Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 3, Issue 5, 2024

Characteristics of the Optimal Model in the Institution-Oriented Prevention of Crimes Against Personal Data With an Adaptive Approach to European Regulations (GDPR)

Leila Badad *[1], Rouhuddin Kordalivande [2], Sudabeh Rezvani [3]

1. PhD Student of Jurisprudence and Criminal Law, Faculty of Law and Political Sciences, Kharazmi University, Tehran, Iran. (Corresponding Author)
2. PhD in Criminal law and Criminology, Lecturer at the University of Poitiers, Poitiers, France.
3. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages:177-189

Corresponding Author's Info
ORCID: *0009-0006-2602-5160*
TELL: *+98 9123402902*
Email: *leilabadad63@gmail.com*

Article history:
Received: *07Aug 2023*
Revised: *03 Dec 2023*
Accepted: *02 Feb 2024*
Published online: *20 Feb 2024*

Keywords:
Privacy, Personal Data, Unauthorized Processing, European General Data Protection Regulation, National Data and Information Management Law.

ABSTRACT

Crimes against personal data are important crimes that need to be discussed and investigated in parallel with the increasing development of cyber space and electronic communication. The purpose of this article is to investigate the characteristics of the ideal model in the institution-oriented prevention of crimes against personal data with an adaptive approach to European regulations. The current article is descriptive and analytical and has investigated the mentioned subject by using the library method. The findings from the descriptive-analytical study of the indicators (substantive and strategic) of the ideal model in protecting personal data with an adaptive approach to European regulations indicate that at the level of the European Union, the European General Data Protection Regulations Relatively. In Iran's legal system, despite the approval of the National Data and Information Management Law, there are shortcomings such as not specifying the rights of the data subject, not criminalizing some criminal acts, excluding some institutions from the inclusion of the data management law at the national level. material indicators; The lack of detail in determining the guarantee of administrative executions, the lack of sufficient monitoring mechanisms and the prediction of multiple institutions with overlapping tasks are visible at the level of strategic indicators, which in addition to creating an imbalance between preventive, control and repressive strategies, cause challenges. Serious steps have been taken to achieve the ideal model.

How to Cite This Article: Badad, L; Kordalivande, R & Rezvani, S (2024). "Characteristics of the Optimal Model in the Institution-Oriented Prevention of Crimes Against Personal Data With an Adaptive Approach to European Regulations (GDPR)". *Journal of Comparative Criminal Jurisprudence*, 3(5): 177-189.

فصلنامه فقه جزای تطبیقی
www.jccj.ir

دوره سوم، شماره پنجم، اسفند ۱۴۰۲

شاخصه‌های الگوی مطلوب در پیشگیری نهاد محور از جرایم علیه داده‌های شخصی با رویکردی تطبیقی به مقررات اروپایی

لیلا باداد*[۱]، روح‌الدین کردعلیوند [۲]، سودابه رضوانی [۳]

۱. دانشجوی دکتری فقه و حقوق جزا، دانشکده حقوق و علوم سیاسی، دانشگاه خوارزمی، تهران، ایران (نویسنده مسؤول).
۲. دکتری حقوق کیفری و جرم‌شناسی، مدرس دانشگاه پوآتیه، فرانسه.
۳. استادیار، گروه حقوق جزا و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه خوارزمی، تهران، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱۷۷-۱۸۹

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۹-۰۰۰۶-۲۶۰۲-۵۱۶۰

تلفن: ۹۸۹۱۲۳۴۰۲۹۰۲+

ایمیل: *leilabadad63@gmail.com*

سابقه مقاله:

تاریخ دریافت: ۱۴۰۲/۰۵/۱۶

تاریخ ویرایش: ۱۴۰۲/۰۹/۱۲

تاریخ پذیرش: ۱۴۰۲/۱۱/۱۳

تاریخ انتشار: ۱۴۰۲/۱۲/۰۱

واژگان کلیدی:

حریم‌خصوصی، داده‌شخصی، پردازش غیر مجاز، مقررات عمومی حفاظت از داده اروپا، قانون مدیریت داده‌ها و اطلاعات ملی.

چکیده

جرایم علیه داده‌های شخصی از جرایم مهمی است که به‌موازات توسعه فزاینده فضای مجازی و ارتباطات الکترونیک، نیازمند بحث و بررسی است. هدف مقاله حاضر، بررسی شاخصه‌های الگوی مطلوب در پیشگیری نهاد محور از جرایم علیه داده‌های شخصی با رویکردی تطبیقی به‌مقررات اروپایی است. مقاله حاضر، توصیفی تحلیلی بوده و با استفاده از روش کتابخانه‌ای به‌بررسی موضوع مورد اشاره پرداخته است. یافته‌های ناشی از مطالعه توصیفی- تحلیلیِ شاخصه‌های (ماهوی و راهبردی) الگوی مطلوب در حمایت از داده‌های شخصی با رویکرد تطبیقی به‌مقررات اروپایی، بیانگر آن است که در سطح اتّحادیه اروپا، مقررات عمومی حفاظت از داده اروپا، به‌طور نسبی توانسته است شاخصه‌های الگوی مطلوب را با تجمیعی از احترام به‌حقوق اشخاص صاحب داده و اتّخاذ متناسب راهبردهای پیشگیرانه، کنترلی و سرکوبگر فراهم نماید. در نظام حقوقیِ ایران، با وجود تصویب قانون مدیریت داده‌ها و اطلاعات ملّی، کاستی‌هایی همچون عدم تصریح حقوق شخص موضوع داده، عدم جرم‌انگاریِ برخی اَعمال مجرمانه، مستثنی‌شدن برخی نهادها از شمولیت قانون مدیریت داده‌ها در سطح شاخصه‌های ماهوی؛ فقدان تفصیل در تعیین ضمانت اجراهای اداری، فقدان ساز و کارهای نظارتیِ کافی و پیش‌بینیِ نهادهای متعدد با وظایف متداخل در سطح شاخصه‌های راهبردی به‌چشم می‌خورند که علاوه بر ایجاد عدم توازن میان راهبردهای پیشگیرانه، کنترلی و سرکوبگرانه، موجب ایجاد چالش‌های جدّی در راه تحقق الگوی مطلوب نیز گردیده است.

مقدمه

در عصر تکنولوژی، ثبت و تبادل داده‌های شخصی جهت پیشبرد بسیاری از فعالیت‌های انسانی امری ضروری است. اهمیت داده (دیتا) به‌قدری است که از آن به‌عنوان طلای قرن ۲۱ یا نفت عصر دیجیتال یاد می‌کنند. یکی از چالش‌برانگیزترین دل‌مشغولی‌های امروز افراد در عصر دیجیتال، حفظ امنیت حریم خصوصی و داده‌های شخصی‌شان است؛ زیرا فضای مجازی درعین حال که به‌افراد اجازه می‌دهد در مقابل سایرین به‌صورت بی‌نام فعالیت کنند، برای دولت‌ها و شرکتهای عرضه‌کننده خدمات نیز امکان رصد داده‌هایی را فراهم می‌کند که درصورت پردازش، ممکن است دارای ارزش اقتصادی یا سیاسی باشند (Wachter, 2019: 127). در اقتصاد دیجیتالِ دنیای مدرن، این حقیقت است که افراد، با ارزش‌ترین داده‌های مربوط به‌خود را برای بهره‌مندی از خدمات اینترنتی به‌رایگان در اختیار شرکت‌ها و سازمان‌ها می‌گذارند و سپس همان شرکت‌ها و سازمان‌ها با استفاده از شیوه‌های فروش و بازاریابی، داده‌های باارزش و بعضاً غیررمزگذاری شده کاربران را به‌قیمت گزافی به‌خود آن‌ها می‌فروشند (Kortesniemi & Lehtiniemi, 2017: 54). در صورت نقض داده‌های شخصی پیامدهای منفی برای هزاران نفر از افراد آسیب دیده وجود دارد. سارقان هویت می‌توانند از افراد آسیب‌دیده باج‌گیری کنند؛ هویت آن‌ها را برای به‌دست آوردن کالاها و خدمات (مانند اسناد دولتی یا اعتبار) جعل کنند، کپی‌هایی از داده‌های آن‌ها را بفروشند یا حساب‌های ایمیلشان را اسپم کنند (Phua,2009: 13- 14). بنابراین، حق شهروندان است که از امنیت سایبری و حفاظت از داده‌های شخصی و حریم خصوصی داده برخوردار باشند. در این راستا، اتّحادیه اروپا، مقررات عمومی حفاظت از داده (GDPR) مشتمل بر ۱۱ فصل و ۹۹ ماده را در ۲۷ آوریل سال ۲۰۱۶ به‌تصویب رساند که جامع‌ترین بستر قانونی در خصوص حمایت از داده شخصی است و به‌استاندارد طلایی نسبت به‌حمایت از داده‌های شخصی معروف است (لطیف‌زاده و همکاران، ۱۴۰۱: ۳۲۶). این مقررات به‌طور مستقیم در تمام کشورهای عضو اتحادیهٔ اروپا لازم الاجراست؛ این بدان معناست که این مقررات نیاز به‌هیچ‌گونه اقدامی در قانون ملّی ندارد و مستقیماً توسط شهروندان، ادارات دولتی و سایر شرکت‌ها، نهادها و سازمان‌هایی که داده‌های شخصی را پردازش می‌کنند، باید رعایت شود (لطیف‌زاده و همکاران، ۱۴۰۰: ۴۴۳). بنابراین، الگوی اتحادیه اروپا، زمینه هماهنگ‌سازی بین الگوهای ملّی در کشورهای عضو اتحادیه را به‌وجود آورده است. در نظام حقوقیِ ایران نیز تصویب قانون مدیریت داده‌ها و اطلاعات ملّی و همچنین تهیه لایحه صیانت و حفاظت از داده‌های اشخاص را می‌توان به‌عنوان گام‌های ابتدایی در این راستا ارزیابی نمود. بر مبنای مجموع آنچه گفته شد، در این پژوهش بر آن هستیم تا با اتّخاذ رویکرد تطبیقی و بهره‌گیری از شیوه توصیفی – تحلیلی، به‌تبیین و مطالعه شاخص‌های الگوی مطلوب (اعم از شاخصه‌های ماهوی و راهبردی) در راستای حمایت و پیشگیری از جرایم علیه داده‌های شخصی در حقوق موضوعه ایران و اتّحادیه اروپا بپردازیم.

۱- شاخصه‌های ماهوی داده‌های شخصی

شاخصه‌های ماهوی داده‌های شخصی عبارتند از:

۱-۱- مفهوم داده

داده، نمایش قابل تفسیر مجدد اطلاعات به‌شیوه ساختارمندِ مناسب برای ارتباطات، تفسیر یا پردازش است (عطار و پروین، ۱۴۰۰: ۲۸۴). در حقوق اتّحادیه اروپا، تعریفی از داده به عمل نیامده و تنها در ماده ۴ مقررات عمومی حفاظت از داده اتحادیه، داده شخصی تعریف شده است. در نظام حقوقی ایران، بند (ث) ماده ۱ قانون مدیریت داده‌ها و اطلاعات ملّی مصوب ۱۴۰۱، داده را مجموعه‌ای از اعداد، حروف، علایم و نشانه‌هایی می‌داند که به‌صورت قراردادی در ابزارهای الکترونیکی یا رقومی یا توسط هر نوع فناوری جدید ارتباطاتی و اطلاعاتی تولید می‌شوند.

۱-۲- انواع داده

داده برخلاف تمامی منابع موجود در دنیا، موجودیتی است که دارای خواص تبدیل شوندگی و زایش است، یعنی داده‌ها به انفکاک و در امتزاج باهم، همواره منابع جدید دیگری را تولید می‌کنند که آن داده‌ها نیز به‌نوبه خود ارزش و قابلیت تفکیک و امتزاج با دیگر داده‌ها را دارند؛ بنابراین، داده، موجودیتی

زاینده است و از این بابت می‌تواند همواره به عنوان یک منبع و دارایی باارزش، مورد استفاده و استناد قرار گیرد؛ از این رو در قوانین، داده‌ها را در سطوح مختلفی دسته‌بندی نموده است؛ از دیگر تقسیم بندی‌های به‌عمل آمده از داده‌ها، می‌توان به‌تفکیک داده حاکمیتی از داده غیرحاکمیتی اشاره نمود. در ارتباط با داده حاکمیتی، بایستی گفت که حکومت‌ها، حجم گسترده‌ای از داده را تولید، نگهداری و مدیریت می‌کنند که دارای ارزش سیاسی، اقتصادی و اجتماعی بالایی است. طبیعتاً بخشی از این داده‌ها بنا به‌یکی از اقتضائات سه‌گانه امنیت ملی، اسرار تجاری و حریم خصوصی، انحصاراً در اختیار حاکمیت است و در اصطلاح به‌آن، داده حاکمیتی گفته می‌شود. درمقابل، هر داده‌ای که مشمول امتیازات و همچنین محدودیت‌های داده حاکمیتی نباشد را می‌توان داده غیرحاکمیتی قلمداد نمود. تقسیم داده بر مبنای نوع و هدف پردازش به‌عمل آمده نیز از دیگر تقسیم‌بندی‌های آن است و در این خصوص، داده‌ها را می‌توان به‌داده‌های پردازش شده بر مبنای رضایت، داده‌های پردازش شده بر مبنای ضرورت قراردادی، داده‌های پردازش شده به منظور تعهدات قانونی کنترل‌گر، داده‌های پردازش شده به منظور حفاظت از منافع حیاتی اشخاص، داده‌های پردازش شده برای نفع عمومی و انجام وظیفه رسمی و داده‌های پردازش شده برای منافع مشروع کنترل‌گر یا شخص ثالث اشاره نمود (انصاری، ۱۴۰۲: ۱۹۱-۱۴۵). یکی از تقسیم‌بندی‌های رایج از داده که در این پژوهش مورد استفاده فراوان قرار خواهد گرفت، تفکیک آن به‌شخصی و غیرشخصی است. داده‌های شخصی به‌هر نوع داده‌ای اطلاق می‌شود که بتواند یک فرد را به‌طور مستقیم و غیرمستقیم شناسایی کند؛ در مقابل، داده‌های غیرشخصی، هرگونه اطلاعاتی است که به‌فرد شناسایی شده یا قابل شناسایی، مرتبط نباشد (عطار و پروین، ۱۴۰۰: ۲۸۵). یکی از جامع‌ترین و کارآمدترین تعاریفی که از داده‌های شخصی شده است، تعریف اتحادیه اروپا در سند «جی دی پی آر» است که داده‌های شخصی را داده‌هایی تعریف می‌کند که می‌توان با استفاده از آنها، مستقیم و یا غیرمستقیم یک شخص را شناسایی کرد (قناد و شریف،۱۴۰۰: ۶). در بند (الف) ماده ۴ این مقرره، داده‌های شخصی این گونه تعریف شده است: «**هر اطلاعاتی که مرتبط با یک شخص حقیقیِ شناخته شده یا قابل شناسایی باشد**». در مجموع، منظور از داده شخصی، هرگونه اطلاعات مربوط به‌شخص حقیقیِ شناخته شده یا قابل شناسایی است که به‌طور مستقیم یا غیرمستقیم، به‌تنهایی یا با استفاده از شناسه‌ای خاص مانند نام، شماره شناسایی، اطلاعات مکان، شناسه آنلاین یا یک یا چند عامل خاص فیزیکی، فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی به‌شناسایی موضوع داده منجر می‌شود (قناد و علیقلی، ۱۳۹۹:۳۲۰). داده‌های شخصی، خود به‌دو دسته حساس و غیرحساس تقسیم می‌شوند. داده‌های شخصی حساس عبارتند از داده‌ها و اطلاعات مربوط به‌شخص حقیقی که مربوط به‌جنبه‌های کاملاً شخصی و فردی زندگی او از قبیل مشخصات نژادی، عقاید سیاسی و فلسفی، اطلاعات مربوط به سلامتیِ جسمی و روانی، زندگی جنسی، اطلاعات اقتصادی و ... می‌باشد (اصلانی، ۱۳۸۹: ۱۲۴). داده‌های غیرحساس نیز به هرآن‌چه غیر از داده‌های حساس نظیر شماره تلفن همراه، نشانی، نشانی پست‌الکترونیکی، تاریخ تولد و کد ملّی گفته می‌شود.

۱-۳- محرمانگی داده

محرمانگیِ داده به حق شهروندان در کنترل اطلاعات شخصی آنها و تصمیم در مورد (افشا یا عدم افشا آن) گفته می‌شود (رجبی، ۱۴۰۲: ۸). محرمانگیِ داده و حفاظت از آن، دو موضوع مرتبط با یکدیگر هستند. به‌طور کلّی، حفاظت از داده، ساز وکاری حقوقی است که محرمانگیِ آن را تضمین می‌کند. به‌بیان دیگر، محرمانگیِ داده تعریف می‌کند که چه کسی به‌داده دسترسی داشته باشد؛ درحالی که حفاظت از داده، ابزارها و سیاست‌هایی برای محدود کردن بالفعل دسترسی به داده‌ها وضع می‌کند. بر مبنای آنچه گفته شد، یکی از مهم‌ترین شاخصه‌های ماهوی در حمایت از داده‌های شخصی، حفاظت از محرمانگیِ آنهاست. در سطح اتحادیه اروپا، حمایت از محرمانگیِ داده‌های شخصی در عالی‌ترین سطح قانونگذاری یعنی منشور حقوق اساسی اتحادیه اروپا مورد توجّه قرار گرفته است. به‌موجب ماده ۸ منشور فوق - که عیناً در ماده ۱۶ معاهده عملکرد اتحادیه نیز ذکر شده است. «**هرکس حق حفاظت از داده‌های شخصی مربوط به خود**

را دارد ... چنین داده‌هایی باید به‌طور منصفانه، برای اهداف مشخص و براساس رضایت فرد و یا برخی مبانی قانونی دیگر که توسط قانون وضع شده‌اند، پردازش شوند ...». قانون اساسی ایران نیز در اصول ۲۲، ۲۳، ۲۵ و ۳۹، به‌انحا مختلف از حریم خصوصی حمایت کرده است؛ بنابراین قانون اساسی ایران، صراحت بالایی در حمایت از داده‌های شخصی افراد دارد (رجبی، ۱۴۰۲: ۹).

۱-۴- حقوق افراد نسبت به داده

به‌موجب مقررات عمومی حفاظت از داده اتحادیه اروپا، شخص موضوع داده، حقوق مختلفی دارد که در مواد ۱۲ تا ۲۲ بیان شده و متضمن حمایت‌های جامع برای شخص موضوع داده است. از مهمترین این حقوق، می‌توان به‌حق دریافت اطلاعات در مورد پردازش داده‌های شخصی، حق دسترسی به‌داده‌های شخصیِ مربوط به شخص موضوع داده، حق درخواست تصحیح داده‌های شخصی نادرست یا ناقص، حق حذف دادههای شخصی، حق درخواست محدودیت پردازش، حق انتقال داده، حق اعتراض به‌پردازش و حق عدم قرار گرفتن در معرض تصمیمات خودکار اشاره نمود (لطیف‌زاده و همکاران، ۱۴۰۲: ۹۸۳). نکته دیگر که بایستی درخصوص مقررات عمومیِ حفاظت از داده در اتّحادیه اروپا بایستی توجّه داشت، این است که در این مقررات، استثنائاتی از قبیل امنیت ملی پیش‌بینی شده است که براساس آن‌ها، پردازش دادههای شخصی بدون اجازه صریح شخص موضوع داده نیز امکان‌پذیر است (قناد و شریف، ۱۴۰۲: ۱۷).

در حقوق موضوعه ایران، حقوق اشخاص نسبت به‌داده‌های شخصی‌شان، به‌شکلهای مختلف (صریح و ضمنی) مورد حمایت قرار گرفته و قانونگذار، اَعمال مختلفی همچون دسترسی، ذخیره‌سازی، پردازش، انتشار، توزیع و انتقال را در ارتباط با داده‌های شخصی مدنظر قرار داده و مبادرت به‌جرم‌انگاریِ آن‌ها نموده است؛ در حالی که گردآوریِ غیرمجاز داده‌های شخصی را جرم‌انگاری نکرده و این موضوع و به‌تبع آن، سایر تکالیف پردازشگر در این خصوص، مشمول حمایت کیفری نمی‌گردد (محسنی، ۱۳۸۹: ۵۷۰؛ حیدری و جعفری، ۱۳۹۹: ۶۳). با نگاهی به‌قانون جرایم رایانه‌ای نیز مشخص می‌شود که اَعمال مرتبط با پردازش غیرمجاز داده‌های شخصی تنها در ماده ۸ (ماده ۷۳۶ قانون مجازات اسلامی) مورد توجّه قانونگذار واقع گردیده است. علیرغم اشاره قانونگذار به‌سایر اَعمال مجرمانه مرتبط با داده‌های شخصی همچون حذف، تخریب و یا مختل کردن در ماده مزبور، دسترسی غیرمجاز به داده‌های شخصی دیگری به‌طور عام مورد حمایت کیفری قانونگذار واقع نشده و تنها دسترسی غیرمجاز به‌داده‌های محافظت شده توسط تدابیر امنیتی (ماده ۱) و دسترسی غیرمجاز به‌داده‌های سریِ درحال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی (ماده ۳) مستوجب ضمانت اجرای کیفری، شناخته شده‌اند. انتخاب عنوان مجرمانه «دسترسی غیرمجاز به‌سیستم‌های پردازش خودکار» برای عمل مزبور در قانون جزای فرانسه و تقسیم دسترسی غیرمجاز رایانه‌ای به «دسترسی ساده» و «دسترسی به قصد ارتکاب جرایم دیگر» و تشدید مجازات برای مرتکبان شق أخیر در حقوق انگلستان، از ابتکارات جالب قانونگذاران آن دو کشور است که در کشور ما نیز قابل الگوگیری است (محمّد نسل و همکاران، ۱۳۹۹: ۱۰۵). علاوه بر موارد گفته شده، عدم جرم‌انگاریِ اَعمالی همچون فراهم نمودن موجبات دسترسی غیرمجاز به داده‌های شخصی و پردازش غیرمجاز آنها و همچنین فروش داده‌های شخصیِ متعلّق به‌دیگری (علاوه بر فروش یا انتشار یا در دسترس قراردادن گذر واژه متعلق به دیگری در ماده ۲۵) از جانب قانونگذار، به‌شدت قابل تأمّل و انتقاد به نظر می‌رسد. با تصویب قانون جدید آیین دادرسی کیفری، حمایت از داده‌ها نقشی پررنگ‌تر به‌خود گرفت. تشکیل «مرکز ملّی داده‌های قوه قضائیه» (ماده ۶۵۰)، وظیفه قوه قضاییه مبنی بر فراهم آوردن تمهیدات فنی و قانونی لازم برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان (ماده ۶۵۸) و همچنین تعیین ضمانت اجرا به‌منظور مقابله با نقض عمدی و غیرعمدی حریم داده‌های شخصی (مادتین ۶۶۰ و ۶۶۱) از مهم‌ترین مصادیق حمایت از داده‌ها در قانون مزبور است. آخرین گام برداشته‌شده در سطح قانونگذاری به منظور حمایت از داده‌های شخصی را می‌توان در تصویب قانون مدیریت داده‌ها و اطلاعات ملّی در سال ۱۴۰۱ ملاحظه نمود. هدف کلّی قانون مذکور، یکپارچه‌سازیِ تمام داده‌ها، منسجم

کردن اطلاعات و مدیریت دولت بر اطلاعات دستگاه‌های مختلف است. در ارتباط با گستره دستگاه‌ها و نهادهای مشمول این قانون که در ماده ۱ آمده است، منوط شدن شمول آن درخصوص نهادها، مؤسسات، تشکیلات و سازمان‌های زیرنظر مقام رهبری به موجب تبصره آن، محلّ تأمّل و انتقاد به‌نظر می‌رسد؛ چرا که به‌طور مثال، حفاظت از داده‌های شخصی در سازمان صدا و سیما – که تحت نظر رهبری است – از اهمیت بالایی برخوردار است. نکته دیگر اینکه برخلاف مقررات عمومیِ حفاظت از داده در اتّحادیه اروپا، در قانون مدیریت داده‌ها و اطلاعات ملّی، تصریحی در ارتباط با حقوق مختلف شخص موضوع داده دیده نمی‌شود و تنها در ماده ۵، به‌تکلیف مشمولین قانون مبنی بر اِعمال و اجرای سیاست‌ها و نظامات مصوب شورای عالی فضای مجازی و مصوبات کارگروه تعامل‌پذیری دولت الکترونیکی اشاره شده است.

۲- شاخصه‌های راهبردی داده‌های شخصی

رویکرد مقابله با پردازش غیرمجاز داده‌ها در اتحادیه اروپا بر سه راهبرد پیشگیری، کنترل و سرکوب اتکا دارد. با اقتباس از این رویکرد، باید گفت که سیاست جناییِ مطلوب در زمینه حمایت از داده‌های شخصی، باید بر این سه راهبرد، مبتنی باشد؛ این سیاست جنایی همچنین در مقام پاسخ‌دهی به پردازش غیرمجاز داده‌ها، دو رویکرد تنظیم‌گریِ اداری و سرکوب کیفری را با هم هماهنگ می‌سازد.

۲-۱- راهبرد پیشگیری

پیشگیری یکی از شاخصه‌های مهم راهبردی در حمایت از داده‌های شخصی است. شیوه‌های مختلف راهبرد پیشگیری، عبارتند از: آگاه‌سازی، حفاظت از داده‌های اشخاص و خود تنظیم‌گری.

۲-۱-۱- آگاه‌سازی

«آگاه‌سازی به‌عنوان یکی از وظایف اولیه کمیسیون ملّی انفورماتیک و آزادی فرانسه، در بند یک ماده ۱۱ قانون حمایت از داده این کشور آمده است؛ بدین شرح که آگاه سازیِ اشخاص از حقوق ذکرشده آنها طبق قانون حمایت از داده‌های شخصی فرانسه باید صورت گیرد. این وظیفه با اطلاع‌رسانی به شهروندان و کنترل‌کننده‌های داده انجام می‌پذیرد. گفتنی است کمیسیون، این وظیفه را با شرکت در کنفرانس‌ها، سمینارها و کارگاه‌های آموزشی با موضوعاتی نظیر اطلاع‌رسانی به شهروندان اجرایی می‌کند» (زارعیان، ۱۳۹۹: ۵۱). اطلاع‌رسانی توسط نهادهای نظارتیِ مستقل در قالب شیوه‌هایی همچون افزایش آگاهی عمومی و فهم ریسک‌ها به‌اشخاص موضوع داده، ارائه توصیه‌های لازم براساس قانون کشور توسط مؤسسات و ارگان‌های مدیریتی و قانونی، افزایش آگاهی کنترل‌گرها و پردازشگرها از تعهدات مربوط به‌خود از مهمترین شیوه‌های آگاه‌سازی هستند که در ماده ۵۷ مقررات عمومی حفاظت از داده‌های اروپا مورد اشاره قرار گرفته‌اند. در نظام حقوقی ایران، می‌توان از مرکز ملّی فضای مجازی، آپا و مرکز ماهر به‌عنوان نهادهایی که بخش قابل توجّهی از کارکرد آنها در ارتباط با راهبرد پیشگیری از طریق آگاهی‌رسانی است، نام برد. یکی از وظایف و اختیارات «مرکز ملّی فضای مجازی»، ارزیابی در همه ابعاد فضای مجازی کشور در چارچوب مصوبات شورای عالی فضای مجازی می‌باشد؛ طبیعی است که حریم خصوصی نیز یکی از ابعاد فضای مجازی و داده‌های شخصی، ضمن آن معنا پیدا می‌کند؛ بنابراین نقش مرکز در حمایت از داده‌های شخصی، از حیث آگاهی‌رسانی، نقشی پیشگیرانه است. «آپا» به‌شهروندان هشدارهایی برای حفاظت از اطلاعات‌شان در فضای سایبر می‌دهد (وطنی و اسدی، ۱۳۹۵: ۱۱۸-۱۱۷)؛ بنابراین عمده‌ترین کارکرد آن را می‌توان دربُعد پیشگیرانه و عمدتاً آگاه سازی ملاحظه نمود. مرکز ماهر نیز براساس چارچوب‌های قانونی و مأموریت‌های محوله، حوادث مختلف فضای مجازی کشور را کشف و یا از افرادی که به‌صورت مسؤولانه و صادقانه اطلاع‌رسانی می‌کنند؛ دریافت می‌نماید. تمام این موارد، پس از بررسی‌های فنی جهت راستی‌آزمایی و استخراج شواهد و راهکار مقابله براساس چارچوب‌های قانونی، به‌صورت محرمانه به صاحبان سرویس‌ها و داده‌ها اطلاع‌رسانی می‌شود؛ مرکز همچنین جمع‌بندی و تحلیل خود درخصوص حوادث را صرفاً برای مقامات مسؤول ارسال می‌کند؛ بنابراین چون به ارائه هشدارها، اعلانات، مخاطرات

و ضعف‌های سامـانه‌ها در سطـح ملّی مبـادرت می‌ورزد، دارای کارکرد پیشگیری از طریق آگاه‌سازی است.

۲-۱-۲- حفاظت از داده‌های اشخاص

درخصوص حفاظت از داده‌ها می‌توان به ماده ۸۷ مقررات عمومی حفاظت از داده‌های شخصی اروپا درباره نظارت بر پردازش شماره شناسایی ملّی در این زمینه، اشاره داشت که تصریح می‌کند قانون، باید شرایط خاصی را به‌منظور پردازش شماره شناسایی ملّی یا هرگونه کد شناسایی فردی در رابطه با کاربردهای عمومی تعیین نماید. در واقع از شماره شناسایی ملّی فقط تحت حفاظت و تدابیر مناسب برای حقوق و آزادی شخص موضوع داده، استفاده شود. ماده ۸۸ نیز به‌پردازش داده‌های شخصی در حوزه استخدام، پرداخته است. طبق این ماده باید براساس قانون یا توافق‌های جمعی، قوانین خاص‌تری تصویب شود که حمایت و حفاظت حقوق و آزادی‌های مربوط به پردازش داده‌هایِ شخصی کارکنان در زمینه استخدام را تضمین کند؛ این قواعد باید شامل اقدامات مناسب و خاص برای حفاظت از کرامت انسانی موضوع داده، منافع مشروع و حقوق اساسی با توجه به‌شفافیت پردازش، انتقال داده‌های شخصی بین گروهی از شرکت‌ها یا گروهی از شرکت‌های فعال در فعالیت‌های اقتصادی مشترک و سیستم‌های نظارتی در محل کار باشند. در نظام حقوقی ایران، مرکز ماهر، مهم‌ترین نهاد متولّی در زمینه راهبردهای پیشگیرانه از طریق حفاظت از داده‌های اشخاص بوده و این امر در اهداف و مأموریت‌های آن نیز درج گردیده است.

۲-۱-۳- خود تنظیم‌گری

خود تنظیم‌گری نیز شیوه‌ای جهت حمایت از داده است، «باگوت در سال ۱۹۸۹ در مقاله‌ای، خودتنظیمی را ترتیبی نهادی تعریف کرد که از طریق آن، یک سازمان، استانداردهای رفتاریِ اعضای خود را تعیین و تنظیم می‌کند. از این منظر، جوهره خود تنظیمی را می‌توان نوعی حکمرانیِ جمعی، شرکتی و خصوصی تلقی کرد. در تعریفی دیگر، خودتنظیمی یعنی سپردن وظایف سیاست عمومی به‌بازیگران بخش خصوصی در شکلی سازمانی و ساختارمند به‌هدف تنظیم بازار از سوی مشارکت‌کنندگان و بازیگران. به‌تعبیر ترودل، خودتنظیمی هنجارهایی هست که به‌صورت داوطلبانه توسط افرادی که در آن فعالیت مشارکت می‌کنند، ساخته شده و پذیرفته می‌شوند. از این منظر، خودتنظیمی مفهومی است که به‌موجب آن، گروه‌های خصوصی به‌ابتکار خـودشان تصمیماتی را اتّخاذ می‌کنند که رفتارهایشان را محدود می‌کند و تنها به‌قوانین کلّی وضع شده توسط دولت ملزم نباشند» (رهایی و متاجی، ۱۴۰۱: ۲۱۳۲). در نظام حقوقی ایران، قانون مدیریت داده‌ها و اطلاعات ملّی مصوب ۱۴۰۱ در ماده ۳ خود، نهادی موسوم به «کارگروه تعامل‌پذیری دولت الکترونیکی» را به‌موجب مصوب شورای عالی فضای مجازی، پیش‌بینی کرده و آن را موظّف نموده است که در تصمیم گیری‌های خود (به‌استثنای امر قضا) نسبت به‌اِعمال سیاست‌ها و راهبردهای کلان و نظارت و مدیریت بر نحوه نگهداری، پردازش، دسترسی، یکپارچه‌سازی، امنیت و بویژه تبادل و به‌اشتراک‌گذاری داده‌ها و اطلاعات موضوع قانون مزبور اقدام نماید. علاوه بر این، همانگونه که پیشتر نیز اشاره شد، قانون مزبور، ارائه دهندگان خدمات ذیلِ تنظیم گران بخشی را نیز به‌موجب بند (ب) ماده ۱ پیش‌بینی نموده است که به‌موجب تبصره ماده ۵، ملزم به‌اجرای مصوبات کارگروه فوق‌الذکر و اِعمال سیاست‌ها و نظامات این قانون از طریق درج یا الحاق در پروانه یا مجوزهای فعالیت، تأسیس، موافقت اصولی یا قرارداد ارائه دهندگان خدمات ذیلِ خود هستند. علاوه بر کارگروه مورد اشاره، سازمان فناوری اطلاعات ایران و اتحادیه کشوری کسب و کارهای مجازی نیز دارای وظایف مشخص در حیطه راهبردهای پیشگیرانه از نوع خودتنظیم‌گری هستند. سازمان فناوری اطلاعات ایران، در راستای اجرای اصل ۴۴ قانون اساسی مبنی بر آزادسازی و خصوصی‌سازی فعالیت می‌نمـاید. تدوین و بروزرسانی شاخصه‌های بومی با توجه به‌شاخصه‌ها و مدل‌های بین المللی، ارزیابی فعالیت‌های حوزه فاوا، تدوین ضوابط، مقررات و نظام‌های کیفیت در حوزه فناوری اطلاعات و تدوین و پایش استانداردهای مربوطه با هماهنگی مراجع ذی‌ربط از جمله وظایف این نهاد است؛ بنابراین، فعالیت و وظیفه این نهاد عمدتاً دارای کارکرد پیشگیرانه از نوع خود تنظیم‌گری است و شامل تعیین معیارها و شاخصه‌های بومی و تدوین و پایش استانداردهای مربوطه در حوزه داده‌های شخصی نیز

می‌شود. اتحادیه کشوری کسب و کارهای مجازی نیز به‌موجب آیین‌نامه اجرایی آن، جهت چگونگی صدور مجوز و نحوه نظارت بر فعالیت افراد صنفی در فضای مجازی و بازاریابیِ شبکه‌ای (موضوع مواد ۲، ۱۲ و تبصره ماده ۸۷ قانون نظام صنفی) فعالیت می‌کند.

۲-۲- راهبرد کنترل

همه سازمان‌ها (اعم از خصوصی یا دولتی) مستقل از اندازه و بخش فعالیت‌شان، باید یک افسر به‌منظور کنترل حفاظت از داده‌های شخصی را تعیین کنند که ممکن است یک شخص حقیقی یا حقوقی، داخلی یا خارجی برای سازمان متقاضی باشد، خواه مشترک با دیگران باشد یا نباشد؛ بر این مبنا، کنترل، یکی از مهمترین شاخصه‌های راهبردی در حمایت از داده‌های شخصی است. بدیهی است، کنترل (نظارت) به‌نهاد متولی این امر نیاز دارد. نهادی نظارتی که براساس قانون تأسیس شود. با توجه به‌ماده ۵۱ الی ۵۴ بخش اول از فصل ششم مقررات حفاظت از داده‌های شخصی اروپا، نهاد نظارتی باید استقلال کامل و آزادی در اجرای وظایف و اِعمال قدرت طبق مقررات جامع تدوین شده داشته باشد. با اقتباس از بند ۱ و ۲ ماده ۵۱، یکی از راه‌های کنترلِ نقض داده‌های شخصی پس از تدوین مقررات جامع و کامل در رابطه با داده‌های شخصی، ایجاد یک نهاد نظارتیِ مستقل با مسؤولیت تنظیم و نظارت صحیح بر کاربرد این مقررات می‌باشد. در نظام حقوقیِ ایران، به‌موجب ماده ۲۵ لایحه حمایت از داده و حریم خصوصی، کمیسیون‌های استانی حمایت از داده‌ها باید در محلّ استانداری تشکیل شود تا بر اجرای صحیح مقررات تدوین شده و رسیدگی به‌شکایات راجع به تخلّف از مقررات این قانون در سراسر ایران سهمی داشته باشد. برمبنای قوانین مصوب موجود نیز مسؤولیت نظارت بر نحوه نگهداری، پردازش، دسترسی، یکپارچه‌سازی، امنیت و به‌ویژه تبادل و به‌اشتراک‌گذاری داده‌ها و اطلاعات، به‌موجب ماده ۳ قانون مدیریت داده‌ها و اطلاعات ملّی مصوب ۱۴۰۱، برعهده نهادی موسوم به «کارگروه تعامل‌پذیری دولت الکترونیکی» قرار گرفته است که ترکیب اعضا و نحوه اداره آن توسط شورای عالی فضای مجازی تعیین شده (تبصره ۱)؛ و مکلف است گزارش‌های عملکرد دستگاه‌ها و نهادهای مشمول این قانون را هر سه ماه یک بار به‌مجلس شورای اسلامی و شورای عالی فضای مجازی ارائه نماید (تبصره ۲). نظارت بر اجرای مقررات، بازرسی و بررسی شکایت‌ها، شیوه‌های کنترل هستند. علاوه بر کارگروه مورد اشاره، نهادهای مختلفی همچون مرکز ملّی فضای مجازی، اتّحادیه کشوری کسب و کارهای مجازی، سازمان تنظیم مقررات و ارتباطات رادیویی، مرکز ماهر، بخش ستادی پلیس‌فتا و دادسرای جرایم رایانه‌ای نیز به‌انحا و درجات مختلف، متصدی راهبردهای کنترلی هستند که در ادامه به آنها خواهیم پرداخت. نظارت بر اجرای مقررات، بازرسی و بررسی شکایت‌ها، مهم‌ترین شیوه‌های راهبرد کنترل هستند.

۲-۲-۱- نظارت بر اجرای مقررات

به‌طور کلّی، نظارت، به‌دسترسی مرجع ناظر به‌سامانه‌های پذیرنده داده نیاز دارد؛ این مسأله در ماده ۵۸ مقررات عمومی حفاظت از داده‌های شخصی اروپا تصریح شده است و به‌موجب آن اختیارات (قدرت اجرایی) نهاد نظارتی شامل موارد زیر هستند: (الف) دستور به‌کنترل‌گر و پردازشگر (یا در صورت لزوم نمایندگان آن‌ها)، برای ارائه اطلاعات لازم برای انجام وظایف خود؛ (ب) انجام تحقیقات به‌شکل ارزیابی حفاظت داده؛ (ج) انجام بازنگری در مورد گواهی‌های صادرشده طبق بند ۷ ماده ۴۲؛ (د) هشدار به‌کنترل‌گر یا پردازش‌گر در رابطه با نقض این مقررات؛ (ه) دریافت تمامی اطلاعات شخصی و تمامی اطلاعات لازم برای انجام وظایف خود از کنترل‌گر و پردازشگر؛ (و) دسترسی به‌تمامی قلمروی کار کنترل‌گر و پردازشگر، از جمله تجهیزات و ابزار پردازش داده، مطابق با قانون. همچنین طبق ماده ۵۷ مقررات عمومی حفاظت از داده‌های شخصی اروپا، نهاد نظارتی باید وظایف زیر را انجام دهد: نظارت و اجرای مقررات جامع، همکاری با دیگر نهادهای نظارتی با نگاهی بر تضمین سازگاری کاربرد و اجرای مقررات وضع شده. در نظام حقوقی ایران، مرکز ملّی فضای مجازی (به‌دلیل دارا بودن حق نظارت بر برخی مصوبات) و سازمان تنظیم مقررات و ارتباطات رادیویی (از حیث نظارت بر فعالیت‌های پستی و فعالیت‌های فناوری اطلاعات و ارتباطات) مهم‌ترین نهادهای متولّی در زمینه راهبردهای کنترلی از طریق نظارت بر اجرای مقررات هستند.

۲-۲-۲- بازرسی

در ارتباط با بازرسی، به‌موجب ماده ۴۴ قانون حمایت از داده‌های شخصی فرانسه، «بازرسی یکی از مهم‌ترین ابزارهای کمیسیون برای نظارت بر حسن اجرای این قانون است. بر همین اساس اعضای کمیسیون و مأموران آن با مجوز کمیسیون، اختیار دارند تا مکان‌ها، تجهیزات و ساختمان‌های پردازش‌کنندگان داده را از ساعت شش صبح تا نه شب بازرسی کنند. بدیهی است این نظارت، تنها شامل مکان‌های عمومی شده و مکان‌های خصوصی را در بر نمی‌گیرد؛ شایان ذکر است که در هر مورد بازرسی میدانی، دادستان عمومی بخش مورد بازرسی، باید در جریان قرار گیرد؛ همچنین ضروری است مأموران کمیسیون در صورت کشف جرم، دادستانی را همراه با دلایل و مدارک مطلع سازند. در صورت ممانعت پردازش‌کنندگان داده از ورود و بازرسی مأموران کمیسیون، عدم ارائه اطلاعات مورد نیاز مأموران، تخریب یا نابودی اطلاعات و یا فریب مأموران، به‌مجازات حبس و جزای نقدی تا ۱۵ هزار یورو محکوم خواهند شد» (زارعیان، ۱۳۹۹: ۵۵ -۵۴). در نظام حقوقی ایران، به موجب تبصره ۲ ماده ۱۰ قانون مدیریت داده‌ها و اطلاعات ملّی مصوب ۱۴۰۱، دستگاه‌ها و نهادهای مشمول این قانون حسب اعلام کارگروه تعامل‌پذیری دولت الکترونیکی، ضمن بروزرسانی داده‌ها و اطلاعات خود، موظّف به‌همکاری با متولّیان پایگاه‌های داده‌ها و اطلاعات پایه می‌باشند؛ ضمانت اجرای عدم همکاری مزبور نیز به‌موجب ماده ۹، مجازات انفصال از خدمت به‌مدت شش ماه تا پنج سال یا حبس تعزیری به‌مدت نود و یک روز تا شش ماه تعیین شده است؛ علاوه بر کارگروه مورد اشاره، مرکز ماهر (از حیث رسیدگی فوری به‌حوادث فضای مجازی کشور براساس درخواست سازمانهای مختلف)؛ اتحادیه کشوری کسب و کارهای مجازی (از حیث بازرسی و نظارت بر فعالیت افراد صنفی در فضای مجازی و بازاریابیِ شبکه‌ایِ موضوع مواد ۲، ۱۲ و تبصره ماده ۸۷ قانون نظام صنفی)، بخش ستادیِ پلیس فتا (از حیث رصد سایت‌ها یا درگاه‌های الکترونیک) و دادسرای جرایم رایانه‌ای (از حیث رسیدگی به شکایات مطروحه) نیز به درجات مختلف متولّی راهبردهای کنترلی از طریق انجام بازرسی و نظارت هستند.

۲-۲-۳- بررسی شکایات

بررسی شکایت‌های تسلیم‌شده توسط شخص موضوع داده، باید توسط نهاد نظارتی صورت گیرد. ماده ۷۷ مقررات عمومی حفاظت از داده‌های شخصی اروپا درباره حق تسلیم شکایت به نهاد نظارتی تصریح می‌کند که موضوع داده، باید حق تسلیم شکایت به‌نهاد نظارتی واقع در کشور و محل سکونت خود، محل کار یا محل وقوع پردازش غیرمجاز داده‌های شخصی، داشته باشد. مرجع نظارتی که شکایت نزد آن تسلیم شده است باید شاکی را از پیشرفت و نتیجه شکایت از جمله امکان رسیدگی قضایی بر اساس همچنین به‌موجب بخش C بند ۲ ماده ۱۱ قانون حمایت از داده‌های شخصی فرانسه، کمیسیون، ملزم شده است که کلیه ادعاها، درخواست‌ها و شکایت‌های مربوط به‌پردازش غیرمجاز داده شخصی را دریافت و متقاضی آن‌ها را از اقدام‌های صورت‌گرفته در این مورد مطلع کند. البته شایان توجه است که نهاد نظارتی فقط مرجع دریافت شکایت‌ها و تهیه گزارش نسبت به شکایت واصل شده است، لیکن رسیدگی به‌شکایت‌ها خود در دو بخش تخلفات و جرایم قابل بحث است (زارعیان، ۱۳۹۹: ۵۴). که در ادامه مقاله بررسی خواهد شد. در نظام حقوقیِ ایران، دادسرای جرایم رایانه‌ای مهم‌ترین نهادی است که متولّی راهبردهای کنترلی از طریق بررسی شکایات مطروحه است. نهاد مزبور، مرجعی قضایی است که در دعاوی مربوط به جرایم رایانه‌ای، صالح است. قانونگذار در مواد ۲۸ تا ۳۱ قانون جرایم رایانه‌ای، صلاحیت این نهاد در رسیدگی به جرایم مزبور را پیش‌بینی کرده است، یکی از این جرایم، جرایمی است که موضوع آنها داده‌های شخصی است، این جرایم می‌توانند شامل دسترسی غیرمجاز به داده‌های شخصی، جعل، سرقت و ... باشند.

۲-۳- راهبرد سرکوب

سرکوب، واکنش تنبیه‌گرایانه‌ای است که بر مرتکب پدیده مجرمانه (اعم از جرم، تخلّف و انحراف) تحمیل می‌گردد؛ بالطّبع «محدودیت در حقوق» از مفهوم سرکوب، غیرقابل تفکیک بوده و حتی می‌توان مدعی شد که مشخصّه اصلی

آن نیز می‌باشد (نجفی ابرندآبادی، ۱۳۸۴: ۱۲۶). سرکوب شامل دو بخش کیفری و اداری – انتظامی است. بدیهی است مجازات در مقابل جرم، در بخش سرکوب کیفری قرار می‌گیرد و بخش اداری – انتظامی در مقابل تخلّفات ناقضان حریم داده‌های شخصی قرار می‌گیرند. در تفاوت تخلّف با جرم باید گفت که تخلّف، متضمن نقض ارزش و هنجاری است که میان قشر خاصی مورد شناسایی واقع گردیده است (یوسفی و مهدوی ثابت، ۱۳۹۴: ۳۶)؛ لیکن جرم، متضمن نقض ارزش و هنجاری است که میان عموم جامعه، مورد احترام و ارزش‌گذاری است. همان طور که بیان شد، سرکوب شامل دو بخش اداری و کیفری است که اکنون در دو بخش مجزا بررسی خواهد شد.

۲-۳-۱- سرکوب اداری

اِعمال مجازات در برابر جرایم اداری ضمن ماده ۸۳ مقررات عمومی حفاظت از داده‌های شخصی اروپا بیان شده است و در بند ۲ ماده مذکور، تصریح شده است که هنگام تصمیم‌گیری درمورد اعمال جرایم اداری و میزان آن در هر مورد، باید موارد زیر مورد توجه قرار گیرد: ماهیت، میزان و مدت نقض مقررات با درنظر گرفتن دامنه یا اهداف پردازش مربوطه و همچنین تعداد اشخاص موضوع داده و سطح خسارتی که به‌آن ها وارد شده، ماهیت عمدی یا سهوی نقض مقررات، هر اقدامی که توسط کنترل‌گر یا پردازشگر برای کاهش خسارت وارد شده به اشخاص موضوع داده انجام شود، میزان مسؤولیت‌پذیری کنترل‌گر و پردازشگر با در نظرگرفتن اقدامات فنی و سازمانی اجرا شده توسط آنها طبق مواد ۲۵ و ۳۲، هرگونه تخلف قبلی مرتبط توسط کنترل کننده یا پردازشگر؛ میزان همکاری به منظور رفع تخلف و کاهش اثرات نامطلوب تخلف؛ دسته بندی داده‌های شخصی نقض شده؛ مشخص کردن نحوه شناسایی نقض مقررات توسط نهاد نظارتی به ویژه نحوه اطلاع رسانی نقض داده از سوی کنترلگر یا پردازشگر، هماهنگی با اقدامات مذکور در ماده ۵۸ (۲) که قبلاً در مورد کنترلگر یا پردازشگر ذکر شده، پایبندی به‌کدهای اجرایی طبق ماده ۴۰ یا سازوکارهای تأیید شده صدور گواهینامه طبق ماده ۴۲، هرگونه عامل تشدیدکننده یا تخفیف دهنده دیگری که بتوان برای شرایط موردنظر اعمال کرد؛ همانند منافع مالی کسب شده یا خسارت‌های ناشی از تخلف. با وجود تفصیل مقررات عمومیِ حفاظت از داده‌های شخصی اروپا در ارتباط با تعیین ضمانت اجرای اداری درقبال نقض حریم داده‌های شخصی، این موضوع در حقوق ایران و قانون مدیریت داده‌ها و اطلاعات ملّی، مسکوت مانده و تنها در ماده ۹ قانون مزبور، ضمانت اجرای کیفریِ انفصال از خدمت به‌مدت شش ماه تا پنج سال یا حبس تعزیری به‌مدت نود و یک روز تا شش ماه برای متخلّف یا اخلال‌کننده در پردازش و تبادل یا مستنکف از اجرای این قانون، پیش‌بینی شده است. به‌بیان دیگر، قانونگذار ایرانی علاوه بر عدم تفصیل در تعیین مجازات اداری، در قبال تخلّف اداریِ منجر به‌نقض حریم داده‌های شخصی نیز مبادرت به تعیین ضمانت اجرای کیفری نموده است. در ارتباط با نهاد یا نهادهای متولّی راهبرد سرکوب اداری در حقوق ایران نیز، اتحادیه کشوری کسب و کارهای مجازی از مهم‌ترین آن‌هاست که با اِعمال ضمانت اجرای تعلیق فعالیت و نماد، می‌تواند مبادرت به‌اِعمال سرکـوب اداری درقبال پردازش غیرمجاز داده‌ها در کسب و کارهای مجازی نماید.

۲-۳-۲- سرکوب کیفری

سرکوب در بخش جزایی در سه بخش جرم‌انگاری، تعیین کیفر و اِعمال مجازات قابل بررسی است. از آنجا که در بحث شاخصه‌های ماهوی، از جرم‌انگاریِ اَعمال مرتبط با داده‌های شخصی سخن گفتیم، در این قسمت از ذکر دوباره آنها خودداری و به‌حیطه تعیین کیفر و اِعمال مجازات می‌پردازیم. پیش از ورود به‌بحث، یادآوری یک نکته الزامی است و آن اینکه حقوق کیفری نمی‌تواند اولین گزینه برای ایجاد نظم باشد؛ بلکه به‌عنوان آخرین پیشنهاد است که به‌کنترل اَعمال افراد می‌پردازد (معظّمی و همکاران، ۱۳۹۶: ۱۷۹)؛ بنابراین توسّل به‌سرکوب کیفری وقتی مجاز خواهد بود که دیگر تدابیر و ساز و کارهای موجود (پیشگیری، کنترل و سرکوب اداری) کافی و یا نتیجه‌بخش نبوده و در واقع، چاره‌ای به‌جز توسّل به ابزار کیفری وجود نداشته باشد. در حیطه تعیین کیفر و اِعمال آن، بدیهی است که مجازات، باید با جرم تناسب داشته باشد و جرایم مرتبط با داده‌های شخصی، مجازات متناسب را می‌طلبد. برخی از این مجازات‌ها در قالب مجازات

اداری اِعمال می‌شوند، ولی یک الگوی مطلوب باید از خلط مجازات اداری با مجازات در مقابل جرم به‌معنای أخص جلوگیری کند؛ بنابراین، اقسام کیفر در این مورد عبارت از مجازات سالب حق، مجازات مالی، مجازات سالب آزادی هستند که بسته به‌نوع جرم باید اِعمال شود. به‌نظر می‌رسد آنجا که پردازش غیرمجاز داده‌های شخصی، وسیله یا مقدمه ارتکاب جرم دیگر باشد، مجازات سالب حق و هنگامی که عمل مزبور به‌عنوان یک هدف و غایت مجرمانه انجام پذیرد، مجازات مالی و زمانی که دامنه عمل مجرمانه فوق، فراتر از اضرار به‌شخص معین بوده و گستره وسیعی از بزه دیدگان را در بربگیرد، مجازات سالب آزادی واجد کارآیی بیشتری خواهند بود. مبرهن است، این مجازات مانع از احقاق حق بزه‌دیده از جنبه خصوصی جرم نیست.

در ارتباط با نهادهای متولّی راهبرد سرکوب کیفری درقبال نقض داده‌های شخصی در حقوق ایران، دادسرای جـرایم رایانه‌ای (که پیشتر و در راهبرد سرکوب اداری نیز به‌آن اشاره شد) و همچنین کارگروه تعیین مصادیق مجرمانه از مهم‌ترین آن‌ها هستند. کارگروه اخیرالذّکر، بر اساس ماده ۲۲ قانون جرایم رایانه‌ای تشکیل و مسؤولیت نظارت بر فضای مجازی و پالایش تارنماهای حاوی محتوای مجرمانه و رسیدگی به شکایات مردمی را به‌عهده دارد. بموجب ماده ۲۱ قانون جرایم رایانه‌ای، «ارائه‌دهندگان خدمات دسترسی موظف هستند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه مزبور، محتوای مجرمانه (اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای به‌کار می‌رود) را پالایش (فیلتر) کنند». همچنین ماده ۲۳ قانون مورد اشاره، «ارایه‌دهندگان خدمات میزبانی موظّفند به‌محض دریافت دستور کارگروه (کمیته) تعیین مصادیق مذکور در مادهٔ فوق یا مقام قضایی رسیدگی‌کننده به‌پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ایِ خود از ادامهٔ دسترسی به‌آن ممانعت به‌عمل آورند». همانگونه که ملاحظه می‌گردد، کارگروه مزبور دارای اختیارات عمدتاً قضایی و کارکردهای سرکوبگرانه است که باتوجّه به‌تعداد اندک اعضای حقوقی آن، قابل تأمّل و انتقاد به‌نظر می‌رسد.

به‌نظر می‌رسد درخصوص متولّیان راهبردهای مختلف پیشگیری، کنترل و سرکوب در ارتباط با داده‌های شخصی، مهم‌ترین مشخصه حقوق موضوعه فعلیِ ایران، تشتّت و عدم انسجام نهادهاست؛ به‌عنوان نمونه در حوزه راهبرد پیشگیری، می‌توان به‌انجام آگاه سازی از جانب سه نهاد (مرکز ملّی فضای مجازی، مرکز ماهر و آپا) و انجام خود تنظیم گری از جانب سه نهاد (کارگروه تعامل‌پذیریِ دولت الکترونیک، سازمان فناوری اطلاعات و اتحادیه کشوری کسب و کارهای مجازی) اشاره نمود. در حوزه راهبرد کنترل نیز انجام نظارت بر اجرای مقررات از جانب دو نهاد (مرکز ملّی فضای مجازی، سازمان تنظیم مقررات و ارتباطات رادیویی)؛ و انجام بازرسی از جانب پنج نهاد (کارگروه تعامل‌پذیریِ دولت الکترونیک، مرکز ماهر، اتحادیه کشوری کسب و کارهای مجازی، بخش ستادی پلیس فتا و دادسرای جرایم رایانه‌ای) محلّ تأمّل بوده و ضمن ایجاد تداخل در وظایف و موازی‌کاری در انجام راهبردهای مربوطه، دستیابی به‌الگوی مطلوب را نیز با چالش مواجه نموده است. علاوه بر اینها، اعطای اختیارات سرکوبگرانه به‌کارگروه تعیین مصادیق مجرمانه (با اکثریت اعضای غیرحقوقی) نیز مورد انتقاد به نظر می‌رسد.

نتیجه‌گیری

سیاست جنایی مطلوب در زمینه حمایت از داده‌های شخصی، مقتضیِ درنظرگرفتن تمامیِ شاخصه‌های ماهوی و راهبردی است. در سطح شاخصه‌های ماهوی، پاسداشت محرمانگیِ داده و درنظرگرفتن حقوق و امتیازات مختلف برای اشخاص صاحب داده، ضرورتی انکارناپذیر است. در سطح شاخصه‌های راهبردی نیز توجّه متناسب و همزمان به‌تمامیِ راهبردهای پیشگیرانه (مشتمل بر آگاه‌سازی، حفاظت از داده‌های اشخاص و خود تنظیم‌گری)، کنترلی (شامل نظارت بر اجرای مقررات، بازرسی و بررسی شکایت‌ها) و سرکوبگرانه (اعم از سرکوبگری اداری و کیفری)، ضروری است. به‌بیان دیگر، رویکرد صرفاً کیفری در حمایت از داده‌های شخصی، مؤثر نیست.

اتّحادیه اروپا با درنظر گرفتن این نکته مهم در مقررات عمومیِ حفاظت از داده مصوب ۲۰۱۶، به‌طور نسبی توانسته

است شاخصه‌های الگوی مطلوب را با تجمیعی از ساز و کارهای مورد اشاره فراهم نماید.

در نظام حقوقیِ ایران، گام‌های نخستین در راستای حمایت از داده‌های شخصی با تصویب قانون مدیریت داده‌ها و اطلاعات ملّی و همچنین تهیه لایحه صیانت و حفاظت از داده‌های برداشته شده است. با وجود آنچه گفته شد، کاستی‌هایی همچون عدم تصریح حقوق شخص موضوع داده، عدم جرم‌انگاریِ برخی اَعمال همچون گردآوری غیرمجاز داده‌های شخصی، دسترسی غیرمجاز به داده‌های شخصی به طور عام، فراهم نمودن موجبات دسترسی غیرمجاز به‌داده‌های شخصی و فروش داده‌های شخصی و همچنین مستثنی‌شدن نهادهای زیرنظر مقام رهبری از شمولیت قانون مدیریت داده‌ها و اطلاعات ملّی در سطح شاخصه‌های ماهوی و فقدان تفصیل در تعیین ضمانت‌اجراهای اداریِ مرتبط با نقض داده‌های شخصی، فقدان ساز و کارهای نظارتیِ کافی در حمایت از داده‌های شخصی و پیش‌بینیِ نهادهای متعدد با ساز و کارهای عمدتاً مشابه و وظایف متداخل به‌موجب قوانین و آیین نامه‌های مختلف در سطح شاخصه‌های راهبردی به‌چشم می‌خورند که علاوه بر ایجاد عدم توازن میان راهبردهای پیشگیرانه، کنترلی و سرکوبگرانه، موجب ایجاد چالش‌های جدّی در راه تحقق الگوی مطلوب نیز گردیده‌اند.

ارتقا سیاست جنایی در حمایت از داده‌های شخصی مستلزم قانونگذاری مناسب، جرم‌انگاری‌های جدید با درنظرگرفتن اصل حداقلی بودن حقوق جزا، ایجاد نهادی تنظیم‌گر جهت پیشگیری، نظارت و پاسخ دهی است. ایجاد هماهنگی متقابل میان دو نظام اداری و کیفری نیز از دیگر عوامل مؤثر در انطباق سیاست جنایی با نیازهای مربوط به‌این حوزه است. علاوه بر اینها، به‌منظور تحقق سیاست جنایی سنجیده در حمایت از داده‌های شخصی و حریم خصوصی افراد در فضای مجازی، یکپارچه نمودن کلّیه قوانین و مقررات مربوطه (همچون الگوی اتحادیه اروپا در تصویب مقررات عمومی حفاظت از داده اروپا) امری ضروری به نظر می‌رسد.

ملاحظات اخلاقی: در این پژوهش تمامی ملاحظات اخلاقی رعایت گردیده است.

تعارض منافع: نگارش این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان:

لیلا باداد: جمع‌آوری مطالب و تدوین مقاله

روح‌الدین کردعلیوند: ارائه ایده و موضوع.

سودابه رضوانی: معرفی منابع.

کلیه نویسندگان به صورت برابر در تهیه و تدوین پژوهش حاضر مشارکت داشته‌اند

تشکر و قدردانی: لازم است از اساتید گرامی که در تدوین و ارائه انتقادات باعث غنای مقاله شدند، قدردانی نمایم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین مالی انجام گرفته است.

منابع

الف. منابع فارسی

– اصلانی، حمیدرضا (۱۳۸۹). *حقوق فناوری اطلاعات*. چاپ اول، تهران: انتشارات میزان.

– انصاری، باقر (۱۴۰۲). *حقوق داده (اصول پردازش داده‌های شخصی)*. چاپ اول، تهران: شرکت سهامی انتشار.

– حیدری، علی‌مراد و جعفری، علی (۱۳۹۹). «جرایم علیه داده‌پیام‌های شخصی در تجارت الکترونیکی». *فصلنامه پژوهشنامه حقوق کیفری*، ۱۱ (۱): ۵۱–۷۴.

– رجبی، ابوالقاسم (۱۴۰۲). «*شناسایی خلأهای قانونی حفاظت از داده‌ها در زنجیره ارزش داده‌ها با مقایسه قوانین ایران و ایالات متحده آمریکا – قانون اساسی، قوانین و مقررات فدرال و ایالتی*». تهران: گزارش مرکز پژوهش‌های مجلس.

– رهایی، سعید و متاجی، محسن (۱۴۰۱). «تأملی بر مقررات گذاری خودتنظیمی در فضای سایبر». *فصلنامه مطالعات حقوق عمومی*، ۵۲ (۴): ۲۱۲۷–۲۱۴۸.

– زارعیان، داود و واحد، فائزه (۱۳۹۹). «بررسی حقوقی رگولاتوری‌های حمایت از داده». *فصلنامه رسانه*، ۳۱ (۱): ۴۷–۷۲.

– عطار، شیما و پروین، فرهاد (۱۴۰۰). «حقوق اتحادیه اروپا و چالش شناسایی حق مالکیت بر داده‌ها در عصر اقتصاد دیجیتال». *مجلّه حقوقی بین‌المللی*، ۳۸ (۶۵): ۲۸۱–۳۰۴.

– قناد، فاطمه و شریف، الهام (۱۴۰۰). «مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا». *دوفصلنامه تخصصی حقوق فناوری‌های نوین*، ۲ (۴): ۱–۲۲.

– قناد، فاطمه و علیقلی، امیر (۱۳۹۹). «مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی». *دو فصلنامه حقوق قراردادها و فناوری‌های نوین*، ۱ (۱): ۲۹۷–۳۲۲.

– لطیف‌زاده، مهدیه؛ قبولی‌دُرافشان، سید محمّدمهدی؛ محسنی، سعید و عابدی، محمد (۱۴۰۲). «حمایت از داده شخصی در حقوق اتحادیه اروپا و امکان‌سنجی آن در نظام حقوقی ایران». *فصلنامه مطالعات حقوق عمومی*، ۵۳ (۲): ۹۸۱–۱۰۰۵.

– لطیف‌زاده، مهدیه؛ قبولی‌دُرافشان، سید محمّدمهدی؛ محسنی، سعید و عابدی، محمد (۱۴۰۱). «تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا»، *پژوهشنامه پردازش و مدیریت اطلاعات*، ۳۷ (۲): ۴۳۹–۴۷۲.

– لطیف‌زاده، مهدیه؛ قبولی‌دُرافشان، سیدمحمّدمهدی؛ محسنی، سعید و عابدی، محمّد (۱۴۰۰). «تبیین اسباب مشروعیت پردازش داده شخصی از منظر حقوق اتحادیه اروپا و ایران». *فصلنامه مطالعات حقوقی*، ۱۴ (۳): ۳۲۵–۳۶۴.

– محسنی، فرید (۱۳۸۹). *حریم خصوصی اطلاعات (مطالعه کیفری در حقوق ایران– ایالات متحده آمریکا و فقه امامیه)*. چاپ اول، تهران: انتشارات دانشگاه امام صادق (ع).

– محمدنسل، زهرا و محمدنسل، غلامرضا و گلدوزیان، ایرج (۱۳۹۹). «مطالعه تطبیقی دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای در قوانین کیفری ایران و انگلستان و فرانسه». *فصلنامه پژوهش‌های اطلاعاتی و جنایی*،۱۵ (۳): ۸۱–۱۰۶.

– معظّمی، شهلا؛ بطیاری، عاطفه و انصاری‌فر، محمّدعلی (۱۳۹۶). «معیارهای جرم‌انگاری». *فصلنامه قضاوت*،۱۷ (۸۹): ۱۷۹–۱۹۴.

– نجفی‌ابرندآبادی، علی‌حسین (۱۳۸۴). *تقریرات درس جرم‌شناسی*. چاپ اول، تهران: انتشارات دانشگاه شهید بهشتی.

– وطنی، امیر و اسدی، حمید (۱۳۹۵). «سیاست جنایی جمهوری اسلامی ایران در جرایم سایبری با تأکید بر ویژگی‌های خاص این جرایم». *پژوهشنامه حقوق اسلام*، ۱۷(۱): ۹۹–۱۲۶.

– یوسفی، محمّدرضا و مهدوی‌ثابت، محمّدعلی (۱۳۹۴). «بررسی قلمرو کیفری در «ضمانت اجرای انفصال از خدمت» در نظام حقوقی ایران». *فصلنامه دانشنامه حقوق و سیاست*، ۱۵ (۲۵): ۳۳–۴۴.

ب. منابع لاتین

- Phua, C (2009). ‘‘Protecting organisations from personal data breaches’’. *January Computer fraud & security*, (25) (1): 13-18.

–Wachter, S & Mittelstadt, B (2019). *A Right to Reasonable Inferences (Rethinking Data Protection Law in the Age of Big Data and AI)*. 1st ed,. Columbia: Publications Columbia University Academic Commons.

– Lehtiniemi, T & Kortesniemi, Y (2017). ‘‘Can the obstacles to privacy selfmanagement be overcome? (Exploring the consent intermediary approach)’’. *Sage journals*,18(25): 95- 125.