به وی اعطا شده و وظایف‌واختیارات وی ارتباطی با آنچه در مقررات ماده ۳۷ این قانون ذکر شده ندارد.[۲۴]

ثانیاً، انتصاب افسر حفاظت‌ازاطلاعات 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 حفاظت‌ازاطلاعات وجود ندارد. البته این موضوع به معنای ایجاد ممنوعیت در انتصاب وی در فعالیت‌های‌پردازشی کوچک تلقی نمی‌گردد. این موضوع از اهداف تصویب این مقررات قابل برداشت است. چرا که همانطور که ماده ۴۰ مقررات‌مصوب‌سال۲۰۱۶ مورد تصریح قرار داد، هدف اصلی از تصویب این مقررات افزایش ضریب امنیت‌پردازش‌اطلاعات و پیشگیری از نقض‌امنیت فعالیت‌های‌پردازشی خواهدبود. از این رو در صورتی که کنترل‌کننده و پردازنده نسبت به انتصاب چنین مقامی در هر فعالیتی اقدام نمایند، مانعی وجود نخواهد داشت.

نکته‌قابل‌توجه امکان انتصاب این افسر ازسوی پردازنده و کنترل‌کننده به صورت توامان می‌باشد (Hintze,2018,4) . اما سؤال موجود این‌است که چرا با توجه به اینکه پردازنده تحت راهنمایی و دستورات صادره ازسوی کنترل‌کننده مبادرت‌به انجام

[24] Personal Data Protection Commission, Data Protection Officers, https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers, Last Visited 22/07/2023

وظیفه می‌نماید، قانون این شخص را نیز موظف به انتصاب مقام حفاظت‌ازاطلاعات نموده‌است؟ 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 دربردارنده اهمیت پردازش‌اطلاعات 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 ازسوی 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 ازسوی کنترل‌کننده صورت نگرفته باشد.

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

نکته دیگر این‌است که برای تشخیص بزرگ و کوچک بودن فرایندپردازش، معیاری در مقررات‌مصوب‌سال۲۰۱۶ معین نشده‌است و بر این مبنا می‌توان نتیجه گیری نمود که این موضوع امری نسبی بوده و بنظر نگارنده توجه به اثرات پردازش می‌تواند نشان دهنده 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 سلایق هر مراجعه کننده(لطیف زاده و دیگران، پیشین، ۱۴۰۲، ۲۵۳) یا پردازش‌داده‌های‌شخصی توسط شرکت‌های تبلیغاتی برای ارسال تبلیغات به مشتریان(همانجا) را پردازش در مقیاس بزرگ محسوب نموده‌اند، این نوع اقدامات به منزله فعالیت‌های‌پردازشی 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 سفید پوستان، داروی خاصی تولید گردد، می‌توان این اقدامات را به عنوان فعالیت‌های‌پردازشی در مقیاس بزرگ محسوب نمود.

در کنار معیار بیان‌شده، بنظر برخی دیگر می‌توان از طریق معیارهای دیگری نیز مقیاس بزرگ فعالیت‌های‌پردازشی را شناسایی نمود. معیارهای موجود به قرار ذیل هستند:[۲۵]

- تعداد موضوع‌داده درگیر درفرایند 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 این‌است که تعداد اشخاص موضوع‌داده یا حجم داده‌های مورد پردازش یا مدت پردازش، برای یک عملیات‌پردازش ملاک می‌باشند یا در صورتی که تعدادی عملیات‌پردازش مرتبط با هم انجام

[25] 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

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 عملیات‌پردازش 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 انبوده و مدت زمانی طولانی انجام می‌شود. اگر ملاک همان عملیات‌پردازش 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 نخواهدبود. بنظر می‌رسد همانطور که در معیار مدنظر نگارنده نیز بیان گردید، در این خصوص ملاک تشخیص، اقدامات صورت گرفته بر روی هر موضوع‌داده خواهدبود مگر اینکه ماهیت اقدامات، تعداد بیشتری از اشخاص موضوع‌داده را در برگیرد.

ثالثاً مقررات بندهای دوم و سوم ماده ۳۷ امکان انتخاب یک افسر حفاظت‌ازاطلاعات را برای چند کنترل‌کننده و پردازنده صرف نظر از اینکه این اشخاص جزو اشخاص حقوقی عمومی باشد یا خیر معین نموده‌است. اما شرط لازم برای این موضوع، دردسترس‌بودن افسر حفاظت‌ازاطلاعات برای کلیه پردازندگان و کنترل‌کنندگانی می‌باشد که نسبت به انتصاب وی اقدام کرده‌اند. مضاف بر آنچه بیان‌شده به حکم بنا ششم از این ماده، انتخاب افسر فوق‌الذکر لزوماً از میان اشخاص خارج از کارکنان پردازنده یا کنترل‌کننده فراهم نبوده و اگرچه این مقامات می‌توانند با کنترل‌کنندگان و پردازندگان با اخذ قرارداد، شروع به همکاری نمایند، اما انتخاب آنها از میان کارکنان پردازندگان و کنترل‌کنندگان فاقد ایراد قانونی خواهدبود.

نکته‌قابل‌توجه دیگر این‌است که این مقام تنها به بالاترین مقام منصوب کننده وی پاسخگو بوده و گزارشات خود را باید به آن شخص اعطا نماید. (بندسوم ماده ۳۸) از این رو سایر اشخاص نه حق و نه اختیار اخذ گزارش از مقام حفاظت از داده‌ها در یک فرایندپردازشی را خواهند داشت. در مقابل این افسر برای انجام وظایف خود حق هرگونه جستجو در اقدامات صورت گرفته درفرایندپردازش را برخوردار خواهدبود.[۲۶] سوالی که در این زمینه می‌توان بیان داشت این‌است که آیا مقام مذکور تنها باید یک شخص حقیقی بوده یا اشخاص حقوقی نیز می‌توانند به این مقام منصوب شوند؟ تدبر در مقررات‌مواد ۳۸ و ۳۹ نشان می‌دهد که شرایط تعیین‌شده 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 فوق‌الذکر را خواهند داشت.[۲۷]

رابعاً مقررات بندپنجم ماده ۳۷، وجود شرایط دانش و تخصص در افسر حفاظت‌ازاطلاعات را جزو شرایط اساسی انتخاب وی جهت انجام وظایف ماده ۳۹ محسوب نموده‌است. مواد ۳۹ مقررات‌مصوب‌سال۲۰۱۶ ماده مقرر می‌دارد:

۱- افسر حفاظت از داده‌ها باید حداقل وظایف زیر را داشته‌باشد:

- اطلاع رسانی و توصیه به کنترل‌کننده یا پردازنده و کارکنانی که تعهدات خود را طبق این مقررات و سایر مقررات حفاظت از داده‌های اتحادیه یا کشورهای‌عضو انجام می‌دهند
- نظارت بر انطباق با این مقررات، سایر مقررات حفاظت از داده‌های اتحادیه یا کشورهای‌عضو و سیاست‌های کنترل‌کننده یا پردازنده در رابطه با حفاظت از داده‌های‌شخصی، ازجمله واگذاری مسئولیت‌ها، افزایش آگاهی و آموزش کارکنان درگیر در عملیات‌پردازش، 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

---

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

[27] 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

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

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

با بررسی مفاد بندپنجم ماده ۳۷ و مقررات ماده ۳۸ می‌توان‌به این نتیجه رسید که ذکر عنوان ماده ۳۹ در بندپنجم ماده ۳۷، ناشی از مسامحه قانون گذار اتحادیه‌اروپا و تاکید آن مقام بر مطلق وظایف افسر حفاظت‌ازاطلاعات می‌باشد. از این رو می‌توان بیان داشت که وظایف مقرر در ماده ۳۹، تنها وظایف افسر حفاظت‌ازاطلاعات 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 خواهدبود. در این زمینه بندهای پنجم این ماده افسر حفاظت‌ازاطلاعات را ملزم به محرمانگی فرایندپردازش و حفظ رازداری و بندششم نیز عدم انجام اقداماتی که با منافع کنترل‌کننده و پردازنده در تعارض باشد، نموده‌است. نکته‌قابل‌توجه این‌است که وظایف مندرج در مواد ۳۸ و ۳۹ مقررات‌مصوب‌سال۲۰۱۶، 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 خواهدبود. البته این اقدامات نیز تا جایی جریان دارد که با مقررات‌مواد ۳۸ و ۳۹ تعارضی نداشته باشند.

در خصوص تعارض منافع مندرج در بندششم 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 ازسوی مقام منصوب نباید وجود داشته‌باشد. به عنوان مثال در صورتی که شخصی به عنوان افسر حفاظت‌ازاطلاعات توسط پردازنده یا کنترل‌کننده‌ای منصوب شود، در صورتی قابلیت انعقاد قرارداد با کنترل‌کننده دیگر جهت نظارت بر فرایندپردازش در محلی دیگر را خواهد داشت که منافع مقام منصوب کننده اول وی تحت الشعاع قرار نگیرد. علاوه‌برآن الزامات دیگر ازجمله 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 حفاظت‌ازاطلاعات با مقررات قانونی حکایت دارد. به عنوان مثال ماده ۳۰ مقررات‌مصوب‌سال۲۰۱۶ کنترل‌کننده و پردازنده را موظف به حفظ سوابق پردازشی نموده‌است. در صورتی که این اشخاص، وظیفه بیان‌شده را جزو وظایف افسر حفاظت‌ازاطلاعات قرار دهند، این موضوع با وظایف ذاتی آن شخص در تعارض نبوده و بنابراین امکان انجام آن توسط فرد بیان‌شده 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 مقررات‌مصوب‌سال۲۰۱۶ بوده و تعیین اهداف پردازش، با وظایف نظارتی او در تعارض می‌باشد، نمی‌توان چنین وظیفه‌ای را برای رو درنظر گرفت (لطیف زاده و دیگران، پیشین، ۱۴۰۲، ۲۶۲).

٤-۲-۲. وظایف واختیارات مقام صلاحیت دار نظارتی

مقررات‌مصوب‌سال۲۰۱۶ اتحادیه‌اروپا، علاوه بر اختصاص موادی بر تعیین افسر حفاظت‌ازاطلاعات، در مواد ۵۱-۵۹ موادی را به تعیین مقامات نظارتی دولتی نیز بر فرایندپردازش‌اطلاعات و حدود اختیارات آنها اختصاص داده است. وجود این مقامات در کنار افسر حفاظت‌ازاطلاعات می‌تواند یکی از سازوکارهای مهم نظارت و پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات به دلایل بیان‌شده در مطالب پیشین در باب افسر حفاظت‌ازاطلاعات تلقی گردد.

ماده ۵۱ از مقررات‌مصوب‌سال۲۰۱۶ مقرر می‌دارد که هریک از کشورهای‌عضواتحادیه‌اروپا باید یک یا چند مقام دولتی مستقل را برای نظارت بر فرایندپردازش‌اطلاعات، صیانت از حقوق‌موضوع‌داده و تبادل آزاد اطلاعات در کشور خود منصوب نمایند. این مقامات باید با یکدیگر و مقامات سایر کشورهای‌عضو در ارتباط بوده و همکاری‌های لازم را با کمیسیون مقرر در ماده ۴۰ مقررات‌مصوب‌سال۲۰۱۶ نیز داشته باشند. علاوه‌برآن 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 فرایندپردازش‌اطلاعات در محدوده سرزمینی آن کشور تحت نظارت و تصمیم گیری آن مقام صورت پذیرد.

مقامات نظارتی تعیین‌شده 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. علاوه‌برآن کشورهای‌عضواتحادیه‌اروپا 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 نموده‌است.

هریک 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 ازجمله 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 این‌است که معیار تعیین سوءرفتار جدی برای برکناری مقامات نظارتی مقرر در ماده ۵۱ مقررات‌مصوب‌سال۲۰۱۶ چه می‌باشد؟ در این زمینه اظهارنظر شده‌است 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.[۲۸] ازجمله این مصادیق می‌توان‌به انتقال عمدی اطلاعات، بی توجهی به استانداردهای تعیین‌شده، عدم ارائه گزارش جامع و مانع به مقام مسئول در موارد مقتضی، عملکرد مداوم ضعیف و اشتباهاتی که باعث ضررهای مالی یا معنوی ازجمله آسیب رساندن به شهرت گردد، اشاره‌نمود[۲۹].

هریک از مقامات نظارتی تعیین‌شده در کشور حوزه فعالیت خود، صلاحیت رسیدگی داشته و امکان فعالیت در کشور دیگری را نخواهند داشت. (بنداول ماده ۵۵) علاوه‌برآن، این مقامات نیز همانند افسر حفاظت‌ازاطلاعات، 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 درفرایند تبادل فراملی اطلاعات خواهدبود 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 مبادرت‌به نصب مقام نظارتی نموده‌باشد، نحوه نظارت بر اقدامات پردازنده توسط مقام مزبور به چه نحوی خواهدبود؟ برای پاسخ به این سؤال باید به ماده ۶۰ مقررات‌مصوب‌سال۲۰۱۶ 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 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

---

[28] 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

[29] 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

اقدام نماید. آنچه در بررسی مقررات ماده ۶۰ بنظر می‌رسد این‌است 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 تعیین‌شده برای وی توسط مجاس یا دولت منصوب کننده او خواهدبود. بنظر می‌رسد عدم اطلاع به موقع اقدامات ازسوی مقام ناظر اول به مقام ناظر کشور هدف، بر مبنای ماده ۵۳ مقررات‌مصوب‌سال۲۰۱۶، به منزله سوءرفتار جدی تلقی شده و حتی امکان برکناری وی را نیز فراهم آورد.

نکته آخر در این زمینه وظایف‌واختیارات مقام نظارتی می‌باشد که در مواد ۵۷ و ۵۸ مقررات‌مصوب‌سال۲۰۱۶ پیش بینی شده‌است. 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 پردازش‌اطلاعات، آموزش، افزایش آگاهی عمومی و ارائه مشاوره به موضوع‌داده و کنترل‌کنندگان شبکه‌های‌تبادل‌اطلاعات و پردازندگان اطلاعات و همچنین تصویب و ابلاغ دستورالعمل‌های مختلف در زمینه چگونگی عملکرد نهادهای فعال در حوزه پردازش‌اطلاعات و صدور گواهینامه‌ها و مجوزهای لازم برخوردار خواهدبود. این مقام بر مبنای مفاد ماده ۵۸ از این مقررات، حق هرگونه وارسی و درخواست اطلاعات از کلیه اشخاص درگیر درفرایندپردازش‌اطلاعات را داشته و اشخاص مذکور الزاماً باید با این مقامات همکاری‌های لازم را داشته باشند. ازجمله اختیارات ذکر شده در ماده ۵۸ می‌توان‌به درخواست ارائه اطلاعات در ارتباط با اختیارات پردازنده و کنترل‌کننده، محل استقرار پردازنده و کنترل‌کننده 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 فرایندپردازش در زمان مشخص، اعمال محدودیت در انجام پردازش اشاره نمود.

نتیجه گیری

پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات نیازمند سازوکارهایی است که برخی از آنها در ماده ۳۲ مقررات عمومی حفاظت از داده‌های اتحادیه‌اروپا با عنوان مستعارسازی و رمزگذاری داده‌های‌شخصی، اطمینان از محرمانه‌بودن، یکپارچگی، دردسترس‌بودن و انعطاف‌پذیری سیستم‌ها و خدمات‌پردازشی، خطرات (ریسک) مرتبط با پردازش‌اطلاعات و رعایت الزامات شکلی پیش بینی شده‌است. هریک از سازوکارهای بیان‌شده در فوق به صورت مفصل در متن این پژوهش مورد بررسی قرار گرفته‌اند. این سازوکارها در عین کارایی و ضرورت بکارگیری در نظام‌حقوقی ایران نیازمند برخی زیرساخت‌ها می‌باشند که بیان برخی توصیه‌های سیاستگذارانه به شرح ذیل در این خصوص ایجاب می‌گردد:

۱- اصلاح قوانین و مقررات‌مصوب در کشور ایران: متاسفانه در بررسی قوانین و مقررات موجود در حقوق ایران ملاحظه می‌شود که قوانین و مقررات بخصوصی در جهت پیشگیری از نقض‌امنیت‌شبکه‌های‌تبادل‌اطلاعات 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 نظام‌حقوقی‌اتحادیه‌اروپا با تصویب مقررات‌مصوب‌سال۲۰۱۶ 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 امنیت اطلاعات‌شخصی یا شبکه‌های تبادل‌اطلاعاتی که در آن فعالیت دارند، باید در دستور کار دولت قرار گیرد.

۳- نظام‌مند نمودن اعطای مجوز به فعالیت شرکت‌های فراملی: متاسفانه رویه‌ای که در کشور ایران حاکم می‌باشد این‌است که متاسفانه رویکردهای شدیدی 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 تبادل‌اطلاعات به نحو مطلوبی حل و فصل شود. چرا که در عصر حاضر، فیلترینگ شبکه‌های‌تبادل‌اطلاعات 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 شبکه های 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 می تواند مورد پیش بینی و در دستور کار قرار گیرد؟ این امر، موضوعی است که می تواند محل انجام پژوهش های 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، گام های اولیه در راستای انجام هرچه بهتر سیاست گذاری های تقنینی و بهره مندی از تجربیات نظامات حقوقی کشورهای توسعه یافته جهت رفع خلاء های 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 اتحادیه‌اروپا 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 داده‌های‌شخصی در رسانه‌ها از منظر حقوق اتحادیه‌اروپا و نظام‌حقوقی 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.