How to Process Specific Personal Data in EU Law and Examine it in the Iranian Legal System

Mahdieh Latifzadeh
PhD in Private Law; Faculty of Law and Political Science; Ferdowsi University of Mashhad' Mashhad, Iran;
Email: m.latifzadeh@mail.um.ac.ir

Sayyed Mohammad Mahdi Qabuli Dorafshan*
PhD in Private Law; Associate Professor; Ferdowsi University of Mashhad; Mashhad, Iran Email: s-mohseni@um.ac.ir

Saeed Mohseni
PhD in Private Law; Associate Professor; Ferdowsi University of Mashhad; Mashhad, Iran Email: sdilmaghani6@gmail.com

Mohammed Abedi
PhD in Private Law; Associate Professor; Ferdowsi University of Mashhad; Mashhad, Iran Email: dr.m.abedi@um.ac.ir

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 39 | No. 1 | pp. 157-200
Autumn 2023
https://doi.org/jipm.39.1

Received: 11, Oct. 2021 **Accepted: 18, Apr. 2023**

Abstract: To provide comprehensive protection of personal data and data subjects, the General Data Protection Regulation (GDPR) has addressed various aspects. One of these protections is to pay attention to personal data that due to their sensitive nature, need more protection (specific personal data). This regulation sets out various requirements for the processing of specific personal data. These requirements include the principle of prohibition of sensitive personal data processing unless there is a legal exception. Another requirement is the need for official authority oversight and legal authorization to process personal data relating to criminal convictions and offences. Determining a certain age for consent to processing is also a requirement for protecting children's personal data. In this study, by explaining in detail these requirements and clarifying how specific personal data is processed in EU law, the protection of specific personal data in Iranian law has also been examined. The conclusion is that although Iranian law on personal data does not have an independent law to rely on to protect specific personal data, however, according to the laws and regulations, legal doctrine, principles of Iranian law, there are many requirements for the processing of specific personal data set out in the GDPR, also in Iranian law.

* Corresponding Author

Keywords: Processing of Specific Personal Data, Sensitive Personal Data, Personal Data of Children, Personal Data Relating to Criminal Convictions and Offences, General Data Protection Regulation (GDPR)

چگونگی پردازش داده شخصی خاص در حقوق اتحادیه اروپا و بررسی آن در نظام حقوقی ایران[1]

(پردازش داده شخصی خاص)

مهدیه لطیف‌زاده
دکتری حقوق خصوصی؛ پژوهشگر پسادکتری؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛
m.latifzadeh@mail.um.ac.ir

سید محمدمهدی قبولی درافشان
دکتری حقوق خصوصی؛ دانشیار؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛
پدیدآور رابط ghaboli@um.ac.ir

سعید محسنی
دکتری حقوق خصوصی؛ دانشیار؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛
s-mohseni@um.ac.ir

محمد عابدی
دکتری حقوق خصوصی؛ دانشیار؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛
dr.m.abedi@um.ac.ir

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۴۰۰/۰۷/۱۹ | **پذیرش:** ۱۴۰۲/۰۱/۲۹ | مقاله برای اصلاح به مدت ۴۱ روز نزد پدیدآوران بوده است.

چکیده: در راستای حمایت جامع از داده‌های شخصی و اشخاص موضوع داده، مقررات اروپایی مربوط به حفاظت از داده (GDPR) جنبه‌های مختلفی را مورد توجه قرار داده است. یکی از این حمایت‌ها، توجه ویژه به داده‌های شخصی است که به‌دلیل ماهیت حساس (داده‌های شخصی خاص) نیازمند حفاظت بیشتری است. این مقررات برای پردازش داده‌های شخصی خاص که شامل داده‌های شخصی حساس، داده شخصی مرتبط با امور کیفری و داده شخصی کودکان است، الزامات مختلفی را مقرر نموده است. این الزامات از جمله اصل ممنوعیت پردازش داده‌های شخصی حساس است،

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۹ | شمارهٔ ۱ | ص‌ص ۱۵۷-۲۰۰
پاییز ۱۴۰۲
https://doi.org/jipm.39.1

۱. این اثر تحت حمایت مادی صندوق حمایت از پژوهشگران و فناوران کشور (INSF) برگرفته از طرح شماره ۹۸۰۲۸۶۸۹ انجام شده است.

مگر اینکه استثنای قانونی وجود داشته باشد. الزام دیگر، ضرورت وجود نظارت مرجع رسمی و جواز قانونی برای پردازش داده‌های شخصی مرتبط با امور کیفری است. همچنین تعیین سن معین برای رضایت به پردازش نیز از الزامات پیش‌گفته برای حمایت از داده‌های شخصی کودکان است. این پژوهش با تبیین تفصیلی الزامات پیش‌گفته و شفاف‌سازی چگونگی پردازش داده شخصی خاص در حقوق اتحادیه اروپا، حمایت از داده شخصی خاص در حقوق ایران را نیز مورد بررسی قرار داده است. بررسی‌های انجام‌شده حکایت از این دارد که گرچه حقوق ایران در خصوص داده‌های شخصی قانونی مستقل ندارد تا برای حمایت از داده‌های شخصی خاص به آن استناد شود، ولی می‌توان با توجه به قوانین و مقررات موجود، نظریات دکترین، مبانی حقوق ایران، بسیاری از الزامات پردازش داده شخصی خاص موجود در مقررات اروپایی را در حقوق ایران نیز جاری دانست.

کلیدواژه‌ها: پردازش داده شخصی خاص، داده شخصی حساس، داده شخصی کودکان، داده شخصی مرتبط با امور کیفری، مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)

۱. مقدمه

با تصویب مقررات عمومی حفاظت از داده اتحادیه اروپا (مقررات اروپایی حفاظت از داده)[1] در خصوص حمایت از داده شخصی در سال ۲۰۱۶، و لازم‌الاجرا شدن آن در سال ۲۰۱۸، تمامی کشورهای عضو اتحادیه اروپا ملزم به حمایت حداکثری از داده‌های شخصی و اشخاص موضوع داده شدند. داده شخصی به‌موجب مقررات اروپایی حفاظت از داده، به معنای هر اطلاعاتی است که به شخص حقیقی شناخته‌شده یا قابل شناسایی (شخص موضوع داده) مربوط باشد. یک فرد حقیقی قابل شناسایی کسی است که به‌طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به یک شناسه از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه آنلاین یا به یک یا چند ویژگی خاص مانند هویت فیزیکی، فیزیولوژیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی، شناسایی شود (EUR-Lex 2016, 33).

1. General Data Protection Regulation (GDPR)

به‌موجب GDPR برای پردازش داده‌های شخصی[1] رعایت اصول خاصی لازم است[2] که مربوط به داده‌هایی است که دارای وضعیت عمومی‌اند[3] و حالت ویژه‌ای ندارند. در مقابل، برای پردازش سایر داده‌های شخصی که به‌واسطه ماهیت خود، خاص تلقی می‌شوند (دسته‌های خاص داده شخصی)[4] افزون بر اصول یادشده، باید الزامات ویژه‌ای رعایت شوند. این داده‌ها شامل داده‌های شخصی حساس[5]، داده‌های شخصی مربوط به محکومیت و جرائم کیفری[6] و داده‌های شخصی مربوط به کودکان است. علت ضرورت حمایت

---

۱. پردازش داده‌های شخصی بر اساس GDPR، به معنای عملیات یا مجموعه‌ای از عملیات است که بر روی دادهٔ شخصی یا مجموعه داده‌های شخصی با ابزار خودکار یا به‌صورت دستی، صورت گیرد. چنین عملیاتی اعم از جمع‌آوری، ضبط، سازماندهی، طبقه‌بندی، ذخیره‌سازی، اشتراک‌گذاری، تغییر، بازیابی، استفاده‌کردن، تجزیه و تحلیل کردن، انتشار، افشا به‌وسیله مخابره‌کردن یا ایجاد دسترسی به شیوه‌های دیگر، ترکیب‌کردن، محدود نمودن، حذف و پاک کردن و یا تخریب است (EUR-Lex 2016, 33).

۲. مقررات اروپایی حفاظت از داده برای پردازش داده‌های شخصی، اصول خاصی را در ماده ۵ با عنوان «اصول مربوط به پردازش دادهٔ شخصی» مقرر کرده است. این اصول پایه و اساس GDPR را تشکیل می‌دهند و با وجود اینکه الزامات پیچیده‌ای ندارند، عدم رعایت آن‌ها، اشخاص پردازش‌کننده داده (کنترل‌کننده‌ها و پردازنده‌ها) را در معرض ضمانت اجراهای متعددی قرار می‌دهد. ماده ۵ GDPR اصول حاکم بر پردازش داده‌های شخصی را به‌شرح زیر مقرر می‌نماید: «۱. داده‌های شخصی باید الف- به‌طور مشروع، منصفانه و به شیوه‌ای شفاف در رابطه با شخص موضوع داده پردازش شوند (اصل مشروعیت، انصاف و شفافیت)؛ ب- برای اهداف مشخص، صریح و مشروع جمع‌آوری شده و به شیوه‌ای که با آن اهداف ناسازگار است، پردازش نشوند. پردازش بیشتر -نسبت به هدف پردازش- در جهت بایگانی برای منافع عمومی، اهداف تحقیقات علمی یا تاریخی یا اهداف آماری، مطابق با ماده ۸۹ (۱)، با اهداف اولیه ناسازگار تلقی نمی‌شود (اصل محدودیت هدف)؛ ج- کافی، مرتبط و محدود به آنچه در ارتباط با اهداف پردازش داده لازم است، پردازش شوند (اصل به حداقل رساندن داده)؛ د- صحیح و در صورت لزوم به‌روز باشند، هر گام باید معقول و منطقی برداشته شود تا اطمینان حاصل شود که داده‌های شخصی نادرست با توجه به اهداف پردازش بدون تأخیر حذف یا تصحیح می‌شوند (اصل صحت)؛ ه- به شکلی نگهداری شوند که موجبات شناسایی اشخاص موضوع داده بیش از آنچه برای هدف پردازش لازم است، ایجاد نشود. داده‌های شخصی را می‌توان برای مدت طولانی‌تری ذخیره نمود، البته صرفاً تا زمانی که داده‌ها برای مقاصد بایگانی به نفع عموم، اهداف تحقیقات علمی یا تاریخی یا اهداف آماری مطابق با ماده ۸۹ (۱) پردازش شوند. این امر نیز مشروط به اجرای اقدامات فنی و سازمانی مد نظر این مقررات به‌منظور حفظ حقوق و آزادی‌های شخص موضوع داده است (اصل محدودیت ذخیره‌سازی)؛ و- به شیوه‌ای پردازش شوند که امنیت مناسب داده‌های شخصی تضمین شود. این امر از جمله محافظت در برابر پردازش غیرمجاز یا غیرقانونی و حفاظت در برابر ضرر ناگهانی، تخریب یا آسیب با توسل به روش‌ها و اقدامات فنی و سازمانی مناسب است (اصل تمامیت و محرمانگی) ۲. ... (EUR-Lex 2016, 35)

3. generic personal data 4. special category data 5. sensitive personal data

6. personal data relating to criminal convictions and offences

ویـژه از داده‌هـای شـخصی پیش‌گفتـه، در مـواردی بـه ماهیـت خـود آن داده برمی‌گـردد؛ ماننـد داده‌هـای شـخصی حسـاس و داده‌هـای مرتبـط بـا امـور کیفـری کـه بـا توجـه بـه ماهیتشـان بـر حقـوق و آزادی‌هـای اساسـی افـراد مؤثرنـد و پـردازش بـدون ضابطـه آن‌هـا می‌توانـد خطـرات مهمـی را بـرای حقـوق و آزادی‌هـای اساسـی ایجـاد نمایـد. از سـوی دیگـر، لـزوم حمایـت ویـژه، بـه شـخص موضـوع داده مربـوط اسـت؛ ماننـد کـودکان کـه به‌دلیـل شـرایط سـنی، درک کمتـری از پـردازش و مسـائل مربـوط بـه داده‌هـای شـخصی خـود دارنـد. بـا توجـه بـه ایـن مهـم، رسـالت پژوهـش حاضـر، پاسـخ بـه ایـن پرسـش اسـت کـه مبانـی پـردازش داده‌هـای شـخصی خـاص به‌موجـب مقـررات اروپایـی حفاظـت از داده چیسـت. بـه دیگـر سـخن، ایـن مقـررات اروپایـی در برخـورد بـا داده‌هـای شـخصی خـاص چـه حمایت‌هـای متفاوتـی را -نسـبت بـه داده‌هـای عمومـی- مـد نظـر قـرار داده اسـت. همچنیـن رویکـرد نظـام حقوقـی ایـران نسـبت بـه داده‌هـای شـخصی خـاص چیسـت و به‌طـور ویـژه آیـا الزامـات مقـررات اروپایـی در حقـوق ایـران قابـل جریـان اسـت. بدیـن جهـت در پژوهـش حاضـر، ابتـدا پـردازش داده‌هـای شـخصی حسـاس و در گام بعـد پـردازش داده‌هـای شـخصی مرتبـط بـا محکومیـت و جرائـم کیفـری و سـرانجام، حفاظـت خـاص از کـودکان به‌موجـب مقـررات اروپایـی تبییـن خواهـد شـد. سـپس، رویکـرد نظـام حقوقـی ایـران در هـر مـورد به‌طـور مجـزا مـورد بررسـی قـرار خواهـد گرفـت.

۲. پیشینه پژوهش

رسـالت پژوهـش حاضـر، شفاف‌سـازی چگونگـی حفاظـت از داده شـخصی خـاص بـا تمرکـز بـر سـند قانونـی اتحادیـه اروپـا اسـت. در ایـن راسـتا، مـواد مختلـف مقـررات اروپایـی حفاظـت از داده بـرای ایجـاد درک جامعـی از حفاظت‌هـای موجـود در ایـن مقـررات بررسـی شـده اسـت تـا در کنـار بررسـی چنیـن حمایتـی در نظـام حقوقـی ایـران، جریـان حمایت‌هـای کارآمـد از داده‌هـای شـخصی خـاص در حقـوق ایـران تقویـت شـود. بـا لحـاظ دامنـهٔ پژوهشـی پیش‌گفتـه، اثـر علمـی کـه به‌طـور قابـل توجهـی بـا موضـوع حاضـر همپوشـانی داشـته باشـد، مشـاهده نشـده اسـت؛ ولـی به‌دلیـل اهمیـت و نویـن بـودن موضـوع حفاظـت از داده‌هـای شـخصی و توجـه پژوهشـگران بـه ایـن مهـم، آثـاری مشـابه وجـود دارنـد کـه نزدیـک بـه دامنـهٔ موضوعـی پژوهـش حاضـر هسـتند و در همـان حـال، در جنبه‌هـای مختلفـی بـا ایـن پژوهـش متمایزنـد. به‌عنـوان نمونـه، «افراسـیاب و ناصـر» (۱۳۹۹) مقالـه‌ای بـا عنـوان «چارچوب‌هـای حقوقـی حفـظ امنیـت پـردازش داده‌هـای خصوصـی مطالعـه تطبیقـی حقـوق ایـران و اتحادیـه اروپـا» تدویـن

نموده‌انـد. فـارغ از اینکـه، ایـن مقالـه ناظـر بـر داده‌هـای شـخصی خـاص نیسـت و بـه انـواع داده‌هـای شـخصی خـاص و رویکـرد ویـژه نظـام حقوقـی ایـران در هـر نـوع اشـاره نکـرده اسـت، ایـن مقالـه در دامنـه اینترنـت اشـیا اسـت و از ایـن جهـت نیـز خاص‌تـر از موضـوع پژوهـش حاضـر اسـت. همچنیـن ایـن مقالـه به‌طـور خـاص بـر هـدف تبییـن چارچوب‌هـای حقوقـی بـرای حفاظـت از اطلاعـات شـخصی در راسـتای حفـظ امنیـت داده‌هـای شـخصی اسـت کـه در ایـن خصـوص نیـز دامنـه‌ای محدودتـر نسـبت بـه پژوهـش حاضـر -کـه به‌طـور کلـی، مبانـی پـردازش داده‌هـای شـخصی خـاص را روشـن نمـوده و حفاظت‌هـای ویـژه در ایـن خصـوص را شـفاف می‌سـازد- دارد. همچنیـن «آقایـی طـوق و ناصـر» (۱۳۹۹) مقالـه‌ای بـا عنـوان «چالش‌هـای حفاظـت از داده‌هـای خصوصـی در حـوزه اینترنـت اشـیا؛ مطالعـه تطبیقـی حقـوق ایـران و اتحادیـه اروپـا» در «مجلـه حقـوق اداری» تدویـن نموده‌انـد. وجـوه افتـراق پیش‌گفتـه در مـورد ایـن مقالـه نیـز قابـل بیـان اسـت. به‌عنـوان نمونـه، مقالـه مذکـور در مـورد داده‌هـای شـخصی به‌طـور کلـی، نـه خصـوص داده‌هـای شـخصی خـاص اسـت. از سـوی دیگـر، در خصـوص حمایـت از داده در دامنه اینترنـت اشـیا بـوده و بـه سـایر بسـترهای پـردازش اشـاره نکـرده اسـت و بدیـن جهـت دامنـه مضیـق نسـبت بـه پژوهـش حاضـر دارد. هـدف آن نیـز -یعنـی چگونگـی مدیریـت چالش‌هـای مربـوط بـه حفاظـت از داده خصوصـی نسـبت بـه اینترنـت اشـیا- بـا غایـت پژوهـش حاضـر متفـاوت اسـت.

گفتنـی اسـت کـه بـا توجـه بـه روزآمـدی و کاربـردی بـودن مقـررات اروپایـی، محققـان سـایر کشـورها نیـز در مـورد شفاف‌سـازی ایـن مقـررات و مـواد مختلـف آن، آثـار علمـی مختلفـی را تدویـن نموده‌انـد کـه مبیـن اهمیـت ایـن موضـوع و لـزوم بررسـی آن در نظـام حقوقـی ایـران اسـت. از جملـه آثـار نزدیـک بـه پژوهـش حاضـر می‌تـوان بـه مـوارد زیـر اشـاره نمـود: «ولوسـوویچ» مقالـه‌ای بـا عنـوان «حمایـت از کـودکان بـه موجـب مقـررات اروپایـی حفاظـت از داده» تدویـن نمـوده اسـت. در ایـن اثـر، مـواد مختلـف مقـررات اروپایـی بـه هـدف چگونگـی جریـان حفاظت‌هـای ویـژه از کـودکان، مـورد واکاوی قـرار گرفتـه اسـت. بـه موجـب برآمـد ایـن پژوهـش، الزامـات خـاص موجـود در مقـررات اروپایـی در خصـوص حمایت‌هـای کافـی نسـبت بـه کـودکان ضـروری اسـت (Volosevici 2019). افـزون بـر آن، «اسـکیوپو» مقالـه‌ای بـا عنـوان «ملاحظـات مختصـر در مـورد پـردازش داده‌هـای شـخصی کـودکان» نـگارش نمـوده. در ایـن مقالـه بـه حمایت‌هـای خـاص در مـورد داده‌هـای شـخصی کـودکان اشـاره شـده اسـت. از اهـداف آن چگونگـی حمایـت از کـودکان در مـورد خدمـات اجتماعـی اسـت کـه آن‌هـا را به‌طـور مسـتقیم مـورد خطـاب قـرار می‌دهـد. یافته‌هـای ایـن پژوهـش حکایـت از ایـن دارد کـه

حتی با وجود مقررات اروپایی جدید در خصوص داده‌های شخصی، همچنان چالش‌های مربوط به حمایت‌های جامع از کودکان وجود دارد (Dorin Schiopu 2019). «کاباناس، آنجل کوواس و روبن کوواس» نیز مقاله‌ای با عنوان «استفاده فیس‌بوک از داده‌های شخصی حساس برای تبلیغات در اتحادیه اروپا» تدوین نموده‌اند. این مقاله در جهت ممنوعیت استفاده از داده‌های شخصی اشخاص موجود در اتحادیه اروپا، به‌دلیل اهداف تبلیغاتی، توسط بسترهای مجازی به‌طور خاص «فیس‌بوک» است. به‌موجب نتایج این پژوهش، این بستر مجازی از داده‌های حساس به‌طور شایسته حمایت نمی‌کند و بدین جهت پیشنهاداتی فنی برای کاربران «فیس‌بوک» ارائه شده است تا آن‌ها را نسبت به استفاده از داده‌هایشان مطلع نماید (Cabañas, Cuevas & Cuevas 2018).

۳. روش پژوهش

با توجه این امر که پژوهش حاضر به توسعه مرزهای دانش در علم حقوق کمک می‌کند، این پژوهش بر اساس هدف، از نوع بنیادی، و بدین‌جهت که به‌دنبال شفاف‌سازی مواد مختلف مقررات اروپایی حفاظت از داده در خصوص تبیین چگونگی پردازش داده‌های شخصی خاص است، بر اساس ماهیت، توصیفی-تحلیلی است. همچنین باید گفت از آنجا که جامعه مورد بررسی در این پژوهش سند قانونی اتحادیه اروپا در خصوص حفاظت از داده شخصی و تطبیق آن با نظام حقوقی ایران است، پژوهش حاضر جنبه تطبیقی نیز دارد. روش پژوهش نیز به‌صورت روش پژوهش اسنادی[1] است. این روش با تحلیل اسنادی که حاوی اطلاعاتی در مورد موضوع مد نظر است و از طریق بررسی اسناد مختلف مانند اسناد رسمی به‌عنوان منبع اطلاعات انجام می‌شود، یکی از پایه‌های اصلی در تحقیقات علوم انسانی و اجتماعی است (Ahmed 2010, 2). بدین جهت در این پژوهش اسناد به‌صورت مطالعات کتابخانه‌ای از پایگاه‌های اطلاعاتی علمی از جمله «سایمگو»[2]، «الزویر»[3]، تارنماهای مربوط به انتشارات بین‌المللی از جمله «نشر اشپرینگر»[4] و تارنماهای مربوط به قوانین و مقررات ایران[5] و اتحادیه اروپا[6] مورد بررسی قرار گرفته‌اند. در این راستا کلیدواژگان مرتبط از جمله کلمات بیان‌شده در واژگان کلیدی ابتدای پژوهش معیار جست‌وجو قرار گرفته و به‌عنوان مرز پژوهش تلقی شدند. همچنین همان‌طور که

1. documentary research method
2. Scimago
3. Elsevier
4. Springer Publication
5. https://dotic.ir . https://rc.majlis.ir/fa
6. https://eur-lex.europa.eu

از رویکـرد پژوهـش روشـن اسـت، اسـناد دارای اولویـت در ایـن پژوهـش، مقـررات اروپایـی حفاظـت از داده نسـبت بـه حقـوق اتحادیـه اروپـا و قوانیـن و مقـررات مرتبـط بـا حریـم خصوصـی اطلاعاتـی در خصـوص حقـوق ایـران هسـتند. در گام بعـد سـایر آثـار علمـی از جملـه مقـالات و کتـب مربـوط بـه داده‌هـای شـخصی و حریـم خصوصـی اطلاعاتـی مـورد توجـه قـرار گرفته‌انـد.

٤. پردازش داده شخصی حساس

در ایـن بنـد، ابتـدا بـه چگونگـی پـردازش داده‌هـای شـخصی حسـاس به‌موجـب مقـررات اروپایـی حفاظـت از داده پرداختـه خواهـد شـد. سـپس، رویکـرد نظـام حقوقـی ایـران در ایـن خصـوص بررسـی می‌شـود.

٤-١. پردازش داده شخصی حساس به موجب مقررات اروپایی حفاظت از داده

بـه موجـب مـاده ۹ (۱) مقـررات اروپایـی حفاظـت از داده، داده‌هـای شـخصی کـه به‌واسـطه ماهیـت خـاص خـود، به‌ویـژه نسـبت بـه حقـوق و آزادی‌هـای اساسـی افـراد حسـاس هسـتند[1]، شایسـته حفاظـت ویژه‌انـد. علـت برجسـته‌نمودن چنیـن داده‌هایـی آن اسـت کـه پـردازش ایـن دسـته از داده‌هـای شـخصی می‌توانـد خطـرات مهمـی را بـرای حقـوق و آزادی‌هـای اساسـی افـراد ایجـاد کنـد. داده‌هـای حسـاس بـا آزادی فکـر و مذهـب، آزادی بیـان، آزادی اجتماعـات، حـق احتـرام بـه زندگـی خصوصـی و خانوادگـی، رهایـی از تبعیـض و ... ارتبـاط نزدیکـی دارنـد؛ به‌طـوری کـه جمع‌آوری و اسـتفاده از ایـن داده‌هـا بـا حقـوق اساسـی افـراد تداخـل دارد (ICO 2019). همچنیـن داده‌هـای شـخصی حسـاس شـامل داده‌هایـی هسـتند کـه بـه لحـاظ ماهـوی، خـاص باشـند یـا داده‌هایـی کـه از آن‌هـا بتـوان اطلاعـات حسـاس در مـورد یـک فـرد را نتیجـه گرفـت (Shabani & Borry 2018, 151).

تمرکـز ویـژه مقـررات اروپایـی حفاظـت از داده نسـبت بـه داده‌هـای شـخصی حسـاس، بـه رویکـرد مبتنـی بـر خطـر ایـن مقـررات برمی‌گـردد[2] (ICO 2019). همچنیـن فراگیـر بودن بسـترهایی کـه داده‌هـای حسـاس افـراد را جمع‌آوری می‌کننـد، یکـی از عوامـل اصلـی بـود کـه قانون‌گـذار

---

۱. معـادل دادۀ شـخصی حسـاس sensitive personal data اسـت. در مقابـل، بـه سـایر داده‌هـای شـخصی generic personal data گفتـه می‌شـود. همچنیـن در منابـع مختلـف واژه‌هـای specially protected data, special categories of personal data بـرای داده‌هـای شـخصی حسـاس بـه‌کار رفتـه اسـت.

2. GDPR rely on a risk-based approach

اتحادیه اروپا را به حفاظت خاص از داده‌های حساس تشویق نمود. به‌عنوان مثال، امروزه تقریباً تمام افراد از دستگاه‌های تلفن همراه استفاده می‌کنند که حاوی خدماتی است که طیف گسترده‌ای از داده‌های حساس -مانند عضویت در اتحادیه‌های صنفی، سلامتی و ...- را جمع‌آوری می‌کند و ممکن است چنین داده‌هایی را برای اهداف مختلف پردازش کند؛ در حالی که این داده‌ها به‌واسطه ماهیت خاص خود نیاز به حفاظت ویژه دارند، زیرا پردازش این داده‌ها به حقوق و آزادی‌های اساسی افراد مربوط می‌شود و ممکن است خطرات زیادی را برای افراد دربرداشته باشد (Ferrara & Spoto 2018, 1). به‌عنوان نمونه «فیس‌بوک» به‌صورت تجاری از داده‌های شخصی حساس برای اهداف تبلیغاتی با توجه به علایق کاربران -اشخاص موضوع داده- استفاده می‌کند. ولی در حال حاضر و با توجه به لازم‌الاجرا شدن مقررات اروپایی حفاظت از داده، پردازش داده‌های شخصی حساس ممنوع شده است و این بستر مجازی، باید نسبت به کاربران اتحادیه اروپا الزامات مذکور در این مقررات را رعایت نماید (Cabañas, Cuevas & Cuevas 2018, 14).

به‌دلیل ماهیت ویژه داده‌های شخصی حساس، پردازش چنین داده‌هایی به‌موجب مقررات اروپایی حفاظت از داده ممنوع است. به‌موجب ماده ۹ (۱) این مقررات «پردازش داده‌های شخصی که مبین منشأ نژادی یا قومی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی، عضویت در اتحادیه‌های صنفی، پردازش داده‌های ژنتیکی، داده‌های زیست‌سنجی به‌منظور شناسایی منحصربه‌فرد یک شخص حقیقی، داده‌های مربوط به سلامت یا داده‌های مربوط به زندگی جنسی یک شخص حقیقی یا گرایش جنسی ممنوع است» (EUR-Lex 2016, 38). گرچه در مقام تقنین، مصادیق داده‌های شخصی حساس توسط مقررات اروپایی حفاظت از داده مورد تصریح قرار گرفته است، ولی در مقام عمل، اینکه چه داده‌ای حساس محسوب می‌شود، نیاز به مداقه دارد. به‌عنوان نمونه، در پرونده «کاتلین ایگان و مارگارت هکت»[1] به شماره T-190/10 در سال ۲۰۱۲، که در دیوان دادگستری اتحادیه اروپا مطرح شده بود،

چنین رویکردی در GDPR بدین معناست که بررسی سطح معینی از خطر برای پردازش الزامی است. این امر از مواد مختلف این مقررات قابل استنباط است. به‌عنوان نمونه، به‌موجب GDPR، قبل از پردازش، کنترل‌کننده باید با در نظر گرفتن ماهیت، دامنه، زمینه و اهداف پردازش و ... احتمال و شدت خطر مهم برای حقوق اشخاص موضوع داده را ارزیابی نماید. احتمال و شدت خطر با توجه به عوامل متفاوت مشخص می‌شود. ارزیابی و در نظر گرفتن خطر موجب عدم نقض بالقوه حقوق اشخاص موضوع داده است (Gellert 2017, 7).

1. Kathleen Egan and Margaret Hacket

دادگاه حکم نمود که ادعای خواهان‌ها مبنی بر اینکه انتشار اسامی دستیارهای سابق عضو پارلمان اروپا، عقاید سیاسی آن‌ها را نشان داده و بدین جهت داده‌های حساس محسوب می‌شوند، اثبات نشده و حق حریم خصوصی این اشخاص به‌موجب قانون نقض نشده است (CURIA n.d).

بدین جهت مصداق‌شناسی داده‌های مذکور در ماده ۹ (۱) مقررات اروپایی حفاظت از داده ضروری است. به‌عنوان نمونه داده‌های زیست‌سنجی[1] مفهومی است که برای نخستین‌بار در این مقررات مورد توجه قانون‌گذار قرار گرفته است. تا زمان تصویب مقررات مذکور، هیچ ماده مشخصی در مورد مفهوم داده‌های زیست‌سنجی یا قواعد خاصی برای تنظیم پردازش چنین داده‌هایی در بسترهای حفاظت از داده اتحادیه اروپا وجود نداشت. در مقررات اروپایی حفاظت از داده به «پردازش فنی خاص» در تعریف داده‌های زیست‌سنجی اشاره شده است[2]، ولی این مقررات مشخص نمی‌کند که چه چیزی باید توسط «پردازش فنی خاص» فهمیده شود و صرفاً بیان می‌کند که هدف از پردازش باید شناسایی یکتای یک شخص باشد. نفس ویژگی‌های زیستی، به‌عنوان داده‌های زیست‌سنجی در نظر گرفته نمی‌شوند، بلکه تنها اطلاعات شخصی حاصله از پردازش آن‌ها، به‌عنوان داده‌های زیست‌سنجی قابل اشاره و تحت حمایت است. بنابراین چهره یک فرد داده زیست‌سنجی نیست، بلکه تصاویر چهره فرد یا تصویر اثر انگشت شخص، به‌عنوان داده زیست‌سنجی مورد حمایت است. این امر به این دلیل است که طبق تعریف پردازش در مقررات اروپایی حفاظت از داده، داده‌های شخصی باید حداقل بخشی از یک سیستم بایگانی باشند یا با ابزارهای خودکار پردازش شوند، در حالی که نفس ویژگی‌های زیستی –چهره فرد یا اثرانگشت– نمی‌توانند پردازش شوند. در خصوص این دسته از داده‌های حساس، برخی نیز بیان نموده‌اند که به‌طور کلی ماهیت چنین داده‌هایی حساس نیستند، مگر اینکه منشأ آشکارشدن نژاد و ژنتیک باشند. به‌عنوان مثال، برخی مطالعات علمی نشان داده‌اند که داده‌های حساس مانند بیماری‌های ژنتیکی می‌توانند از اثرانگشت آشکار شود (Jasseran 2016, 310).

---

1. Biometric Data

۲. ماده ۴ (۱۴) GDPR: «داده‌های زیست‌سنجی– biometric data – به معنای داده‌های شخصی حاصل از پردازش فنی خاص، مربوط به ویژگی‌های فیزیکی، منطقی و یا رفتاری یک شخص حقیقی است که امکان شناسایی یکتای آن شخص حقیقی را فراهم یا تائید می‌کند؛ مانند تصاویر صورت یا داده‌های انگشت‌نگاری» (EUR-Lex 2016, 34).

برای تبیین بهتر چنین داده‌هایی و در مقام مثال، می‌توان گفت زمانی که یک باشگاه ورزشی از یک سیستم اسکن الکترونیکی اثر انگشت استفاده می‌کند و اعضا اثر انگشت خود را اسکن می‌کنند تا از دریچه ورودی عبور کنند. این سیستم در حال پردازش داده‌های بیومتریک برای شناسایی افراد است. بنابراین، باشگاه به یک مبنای معتبر برای پردازش چنین داده‌های شخصی حساسی نیاز دارد. این مثال می‌تواند در خصوص اسکن چهره افراد نیز وجود داشته باشد. همچنین باید گفت در ماده ۴ (۱۴) مقررات اروپایی حفاظت از داده، برای داده‌های زیست‌سنجی به داده‌های تصویر چهره و اسکن اثر انگشت اشاره شده است، ولی باید گفت که این موارد جامع و حصری نیستند و از باب تمثیل بیان شده‌اند. مثال‌های دیگر از داده‌های بیومتریک می‌تواند تحلیل صدای اشخاص، تجزیه و تحلیل امضا و دستنویس افراد باشد (ICO 2019).

تاکنون روشن شد که به‌دلیل ماهیت ویژه داده‌های شخصی حساس، پردازش آن‌ها به‌موجب مقررات اروپایی حفاظت از داده ممنوع است؛ لیکن قانون‌گذار استثناهایی را بر این ممنوعیت لحاظ کرده است. ماده ۹ (۲) این مقررات استثناها از ممنوعیت پردازش داده‌های شخصی حساس را بیان می‌کند. این موارد حصری است و قابل تعمیم نیست (van Veen 2018, 72)؛ چرا که قانون‌گذار اتحادیه اروپا در مقام بیان، صرفاً به موارد ذیل بسنده کرده است. این استثناها، پردازش بر اساس رضایت صریح شخص موضوع داده، پردازش داده‌های شخصی حساس علنی‌شده، پردازش در زمینه مربوط به استخدام و تأمین اجتماعی، پردازش به‌دلیل حفاظت از منافع حیاتی افراد، پردازش توسط سازمان‌ها و نهادهای غیرانتفاعی در مسیر فعالیت‌های قانونی‌شان، پردازش بر اساس منافع عمومی، پردازش بر اساس زمینه‌های مربوط به مراقبت‌های بهداشتی و مسائل سلامت عمومی، پردازش به جهت اهداف تحقیقاتی (معافیت تحقیقاتی)، و پردازش برای رسیدگی به دعاوی حقوقی است (EUR-Lex 2016, 38 & 39).

از میان موارد مذکور، سه مورد، یعنی پردازش بر اساس رضایت صریح شخص موضوع داده[1]، پردازش به‌دلیل حفاظت از منافع حیاتی افراد، و پردازش بر اساس منافع عمومی با مبانی حقوقی پردازش مذکور در ماده ۶ مقررات اروپایی حفاظت از داده[2] -که مربوط به اصول حاکم بر پردازش به‌طور کلی است- مشترک است. در خصوص این سه مورد باید گفت اگر که شخص موضوع داده به صراحت به پردازش داده شخصی حساس خود برای یک یا چند هدف مشخص رضایت دهد، چنین رضایتی پردازش داده شخصی حساس را مجاز می‌نماید. چنین اقدام ایجابی نه‌تنها باید شرایط کلی رضایتِ معتبر بر

1. explicit consent

البته در ماده ۶ GDPR که مبانی حقوقی پردازش مقرر شده، واژه «رضایت» و برای پردازش داده شخصی حساس «رضایت صریح» بیان شده است. رضایت صریح در GDPR تعریف نشده است، ولی به نظر می‌رسد تفاوت چندانی با لزوم وجود مجموعه شرایط رضایت که در ماده ۴ (۱۱) GDPR بیان شده است، ندارد. طبق ماده ۴ (۱۱) GDPR، رضایت به معنای هرگونه اشاره آزادانه، خاص، آگاهانه و بدون ابهام اشخاص موضوع داده است که توسط شخص موضوع داده با گفتار یا با اقدام ایجابی روشن دال بر موافقت اشخاص موضوع داده نسبت به پردازش داده‌های شخصی‌شان باشد- تفاوت اصلی به احتمال در این است که رضایت باید در یک اظهارنامه واضح (اعم از شفاهی یا کتبی) تائید شود. در واقع، رضایت صریح باید به صراحت در کلمات تائید شود. به‌طور مثال، درخواست رضایت در اظهارنامه کتبی باید برجسته شود؛ به‌طوری که درخواست رضایت را واضح سازد و به‌طور صریح از کلمه «رضایت» استفاده شود تا شخص موضوع داده آن را تائید نماید (ICO n.d.-d).

۲. ماده ۶ GDPR مقرر می‌کند «پردازش مجاز است اگر حداقل یکی از موارد زیر وجود داشته باشد: الف- شخص موضوع داده به پردازش داده‌های شخصی خود برای یک یا چند هدف خاص رضایت داده باشد؛ ب- پردازش برای اجرای قرارداد ضروری است، شخص موضوع داده باید یکی از اطراف قرارداد باشد یا پردازش به‌منظور انجام مراحل به درخواست شخص موضوع داده قبل از انعقاد قرارداد رخ دهد؛ ج- پردازش برای انجام تعهد قانونی که کنترل‌کننده تابع آن است، ضروری است؛ د- پردازش برای حفظ منافع حیاتی شخص موضوع داده یا شخص حقیقی دیگری ضروری است؛ ه- پردازش برای انجام وظیفه‌ای در جهت منافع عمومی یا اعمال اختیارات رسمی واگذار شده به کنترل‌کننده ضروری است؛ و- پردازش برای اهداف مشروع دنبال‌شده توسط کنترل‌کننده یا شخص ثالث، ضروری است، مگر در مواردی که این منافع تحت‌الشعاع منافع، حقوق یا آزادی‌های اساسی شخص موضوع داده قرار گیرند که نیازمند حفاظت از داده‌های شخصی است، به‌خصوص در صورتی که شخص موضوع داده کودک است. بند (و) برای پردازش توسط مراجع عمومی در انجام وظایف شان اعمال نمی‌شود» (EUR-Lex 2016, 36).

اساس ماده ۷ مقررات اروپایی حفاظت از داده را داشته باشد[۱]، بلکه باید به داده‌های شخصی حساس که در معرض پردازش هستند، به صراحت اشاره کند. به‌عنوان نمونه در زمانی که اشخاص موضوع داده از رسانه‌های اجتماعی -مانند فیس‌بوک- استفاده می‌کنند، فعالیت‌های چنین اشخاصی حاکی از رضایت صریح آن‌ها برای استفاده از علایقی که حاوی داده‌های شخصی حساس هستند، به‌منظور اهداف تبلیغاتی نیست (Cabañas, Cuevas & Cuevas 2018, 3). همچنین پردازش داده‌های شخصی حساس مجاز است، اگر چه برای حفاظت از منافع حیاتی شخص موضوع داده یا فرد دیگری ضروری باشد. این امر در صورتی است که شخص موضوع داده از لحاظ جسمی یا قانونی قادر به رضایت دادن نیست. منافع حیاتی، تمام نیازها و منافع وجودی، به‌ویژه حفاظت از زندگی و تمامیت جسمی است (Voigt & von dem Bussche 2017: 113). افزون بر پردازش بر اساس منافع عمومی نیز سببی برای پردازش داده شخصی حساس است، در صورتی که پردازش بر اساس قانون اتحادیه یا کشور عضو و متناسب با هدف مورد نظر ضروری باشد، همچنین حق حفاظت از داده محترم شمرده شود و برای حفاظت از حقوق اساسی و منافع شخص موضوع داده اقدامات مناسب و خاصی فراهم شده باشد. منافع عمومی طیف وسیعی از ارزش‌ها و اصول مربوط به یک جامعه را پوشش می‌دهد. منافع تجاری یا خصوصی با منافع عمومی یکسان نیستند و برای پردازش، اشاره به منافع کنترل‌کننده کافی نیست. منافع عمومی باید بالفعل و واقعی باشند؛ چرا که با توجه به ماهیت ویژه داده‌های شخصی حساس، یک استدلال مبهم یا کلی، منفعت عمومی را ایجاد نمی‌کند، بلکه باید استدلال‌های خاص صورت گیرد. چنین منافعی می‌تواند تضمین برابری یا جلوگیری از

---

۱. «ماده ۷ - شرایط رضایت: ۱- در جایی که پردازش بر اساس رضایت است، کنترل‌کننده باید بتواند ثابت کند که شخص موضوع داده با پردازش داده‌های شخصی خود موافقت کرده است؛ ۲- اگر رضایت شخص موضوع داده در ضمن اظهارنامه کتبیِ مرتبط با موضوعات دیگر کسب شود، درخواست رضایت باید به شیوه‌ای ارائه شود که به‌وضوح از سایر موارد، به شکلی قابل فهم و در دسترس، با استفاده از زبانی روشن و ساده قابل تشخیص باشد. هر بخشی از چنین اظهارنامه کتبی که ناقض این مقررات است، الزام‌آور نیست؛ ۳- شخص موضوع داده باید این حق را داشته باشد که در هر زمان رضایت خود را پس بگیرد. پس‌گرفتن رضایت، بر مجاز بودن پردازش مبتنی بر رضایت قبل از پس گرفتن، تأثیری نخواهد داشت. قبل از کسب رضایت، شخص موضوع داده باید از حق پس گرفتن مطلع شود. انصراف از رضایت باید به‌راحتیِ کسب رضایت باشد؛ ۴- هنگام ارزیابی اینکه آیا رضایت آزادانه است، باید حداکثر توجه را مبذول داشت که آیا اجرای یک قرارداد، از جمله ارائه یک خدمت، مشروط به رضایت برای پردازش داده‌های شخصی است که برای اجرای آن قرارداد ضروری نیستند یا خیر» (EUR-Lex 2016, 37).

تقلب باشد. با این حال، کنترل‌کننده باید بتواند نشان دهد که تمام مراحل پردازش برای دستیابی به چنین منفعتی ضروری است و با اصلِ به‌حداقل رساندن داده‌ها مطابقت دارد (ICO 2019). افزون بر سه مورد مذکور، سایر دلایلی که به‌موجب آن‌ها پردازش داده‌های شخصی حساس مجازند، به‌شرح زیر است:

- علنی‌شدن توسط شخص موضوع داده: داده‌های شخصی حساسی که به‌وضوح توسط شخص موضوع داده، علنی و افشا شده، و قابل پردازش است. افشا باید ناشی از تصمیم آزاد شخص موضوع داده باشد. در واقع، شخص موضوع داده باید اقداماتی را انجام دهد که داده‌ها را عمومی می‌کند. بدین جهت اگر اطلاعات مربوط به وضعیت سلامتی یک فرد به‌صورت عمومی از تارنمای مراکز بهداشت در دسترس باشد، به‌طور منطقی این داده‌های عمومی‌شده اقدامی عمدی از سوی شخص موضوع داده نبوده و بدین دلیل، مجوزی برای پردازش این داده‌های بهداشتی نیست. در مقابل، وابستگی‌های سیاسی یک عضو مجلس داده‌های شخصی حساس هستند (عقاید سیاسی). با این حال، چنین عقایدی به‌وضوح توسط شخص موضوع داده علنی شده است، زیرا این شخص به‌طور آزادانه برای توصیف جایگاه خود به عموم مردم، چنین داده‌هایی را آشکار نموده است. در این فرض، خود شخص موضوع داده به‌طور خودمختار تصمیم گرفته است داده‌های حساس خود را عمومی نماید و این امر بدون شک یک اقدام عمدی از جانب او بوده است. در سایر موارد تشخیص عمومی‌شدن داده‌ها توسط خود شخص دشوار است و باید اشخاص پردازش‌کننده داده، جانب احتیاط را برگزینند و به مبنای دیگری برای پردازش تمسک نمایند. این موارد از جمله در جایی است که فرد ضمن مطلبی در رسانه اجتماعی برای خانواده و دوستان داده‌های حساسی را منتشر می‌کند، ولی تنظیمات پیش‌فرض آن رسانه، داده‌ها را عمومی می‌کند. در این موارد، قابلیت جریان این مبنا بسیار دشوار است؛ زیرا در جایی این مبنا قابل استفاده است که به‌طور واقع‌بینانه داده‌ها با اقدامی عمدی از جانب شخص موضوع داده برای عموم افراد قابل دسترسی شوند و افشای اطلاعات برای مخاطبان محدود، لزوماً به معنای «افشای عمومی» نیست (ICO 2019)؛
- زمینه‌های مربوط به استخدام و تأمین اجتماعی: در صورتی که پردازش برای انجام تعهدات و اعمال حقوق خاص کنترل‌کننده یا شخص موضوع داده در زمینه استخدام و تأمین اجتماعی ضروری باشد، البته تا جایی که به‌موجب قانون اتحادیه اروپا

یـا کشـورهای عضـو مجـاز باشـد یـا در صورتـی کـه یـک توافـق جمعـی مطابـق قانـون کشـورهای عضـو اتحادیـه اروپـا، تدابیـر حفاظتـی مناسـب بـرای حقـوق و منافـع اساسـی شـخص موضـوع داده را فراهـم کنـد. بـا وجـود ایـن اسـتثنا —از ممنوعیـت پـردازش داده‌هـای شـخصی حسـاس- کارفرمایانـی کـه به‌طـور منظـم بـه پـردازش داده‌هـای شـخصی حسـاس، ماننـد داده‌هـای بهداشـتی در رابطـه بـا اسـتخدام نیـاز دارنـد، بایـد تدابیـر حفاظتـی‌ای را ارائـه دهنـد کـه مطابـق بـا سـطح بـالای حفاظـت از داده‌هـای شـخصی حسـاس باشـد (Voigt & von dem Bussche 2017, 112)؛

- پـردازش توسـط سـازمان‌ها و نهادهـای غیرانتفاعـی در مسـیر فعالیت‌هـای قانونی‌شـان: پـردازش توسـط نهادهـای غیرانتفاعـی بـا هـدف اتحـاد سیاسـی، مذهبـی یـا صنفـی اسـت کـه صرفـاً بـه اعضـای سـابق یـا اشـخاصی کـه بـا آن نهـاد ارتبـاط دارنـد، مربـوط می‌شـود و داده‌هـای شـخصی در خـارج از آن نهـاد بـدون رضایـت اشـخاص موضـوع داده افشـا نمی‌شـوند (EUR-Lex 2016, 38). به‌عنـوان مثـال، یـک کلیسـا داده‌هـای شـخصی اعضـا و حامیانـش را پـردازش می‌کنـد تـا فعالیت‌هـای کلیسـا را اداره کـرده و مراقبت‌هـای معنـوی را فراهـم کنـد. کلیسـا می‌توانـد بـرای پـردازش داده‌هایـی کـه عقایـد مذهبـی آن‌هـا را نشـان می‌دهـد، بـه ایـن اسـتثنا اسـتناد کنـد. لیکـن اگـر ایـن کلیسـا یـک گـزارش سـالانه منتشـر می‌کنـد کـه بـرای اشـخاص ثالـث نیـز در دسـترس اسـت، کلیسـا بایـد قبـل از نام‌گـذاری هـر یـک از اعضـای خـود در گـزارش سـالانه به‌دنبـال رضایـت صریـح آن‌هـا باشـد (ICO 2019)؛
- زمینه‌هـای مربـوط بـه مراقبت‌هـای بهداشـتی و مسـائل سـلامت عمومـی: در صورتـی کـه پـردازش بـرای اهـداف مراقبت‌هـای بهداشـتی مذکـور در مـاده ۹ (۲) (ح) ایـن مقـررات (اهـداف پزشـکی پیشـگیرانه یـا شـغلی، تشـخیص پزشـکی، ارائـه مراقبت‌هـای بهداشـتی، اجتماعـی یـا درمـان، مدیریـت سـامانه‌ها و خدمـات بهداشـتی یـا اجتماعـی) اسـت و بـر اسـاس قانـون کشـورهای عضـو اتحادیـه اروپـا یـا اتحادیـه اروپـا یـا پیـرو قـرارداد بـا یـک متخصـص بهداشـت ضـروری اسـت. به‌موجـب مـاده ۹ (۳) «درجایـی کـه پـردازش پیـرو قـرارداد بـا متخصـص بهداشـت انجـام می‌شـود، پـردازش بایـد توسـط یـا تحـت مسـئولیت یـک متخصـص حرفـه‌ای متعهـد بـه رازداری حرفـه‌ای -ماننـد پزشـک- به‌موجـب قوانیـن اتحادیـه اروپـا یـا کشـور عضـو انجـام شـود. ایـن امـر باعـث می‌شـود کـه محافظـت از داده‌هـا در مـواردی کـه پـردازش مبتنـی بـر قانـون نیسـت، لیکـن داده‌هـای شـخصی حسـاس وجـود

دارد، تقویت شود (EUR-Lex 2016, 38). به‌عنوان مثال، یک پزشک روزانه تعدادی از بیماران را در مطب خود معاینه می‌کند. پزشک معاینات را در یک پایگاه داده ثبت می‌کند که شامل نام و نام خانوادگی بیمار، توصیف علائم و داروهای تجویز شده است. این داده‌ها به‌عنوان داده‌های شخصی حساس در نظر گرفته می‌شوند، اما پردازش داده‌های مربوط به سلامت توسط مطب مجاز است، زیرا برای اهداف درمانی مورد نیاز است و تحت مسئولیت یک پزشک با تعهد رازداری حرفه‌ای انجام می‌شود (European Commission 2018c). در خصوص مسائل سلامت عمومی –ماده ۹ (۲) (ت) مقررات اروپایی حفاظت از داده– نیز باید گفت پردازش مجاز است در صورتی که با دلایل مهم منافع عمومی در زمینهٔ بهداشت عمومی ضروری باشد و چنین پردازشی بر اساس قانون کشورهای عضو اتحادیه اروپا یا اتحادیه اروپا صورت گیرد. دلایل مهم در این قسم می‌تواند محافظت در برابر تهدیدهای جدی فرامرزی برای سلامت یا تضمین استانداردهای بالا و ایمنی مراقبت‌های بهداشتی، محصولات پزشکی یا دستگاه‌های پزشکی باشد (EUR-Lex 2016, 38). مثال این قسم را می‌توان اپیدمی کرونا بیان نمود که در شرایط فعلی از مسائل مهم مربوط به سلامت عمومی است. اتحادیه اروپا با تنظیم دستورالعمل مستقلی در خصوص «پردازش داده‌های مربوط به سلامت در خصوص تحقیقات نسبت به اپیدمی کرونا»[1] مقرر نموده است که مفاد مقررات اروپایی حفاظت از داده نسبت به پردازش داده‌های مربوط به سلامت در زمینهٔ تحقیقات مخصوص به بیماری کرونا نیز قابل اجراست (European Data Protection Board 2020, 13). بنابراین، مقابله با اپیدمی مذکور نیز پردازش داده‌های شخصی را مجاز می‌نماید. علت وجود این استثنا –از ممنوعیت پردازش داده‌های شخصی حساس– ضرورت دستیابی، درک بهتر، شناسایی بالقوه بیماری‌ها و مسائل درمانی است (Shabani & Borry 2018, 149)؛ لیکن استثنای مذکور در این قسمت بدان معنا نیست که کسانی که به‌دلایل محرمانه پزشکی به داده‌های شخصی دسترسی ندارند، اکنون می‌توانند دسترسی داشته باشند. همچنین اگر داده‌های شخصی برای انجام موارد مرتبط، به یک نهاد قانونی دیگر منتقل شود، کنترل‌کننده جدید به مبنای حقوقی مخصوص به خود نیاز خواهد داشت (van Veen 2018 72 & 73). افزون

1. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak

بـر ایـن، از آنجـا کـه داده‌هـای شـخصی مربـوط بـه سـلامت می‌توانـد بـرای اهدافـی بـه غیـر از درمـان و امـور درمانـی اسـتفاده شـود کـه منجـر بـه تجاری‌سـازی داده‌هـا و اسـتفاده از داده‌هـا بـه ضـرر اشـخاص موضـوع داده تمـام شـود، بایـد در خصـوص اینکـه اسـتفاده از داده‌هـا، به‌طـور مسـتقیم بـرای اهـداف درمانـی و مسـایل مرتبـط بـا درمـان باشـد، دقـت نمـود و محـدودهٔ اسـتثنا را تـا ایـن مـرز دانسـت (Skovgaard, Wadmann & Hoeyer 2019, 570)؛

- اهـداف تحقیقاتـی (معافیـت تحقیقاتـی): در صورتـی کـه پـردازش بـرای اهـداف بایگانـی در جهـت منافـع عمومـی، اهـداف تحقیقـات علمـی یـا تاریخـی یـا اهـداف آمـاری مبتنـی بـر مـاده ۸۹ (۱) مقـررات اروپایـی حفاظـت از داده، ضـروری اسـت و چنیـن پردازشـی بـر اسـاس قوانیـن کشـورهای عضـو اتحادیـه اروپـا یـا اتحادیـه اروپـا صـورت گیـرد، پـردازش داده‌هـای شـخصی حسـاس مجـاز اسـت. ایـن فعالیت‌هـا بـه نفـع عمـوم اسـت و بدیـن جهـت در زمـره اسـتثنائات اسـت. بـا وجـود ایـن، پـردازش انجام‌شـده به‌موجـب ایـن مفـاد منـوط بـه حفاظـت مناسـب اسـت و بـرای اطمینـان از اصـل بـه حداقـل رسـاندن داده بایـد اقدامـات حفاظتـی مطابـق بـا ماهیـت حسـاس داده‌هـای شـخصی مربوطـه بـه‌کار گرفتـه شـود[1] (EUR-Lex 2016, 39). دامنـهٔ اهـداف تحقیقاتـی به‌طـور موسـع تفسـیر می‌شـود، از جملـه توسـعه و عرضـهٔ فنـاوری، تحقیقـات بنیـادی، تحقیقـات کاربـردی و تحقیقـات بـا بودجـهٔ خصوصـی، همچنیـن اهـداف تحقیقـات علمـی می‌تواننـد مطالعـات بـه نفـع عمـوم در زمینـهٔ سـلامت عمومـی باشـد (Olimid, Rogozea & Olimid 2018, 635). وجـود چنیـن دامنـهٔ گسـترده‌ای در خصـوص معافیـت تحقیقاتـی ممکـن اسـت ایـن امـر را بـه ذهـن متبـادر سـازد کـه داده‌هـای شـخصی حسـاس در هـر زمـان و بـه هـر هـدف تحقیقاتـی می‌تواننـد پـردازش شـوند و بـرای زمـان نامعیـن می‌تواننـد ذخیـره شـوند؛ در حالـی کـه ایـن امـر بـا برخـی از اصـول مقـررات اروپایـی حفاظـت از داده ماننـد محدودیـت ذخیره‌سـازی داده‌هـای شـخصی مغایـر اسـت. در پاسـخ بایـد گفـت گرچـه چنیـن اسـتثنایی وجـود دارد و دامنـه توسـعه‌ای نیـز بـرای آن

---

۱. در ایـن خصـوص مـاده ۸۹ (۱) GDPR مقـرر می‌کنـد: «پـردازش بـرای اهـداف بایگانـی در جهـت منافـع عمومـی، اهـداف تحقیقـات علمـی، تاریخـی یـا آمـاری، بایـد مطابـق بـا ایـن مقـررات نسـبت بـه حقـوق و آزادی‌هـای شـخص موضـوع داده، تحـت تدابیـر حفاظتـی مناسـب قـرار گیرنـد. تدابیـر حفاظتـی دال بـر وجـود اقدامـات فنـی و سـازمانی به‌طـور خـاص بـرای رعایـت اصـل بـه حداقـل رسـاندن داده‌هاسـت. ایـن تدابیـر ممکـن اسـت شـامل مستعارسـازی باشـد، بـه شـرطی کـه اهـداف مذکـور در ایـن مـاده، بـا مستعارسـازی محقـق شـوند. در صورتـی کـه ایـن اهـداف را می‌تـوان بـا پردازشـی کـه اجـازه شناسـایی اشـخاص موضـوع داده را نمی‌دهـد یـا دیگـر اجـازه نمی‌دهـد، انجـام داد، ایـن اهـداف بایـد بـا آن روش پردازشـی انجـام شـوند» (EUR-Lex 2016, 84 & 85).

مقرر شده است (Pormeister 2017, 146)، لیکن مقررات اروپایی حفاظت از داده تعادلی بین نیاز به حفاظت مؤثر از حقوق اشخاص موضوع داده و پردازش داده‌های شخصی حساس برای اهداف تحقیقاتی برقرار می‌سازد؛ زیرا به‌موجب ماده ۸۹ (۱) مقررات اروپایی حفاظت از داده، پردازش برای اهداف تحقیقاتی باید تحت تدابیر حفاظتی مناسب صورت گیرد. چنین تدابیری می‌تواند مستعارسازی داده‌های شخصی حساس باشد، به‌گونه‌ای که به شخص موضوع داده یکتایی اشاره نکند (Chassang 2017, 11 & 12) یا طراحی زیرساخت لازم برای ابزارهای فناوری اطلاعات و مدیریت داده‌ها به‌منظور تضمین حفاظت از داده باشد. حتی باید گفت اگر داده‌های پردازش‌شده مرکب از داده‌هایی در خصوص مراقبت‌های بهداشتی و تحقیقات علمی باشد، باید به‌وضوح این دو مورد از هم متمایز شود و در نتیجه، برای هر یک از این اقسام، بسترهای حفاظتی مناسب دنبال شود (Amram 2020: 6)؛

- رسیدگی به دعاوی حقوقی: ضرورت پردازش برای ایجاد، اِعمال و یا دفاع از دعاوی حقوقی -یا هر زمان که دادگاه‌ها به موجب صلاحیت قضایی‌شان عمل می‌کنند- نیز جوازی بر پردازش داده شخصی حساس است. این امر شامل رسیدگی به دعاوی در دادرسی دادگاه‌ها و در رویه‌های اجرایی یا خارج از دادگاه‌هاست. ماهیت ویژه داده‌های شخصی حساس به‌موجب ماده ۹ مقررات اروپایی حفاظت از داده به تقابل منافع برای واقع‌شدن تحت این استثنای قانونی نیاز دارد (در واقع باید منفعت شخص موضوع داده در حفظ داده‌های خود و رسیدگی به دعاوی حقوقی در مقابل هم سنجیده شود و به منفعت غالب عمل شود). به‌عنوان مثال، بیمار سابق یک بیمارستان (A)، از بیمارستان شکایت می‌کند. بیمارستان از پرونده پزشکی A استفاده می‌کند تا از خود در برابر طرح دعوی دفاع کند. در این مثال، پرونده پزشکی، داده‌های مربوط به سلامت A را نشان می‌دهد و در نتیجه، شایستگی حفاظت به‌موجب ماده ۹ مقررات اروپایی حفاظت از داده را دارد. با این حال، بیمارستان از داده‌های شخصی A برای دفاع از خودش در برابر طرح دعوی A استفاده می‌کند. داده‌های شخصی برای اهداف اثباتی در جریان دادرسی لازم است. در این مثال، حق حریم خصوصی A با توجه به ضروری بودن پردازش داده‌های A به‌منظور ارائه مدرک در جریان دادرسی از بین می‌رود (استفاده از داده‌ها در جریان دادرسی نسبت به حفظ داده‌ها برای A غالب است) (Voigt & von dem Bussche 2017, 113 & 114).

۴-۲. پردازش داده شخصی حساس در نظام حقوقی ایران

از آنجا که حقوق ایران به‌طور ویژه و جامع به چگونگی حمایت از داده‌های شخصی حساس نپرداخته است، چنین حمایتی باید از منابع مختلف حقوق ایران کشف شود. در این مسیر ابتدا قوانین موضوعه ایران قابل بررسی است. از میان قوانین موضوعه، صرفاً ماده ۵۸ قانون تجارت الکترونیکی مصوب ۱۳۸۲ است که به صراحت، داده‌های شخصی حساس را مورد توجه قرار داده است. این ماده مقرر می‌کند «ذخیره، پردازش و یا توزیع «داده‌پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیرقانونی است». نسبت به این ماده چند نکته قابل بیان است. اول اینکه گرچه قانون‌گذار ایرانی بر حساس‌بودن داده‌های مذکور در این ماده صراحتی ندارد، لیکن ممنوعیت پردازش آن‌ها و اشتراک مصادیق این ماده با ماده ۹ (۱) مقررات اروپایی حفاظت از داده، مبین حساس بودن داده‌های مذکور است. همچنین این ماده صرفاً به یکی از مبانی حقوقی پردازش داده شخصی حساس -رضایت صریح- اشاره نموده است و از اصل ممنوعیت پردازش داده شخصی حساس تنها مواردی را که رضایت صریح شخص موضوع داده وجود دارد، استثنا نموده است. بدین جهت با توجه به این ماده، اصل ممنوعیت پردازش داده شخصی حساس[1] و رضایت صریح به‌عنوان استثنائی از ممنوعیت، قابل پذیرش است؛ هرچند پذیرش این دو امر نیز به‌طور کلی است و در جزئیات تفاوتی‌هایی وجود دارد. به‌عنوان نمونه مادهٔ مربوطه از قانون تجارت الکترونیکی، برخی از مصادیق داده‌های شخصی حساس مانند عقاید سیاسی، عضویت در اتحادیه‌های صنفی و داده‌های زیست‌سنجی را مورد تصریح قرار نداده است. افزون

۱. در ارتباط با چنین ممنوعیتی می‌توان به اصل ۲۵ قانون اساسی ایران اشاره نمود. به‌موجب این اصل، تجسس که به معنای دسترسی به اسرار افراد بدون رضایت آن‌هاست، ممنوع است. توضیح ارتباط اینکه از یک‌سو تجسس نوعی پردازش است و از سویی دیگر، یکی از مصادیق اسرار می‌تواند اطلاعات و داده‌های شخصی حساس باشد. در خصوص اینکه داده‌های شخصی سر هستند باید گفت: سر امری نسبی است و مصادیق آن با توجه به شرایط افراد و انگیزه آن‌ها در پنهان‌کردن امری متفاوت می‌شود (قماشی ۱۳۸۵، ۴). همچنین، داده‌های شخصی ارزشمند هستند و غالباً اشخاص حقیقی تمایل ندارند که داده‌های شخصی آن‌ها برای تمامی افراد آشکار شود و موجب شناسایی آن‌ها گردد. در این راستا یکی از اصول حاکم بر داده‌های شخصی حفظ تمامیت و محرمانگی داده‌های شخصی است. هدف از این اصل عدم تعرض به حقوق اشخاص موضوع داده و قرار نگرفتن در معرض سوءاستفاده است. با توجه به این امر در بسیاری از موارد می‌توان داده‌های شخصی را به‌نوعی سر دانست.

بر این، حمایت‌های قانون تجارت الکترونیکی برای تمامی بسترهای پردازشی داده‌های شخصی قابل جریان نیست و از این جهت نیز محدود است. با این حال و به‌دلیل فقدان تصریح قانونی نسبت به داده‌های شخصی حساس، در سایر قوانین موضوعه، می‌توان این ماده را مشعر به ممنوعیت پردازش داده‌های شخصی حساس و رضایت به‌عنوان استثنایی از این ممنوعیت دانست.

فارغ از مادهٔ مذکور، در قوانین موضوعه الزاماتی نسبت به داده‌های شخصی حساس وجود ندارد. البته، گفتنی است که «پیش‌نویس لایحه صیانت و حفاظت از داده‌های شخصی»[1] در بند ب ماده ۲ به تعریف دادهٔ شخصی حساس پرداخته و بیان نموده «داده شخصی حساس عبارت است از داده شخصی که ریشه قومی یا قبیله‌ای، نظرات سیاسی، مذهبی و فلسفی، مشخصات وراثتی یا اطلاعات سلامت شخص موضوع داده را آشکار می‌سازد». فارغ از وضعیت این سند و عدم شمول این مفاد بر تمامی مصادیق داده‌های شخصی حساس، این پیش‌نویس الزامات و اصولی برای پردازش این‌گونه داده‌ها مقرر نکرده و صرف این تعریف نیز مبین حمایت ویژه‌ای نیست. بدین جهت برای پذیرش یا عدم پذیرش سایر استثنائات از ممنوعیت پردازش داده شخصی حساس به‌موجب مقررات اروپایی حفاظت از داده —به‌غیر از رضایت- در نظام حقوقی ایران، باید به نظریات دکترین، مبانی حقوق ایران به‌ویژه فقه امامیه تمسک جست.

در این راستا ابتدا پردازش داده شخصی حساس به‌دلیل وجود منافع حیاتی قابل بحث است. با توجه به اینکه حفاظت از منافع حیاتی افراد به معنای حفاظت از جان شخص موضوع داده و افراد دیگر است، جریان این استثنا –از ممنوعیت پردازش- در نظام حقوقی ایران پذیرفتنی است. این امر بدین دلیل است که اهمیت حفظ جان در فقه، حقوق و

---

۱. پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» در تیرماه سال ۱۳۹۷ در سایت وزارت ارتباطات و فناوری اطلاعات ایران در خصوص حمایت از دادهٔ شخصی منتشر شده است. چنین سندی پیش‌نویس است و تاکنون حتی نسخه نهایی برای این پیش‌نویس منتشر نشده است. البته به نظر می‌رسد با ارائه طرح «حمایت و حفاظت از داده و اطلاعات شخصی» که در بیست‌وچهارم شهریورماه ۱۴۰۰ در صحن علنی مجلس اعلام وصول شده است، پیش‌نویس مذکور در همین مرحله رهاشده باشد. خصوصاً اینکه طرح مذکور گزیده‌ای از پیش‌نویس سابق است. در واقع، این طرح که با چند سال فاصله از ارائه پیش‌نویس، به‌تازگی در خصوص حمایت از داده شخصی و اشخاص موضوع داده، در مجلس وصول شده است، در محتوا نسبت به مواد استفاده‌شده از پیش‌نویس، تغییری نکرده است و با عدم شفافیت و فقدان افزایش حمایت از داده شخصی و اشخاص موضوع داده، با همان کیفیت مقرر در پیش‌نویس، به حمایت از داده‌های شخصی و اشخاص موضوع داده پرداخته است.

قوانین موضوعه ایران مورد تصریح قرار گرفته است. در واقع، حفظ جان خود و افراد دیگر واجب است و در معرض هلاکت قراردادن آن و همچنین تعرض به جان انسان محترم حرام است (هاشمی شاهرودی ۱۳۸۲ ق، ۳/ ۳۱۶؛ مکارم شیرازی ۱۳۸۵، ۴۸۴/۱) حتی برای حفظ جان ارتکاب به بعضی از محرمات جایز می‌شود (مدرسی ۱۳۹۳، ۱۶۹). از قوانین موضوعه ایران نیز این امر قابل استنباط است. به‌عنوان نمونه به‌موجب ماده ۱۵۸ قانون مجازات اسلامی مصوب ۱۳۹۲ «ارتکاب رفتاری که طبق قانون جرم محسوب می‌شود، در صورتی که ارتکاب رفتار برای اجرای قانون اهم لازم باشد، قابل مجازات نیست». به‌موجب این ماده در صورتی که امری اهم وجود داشته باشد، لطمه به منافع افراد قابل مجازات نیست. در نظریات دکترین مصادیق این ماده افزون بر سایر موارد، تخریب اموال و اشیا برای نجات جان، سلب آزادی برای نجات جان و ورود با قهر و غلبه به ملک دیگری برای نجات جان بیان شده است (گلدوزیان ۱۳۹۷، ۲۳۵-۲۳۷). این مصادیق مبین اهمیت حفظ جان در مقابل سایر منافع از جمله پردازش داده‌های شخصی است. همچنین به‌موجب ماده ۴۹۷ قانون پیش‌گفته «در موارد ضروری که تحصیل برائت ممکن نباشد و پزشک برای نجات مریض، طبق مقررات اقدام به معالجه نماید، کسی ضامن تلف یا صدمات وارده نیست». اهمیت حفظ جان افراد، علت عدم ضمان در ماده مذکور است —حتی تشخیص فوریت و ضرورت نیز بر عهده پزشک معالج است (کارخیران ۱۳۹۸، ۱۰۱۰) - بنابراین به طریق اولی چنین امر مهمی موجب پردازش داده شخصی شخص موضوع داده و از مبانی حقوقی پردازش داده‌های شخصی حساس است.

استثنای دیگری -از ممنوعیت پردازش- که قابل بررسی است، وجود منفعت عمومی است. منفعت عمومی[1] در اصطلاح به معنای سود و فایده‌ای است که همگان از آن برخوردار خواهند شد و شامل اموری است که برای توده مردم مطلوبیت دارد و آنان را بهره‌مند می‌نماید (منصوریان و شیبانی ۱۳۹۵، ۱۲۲). در فقه امامیه افزون بر منفعت عمومی چنین معنایی با اصطلاح مصلحت عمومی یا مصالح عامه نیز مورد توجه قرار گرفته است. از منظر فقه امامیه، قوانین موضوعه ایران و دکترین حقوقی، منافع عمومی یا مصالح عامه بر منافع خاصه یا مصالح فردی مقدم‌اند (منتظری ۱۳۶۷، ۳۷۶/۵؛ مکارم شیرازی ۱۳۸۵، ۲۷۹/۲؛ میرزای قمی ۱۳۷۱، ۷۱/۴). مبنای چنین تقدمی رعایت صلاح عموم مردم و توجه

1. public interest

به احوال کلی آنان است؛ چرا که منافع عمومی، مصالحی است که نفع آن ناظر به جمع زیادی از مردم است و منافعی نیست که صرفاً جنبه شخصی داشته یا در جهت حفظ منافع فرد، دسته، گروه و جمعیتی خاصی باشد (ایازی ۱۳۸۹، ۳۴۹ و ۳۶۰). این امر در قوانین موضوعه ایران نیز مشهود است. به‌طور نمونه، می‌توان به اصل چهلم قانون اساسی[1]، ماده ۳ قانون نحوه واگذاری و احیای اراضی در حکومت جمهوری اسلامی ایران مصوب ۱۳۵۸[2]، ماده ۱۷ قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری مصوب ۱۳۸۶[3] و ماده ۹ قانون تشویق و حمایت سرمایه‌گذاری خارجی مصوب ۱۳۸۰[4] اشاره کرد. بدین جهت قابل درک است که تقدم منفعت عمومی مقتضای نظم عمومی و عدالت است و دلیلی برای پردازش داده‌های شخصی حساس است (عمید زنجانی ۱۳۹۱، ۱۷۹). همچنین از آنجا که چند استثنای دیگر از ممنوعیت پردازش یعنی پردازش بر اساس زمینه‌های مربوط به مراقبت‌های بهداشتی، مسائل سلامت عمومی و اهداف تحقیقاتی نیز به اهمیت منافع عمومی برمی‌گردد، با پذیرش منفعت عمومی به‌عنوان جوازی بر پردازش داده شخصی حساس، سه مورد مذکور نیز به‌موجب حقوق ایران قابل پذیرش است.

علنی‌شدن داده شخصیِ حساس توسط شخص موضوع داده، استثنای بعدی است. این امر نیز با توجه به «قاعدهٔ اقدام» در نظام حقوقی ایران مورد پذیرش است. به‌موجب این قاعده هرگاه شخصی با آگاهی عملی را انجام دهد، خود مسئول عواقب آن است. بدین جهت حتی اگر اقدام شخص موجب ورود زیان توسط دیگران به او گردد، واردکننده زیان که شخص دیگری است، مسئول خسارت نخواهد بود (محقق داماد ۱۳۸۴، ۱۲۲). به دیگر سخن، اگر کسی اقدام به اسقاط احترام مال خود نماید –داده‌های شخصی نیز به‌دلیل داشتن بعد مالی در زمرهٔ مال‌اند– حق ندارد از باب خسارتی که دیده تقاضای

---

۱. «هیچ‌کس نمی‌تواند اعمال حق خویش را وسیله اضرار به‌غیر یا تجاوز به منافع عمومی قرار دهد».

۲. «حقوق اشخاص بر اراضی دایر توأم با مسئولیت و تکلیفی است که در مورد استفاده و بهره‌برداری مشروع از آن دارند ...».

۳. «دولت یا شخص مجاز از طرف آن، با رعایت ترتیبات زیر می‌توانند از اختراع بهره‌برداری نمایند:
الف– در مواردی که با نظر وزیر یا بالاترین مقام دستگاه ذی‌ربط منافع عمومی مانند امنیت ملی، تغذیه، بهداشت یا توسعه سایر بخش‌های حیاتی اقتصادی کشور، اقتضا کند که دولت یا شخص ثالث از اختراع بهره‌برداری نماید ...».

۴. «سرمایه‌گذاری خارجی مورد سلب مالکیت و ملی‌شدن قرار نخواهد گرفت مگر برای منافع عمومی، به‌موجب فرایند قانونی، به روش غیر تبعیض‌آمیز و در مقابل پرداخت مناسب غرامت به مأخذ ارزش واقعی آن سرمایه‌گذاری بلافاصله قبل از سلب مالکیت».

جبران خسارت نماید و اقدام شخصی بر ضرر خود از مسقطات ضمان است (کاتوزیان ۱۳۹۵، ۱/ ۱۶۴ و ۱۶۵). در بحث حاضر نیز شخص موضوع داده با علنی نمودن داده‌های شخصی حساس خود، زمینهٔ پردازش و یا حتی تعرض به داده‌های شخصی‌اش را فراهم نموده است. مؤید این قسمت می‌تواند بند دهم از سند «سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی» مصوب شورای عالی فضای مجازی در تاریخ ۱۳۹۶/۰۳/۱۳ باشد که مقرر می‌کند «مسئولیت اقدامات کاربران در شبکه‌های اجتماعی بر عهده خود کاربران بوده ...»؛ گرچه این مفاد مربوط به شبکه‌های اجتماعی است، لیکن از آنجا که یکی از بسترهای پردازش چنین شبکه‌هایی است برای بحث حاضر نیز قابل استفاده است.

برای بررسی پردازش در زمینه مربوط به کار و تأمین اجتماعی به‌عنوان استثنایی دیگر، می‌توان به‌تصریح قانون کار استناد نمود. توضیح اینکه به‌موجب ماده ۱۰ قانون کار «قرارداد کار علاوه بر مشخصات دقیق طرفین، باید حاوی موارد ذیل باشد ...». از نص ماده قابل درک است که پردازش داده‌های شخصی از ضروریات چنین قراردادی است و دسترسی به داده شخصی برای زمینه‌های مربوط به کار و تأمین اجتماعی لازم است. بدین جهت از آنجا که کار و تأمین اجتماعی از ضروریات زندگی جمعی است و پردازش داده‌ها در زمینهٔ مذکور نیز برای ضرورت پیش‌گفته لازم است؛ پردازش در این خصوص بلامانع است. البته، چنین پردازشی باید به‌موجب قانون باشد، و همچنین تدابیر حفاظتی مناسب برای حقوق و منافع اساسی شخص موضوع داده نیز فراهم شود.

همچنین استثنای دیگر یعنی پردازش برای رسیدگی به دعاوی حقوقی نیز در نظام حقوقی ایران قابل پذیرش است. این امر بدین دلیل است که به‌موجب اصل سی‌وچهارم قانون اساسی «دادخواهی حق مسلم هر فرد است و هر کس می‌تواند به‌منظور دادخواهی به دادگاه‌های صالح رجوع نماید. همه افراد ملت حق دارند این‌گونه دادگاه‌ها را در دسترس داشته باشند و هیچ‌کس را نمی‌توان از دادگاهی که به‌موجب قانون حق مراجعه به آن را دارد منع کرد». این حق قانونی که در نظام‌های مردم‌سالار، متضمن حقوق و آزادی‌های افراد است (هاشمی ۱۳۹۰، ۳۰۶) لوازم ذاتی و عقلی، عرفی و قانونی خود را نیز دربرمی‌گیرد (محقق داماد ۱۳۸۴، صص ۲۳۶ و ۲۳۷). همچنین شامل تمسک به ادله است. بدین جهت در صورتی که پردازش داده‌های شخصی حساس به‌عنوان دلیل، برای دادرسی و احقاق حق ضروری باشد، چنین پردازشی مجاز بوده و دلیلی بر پردازش داده‌های شخصی حساس است. البته باید دقت شود که در مقام تقابل دو حق حفاظت از

داده و دادخواهی و احقاق حق، مورد دوم غالب باشد.

سرانجام، باید گفت که از میان استثنائات مذکور در مقررات اروپایی حفاظت از داده برای پردازش داده شخصی حساس، صرفاً پردازش توسط سازمان‌ها و نهادهای غیرانتفاعی در جهت فعالیت‌های قانونی‌شان، از منابع مختلف حقوق ایران قابل استنباط نیست. بدین جهت و با جریان اصل عدم، استثنای مذکور در نظام حقوقی ایران قابل پذیرش نیست.

۵. پردازش داده شخصی مربوط به محکومیت و جرائم کیفری

داده‌های شخصی مربوط به محکومیت و جرائم کیفری نیز قسمی از داده‌های شخصی خاص هستند که به موجب مقررات اروپایی حفاظت از داده جهت پردازش آن‌ها باید الزامات خاصی رعایت شود. در این بند، ابتدا به چگونگی پردازش چنین داده‌هایی بر اساس این مقررات و سپس به تطبیق آن با نظام حقوقی ایران پرداخته خواهد شد.

۵-۱. پردازش داده شخصی مربوط به محکومیت و جرائم کیفری به موجب مقررات اروپایی حفاظت از داده

داده‌های شخصی مرتبط با جرائم یا محکومیت‌های کیفری در زمرهٔ داده‌های شخصی حساس نیستند و بدین جهت ماده ۹ مقررات اروپایی حفاظت از داده بر چنین داده‌هایی جاری نیست. لیکن داده‌های شخصی مربوط به محکومیت و جرائم کیفری، داده‌های شخصی خاص محسوب می‌شوند (ICO 2019) و مستلزم حفاظت ویژه هستند، زیرا پردازش این داده‌ها می‌تواند خطرات قابل توجهی برای حقوق و آزادی‌های اساسی افراد ایجاد کند. به‌عنوان مثال، داده‌های مربوط به اتهامات یا محکومیت‌های کیفری می‌تواند تأثیر خاصی بر حق آزادی و امنیت، حق محاکمه عادلانه، حق احترام به زندگی خصوصی و خانوادگی، آزادی انتخاب شغل و حق مشارکت در مشاغل، آزادی انجام یک تجارت و ... داشته باشند (ICO n.d.-c).

برای پردازش چنین داده‌هایی به موجب مقررات اروپایی حفاظت از داده الزامات

خاصی باید رعایت گردد[1]. با این توضیح که جهت مجاز بودن پردازش داده‌های شخصی مرتبط با محکومیت و جرائم کیفری، پردازش باید با تدابیر حفاظتی مناسب، مذکور در ماده ۱۰ این مقررات انجام شود. ماده ۱۰ مقرر می‌کند «پردازش داده‌های شخصی مربوط به محکومیت‌های کیفری و جرائم و یا اقدامات تأمینی مربوطه مبتنی بر ماده ۶ (۱) مقررات اروپایی حفاظت از داده باید صرفاً تحت کنترل مرجع رسمی باشد یا زمانی انجام شود که توسط قانون اتحادیه و یا کشور عضو مجاز است و برای حقوق و آزادی‌های اشخاص موضوع داده ضروری است. هرگونه ثبت جامع از محکومیت‌های کیفری، صرفاً تحت کنترل مرجع رسمی نگهداری می‌شود» (EUR-Lex 2016, 39). با توجه به مفاد مذکور داده‌های شخصی مربوط به محکومیت‌ها و جرائم کیفری، صرفاً در صورتی قابل پردازش است که تحت نظارت مرجع رسمی باشد، گرچه دامنهٔ چنین نظارت و کنترلی مشخص نیست؛ لیکن قواعد مربوطه و سازماندهی آن در صلاحیت کشورهای عضو اتحادیه اروپاست یا زمانی که پردازش توسط قانون کشورهای عضو اتحادیه اروپا یا اتحادیه اروپا برای حمایت مناسب از حقوق و آزادی‌های افراد مجاز باشد (Voigt & von dem Bussche 2017, 115). بنابراین، نهادهای عمومی یا نهادهای خصوصی که وظایف بخش عمومی را بر عهده دارند، مجاز به پردازش داده‌های مرتبط با امور کیفری هستند، در صورتی که توسط قانون برای پردازش چنین داده‌هایی، «اختیار رسمی» به آن‌ها داده شده باشد. این اختیار رسمی می‌تواند از قوانین عادی یا اساسنامه نهادهای مذکور نشأت گیرد. چنین نهادهایی مؤظف هستند قانون خاصی را که به آن‌ها اختیار رسمی پردازش داده‌های مرتبط با امور کیفری را می‌دهد، مشخص کنند. از سوی دیگر، با نبود اختیار رسمی برای پردازش، پردازش داده‌های مرتبط با امور کیفری باید توسط قوانین

---

۱. گفتنی است دستورالعمل (EU) ۶۸۰/۲۰۱۶ که در ۲۷ آوریل ۲۰۱۶ تصویب شده و از ۶ می ۲۰۱۸ لازم‌الاجراست (European Data Protection Supervisor, n.d.) بستر قانونی خاص جهت حمایت از داده‌های شخصی مرتبط با محکومیت‌ها و جرائم کیفری در اتحادیه اروپاست. این دستورالعمل از سویی در خصوص حفاظت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی توسط مقامات صالح به‌منظور پیشگیری، تحقیق، کشف یا پیگرد قانونی جرائم یا اجرای مجازات کیفری و از سوی دیگر، در مورد حرکت آزادانه چنین داده‌هایی است. همچنین این دستورالعمل از حقوق اساسی شهروندان با وجود چنین داده‌هایی حمایت می‌کند و به‌ویژه تضمین خواهد کرد که داده‌های شخصی قربانیان، شاهدان و متهمان باید به‌درستی محافظت می‌شوند. این دستورالعمل همکاری فرامرزی در مبارزه با جرم و تروریسم را تسهیل نموده است (European Commission 2016).

داخلی مجاز باشد. این امر را هر یک از کشورهای عضو اتحادیه اروپا باید در قوانین ملی خود وضع نمایند (ICO, n.d.-b).

اصطلاح «مربوط به» در مادهٔ مذکور باید به‌طور موسع تفسیر شود و بدین جهت مفاد مذکور شامل طیف گسترده‌ای از اطلاعات و داده‌ها در خصوص امور کیفری، اتهامات و ادعاها، امور تحقیقاتی و مقدماتی و ... است. بنابراین، این مفاد نه‌تنها شامل داده‌هایی است که به‌وضوح در مورد محکومیت کیفری به معنای خاص است، بلکه شامل هرگونه اطلاعات و داده‌های شخصی دیگر در ارتباط با محکومیت‌ها و جرائم کیفری نیز هست که شامل اتهامات و ادعاهای اثبات‌نشده، اطلاعات مربوط به نبود محکومیت و اطلاعات و داده‌های شخصی قربانیان و شاهدان است (ICO, n.d.-b). به‌عنوان نمونه، اتهامات یا ادعاهای اثبات‌نشده از آن جهت که به‌طور بالقوه می‌توانند تأثیر نامطلوبی بر منافع، حقوق و آزادی‌های افراد داشته باشند، نیاز به حمایت ویژه دارند. در قالب مثال، می‌توان موردی را فرض کرد که یک مدیر فروشگاه به یکی از کارمندانش مظنون به سرقت از فروشگاه است. مدیر گزارشی تهیه می‌کند که رفتار این کارمند را نشان می‌دهد و تصاویر دوربین مداربسته از کارمند را جمع‌آوری می‌کند. این داده‌های شخصی، داده‌های مرتبط به امور کیفری است؛ هرچند مربوط به ارتکاب جرمی است که هنوز اثبات نشده است (ICO, n.d.-c). یا اطلاعات مربوط به عدم محکومیت که فقدان محکومیت کیفری در مورد یک شخص را نشان می‌دهد، داده‌های مرتبط با محکومیت‌های کیفری است. بنابراین، برای بررسی عدم محکومیت یک شخص باید الزامات ماده ۱۰ مقررات اروپایی حفاظت از داده وجود داشته باشد. به‌عنوان مثال، یک مدرسه، پس از بررسی دقیق سوابق کیفری، معلم استخدام می‌کند. آن‌ها این نتیجه را در پرونده‌های پرسنلی خود نگه می‌دارند. این داده‌ها مربوط به محکومیت‌های کیفری است و بنابراین جمع‌آوری و نگهداری آن‌ها به این معناست که مدرسه داده‌های کیفری را پردازش می‌کند و ملزم به رعایت ماده ۱۰ این مقررات است (ICO, n.d.-c). افزون بر این، اطلاعات و داده‌های شخصی مربوط به قربانیان و شاهدان نیز مربوط به جرائم کیفری است. بنابراین چنین داده‌هایی مشمول ماده ۱۰ مقررات اروپایی حفاظت از داده است. این امر در راستای حفظ حقوق قربانیان و شهود است؛ چرا که پردازش چنین داده‌هایی، خطرات قابل توجهی برای حریم خصوصی افراد مربوطه ایجاد می‌کند. به‌عنوان مثال، یک نیروی پلیس اطلاعات فردی را که قربانی جنایتی خشونت‌آمیز شده است، به سازمانی که از قربانیان حمایت می‌کند، می‌دهد. این

داده‌های شخصی مربوط به جرم کیفری است، اما از آنجا که در راستای اجرای قانون نیست، باید الزامات ماده ۱۰ مقررات اروپایی حفاظت از داده جهت چنین پردازشی وجود داشته باشد (ICO, n.d.-c). همچنین این ماده شامل اطلاعات و داده‌های شخصی مربوط به اقدامات تأمینی نیز می‌شود. با وجود اینکه مقررات اروپایی حفاظت از داده «اقدامات تأمینی مرتبط»[1] را تعریف نمی‌کند. با این حال، این امر می‌تواند شامل داده‌های شخصی در مورد مجازات‌ها، شرایط یا محدودیت‌های اعمال‌شده برای یک فرد به‌عنوان بخشی از فرایند عدالت کیفری یا اقدامات مدنی که در صورت عدم رعایت آن‌ها منجر به مجازات کیفری می‌شود، باشد. بدین جهت دادرسی‌های مدنی و دستوراتی که در نتیجهٔ آن صادر می‌شود، «اقدامات تأمینی مرتبط» تلقی نمی‌شوند، مگر اینکه عدم رعایت آن‌ها مجازات کیفری داشته باشد (ICO, n.d.-b).

بیان شد که الزامات خاص برای پردازش چنین داده‌هایی مربوط به سطح بالای حساسیت این داده‌هاست؛ چرا که اتهامات و محکومیت‌های کیفری می‌توانند اشخاص موضوع داده را برای مدت طولانی بدنام کنند. بنابراین، در مقایسه با داده‌های شخصی حساس مذکور در ماده ۹ مقررات اروپایی حفاظت از داده، هیچ استثنایی برای پردازش وجود ندارد –مقایسه با ماده ۹ (۲) این مقررات– تا به کنترل‌کنندگان و پردازنده‌ها اجازه دهد که از الزامات ماده ۱۰ مقررات اروپایی حفاظت از داده معاف شوند. با این حال، قانون هر یک از کشورهای عضو اتحادیه اروپا می‌تواند در مورد پردازش در زمینهٔ استخدام، استثناهایی را مقرر کنند؛ مانند به‌دست آوردن و پردازش داده‌ها جهت کسب گواهی عدم سوءپیشینه برای متقاضیِ مشاغلی که نیاز به نداشتن سوءپیشینه دارد (Voigt & von dem Bussche 2017, 115).

۵-۲. پردازش داده شخصی مربوط به محکومیت و جرائم کیفری در نظام حقوقی ایران

برای تبیین چگونگی حمایت از داده‌های شخصی مربوط با محکومیت‌ها و جرائم کیفری در نظام حقوقی ایران –به‌دلیل نبود بستر قانونی مستقل در خصوص داده‌های شخصی– باید موادی از قوانین موضوعه ایران که به‌طور موردی به چنین حمایتی اشاره کرده‌اند و برخی نظریات دکترین، مورد توجه قرار گیرند. در این راستا می‌توان به موادی

1. related security measures

از قانون آئین دادرسی کیفری مصوب ۱۳۹۲ با اصلاحات ۱۳۹۴ اشاره نمود. این موارد از جمله ماده ۴۰ است که مقرر می‌کند «افشای اطلاعات مربوط به هویت و محل اقامت بزه‌دیده، شهود و مطلعان و سایر اشخاص مرتبط با پرونده توسط ضابطان دادگستری، جز در مواردی که قانون معین می‌کند، ممنوع است». در خصوص این ماده چند نکته باید مورد توجه قرار گیرد. اول اینکه گرچه در این ماده لفظ «دادهٔ شخصی» مورد تصریح قرار نگرفته است، لیکن از آنجا که اطلاعات مفهوم عامی دارد که شامل داده‌های شخصی نیز می‌شود، این ماده در خصوص بحث حاضر قابل استفاده است. همچنین گفتنی است این ماده جنبه حمایتی نسبت به اشخاص دخیل در فرایند دادرسی دارد. بدین جهت عدم رعایت این ماده ضابطان دادگستری را با ضمانت اجرای مقرر در ماده ۶۳ این قانون[1] -محکومیت به سه ماه تا یک سال انفصال از خدمات دولتی- مواجه خواهد نمود. با توجه به این امر، این ماده مصداقی خاص از جرم افشای اسرار حرفه‌ای -مقرر در ماده ۶۴۸ قانون مجازات اسلامی ۱۳۷۵- خواهد بود (خالقی ۱۳۹۹ ۸۸). همچنین ممنوعیت مقرر در این ماده شامل افشای اطلاعات مربوط به متهم، به‌عنوان «سایر اشخاص مرتبط» نیز می‌شود. بدین جهت حقوق متهم از جمله حق حفاظت از داده‌های شخصی‌اش محترم شناخته شده است و باید رعایت گردد (کارخیران ۱۳۹۴، ۱۸). احترام به این حقوق در راستای تضمین دادرسی منصفانه و پیشگیری از نقض حقوق بشری متهم به موجب قوانین موضوعه ایران است. در واقع، چنین تضمین‌هایی به هدف حمایت از حقوق و آزادی‌های فردی پیش‌بینی شده‌اند (حیدری ۱۳۹۴، ۲۹) که همان غایت مورد توجه در مقررات اروپایی حفاظت از داده است.

با توجه به آنچه بیان شد، این ماده از دو جهت با مقررات اروپایی حفاظت از داده سازگار است. اول اینکه به موجب تصریح این ماده، پردازش اطلاعات و داده‌های شخصیِ مربوط به امور کیفری، صرفاً با حکم قانون مجاز است و بر اساس نظریات دکترین حقوقی، افزون بر تعیین قانون، تجویز توسط بازپرس نیز لازم است (خالقی ۱۳۹۹، ۸۸). موارد پیش‌گفته (تعیین قانون و تجویز بازپرس) با الزامات ماده ۱۰ مقررات اروپایی حفاظت از داده همسوست. جهت دیگری که قابل تطبیق با مقررات اروپایی حفاظت از

---

۱. «تخلف از مقررات مواد (۳۰)، (۳۴)، (۳۵)، (۳۷)، (۳۸)، (۳۹)، (۴۰)، (۴۱)، (۴۲)، (۴۹)، (۵۱)، (۵۲)، (۵۳)، (۵۵)، (۵۹) و (۱۴۱) این قانون توسط ضابطان، موجب محکومیت به سه ماه تا یک سال انفصال از خدمات دولتی است».

داده است، جرم افشای اسرار حرفه‌ای است که از این ماده قابل استنباط است. بر اساس ماده مربوطه - ماده ۶۴۸ قانون مجازات اسلامی مصوب ۱۳۷۵ (تعزیرات و مجازات‌های بازدارنده)[۱]- افرادی که به مناسبت شغل خود، متعهد به رازداری حرفه‌ای هستند، گرچه می‌توانند به اطلاعات و داده‌های شخصی افراد در دامنهٔ تعهد خود و در موارد قانونی دست پیدا کنند، لیکن اگر چنین افرادی از دامنهٔ تعهد خود تجاوز نموده و در موارد غیرقانونی اطلاعات، اسرار و داده‌های شخصی افراد را افشا نمایند، با ضمانت اجراهای مختلف مواجه خواهند شد. این ماده با ماده ۹۰ (۱) مقررات اروپایی حفاظت از داده قابل تطبیق است (EUR-Lex 2016, 85). طبق این مفاد قانونی، کشورهای عضو اتحادیه اروپا می‌توانند قواعدی را مقرر کنند که اشخاص پردازش‌کننده داده به موجب تعهد رازداری حرفه‌ای از برخی الزامات قانونی -نه همهٔ آن‌ها- معاف باشند (Voigt & von dem Bussche 2017, 223).

افزون بر این، بر اساس ماده ۹۶ قانون پیش‌گفته «انتشار تصویر و سایر مشخصات مربوط به هویت متهم در کلیه مراحل تحقیقات مقدماتی توسط رسانه‌ها و مراجع انتظامی و قضائی ممنوع است، مگر در مورد اشخاص زیر که تنها به درخواست بازپرس و موافقت دادستان شهرستان، انتشار تصویر و یا سایر مشخصات مربوط به هویت آنان مجاز است ...». مادهٔ مذکور در جهت حمایت از داده‌های شخصی متهم در راستای اصل محرمانه‌بودن تحقیقات وضع شده است. با توجه به تصریح ماده، افشای داده‌های شخصی متهمان صرفاً در مواردی خاص -این موارد حصری بوده- مجاز است که به دخالت و موافقت توأمان بازپرس و دادستان نیاز دارد (خالقی ۱۳۹۷، ۲۰۹). این امر در مقررات اروپایی حفاظت از داده نیز وجود دارد که حصول الزامات خاصی را -نظارت مرجع رسمی و تجویز قانون- برای پردازش چنین داده‌هایی ضروری می‌داند. همچنین لازم به ذکر است که حمایت از داده‌های شخصی متهم صرفاً مربوط به مرحلهٔ تحقیقات مقدماتی نیست، بلکه اصل بر ممنوعیت افشا حتی در مرحلهٔ دادرسی است (خالقی ۱۳۹۹، ۱۶۵).

---

۱. «اطبا و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند، هرگاه در غیر از موارد قانونی، اسرار مردم را افشا کنند به سه ماه و یک روز تا یک سال حبس و یا به یک‌میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می‌شوند». البته باید گفت طبق تبصره ماده ۱۰۴ قانون مجازات اسلامی اصلاحی سال ۱۳۹۹، مجازات حبس ماده فوق به نصف تقلیل می‌یابد؛ زیرا تبصره مذکور مقرر می‌کند: «حداقل و حداکثر مجازات‌های حبس تعزیری درجه چهار تا درجه هشت مقرر در قانون برای جرائم قابل‌گذشت به نصف تقلیل می‌یابد».

فارغ از مواد پیش‌گفته که برای حمایت از داده‌های شخصی مرتبط با امور کیفری، الزامات خاصی را مقرر می‌کند (مشابه با رویکرد مقررات اروپایی حفاظت از داده)، برخی مواد دیگر وجود دارند که به‌طور کلی، مبین توجه ویژه حقوق ایران به چنین داده‌هایی است. این مواد از قبیل ماده ۱۰۱ قانون آئین دادرسی کیفری است. به موجب این ماده «بازپرس مکلف است در مواردی که دسترسی به اطلاعات فردی بزه‌دیده، از قبیل نام و نام خانوادگی، نشانی و شماره تلفن، احتمال خطر و تهدید جدی علیه تمامیت جسمانی و حیثیت بزه‌دیده را به همراه داشته باشد، تدابیر مقتضی را برای جلوگیری از دسترسی به این اطلاعات اتخاذ کند. این امر در مرحله رسیدگی در دادگاه نیز به تشخیص رئیس دادگاه و با رعایت مصالح بزه‌دیده اعمال می‌شود». غایت این ماده، تأمین امنیت و کاهش نگرانی‌های بزه‌دیدگان از طریق حمایت از داده‌های شخصی‌شان است. حمایت فوق‌الذکر می‌تواند با شیوه‌های مختلف از جمله استفاده از نام‌های مستعار حاصل شود (لعل‌علیزاده ۱۳۹۶، ۱۰۸). ماده دیگری که در خصوص بحث حاضر می‌توان از آن استفاده نمود، ماده ۹۷ قانون پیش‌گفته است. این ماده مقرر می‌کند «بازپرس به‌منظور حمایت از بزه‌دیده، شاهد، مطلع، اعلام‌کننده جرم یا خانواده آنان و همچنین خانواده متهم در برابر تهدیدات، در صورت ضرورت، انجام برخی از اقدامات احتیاطی را به ضابطان دادگستری دستور دهد. ضابطان دادگستری مکلف به انجام دستورها و ارائه گزارش به بازپرس هستند». گرچه در نص ماده حمایت از داده‌های شخصی قابل مشاهده نیست، ولی می‌توان حمایت از این داده‌ها را با توجه به اصطلاح «اقدامات احتیاطی» استنباط نمود؛ چرا که یکی از اقداماتی که می‌تواند در جهت حمایت از اشخاص دخیل در فرایند دادرسی انجام شود، حمایت از داده‌های شخصی آن‌ها و عدم افشای هویتشان است. همچنین به موجب ماده ۶۶۰ قانون آئین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ «چنانچه اشخاصی که داده‌های موضوع این بخش را در اختیار دارند، موجبات نقض حریم خصوصی افراد یا محرمانگی اطلاعات را فراهم آورند یا به‌طور غیرمجاز آن‌ها را افشا کرده یا در دسترس اشخاص فاقد صلاحیت قرار دهند، به حبس از دو تا پنج سال یا جزای نقدی از بیست تا دویست میلیون ریال و انفصال از خدمت از دو تا ده سال محکوم خواهند شد». به موجب ماده ۶۵۸ این قانون نیز «قوه قضائیه موظف است تمهیدات فنی و قانونی لازم را برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان، در چارچوب اقدامات این بخش فراهم آورد». در نهایت نیز می‌توان از «آئین‌نامه اجرایی حمایت از شهود و مطلعان

مصوب ۱۳۹۴» نام برد که در فصل سوم (مواد ۸ - ۱۲) به عدم افشای اطلاعات و داده‌های شخصی شاهد یا مطلع در جهت حمایت از این اشخاص اشاره دارد.

با توجه به مطالبی که مورد بحث قرار گرفت، چند نکته قابل دریافت است. اولاً اینکه در نظام حقوقی ایران نیز نسبت به داده‌های شخصی مرتبط با امور کیفری توجه و حمایت‌های خاص وجود دارد. این حمایت‌های ویژه از جمله این است که پردازش داده‌های شخصی صرفاً با حکم قانون و تجویز مرجع رسمی قابل انجام است. همچنین در حقوق ایران نیز حمایت از داده‌های شخصی، محدود به داده‌های محکومیت‌ها و جرائم کیفری نیست، بلکه تمامی اطلاعات و داده‌های شخصی مرتبط با محکومیت‌ها و جرائم کیفری مانند اطلاعات بزه‌دیده، شهود، متهمان و تمامی افراد درگیر با امور کیفری را نیز شامل می‌شود. البته باید گفت حمایت‌های پیش‌گفته جزئی است و بدین جهت همچنان خلأ بستر قانونی خاص نسبت به داده‌های شخصی مرتبط با امور کیفری احساس می‌شود. دلیل توجه ویژه به این داده‌ها این است که پردازش داده‌های مذکور می‌تواند تبعات قابل توجهی نسبت به حقوق و آزادی‌های اساسی افراد به‌دنبال داشته باشد. بنابراین، از قانون‌گذار انتظار می‌رود با تصویب قانونی مستقل با الزامات خاص نسبت به چنین داده‌هایی، حمایت از این داده‌ها را کامل نماید.

٦. پردازش داده شخصی کودکان

آخرین مصداق از داده شخصی خاص، داده‌های مربوط به کودکان است. در این بند، ابتدا به چگونگی حفاظت از این داده‌ها به موجب مقررات اروپایی حفاظت از داده و سپس به بررسی الزامات مربوطه در نظام حقوقی ایران پرداخته خواهد شد.

٦-١. پردازش داده شخصی کودکان به موجب مقررات اروپایی حفاظت از داده

به‌دلیل موقعیت ویژه کودکان این مقررات تعهدات بیشتری را برای اشخاص پردازش‌کننده داده، در هنگام پردازش داده‌های شخصی کودکان مقرر کرده است؛ چرا که کودکان نیاز به حفاظت بیشتری نسبت به داده‌های شخصی خود دارند و غالباً نسبت به خطرات، پیامدها و اقدامات حفاظتی مربوط به پردازش داده‌های شخصی‌شان آگاهی کمتری دارند (Dorin Schiopu 2019, 23). بدین جهت قانون‌گذار اروپایی در چارچوب مقررات اروپایی حفاظت از داده به پردازش داده‌های شخصی کودکان حساسیت ویژه ای

نشان داده و پردازش داده‌های شخصی کودکان را با الزامات مضاعفی مقرر نموده است.

به‌موجب این مقررات در زمانی که داده‌های شخصی کودکان پردازش می‌شوند، اشخاص پردازش‌کنندهٔ داده باید از ابتدا با توجه به کودک بودن شخص موضوع داده، فرایند پردازشی خود را طراحی نمایند (حفاظت از داده‌ها با طراحی)[1]. همچنین رعایت اصول حاکم بر پردازش نسبت به کودکان به‌ویژه اصل انصاف بسیار مهم است و همانند بزرگسالان باید برای پردازش داده‌های شخصی مربوط به کودکان مبنای حقوقی وجود داشته باشد. به‌عنوان نمونه، اگر مبنای پردازش رضایت است، افزون بر الزامات کلی مقررات اروپایی حفاظت از داده در خصوص رضایت باید مادهٔ ۸ این مقررات نیز رعایت شود. در غیر این صورت، رضایت «آگاهانه» نیست و اعتباری ندارد. اگر مبنای پردازش ضرورت قراردادی است باید اهلیت کودک جهت موافقت با قرارداد و درک مفاهیم پردازش در نظر گرفته شود. در صورتی که مبنای پردازش منافع مشروع کنترل‌کننده یا شخص ثالث است، چنین منافعی باید در برابر منافع و حقوق و آزادی‌های اساسی کودک متعادل شود. جهت بررسی این امر باید ماهیت و هدف پردازش و خطرات احتمالی آن برای کودکان، همچنین اقدامات مناسب برای حفاظت از کودکان در برابر این خطرات مورد توجه قرار گیرد (ICO, n.d.-a). همچنین کودکان همان حقوقی را دارند که بزرگسالان بر داده‌های شخصی خود دارند[2]. به‌عنوان نمونه، در صورتی که از داده‌های شخصی کودکان برای اهداف بازاریابی استفاده می‌شود، نباید از عدم درک یا آسیب‌پذیری آن‌ها سوءاستفاده شود. بدین جهت کودکان مانند بزرگسالان حق دارند که نسبت به پردازش داده‌های شخصی خود برای بازاریابی مستقیم اعتراض نمایند و با جریان حق اعتراض توسط کودک یا سرپرست قانونی او، پردازش باید متوقف شود (ICO, n.d.-a). با وجود اینکه کودکان همانند بزرگسالان در مبنای حقوقی برای پردازش، اصول حاکم بر پردازش، حقوق شخص موضوع داده و سایر حمایت‌ها مشترک هستند، لیکن برخی از مفاد قانونی

1. data protection by design

۲. چنین حقوقی دریافت اطلاعات در مورد پردازش داده‌های شخصی، دسترسی شخص موضوع داده به داده‌های شخصی مربوط به خود، حق تصحیح داده‌های شخصی نادرست یا ناقص و حذف داده‌های شخصی (فراموش شدن)، حق محدودیت پردازش داده‌های شخصی، حق انتقال داده، اعتراض به پردازش داده‌های شخصی برای اهداف بازاریابی و یا زمینه‌های مربوط به موقعیت‌های ویژه و عدم قرار گرفتن در معرض تصمیمات خودکار است.

مقررات اروپایی حفاظت از داده، جهت تضمین حمایت بیشتر از کودکان الزامات ویژه‌ای را در این خصوص مقرر نموده است. چنین مفادی به‌شرح زیر است.

یکی از مفادی که به حمایت ویژه نسبت به کودکان اشاره دارد، ماده ۸ این مقررات است که مقرر می‌کند: «۱- در صورتی که بند (الف) ماده ۶ (۱) اعمال می‌شود (مبنای حقوقی پردازش رضایت شخص موضوع داده است)، در رابطه با خدمات اجتماعی اطلاعاتی[1] -خدماتی که برای انجام آن دریافت اطلاعات از شخص موضوع داده لازم است- که به‌طور مستقیم به کودک ارائه می‌شود، پردازش داده‌های شخصی کودک تنها در صورتی مجاز است که کودک حداقل ۱۶ سال داشته باشد. در صورتی که کودک زیر ۱۶ سال سن دارد، چنین پردازشی صرفاً زمانی مجاز خواهد بود که رضایت توسط سرپرست قانونی به کودک داده شود یا توسط آن‌ها پردازش اجازه داده شود. کشورهای عضو اتحادیه اروپا می‌توانند به‌طور قانونی سن پایین‌تری را برای این اهداف در نظر گیرند، مشروط بر اینکه کمتر از ۱۳ سال نباشد[2]. ۲- کنترل‌کننده باید با در نظر گرفتن فناوری‌های موجود، تلاش‌های منطقی جهت تائید در مواردی که رضایت توسط سرپرست قانونی به کودک داده شده یا پردازش را اجازه داده‌اند، انجام دهد. ۳- بخش ۱، نباید قواعد عمومی قراردادهای کشورهای عضو مانند قوانین مربوط به اعتبار، تشکیل یا اثر قرارداد در رابطه با کودک را تحت تأثیر قرار دهد» (EUR-Lex 2016, 37 & 38).

به‌موجب ماده ۸ (۲) مقررات اروپایی حفاظت از داده، هنگام ارائه خدمات اجتماعی اطلاعاتی به کودکان در بستر دیجیتال که بر اساس رضایت است، گرچه کنترل‌کننده‌ها نمی‌توانند سن کاربر را متوجه شوند، اما از آن‌ها انتظار می‌رود که تلاش‌های معقولی را برای تائید اینکه کاربر بالای سن رضایت است، انجام دهند (Volosevici 2019, 22)، در برخی منابع بیان شده است که باید برای جلوگیری از خطرات برای کودکان، از یک سیستم مؤثر تائید سن در کنار سایر ابزارها استفاده شود؛ چرا که کودکان باید در مواجهه

1. Information Society Service (ISS)

در این خصوص ماده ۴ (۲۵) GDPR مقرر می‌کند: «خدمات اجتماعی اطلاعاتی به معنای خدماتی است که در بند ب ماده ۱ (۱) دستورالعمل ۱۵۳۵/۲۰۱۵ (EU) تعریف شده است» (EUR-Lex 2016, 35).

۲. خدمات پیشگیرانه یا مشاوره‌ای که مستقیماً به کودک ارائه می‌شود، نیازی به اجازهٔ سرپرست قانونی ندارد؛ چرا که هدف از این موارد، حفاظت از منافع مهم کودکان است و این موارد صرفاً به نفع کودکان است (European Commission 2018a).

بـا محیط‌هـای دیجیتـال محافظـت شـوند (Henrich 2019, 79). بنابرایـن، وقتـی یـک کـودک از ابزارهـا یـا رسـانه‌های اجتماعـی اسـتفاده می‌کنـد، کنترل‌کننده‌هـا بایـد اطمینـان حاصـل کنـد کـه قوانیـن ملـی و اتحادیـه اروپـا را رعایـت کرده‌انـد و از کـودک بخواهنـد کـه توضیـح دهـد چگونـه رضایـت سرپرسـت قانونـی خـود را کسـب کـرده اسـت (E.C. European Commission 2018a: 12). ولـی در مقـام عمـل، بـه نظـر می‌رسـد کـه الزامـات قانونـی مذکـور و دسترسـی آزاد کـودکان بـه ابزارهـا و رسـانه‌های اجتماعـی یـا حتـی اسـباب‌بازی‌های هوشـمند، خصوصـاً آن‌هایـی کـه بـه اینترنـت دسترسـی دارنـد، در تضـاد هسـتند؛ چـرا کـه رضایـت آگاهانـه در اکثـر ایـن مـوارد وجـود نـدارد و کـودکان ناخواسـته داده‌هـای شخصی‌شـان را بـرای اهـداف نامعلـوم در اختیـار دیگـران قـرار می‌دهنـد (Plowman 2021, 4).

همچنیـن یکـی از مسـائل مهـم قابـل بررسـی در خصـوص ایـن مـاده، تعییـن سـن اهلیـت قانونـی اسـت. تعییـن ایـن سـن نه‌تنهـا در حوزه‌هـای قضایـی، بلکـه در بسـترهای مختلفـی ماننـد تحقیقـات، تبلیغـات و غیـره مؤثـر اسـت. به‌دلیـل اختیـار اعطاشـده در مـاده ۸ مقـررات اروپایـی حفاظـت از داده بـه کشـورهای عضـو اتحادیـه اروپـا، بـرای تعییـن محدودیـت سـنی جهـت رضایـت معتبـر در سـطح ملـی و نحـوهٔ اخـذ چنیـن رضایتـی، هماهنگـی در سـطح اتحادیـه اروپـا نسـبت بـه پـردازش داده‌هـای شـخصی کـودکان از بیـن رفتـه اسـت. به‌طـور کلـی، در کشـورهای مختلـف عضـو اتحادیـه اروپـا سـن ۱۴ تـا ۱۶ جهـت رضایـت معتبـر، لازم اسـت؛ لیکـن چگونگـی تعییـن ایـن سـن بـه روش‌هـای متفاوتـی اسـت (Macenaite & Kosta 2017, 152). روش‌هـای مذکـور از قبیـل «رویکـرد معیـار نوعـی واضـح»[1] اسـت، به‌موجـب ایـن روش کـه تعـداد اندکـی از کشـورهای عضـو بـدان پایبنـد هسـتند، قانـون حفاظـت از داده در سـطح ملـی، سـن مشـخصی را مقـرر می‌نمایـد کـه به‌عنـوان یـک معیـار واضـح قابـل اسـتناد اسـت. به‌عنـوان نمونـه، به‌موجـب مـاده ۱۳ قانـون حفاظـت از داده اسـپانیا «داده‌هـای شـخصی افـراد بـالای ۱۴ سـال بـا رضایـت آن‌هـا قابـل پـردازش اسـت ...». روش دیگـر «رویکـرد قیـاس قانونـی»[2] اسـت. به‌موجـب ایـن روش، تعییـن سـن بـا اسـتناد بـه قوانیـن و مقـررات دیگـر کـه عمدتـاً قانـون مدنـی اسـت تعییـن می‌شـود. بنابرایـن، بـا توجـه بـه ایـن امـر کـه در قانـون مدنـی چـه سـنی بـرای برخـورداری از حقـوق و تعهـدات معتبـر اسـت، سـن حـوزهٔ حفاظـت از داده نیـز تعییـن می‌شـود. به‌عنـوان مثـال، در لیتوانـی می‌تـوان کـودکان را از ۱۴ سـالگی دارای اهلیـت قانونـی دانسـت؛

1. an objective bright-line approach
2. regulation by analogy' approach

زیرا از این سن آن‌ها مجاز به انجام اقدامات قانونی بدون رضایت نمایندگان حقوقی خود هستند. در نتیجه، در این سن آن‌ها مجاز به رضایت در خصوص پردازش داده‌های شخصی خود هستند. روش دیگر «رویکرد مبتنی بر معیار شخصی»[1] است. به‌موجب این روش که در کشورهای عضوی که فاقد دو روش سابق هستند، انجام می‌شود، بر حسب مورد سن مذکور ارزیابی و تعیین می‌شود. در هر ارزیابی باید منافع کودک، سطح درک اخلاقی و روانی او، ظرفیت درک پیامدهای رضایت و ارزیابی شرایط خاص کودک مانند هدف پردازش، نوع داده‌های شخصی درگیر و ... باید بررسی شود. چنین ارزیابی تنها بر حسب مورد قابل استفاده است و یک معیار نوعی قابل اجرا در تمامی موارد نیست (Macenaite & Kosta 2017, 153 & 154).

۶-۲. پردازش داده شخصی کودکان در نظام حقوقی ایران

با توجه به فقدان قانونی مستقل نسبت به داده‌های شخصی و جنبه‌های مختلف آن، حمایت‌های ویژه‌ای نسبت به داده‌های شخصی کودکان به‌موجب حقوق ایران مورد توجه قرار نگرفته است؛ حتی پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» نیز به کودکان و داده‌های شخصی مربوط به آن‌ها نپرداخته است. بدین جهت دامنه و چگونگی حمایت از چنین داده‌هایی روشن نیست. با این حال، به این دلیل که حمایت از صغار (کودکان) در نظام حقوقی ایران نیز امری اجتناب‌ناپذیر است و کودکان شایسته حمایت‌های حقوقی خاص هستند، باید با جست‌وجو در منابع مختلف حقوق ایران، حمایت از داده‌های شخصی مربوط به کودکان را استنباط نمود. در این راستا می‌توان به «سند صیانت از کودکان و نوجوانان در فضای مجازی» مصوب شورای عالی فضای مجازی اشاره نمود که با هدف ارتقای بهره‌برداری از فضای مجازی و صیانت از خردسالان، کودکان و نوجوانان تدوین - در جلسات شماره ۶۹ مورخ ۱۳۹۹/۱۱/۲۸، شماره ۷۰ مورخ ۱۳۹۹/۱۲/۲۶ و شماره ۷۱ مورخ ۱۴۰۰/۰۳/۱۷ - به تصویب رسیده است. گرچه این سند به‌طور کلی حاوی حمایت از کودکان در فضای مجازی است و به‌طور خاص، برای داده‌های شخصی مربوط به کودکان در تمامی بسترهای پردازشی مقرر نشده است، لیکن به‌دلیل وجود رویکرد خاص نسبت

1. subjective capacity-based approach

به کودکان قابل استفاده است. سند مذکور حاوی حمایت‌های ویژه‌ای نسبت به کودکان است. به‌عنوان نمونه، به‌موجب بند ب ماده ۴ ایجاد محیطی صیانت‌شده برای فعالیت کودکان در فضای مجازی ضروری است[1]. همچنین بند د ماده ۴ متضمن حمایت‌ها و مراقبت‌های خاص از کودکان است که می‌تواند در زمینهٔ حمایت از داده‌های شخصی کودکان مفید واقع شود.

فارغ از سند اشاره‌شده باید گفت که مهم‌ترین مسئلهٔ قابل بررسی در مورد حمایت از داده‌های شخصی کودکان، سن اهلیت آن‌ها برای رضایت به پردازش است -این مسئله در سایر نظام‌های حقوقی مورد توجه ویژه قرارگرفته و در مورد آن مباحث بسیاری وجود دارد- در این خصوص گفتنی است، به‌دلیل نبود قانونی خاص نسبت به حفاظت از داده‌ها، در حقوق ایران سن معینی -مانند ۱۶ سالگی مصرح در مقررات اروپایی حفاظت از داده- برای اهلیت داشتن برای رضایت به پردازش وجود ندارد. همچنین به‌موجب نظام حقوقی ایران ملاک تعیین این سن نیز مشخص نیست. بنابراین، ۱۶ سالگی در حقوق ایران برای این مسئله، قابل استفاده نیست و باید سن دیگری ملاک عمل قرار گیرد.

در حقوق ایران برای حمایت از صغار سنین مختلفی مطرح شده است. یکی از آن‌ها سن بلوغ است که به‌موجب تبصره ۱ ماده ۱۲۱۰ قانون مدنی «سن بلوغ در پسر پانزده سال تمام و در دختر نه سال تمام قمری است». سن دیگر، سن نکاح است که به‌موجب قانون (ماده واحده) اصلاح ماده ۱۰۴۱ قانون مدنی مصوب ۱۳۸۱، سنین ۱۳ سالگی و ۱۵ سالگی به‌ترتیب، برای نکاح دختران و پسران تعیین شده است[2]. این سنین معین که در قانون و در نظریات دکترین مورد تصریح قرار گرفته‌اند (کاتوزیان ۱۳۹۸، ۵۴- ۵۶؛ صفایی و امامی ۱۳۹۷، ۷۷-۸۱؛ گرجی و همکاران ۱۳۹۲، ۷۸- ۸۳) از فقه امامیه استخراج شده‌اند. به نظر مشهور فقها امامیه نیز سن بلوغ برای دختر و پسر به‌ترتیب، ۹ سال تمام قمری و ۱۵ سال تمام قمری است (عمید زنجانی ۱۳۸۲، ۱۳۶؛ ذهنی تهرانی ۱۳۶۶، ۱۶/ ۹۵؛ فیض ۱۳۸۷، ۵۴) و سن ۱۳ سال برای نکاح نیز به‌موجب اخباری است که در منابع فقهی مختلف بیان شده است (بحرانی ۱۳۶۳، ۲۰/ ۳۴۹؛ حسینی عاملی ۱۴۱۹ ق، ۱۶/ ۳۴).

---

۱. این مفاد مقرر می‌کند: «ایجاد زیرساخت و خدمات پایه و پیشران ویژه محیط‌های صیانت‌شده مجازی اعم از احراز هویت، امکان دسترسی طبقه‌بندی‌شده، امکان نظارت اولیا، گزارش‌دهی ...» لازم است.

۲. «عقد نکاح دختر قبل از رسیدن به سن ۱۳ سال تمام شمسی و پسر قبل از رسیدن به سن ۱۵ سال تمام شمسی منوط است به اذن ولی به شرط رعایت مصلحت با تشخیص دادگاه صالح».

در نظام حقوقی ایران سن دیگری نیز مورد توجه است و آن سن رشد است. به‌موجب رأی وحدت رویه شماره ۳۰ مورخ ۳/ ۱۰/ ۱۳۶۴، صغار در امور غیرمالی با رسیدن به بلوغ از حجر خارج شده و در امور مالی باید رشدشان ثابت شود. البته، در حال حاضر سنی خاص به‌عنوان امارهٔ قانونی بر رشد در حقوق ایران وجود ندارد (قاسم‌زاده، ره پیک و کیایی ۱۳۹۸، ۴۳۵)؛ چرا که با حذف ماده ۱۲۰۹ قانون مدنی مصوب ۱۳۱۴ – که به صراحت ۱۸ سالگی را سن رشد می‌دانست- ماده واحده راجع به رشد متعاملین مصوب ۱۳۱۳ نیز که سن ۱۸ سالگی را اماره بر رشد معرفی نموده است، نسخ ضمنی شده است (صفایی و قاسم‌زاده ۱۳۸۶، ۲۲۱). با وجود این، ۱۸ سالگی همچنان به‌عنوان سن رشد در رویهٔ قضایی مورد استناد است و می‌توان این سن را اماره قضایی بر رشد دانست (انصاری‌پور ۱۳۹۶، ۲۱۶). مؤید این امر می‌تواند بند دوم ماده ۱ «سند صیانت از کودکان و نوجوانان در فضای مجازی» باشد که مقرر می‌کند «خردسالان، کودکان و نوجوانان، کلیه افراد کمتر از ۱۸ سال هستند که در قلمرو حاکمیت جمهوری اسلامی ایران قرار دارند». مؤید دیگر نیز ماده ۳۰۴ قانون آئین دادرسی کیفری مصوب ۱۳۹۲ با اصلاحات ۱۳۹۴ است که به‌موجب آن «به کلیه جرائم اطفال و افراد کمتر از هجده سال تمام شمسی در دادگاه اطفال و نوجوانان رسیدگی می‌شود ...» در این ماده اطفال و افراد زیر ۱۸ سال یک حکم دارند و معادل هم قرار داده شده‌اند.

با وجود عدم صراحت قانون در خصوص مسئلهٔ حاضر، از میان سنین مذکور در حقوق ایران به نظر می‌رسد که سن ۱۸ سالگی، مناسب‌ترین سن برای رضایت به پردازش داده‌های شخصی باشد؛ زیرا داده‌های شخصی دارای ابعاد مالی‌اند، مال محسوب می‌شوند -گرچه ابعاد معنوی نیز دارند[1]- و حمایت‌های قانونی نسبت به اموال بر داده‌های شخصی نیز جاری است. بدین جهت برای تصرف در داده شخصی رشد لازم است و سن مربوط

---

۱. ابعاد مالی دادهٔ شخصی (ابعاد مادی)، حق انحصاری هرگونه بهره‌برداری از دادهٔ شخصی است. بهره‌برداری متناسب با دادهٔ شخصی از طریق پردازش است که مصادیق آن در شماره ماده ۴ (۲) GDPR - مانند جمع‌آوری، ضبط، ذخیره‌سازی، استفاده کردن، افشا یا منتشر کردن و ...- بیان شده است (EUR-Lex 2016, 33). البته، ماهیت داده‌های شخصی در ابعاد مالی منحصر نیست و داده‌های شخصی دارای بُعد غیرمالی (معنوی) نیز هستند. داده‌های شخصی نظیر برخی مصادیق مالکیت معنوی دارای دو بُعد مالی و غیرمالی (معنوی) هستند و ماهیتی دو جنبه‌ای دارد. ابعاد معنوی داده‌های شخصی، حقوقی است که وابسته به شخص موضوع داده است. این حقوق در نظام حقوقی ایران مورد تصریح قرار نگرفته‌اند، لیکن در مواد ۱۲ الی ۲۲ GDPR به آن‌ها اشاره شده است (EUR-Lex 2016, 39-46).

به رشد نیز ۱۸ سالگی است. با توجه به امور پیش‌گفته می‌توان گفت برای رضایت به پردازش داده شخصی سن ۱۸ سال ملاک است و کمتر از این سن، پردازش باید با اجازه یا نظارت سرپرست قانونی انجام شود. همچنین قابل ذکر است که در صورتی که ۱۸ سالگی نیز ملاک عمل قرار نگیرد، با لحاظ شرایط قانونی فعلی نسبت به داده‌های شخصی باید مطابق با «رویکرد مبتنی بر معیار شخصی»[1] که در برخی از کشورهای اروپایی استفاده می‌شود، عمل نمود. در واقع، باید بر حسب مورد و در اوضاع و احوال مختلف، سنین متفاوتی را ملاک قرار داد. بدین جهت و برای رفع تشتت آرا در مقام عمل، از قانون‌گذار انتظار می‌رود که با توجه به اهمیت موضوع حاضر، سن مناسبی را به‌طور خاص مقرر نموده و همچنین بر سایر حفاظت‌های خاص نسبت به پردازش داده‌های شخصی مربوط به کودکان تصریح نماید.

۷. نتیجه

بر اساس مقررات اروپایی حفاظت از داده، داده‌های شخصی حساس، داده‌های مرتبط با امور کیفری و داده‌های شخصی کودکان داده‌های شخصی خاص هستند. این مقررات برای پردازش این داده‌ها الزامات ویژه‌ای را مقرر نموده و به‌طور خاص از آن‌ها حفاظت کرده است. از جملهٔ این الزامات، ممنوعیت پردازش داده‌های شخصی حساس و جواز پردازش صرفاً در چند موقعیت ویژه است (استثنائات از اصل ممنوعیت). این استثنائات به‌صورت حصری رضایت صریح شخص موضوع داده، علنی‌شدن داده‌ها توسط شخص موضوع داده، پردازش برای استخدام و تأمین اجتماعی، پردازش به‌دلیل حفاظت از منافع حیاتی افراد، پردازش توسط سازمان‌ها و نهادهای غیرانتفاعی برای فعالیت‌های قانونی‌شان، پردازش در جهت منافع عمومی، پردازش در زمینه مربوط به مراقبت‌های بهداشتی و مسائل سلامت عمومی، پردازش به جهت اهداف تحقیقاتی (معافیت تحقیقاتی) و پردازش برای رسیدگی به دعاوی حقوقی هستند. با تبیین هر یک از مبانی حقوقی پردازش داده‌های شخصی حساس (استثنائات مذکور) در حقوق اتحادیه اروپا، چگونگی حمایت از داده‌های شخصی حساس و شناسایی موقعیت‌های جواز پردازش این داده‌ها در نظام حقوقی ایران مورد توجه قرار گرفت. بررسی‌های انجام‌شده حکایت از این دارد که صرفاً برخی از مواد

1. subjective capacity-based approach

قانون تجارت الکترونیکی به بعضی از مصادیق داده‌های شخصی حساس و یکی از مبانی حقوقی پردازشِ داده شخصی حساس (رضایت صریح) اشاره کرده‌اند. در واقع، به‌غیر از اصل ممنوعیت پردازش داده شخصی حساس و رضایت صریح به‌عنوان استثنا از این ممنوعیت، قوانین موضوعه ایران به داده‌های شخصی حساس و چگونگی پردازش آن‌ها نپرداخته‌اند. بدین جهت جریان یا عدم جریان سایر مبانی حقوقی پردازشِ داده شخصی حساس، از سایر منابع حقوق ایران از جمله نظریات دکترین، مبانی حقوق ایران به‌ویژه فقه امامیه مورد بررسی قرار گرفت. در این راستا روشن شد که به موجب نظام حقوقی ایران تمامی مبانی مذکور (استثنائات از اصل ممنوعیت پردازش) به‌غیر از پردازش توسط سازمان‌ها و نهادهای غیرانتفاعی در جهت فعالیت‌های قانونی‌شان، پذیرفتنی است.

همچنین مشخص شد به موجب مقررات اروپایی حفاظت از داده پردازش داده‌های شخصی مربوط به محکومیت‌ها و جرائم کیفری یا اقدامات تأمینی مربوطه، صرفاً با نظارت مرجع رسمی و تجویز قانون امکان‌پذیر است. از سوی دیگر، بر اساس برآمدِ بررسی مسئله در نظام حقوقی ایران–با وجود اینکه قانونی مستقل در خصوص حمایت از داده‌های شخصی مرتبط با امور کیفری وجود ندارد- روشن شد که با توجه به مواد مختلفی از قوانین موضوعه و نظریات دکترین، الزامات مقرر در مقررات اروپایی حفاظت از داده برای پردازش داده‌های شخصی مربوط به محکومیت‌ها و جرائم کیفری -یعنی نظارت مرجع رسمی و تجویز قانون- در حقوق ایران نیز قابل جریان است. افزون بر این، طبق یافته‌های این پژوهش، داده‌های شخصی کودکان نیز بر اساس این مقررات از حمایت‌های ویژه‌ای برخوردار است. در میان سایر موارد، برای اینکه داده‌ها توسط شخص موضوع داده در معرض پردازش قرار داده شود، سن معینی (۱۶ سالگی) مقرر شده است. بدین جهت برای پردازش داده‌های اشخاص موضوع داده‌ای که کمتر از سن مذکور هستند، نظارت یا اجازهٔ سرپرست قانونی‌شان لازم است. در مقابل، نظام حقوقی ایران -با وجود اینکه در برخی از اسناد حمایت‌های خاصی از کودکان نموده است- در خصوص سن رضایت به پردازش، صراحتی ندارد. بدین جهت از نظریات دکترین استنباط شد که به‌دلیل وجود ابعاد مالی برای داده‌های شخصی و لزوم جریان حمایت‌های قانونی نسبت به اموال در خصوص داده‌های شخصی برای تصرف در داده‌های شخصی رشد ضروری بوده و سن مربوطه نیز ۱۸ سالگی است.

سرانجام، به قانون‌گذار پیشنهاد می‌شود با توجه به نتایج این پژوهش و سایر آثار

علمی مرتبط، برای جریان حمایت‌های کافی از داده‌های شخصی، قانونی مستقل تصویب نماید که بر جنبه‌های مختلف مربوط به داده شخصی و به‌طور ویژه چگونگی پردازش داده شخصی خاص صراحت داشته باشد. در این خصوص از جمله پیشنهادهای این پژوهش این است که قانون‌گذار با توجه به الگوهای قانونی حفاظت از داده از جمله مقررات اروپایی معهود، انواع داده‌های شخصی خاص به موجب حقوق ایران را مشخص نموده و سپس در خصوص مرز حمایت، موارد جواز پردازش این دسته از داده‌ها و چگونگی پردازش هر قِسم، قانون‌گذاری نماید.

فهرست منابع

افراسیاب، محبوب، و مهدی ناصر. ۱۳۹۹. چارچوب‌های حقوقی حفظ امنیت پردازش داده‌های خصوصی (مطالعه‌ای تطبیقی در حقوق ایران و اتحادیه اروپا). *حقوق اسلامی* ۱۷ (۶۶): ۲۰۹-۲۳۲.

انصاری‌پور، محمدعلی. ۱۳۹۶. بیان موجزی از دلایل ضرورت تعیین سن رشد. *مطالعات حقوق خصوصی* ۴۷ (۲): ۲۱۳-۲۳۰.

ایازی، محمدعلی. ۱۳۸۹. *ملاکات احکام و شیوه‌های استکشاف آن*. قم: دفتر تبلیغات اسلامی حوزه علمیه قم.

آقایی طوق، مسلم، و مهدی ناصر. ۱۳۹۹. چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا. *فصلنامه حقوق اداری* ۷ (۲۳): ۳۳- ۵۵.

آئین‌نامه اجرایی حمایت از شهود و مطلعان مصوب ۱۳۹۴.

بحرانی، یوسف بن احمد. ۱۳۶۳. *الحدائق الناضرة فی أحکام العترة الطاهرة*. قم: مؤسسة النشر الإسلامی.

پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی منتشرشده در تیرماه ۱۳۹۷

حسینی عاملی، محمدجواد بن محمد. ۱۴۱۹ ق. *مفتاح‌الکرامة فی شرح قواعدالعلامة*. قم: دفتر انتشارات اسلامی وابسته به جامعه مدرسین حوزه علمیه قم.

حیدری، الهام. ۱۳۹۴. حقوق دفاعی متهم در «دوران تحت نظر» در قانون آئین دادرسی کیفری و بررسی تطبیقی آن با حقوق انگلستان. *دیدگاه‌های حقوق قضایی* ۲۰ (۷۱): ۲۷- ۵۳.

خالقی، علی. ۱۳۹۷. *آئین دادرسی کیفری*. تهران: شهر دانش.

_____. ۱۳۹۹. *نکته‌ها در قانون آئین دادرسی کیفری*. تهران: شهر دانش.

ذهنی تهرانی، محمدجواد. ۱۳۶۶. *المباحث الفقهیة فی شرح الروضة البهیة*. قم: وجدانی.

سند صیانت از کودکان و نوجوانان در فضای مجازی توسط شورای عالی فضای مجازی مصوب ۱۴۰۰

صفایی، سید حسین؛ و اسدالله امامی. ۱۳۹۷. *مختصر حقوق خانواده*. تهران: میزان.

صفایی، سید حسین و سید مرتضی قاسم‌زاده. ۱۳۸۶. *اشخاص و محجورین*. تهران: سمت.

طرح «حمایت و حفاظت از داده و اطلاعات شخصی» اعلام وصول‌شده در مجلس مورخ شهریور ماه ۱۴۰۰

عمید زنجانی، عباسعلی. ۱۳۸۲. *آیات الأحکام*. تهران: دفتر مطالعات و تحقیقات علوم اسلامی.

ـــــــ. ۱۳۹۱. *قواعد کلی عقود کتاب‌البیع و المتاجر*. تهران: خرسندی.

فیض، علیرضا. ۱۳۸۷. *آراء فقهی ملامحسن فیض کاشانی*. تهران: مدرسه عالی شهید مطهری.

قاسم‌زاده، مرتضی، حسن ره‌پیک، و عبدالله کیایی. ۱۳۹۸. *تفسیر قانون مدنی: اسناد، آراء و اندیشه‌های حقوقی*. تهران: سمت.

قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی ۱۳۸۲

قانون اساسی ایران مصوب ۱۳۵۸

قانون آئین دادرسی کیفری مصوب ۱۳۹۲

قانون تجارت الکترونیکی مصوب ۱۳۸۲

قانون تشویق و حمایت سرمایه‌گذاری خارجی مصوب ۱۳۸۰

قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری مصوب ۱۳۸۶

قانون کار مصوب ۱۳۶۹

قانون مجازات اسلامی مصوب ۱۳۹۲

قانون مدنی مصوب ۱۳۱۴

قانون نحوه واگذاری و احیاء اراضی در حکومت جمهوری اسلامی ایران مصوب ۱۳۵۸.

قماشی، سعید. ۱۳۸۵. بررسی جرم افشای اسرار حرفه‌ای. *دادرسی* ۵۸: ۳-۶.

کاتوزیان، ناصر. ۱۳۹۵. *مسئولیت مدنی*. تهران: انتشارات دانشگاه تهران.

ـــــــ. ۱۳۹۸. *حقوق خانواده*. تهران: میزان.

کارخیران. محمدحسین. ۱۳۹۴. *قانون تطبیقی آئین دادرسی کیفری و مجازات اسلامی*. تهران: راه نوین.

ـــــــ. ۱۳۹۸. *کامل‌ترین مجموعه محشی قانون مجازات اسلامی*. تهران: آریاداد.

گرجی، ابوالقاسم و سید حسین صفایی، سید عزت‌الله عراقی، اسدالله امامی، عباس قاسم‌زاده، محمود صادقی، عادل برزوئی، احمد حمیدزاده، و بتول آهنی. ۱۳۹۲. *بررسی تطبیقی حقوق خانواده*. تهران: انتشارات دانشگاه تهران.

گلدوزیان. ۱۳۹۷. *حقوق جزای عمومی*. تهران: انتشارات دانشگاه تهران.

لعل‌علیزاده، محسن. ۱۳۹۶. بررسی تطبیقی حقوق بزه‌دیدگان در مراحل تعقیب و تحقیق در قانون آئین دادرسی کیفری ۱۳۹۲ با دیوان کیفری بین‌المللی. *پژوهش حقوق کیفری* ۵ (۱۹): ۹۵-۱۲۶.

محقق داماد، سید مصطفی. ۱۳۸۴. *قواعد فقه (بخش مدنی - مالکیت و مسئولیت)*. تهران: مرکز نشر علوم اسلامی.

مدرسی، محمدرضا. ۱۳۹۳. *البیع*. محرر عبدالله امیرخانی و جواد احمدی. قم: دار التفسیر.

مصوبه شورای عالی فضای مجازی با موضوع «سیاست‌ها و اقدامات ساماندهی پیام‌رسان‌های اجتماعی» مصوب ۱۳۹۶.

مکارم شیرازی، ناصر. ۱۳۸۵. *دائرةالمعارف فقه مقارن*. قم: مدرسة الإمام علی بن أبی‌طالب (علیه‌السلام)

منتظری، حسینعلی. ۱۳۶۷. *مبانی فقهی حکومت اسلامی*. مترجم محمود صلواتی. قم: کیهان.

منشور حقوق بیمار ۱۳۸۸.

منصوریان، ناصرعلی و عادل شیبانی. ۱۳۹۵. مفهوم منفعت عمومی و جایگاه آن در قانونگذاری ایران، *دیدگاه‌های حقوق قضایی* ۲۱ (۷۵ و ۷۶): ۱۱۷ – ۱۴۲.

میرزای قمی، ابوالقاسم‌بن محمدحسن. ۱۳۷۱. *جامع‌الشتات*. محقق مرتضی رضوی. تهران: کیهان.

هاشمی، سید محمد. ۱۳۹۰. *حقوق اساسی و ساختارهای سیاسی*. تهران: میزان.

هاشمی شاهرودی، محمود. ۱۳۸۲ ق. *فرهنگ فقه مطابق مذهب اهل بیت علیهم‌السلام*. قم: مؤسسه دائرةالمعارف فقه اسلامی بر مذهب اهل بیت (علیهم‌السلام).

References

Amram, D. 2020. Building up the “Accountable Ulysses” model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks. *Computer Law and Security Review* 37: 1–7.

Cabañas, J. G., Cuevas, Á., & Cuevas, R. 2018. Facebook Use of Sensitive Data for Advertising in Europe. *arXiv preprint,* arXiv:1802.05030: 1–15.

Chassang, G. 2017. The impact of the EU general data protection regulation on scientific research. *Ecancermedicalscience* 11: 1–12.

CURIA. n.d. *Case T-190/10, Kathleen Egan and Margaret Hackett. 2012*. https://curia.europa.eu/juris/document/document.jsf?docid=121109&doclang=EN (accessed April 28, 2021)

Dorin Schiopu, S. 2019. Brief Considerations on Processing a Child’s Personal Data. *Journal of Social and Legal Studies* 6 (2): 23–28.

EUR-Lex. 2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). *Official Journal of the European Union,* OJ L 119, 59: 1–88.

European Commission. 2016. *Data protection in the EU | European Commission*. Data Protection in the EU. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (accessed May 15, 2021).

European Commission. 2018a. *Are there any specific safeguards for data about children?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/are-there-any-specific-safeguards-data-about-children_en (accessed May 13, 2021).

European Commission. 2018b. *Ethics and data protection* (Issue November, pp. 1–21).

European Commission. 2018c. *Under what conditions can my company/organisation process sensitive data?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-

company-organisation-process-sensitive-data_en (accessed March 7, 2021).

European Data Protection Board. 2020. *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak* (Issue April, pp. 1-14).

European Data Protection Supervisor. n.d. *Legislation*. https://edps.europa.eu/data-protection/data-protection/legislation_en (accessed February 11, 2020).

Ferrara, P., & F. Spoto. 2018. Static analysis for GDPR compliance. *CEUR Workshop Proceedings,* Germany, 2058: 1–10.

Gellert, R. 2017. Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing. *In Trends und Communities der Rechtsinformatik-Trends and Communities of legal informatics: Tagungsband des 20. Internationalen Rechtsinformatik Symposions-IRIS 2017-Proceedings of the 20th International Legal Informatics Symposium.* Austrian Computer Society: 1–9.

Henrich, J. 2019. Council of Europe on the protection of children's privacy and their personal data in the digital environment. In *European Data Protection Law Review* 5 (1): 78-79.

ICO. n.d.-a. *Children*. https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/(accessed August 10, 2021)

ICO. n.d.-b. *Criminal offence data*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/ (accessed August 9, 2021)

ICO. n.d.-c. *What is criminal offence data?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/criminal-offence-data/what-is-criminal-offence-data/ (accessed August 9, 2021).

ICO. n.d.-d. *What is valid consent?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ (accessed September 21, 2021).

ICO. 2019. *What are the conditions for processing?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions5 (accessed August 10, 2021).

Jasseran, C. 2016. Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data Which Changes Does the New Data Protection Framework Introduce? *European Data Protection Law Review* 3: 297–311.

Macenaite, M., & E. Kosta. 2017. Consent for processing children' s personal data in the EU : following in US footsteps ? : *Information & Communications Technology Law* 26 (2): 146–197.

Olimid, A. P., L. M. Rogozea, & D. A. Olimid. 2018. Ethical approach to the genetic, biometric and health data protection and processing in the new eu general data protection regulation (2018). *Romanian Journal of Morphology and Embryology* 59 (2): 631–636.

Plowman, L. 2021. Smart toys and children' s understanding of personal data Related papers. *International Journal of Child-Computer Interaction*, 30: 1–23.

Pormeister, K. 2017. Genetic data and the research exemption: Is the GDPR going too far? *International Data Privacy Law* 7 (2): 137–146.

Shabani, M., & P. Borry. 2018. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics* 26 (2): 149–156.

Skovgaard, L. L., S. Wadmann, & K. Hoeyer. 2019. A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. *Health Policy* 123 (6): 564–571.

van Veen, E. Ben. 2018. Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. *European Journal of Cancer 104*: 70–80.

Voigt, P., & A. von dem Bussche. 2017. *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing.

Volosevici, D. 2019. Child Protection Under GDPR. *Journal of Social and Legal Studies* 623–17 :(2) .

مهدیه لطیف‌زاده

متولد سال ۱۳۷۱، دکتری حقوق خصوصی دانشگاه فردوسی مشهد است. ایشان در حال حاضر پژوهشگر پسادکتری این دانشگاه به موجب قرارداد با بنیاد ملی نخبگان هستند.

حقوق مربوط به فناوری‌های نوین اطلاعاتی، حفاظت از داده‌های شخصی و حریم خصوصی از جمله علایق پژوهش وی است.

سید محمدمهدی قبولی درافشان

متولد سال ۱۳۵۶، دارای مدرک تحصیلی دکتری در رشتهٔ حقوق خصوصی از دانشگاه تهران است. ایشان هم‌اکنون دانشیار گروه حقوق خصوصی دانشگاه فردوسی مشهد است.

حوزه‌های مختلف حقوق خصوصی از قبیل حقوق قراردادها، مسئولیت مدنی، حقوق خانواده، حقوق مربوط به فناوری‌های نوین اطلاعاتی و نیز حقوق مالکیت‌های فکری از جمله علایق پژوهشی وی است.

سعید محسنی

متولد سال ۱۳۵۴، دارای مدرک تحصیلی دکتری در رشتهٔ حقوق خصوصی از دانشگاه امام صادق علیه‌السلام است. ایشان هم‌اکنون دانشیار گروه حقوق خصوصی دانشگاه فردوسی مشهد است.

حقوق تجارت و حقوق مالکیت فکری از جمله علایق پژوهشی وی است.

محمد عابدی

متولد سال ۱۳۵۳، دارای مدرک تحصیلی دکتری در رشتهٔ حقوق خصوصی از دانشگاه تهران است. ایشان هم‌اکنون دانشیار گروه حقوق خصوصی دانشگاه فردوسی مشهد است.

تحقیق در زمینهٔ حقوق مسئولیت مدنی، حقوق قراردادها و حقوق بشر و خانواده از جمله علایق پژوهشی وی است.

پژوهش‌نامه

پردازش و مدیریت اطلاعات