

بررسی تطبیقی ضمانت اجرای نقض حق بر داده در حقوق اتحادیه اروپا و نظام حقوقی ایران

مهديه لطيفزاده*، سيدمحمد مهدی قبولی درافشان**، سعید محسنی*** و محمد عابدی****

| | | | |
|-------------------|--------------------------|-------------------------|---------------------|
| نوع مقاله: پژوهشی | تاریخ دریافت: ۱۴۰۰/۱۰/۰۴ | تاریخ پذیرش: ۱۴۰۱/۰۵/۰۶ | شماره صفحه: ۳۷۴-۳۴۱ |
|-------------------|--------------------------|-------------------------|---------------------|

حمایت قانونی از داده‌های شخصی به‌عنوان یکی از جنبه‌های حقوق بشر و مصداقی از حقوق شهروندی، ضروری است. حمایت جامع از داده‌های شخصی و اشخاص موضوع داده در برخی کشورها با وجود قوانین و مقررات خاص در این حوزه تحقق یافته است. در این خصوص مقررات عمومی حفاظت از داده اتحادیه اروپا قابل اشاره است که با حمایت‌های همه‌جانبه از داده‌های شخصی به الگویی در این زمینه تبدیل شده است. یکی از ابعاد حمایتی این مقررات، تصریح ضمانت اجرای نقض حق بر داده‌های شخصی است. جریان عملی ضمانت اجرای مختلفی که در این مقررات بیان شده است تا حد زیادی این مقررات را به هدف خود یعنی احیای حقوق نقض شده اشخاص موضوع داده و تحقق حمایت کامل از داده‌های شخصی نزدیک کرده است. از مهم‌ترین مصادیق چنین ضمانت‌های اجرایی، وجود حق جبران خسارت و اعمال جزای نقدی از سوی مراجع نظارتی است. با تبیین هریک از ضمانت‌های اجرایی یادشده براساس مقررات اروپایی و بررسی تطبیقی آنها در نظام حقوقی ایران، مشخص شد که ضمانت‌های اجرایی پیش‌گفته در حقوق ایران نیز برای نقض حق بر داده‌های شخصی پذیرفتنی است؛ اما حمایت جامع از داده‌های شخصی و تحقق کارآمد این ضمانت‌های اجرا با تصریح قانونگذار حاصل می‌شود.

کلیدواژه‌ها: اشخاص موضوع داده؛ جزای نقدی؛ حق جبران خسارت؛ داده شخصی؛ مقررات عمومی حفاظت از داده اتحادیه اروپا

* دانش‌آموخته دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران؛

Email: m.latifzadeh@mail.um.ac.ir

** دانشیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران (نویسنده مسئول)؛

Email: ghaboli@um.ac.ir

*** دانشیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران؛

Email: s-mohseni@um.ac.ir

**** استادیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران؛

Email: dr.m.abedi@um.ac.ir

فصلنامه مجلس و راهبرد، سال سی‌ام، شماره یکصدوشانزدهم، زمستان ۱۴۰۲

doi: 10.22034/MR-2112-4975

مقدمه^۱

استفاده از داده‌های شخصی^۲ با گسترش ابزارهای دیجیتال و افزایش قابلیت‌های فناوری روزبه‌روز در حال افزایش است. بستریایی که افراد به‌طور مداوم با آنها سروکار دارند، داده‌های شخصی را جمع‌آوری، پردازش^۳ و به شیوه‌های مختلف از آنها استفاده می‌کنند. در واقع به دلیل اهمیت اقتصادی داده‌ها،^۴ تمایل به پردازش و استفاده از داده‌های شخصی افزایش یافته که در عین حال چالش‌های حریم خصوصی را نیز به دنبال دارد. با افزایش استفاده از داده‌ها و ارزشمندی آنها، ضرورت حمایت از حریم

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

۲. داده شخصی (Personal Data) به موجب مقررات اروپایی حفاظت از داده، به معنای هر اطلاعاتی است که به شخص حقیقی شناخته شده 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).

۳. پردازش (Processin) به معنای عملیات یا مجموعه‌ای از عملیات است که روی داده شخصی یا مجموعه داده‌های شخصی، با وسایل خودکار و غیر آن، صورت گیرد، این موارد اعم از جمع‌آوری، ضبط، سازمان‌دهی، طبقه‌بندی، ذخیره‌سازی، اشتراک‌گذاری، تغییر، بازیابی، استفاده کردن، تجزیه و تحلیل کردن، انتشار، افشا با مخبره کردن یا ایجاد دسترسی به شیوه‌های دیگر، ترکیب کردن، محدود کردن، حذف و پاک کردن و یا تخریب است (EUR-Lex, 2016: 33).

۴. داده شخصی ماهیتی دو جنبه دارد که مرکب از بُعد مالی (مادی) و غیرمالی (معنوی) است. بدین جهت این داده‌ها به خودی‌خود ارزشمند و در زمره اموال هستند. ابعاد مالی داده شخصی حق انحصاری هرگونه بهره‌برداری از داده شخصی است. بهره‌برداری متناسب با داده شخصی از طریق پردازش است که مصادیق آن در ماده (۴) بند «۲» مقررات عمومی حفاظت از داده اتحادیه اروپا - مانند جمع‌آوری، ضبط، ذخیره‌سازی، اشتراک‌گذاری، افشا، منتشر کردن و ... بیان شده است (EUR-Lex, 2016: 33). ابعاد معنوی داده شخصی نیز حقوقی است که وابسته به شخصیت شخص موضوع داده است. این حقوق در نظام حقوقی ایران مورد تصریح قرار نگرفته‌اند؛ لیکن در مواد ۱۲ الی ۲۲ این مقررات به آنها اشاره شده است. چنین حقوقی از جمله 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 یا زمینه‌های مربوط به موقعیت‌های ویژه و عدم قرار گرفتن در معرض تصمیمات خودکار است. با توجه به ماهیت داده شخصی، حق بر داده شخصی نمی‌تواند حق مالکیت مرسوم و همچنین حقوق مالکیت معنوی باشد، زیرا قواعد حق مالکیت مرسوم و مصادیق مختلف مالکیت معنوی هیچ‌یک کاملاً منطبق بر داده شخصی نیستند و بدین جهت داده شخصی نمی‌تواند با جریان حق مالکیت مرسوم یا حقوق مالکیت معنوی حمایت شود؛ بنابراین بستر حقوقی مناسب برای حمایت از داده شخصی، حق مالکیت ویژه‌ای است که متفاوت از حق مالکیت مرسوم است. این حق ویژگی‌های خاص خود را دارد که توضیح آن در این مقاله نمی‌گنجد.

خصوصی اشخاص و داده‌های شخصی بیشتر احساس می‌شود. حفاظت از داده‌های شخصی اشخاص حقیقی، از حقوق شهروندی و از جنبه‌های حقوق بشر است. حق بر حریم خصوصی اطلاعاتی و حفاظت از داده‌های شخصی، در اسناد ملی و بین‌المللی مختلفی به‌عنوان جنبه‌ای از حقوق بشر مورد تصریح قرار گرفته است، به‌عنوان نمونه ماده (۱۲) اعلامیه جهانی حقوق بشر، حق بر حریم خصوصی (با همه اقسام آن از جمله حق بر حریم خصوصی اطلاعاتی) را به‌عنوان حق اساسی به رسمیت شناخته است (United Nations, 2015: 26). همچنین در اتحادیه اروپا، حریم خصوصی و حمایت از داده، دو حق حیاتی هستند (European Data Protection Supervisor, n.d.) که در مواد (۷) و (۸) منشور حقوق اساسی اتحادیه اروپا (EUR-Lex, 2012: 397) و ماده (۸) کنوانسیون اروپایی حقوق بشر (Council of Europe, 1950: 11) مقرر شده‌اند. با لحاظ مطالب پیش‌گفته وجود بسترهای قانونی برای حفاظت از داده‌های شخصی ضروری است. حمایت قانونی از داده‌های شخصی و اشخاص موضوع داده در برخی نظام‌های حقوقی مانند اتحادیه اروپا عملی شده است. اتحادیه اروپا با تصویب مقررات عمومی حفاظت از داده^۱ در خصوص حمایت از داده شخصی در سال ۲۰۱۶ و لازم‌الاجرا شدن آن در سال ۲۰۱۸ همه کشورهای عضو اتحادیه اروپا را ملزم به حمایت حداکثری از داده‌های شخصی و اشخاص موضوع داده کرده است. مقررات عمومی حفاظت از داده اتحادیه اروپا الزامات مختلفی را مقرر کرده است تا اشخاص حقیقی، به‌طور کامل از حق بر حریم خصوصی اطلاعاتی و حفاظت از داده‌های شخصی‌شان به‌عنوان یکی از جنبه‌های حقوق بشر، بهره‌مند شوند. حمایت‌های حداکثری این مقررات در مواد مختلفی بیان شده است. یکی از اساسی‌ترین جنبه‌های حمایت از داده‌های شخصی به‌موجب این مقررات، جریان حقوق مختلف برای اشخاص موضوع

1. General Data Protection Regulation (GDPR)

داده در راستای تحقق کامل حق بر حریم خصوصی اطلاعاتی و حفاظت از داده‌های شخصی به‌عنوان یکی از ابعاد حقوق بشر است. در مقابل حقوق اشخاص موضوع داده، اشخاص پردازش‌کننده داده (کنترل‌کننده‌ها و پردازنده‌ها)^۱ تعهدات مختلفی دارند و به رعایت تکالیف متعدد و اصول حاکم بر پردازش ملزم هستند. همه اشخاص پردازش‌کننده داده باید الزامات این مقررات را در خصوص پردازش رعایت کنند و در صورت تخلف از تعهدات و عدم رعایت اصول (نقض حمایت از داده‌های شخصی)، با ضمانت اجرا مواجه خواهند شد. در این راستا مقررات عمومی حفاظت از داده اتحادیه اروپا، در مواد مختلف ضمانت‌اجراهای متفاوتی را مقرر کرده است. اهم این ضمانت‌اجراها، حق جبران خسارت به‌موجب ماده (۸۲) (ضمانت اجرای مدنی) و جزای نقدی مطابق با ماده (۸۳) (ضمانت اجرای کیفری) مقررات پیش گفته است.

در این پژوهش با تبیین چگونگی ضمانت‌اجراهای مذکور، جریان این موارد را در نظام حقوقی ایران امکان‌سنجی می‌کند. البته ایران در خصوص حفاظت از داده‌های شخصی، قانون مستقل ندارد و بالتبع ضمانت‌اجراهای خاص نیز برای نقض حمایت از آن پیش‌بینی نشده است؛ اما با ارائه پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» در تیرماه ۱۳۹۷ - منتشر شده در سایت سازمان فناوری اطلاعات ایران -^۲ و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» اعلام وصول شده در صحن علنی مجلس در شهریورماه ۱۴۰۰،^۳ در این خصوص گام‌هایی برداشته است؛

1. Controller and Processor

۲. لینک دسترسی به پیش‌نویس لایحه:

<https://www.ict.gov.ir/fa/newsagency/21691/%D9%84%D8%A7%DB%8C%D8%AD%D9%87-%D8%B5%DB%8C%D8%A7%D9%86%D8%AA-%D9%88-%D8%AD%D9%81%D8%A7%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87-%D9%87%D8%A7%DB%8C-%D8%B4%D8%AE%D8%B5%DB%8C-%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C-%D8%B4%D8%AF>

<https://dotic.ir/news/10419>

۳. لینک دسترسی به طرح:

اما این اقدامها برای حمایت از داده‌های شخصی کافی نیست. بدین جهت و با عنایت به فقدان قانون مستقل در خصوص حمایت از داده شخصی، در نظام حقوقی ایران، حمایت از داده‌های شخصی و اشخاص موضوع داده باید از خلال قوانین موضوعه، دکترین حقوقی، مبانی حقوق ایران و فقه امامیه استنباط شود. موضوع پژوهش حاضر نیز از این امر مستثنا نیست و چگونگی ضمانت اجرای نقض حمایت از داده شخصی از منابع مختلف ایران استخراج خواهد شد.

۱. حق جبران خسارت (ضمانت اجرای مدنی)

حق جبران خسارت در دو فرض انجام پردازش با هوش انسانی یا هوش مصنوعی متفاوت است. در موارد بسیاری پردازش داده‌های شخصی با هوش انسانی انجام می‌شود و اشخاص پردازش‌کننده داده انسان‌ها هستند (گرچه ممکن است از ماشین‌ها نیز استفاده شود). در مقابل نیز فرضی وجود دارد که اصل پردازش از سوی هوش‌های مصنوعی^۱ انجام می‌شود و اشخاص پردازش‌کننده داده ماشین‌ها و دستگاه‌ها هستند. در خصوص حق جبران خسارت، ورود به مسئله هوش‌های مصنوعی و بررسی مختصر آن در خصوص حفاظت از داده شخصی مهم به نظر می‌رسد. در واقع بررسی این مسئله بایسته است که اگر در فرایند پردازش، هوش مصنوعی دخیل باشد و به شخص موضوع داده، ضرر وارد شود، چنین ضرری چگونه باید جبران شود. بدین ترتیب ابتدا به تبیین حق جبران خسارت در صورت پردازش با هوش انسانی (مبحث ۱-۱) و سپس این امر در صورت پردازش با هوش مصنوعی مورد بررسی قرار خواهد گرفت (مبحث ۱-۲).

۱-۱. تبیین حق جبران خسارت در صورت پردازش با هوش انسانی

در صورتی که اشخاص پردازش‌کننده داده انسان‌ها باشند، حق جبران خسارت

1. Artificial Intelligence (AI)

به موجب مقررات عمومی حفاظت از داده اتحادیه اروپا (مبحث ۱-۱-۱) و نظام حقوقی ایران قابل بررسی است (۱-۱-۲).

۱-۱-۱. تبیین حق جبران خسارت در صورت پردازش با هوش انسانی به موجب مقررات عمومی حفاظت از داده اتحادیه اروپا

حق جبران خسارت در ماده (۸۲) این مقررات لحاظ شده است: «۱. هر شخصی که در نتیجه نقض این مقررات دچار آسیب مادی یا معنوی شده است، حق دریافت غرامت از کنترل کننده یا پردازنده برای خسارت وارد شده دارد. ۲. هر کنترل کننده دخیل در پردازش، مسئول آسیب ناشی از پردازشی است که این مقررات را نقض کرده است. پردازنده تنها در صورتی مسئول آسیب ناشی از پردازش است که از الزامات این مقررات به طور خاص در مورد پردازنده‌ها پیروی نکرده باشد یا در صورتی که خارج یا برخلاف دستورالعمل‌های قانونی کنترل کننده عمل کرده باشد. ۳. کنترل کننده یا پردازنده از مسئولیت بند «۲» معاف هستند، اگر ثابت کنند که به هیچ وجه مسئول حادثه موجب خسارت نیستند. ۴. در جایی که بیش از یک کنترل کننده یا پردازنده، یا کنترل کننده و پردازنده هر دو، در یک پردازش دخیل باشند آنها به موجب بندهای «۲» و «۳»، مسئول هر گونه آسیب ناشی از پردازش هستند، هر کنترل کننده یا پردازنده باید مسئول کل خسارت باشد تا از جبران مؤثر برای شخص موضوع داده اطمینان حاصل شود. ۵. در جایی که کنترل کننده یا پردازنده، مطابق با بند «۴» غرامت کاملی را برای ضرر وارد شده، پرداخت کرده است، آن کنترل کننده یا پردازنده حق دارد به سایر کنترل کننده‌ها یا پردازنده‌های دخیل در همان پردازش که بخشی از غرامت مربوط به مسئولیت آنهاست، مطابق با شرایط مذکور در بند «۲»، جهت بازیافت غرامت به نسبت مسئولیت رجوع کند. ۶. اقامه دعوی برای اعمال حق بازیافت غرامت، باید به موجب قانون کشور عضو مذکور در ماده (۷۹) بند «۲»، در دادگاه‌های صالح طرح شود»

(EUR-Lex, 2016: 81-82). این ماده حق جبران کامل خسارات برای هرگونه آسیب - مادی یا معنوی - ناشی از نقض این مقررات را بیان می‌کند. این حق به مراحل خاصی از پردازش داده یا فعالیت‌های پردازشی خاص محدود نیست. به علاوه، نقض در این مقررات به‌طور موسع تفسیر می‌شود بدین جهت شامل پردازش‌هایی است که قواعد این مقررات یا مصوبات مستند به این مقررات یا قانون کشورهای عضو اتحادیه اروپا را نقض می‌کند (Voigt and Von Dem Bussche, 2017: 205, 207).

هریک از بندهای ماده (۸۲) به شرح ذیل قابل توضیح است. مطابق ماده (۸۲) بند «۱»، خسارت شامل آسیب‌های مادی و معنوی است، زیرا پیامد نقض داده می‌تواند به‌طور گسترده‌ای متفاوت باشد و غالباً ماهیت ناملموس مانند تبعیض اجتماعی، استرس روانی یا لطمه به شخصیت افراد را به دنبال دارد.^۱ افراد باید غرامت کامل و مؤثری برای خساراتی دریافت کنند که متحمل شده‌اند (European Commission, n.d.-a). خسارت باید به‌طور موسع همان‌گونه تفسیر شود که در آیین دادرسی دیوان دادگستری اتحادیه اروپا قابل ملاحظه است. مطابق با رویه قضایی دیوان دادگستری اتحادیه اروپا حق جبران خسارت باید «اثر بازدارندگی واقعی»^۲ بر واردکننده زیان داشته باشد، به همین علت حداکثر خسارت لحاظ می‌شود. برای نمونه می‌توان به رأی شماره C-407/14 مورخ ۱۷ دسامبر ۲۰۱۵ اشاره کرد. این رأی مربوط به دادرسی بین خانم Arjona Camacho علیه Securitas Seguridad España SA - شرکت امنیتی سوئدی - است که با حکم دیوان شرکت سوئدی ملزم به پرداخت «خسارت تنبیهی»^۳

۱. به‌عنوان نمونه نقض داده‌های شخصی مربوط به اتهام‌ها یا محکومیت‌های کیفری که منجر به آشکار شدن هویت شخص موضوع داده است، می‌تواند تأثیر بسیاری بر حق احترام به زندگی خصوصی و خانوادگی شخص، آزادی انتخاب شغل و حق مشارکت در مشاغل، آزادی انجام یک تجارت و ... داشته باشد (ICO, n.d.-b). در واقع اتهام‌ها و محکومیت‌های کیفری می‌توانند اشخاص موضوع داده را برای مدت طولانی بدنام کنند و پیامدهای منفی مختلفی را برای شخص موضوع داده به دنبال داشته باشند.

2. Genuine Deterrent Effect

3. Punitive Damages

به خانم Arjona Camacho پس از برکناری وی به دلیل تبعیض جنسیتی شد (به دلیل لزوم برابری زن و مرد در محیط شغلی). در واقع دیوان حکم کرد که به منظور مؤثر بودن حق جبران خسارت، غرامت پرداخت شده به کارمند باید در خصوص آسیب‌های متحمل شده کافی باشد تا جبران خسارت اثر بازدارندگی واقعی داشته باشد (CURIA, 2015: 7). در عین حال وظیفه دادگاه و قاضی است که تمام شرایط و اینکه نقض تا چه حد جدی بوده و تأثیر آن را بر شخص موضوع داده در نظر گیرد. دادگاه می‌تواند در شرایط خاصی له یا علیه شخص موضوع داده حکم دهد. به‌طور مثال، اگر مشخص شود که برای شخص موضوع داده، صرفاً ناراحتی کمی رخ داده است، دادگاه حکم به جبران خسارت و پرداخت غرامت نخواهد داد (ICO, n.d.-a). به‌علاوه، از آنجایی که در ماده (۸۲) بند «۱» واژه «هر شخصی» مورد استفاده قرار گرفته است، نه تنها اشخاص موضوع داده می‌توانند درخواست غرامت کنند، بلکه هر شخص دیگری که متحمل خسارت ناشی از نقض مفاد این مقررات شده است نیز می‌تواند درخواست غرامت کند؛ البته به موجب این مقررات مشخص نیست که چه کسانی غیر از اشخاص موضوع داده مستحق غرامت هستند؛ بدین جهت وظیفه دادگاه است که چنین امری را تبیین کند (Ungureanu, 2018: 39). همچنین برای وجود حق جبران خسارت، باید رابطه سببیت^۱ بین نقض این مقررات و خسارت وجود داشته باشد که به موجب ماده (۸۲) بند «۱» هر فردی که آسیب ببیند می‌تواند مطالبه غرامت کند. البته حق جبران خسارت قبل از هر چیز شخص موضوع داده را نسبت به جبران خسارت محق می‌کند؛ با این حال این مفاد سایر افراد را نیز که متحمل خسارت شده‌اند، محق می‌سازد؛ اما باید به وجود رابطه سببیت کافی بین آسیب به شخص ثالث و نقض قانون حفاظت از داده - مقررات عمومی حفاظت از داده اتحادیه اروپا یا سایر قوانین

1. Causal Link

حفاظت از داده ملی - توجه کرد. اشخاص پردازش کننده داده باید آگاه باشند که وجود حق جبران خسارت به موجب ماده (۸۲) به مطالبه غرامت ناشی از نقض مقررات دیگر در قانون کشورهای عضو اتحادیه اروپا و یا اتحادیه اروپا خللی وارد نمی کند، بنابراین کنترل کننده ها و پردازنده ها ممکن است با مطالبات بیشتری به موجب قانون مدنی ملی و در زمینه های قراردادی یا به موجب قانون مسئولیت مدنی یا دیگر بسترهای قانونی مواجه شوند (Voigt and Von Dem Bussche, 2017: 205-206).

ماده (۸۲) بند «۲» این مقررات نسبت به بسترهای قانونی سابق در اتحادیه اروپا به عنوان یک نوآوری قابل اشاره است زیرا پردازنده مستقیماً مسئول نقض تعهداتش به موجب مقررات عمومی حفاظت از داده اتحادیه اروپاست و زیان دیده می تواند در دادگاه مستقیماً علیه پردازنده طرح دعوی کند. در این صورت هم کنترل کننده و هم پردازنده در مقابل شخص موضوع داده مسئول هستند و نظام مسئولیت تجمعی^۱ جریان دارد. علت مسئولیت کنترل کننده این است که به عنوان اصل و به طور کلی مسئولیت پردازش غیرقانونی برعهده کنترل کننده است و هرگونه آسیب ناشی از پردازش، بدون توجه به اینکه آیا کنترل کننده به طور مستقیم باعث آسیب شده است یا خیر، باید از سوی کنترل کننده جبران شود. مسئولیت جامع کنترل کننده به دلیل نقش اصلی در تعیین اهداف و ابزار پردازش و همچنین اختیارات کنترل کننده برای دستور به پردازنده در مورد چگونگی انجام پردازش است. با وجود این، به موجب مقررات عمومی حفاظت از داده اتحادیه اروپا پردازنده نیز مسئول است، البته با توجه به اینکه پردازنده از جانب کنترل کننده عمل می کند، مسئولیت پردازنده محدود به خسارات ناشی از نقض تعهداتش به موجب این مقررات در صورتی است که خارج یا خلاف دستورات قانونی کنترل کننده اقدام کرده باشد (Bredin and Riordan, 2017: 1).

1. Cumulative Liability Regime

براساس ماده (۸۲) بند «۳» این مقررات، در صورتی که کنترل کننده یا پردازنده، ثابت کند که به هیچ وجه مسئول واقعه منجر به خسارت نیست، از مسئولیت معاف است. در مقایسه با دستورالعمل حفاظت از داده (بستر قانونی سابق اتحادیه اروپا در خصوص حفاظت از داده) استاندارد اثبات به موجب مقررات عمومی حفاظت از داده اتحادیه اروپا افزایش یافته است؛ بنابراین استفاده از معافیت، برای اشخاص پردازش کننده داده سخت تر خواهد بود؛ زیرا حتی کوچک ترین دخالت در واقعه ای که باعث خسارت شده باشد؛ مسئولیت را در پی دارد و هدف از این بند ماده (۸۲)، صرفاً معافیت کنترل کننده ها و پردازنده هایی است که به طور کامل به تعهدات خود براساس مقررات عمومی حفاظت از داده اتحادیه اروپا عمل کرده اند. البته باید توجه داشت معافیت در جایی که کنترل کننده و پردازنده بتواند تحقق تعهداتش را اثبات کند، اما مانع از وقوع خسارت نشود، اعمال نمی شود. برای مثال یک کنترل کننده همه الزامات و تعهدات خود را براساس این مقررات برای فعالیت های پردازشی اش انجام داده است، با وجود این، شخص ثالث به داده های شخصی دسترسی پیدا می کند و کنترل کننده به تشخیص علت آن قادر نیست و در نتیجه با افشای داده ها، اشخاص موضوع داده آسیب می بینند. در این مثال، کنترل کننده، تعهدات خود را براساس مقررات عمومی حفاظت از داده اتحادیه اروپا انجام داده است، اما به رغم آن، نتوانسته مانع از دسترسی شخص ثالث به داده ها شود. با این حال چون نمی توان با قطعیت گفت که کنترل کننده به هیچ وجه مسئول دسترسی شخص ثالث نبوده است، کنترل کننده مسئول است (Voigt and Von Dem Bussche, 2017: 208).

همچنین مطابق ماده (۸۲) بند «۴» این مقررات و به منظور تضمین جبران خسارت مؤثر برای شخص موضوع داده در فرضی که چندین کنترل کننده یا پردازنده وجود دارند، هر کنترل کننده و پردازنده به صورت جداگانه، مسئول جبران خسارت

است؛ بنابراین هریک از آنها مسئول کل خسارت هستند. مفاد این ماده، اعمال مطالبه برای شخص موضوع داده یا دیگر مدعیان را ساده می‌کند؛ زیرا آنها می‌توانند انتخاب کنند که علیه یکی از اطراف مسئول که معمولاً تواناترین نسبت به پرداخت خسارت است، اقدام کنند (مسئولیت تضامنی). با این حال، رابطه درونی بین اطراف مسئول، تابع اصل مسئولیت نسبی است (Bredin and Riordan, 2017: 2). به موجب ماده (۸۲) بند «۵» نیز طرف مسئول که غرامت کامل را پرداخت کرده است، می‌تواند به دیگر کنترل‌کننده‌ها یا پردازنده‌های دخیل در آن بخشی از خسارت که مربوط به مسئولیت آنهاست، رجوع کند.

در نهایت باید به ماده (۸۲) بند «۶» مقررات عمومی حفاظت از داده اتحادیه اروپا پرداخت که اقامه دعوی را به ماده (۷۹) بند «۲» ارجاع داده است. طبق ماده (۷۹) بند «۲» این مقررات «اقامه دعوی علیه کنترل‌کننده یا پردازنده، باید در دادگاه‌های کشور عضوی طرح شود که کنترل‌کننده یا پردازنده مقر دارند. همچنین اقامه دعوی می‌تواند در دادگاه‌های کشور عضوی طرح شود که محل اقامت عادی شخص موضوع داده است، مگر اینکه کنترل‌کننده یا پردازنده مرجع عمومی از یک کشور عضو باشد که در جهت اعمال اختیارات عمومی خود عمل می‌کند» (EUR-Lex, 2016: 80).

۱-۱-۲. بررسی حق جبران خسارت در صورت پردازش با هوش انسانی در نظام حقوقی ایران

برای بررسی و چگونگی جریان ماده (۸۲) مقررات عمومی حفاظت از داده اتحادیه اروپا در نظام حقوقی ایران، همان‌طور که در فراز سابق به هر بند به صورت مجزا پرداخته شد، در این قسمت نیز به هر بند جداگانه اشاره می‌شود. در خصوص بند «۱» ماده (۸۲) می‌توان گفت، در نظام حقوقی ایران نیز حق جبران خسارت به‌عنوان یکی از

آثار مسئولیت مدنی و به‌عنوان یک قاعده عمومی و مصرح در مواد قانونی،^۱ وجود دارد. بدین جهت با توجه به موجبات متفاوت ضمان قهری از یک‌سو (غصب، اتلاف، تسبیب و...) و ماهیت داده‌های شخصی از سوی دیگر (وجود بُعد مالی برای داده‌های شخصی) در صورت ورود ضرر به شخص موضوع داده، چنین شخصی می‌تواند با استناد به هر یک از موجبات ضمان، متناسب با شرایط مختلف از حق جبران خسارت استفاده کند.

فارغ از اینکه هدف از جبران خسارت، ترمیم وضع زیان‌دیده و بازگرداندن وی به حالت پیشین است، در خصوص بحث جبران خسارت، جنبه تنبیهی خسارت یا در اصطلاح «خسارت تنبیهی»^۲ نیز قابل بررسی است. این خسارت غرامتی است که دادگاه، در صورتی که ضرر ناشی از تقصیر عمدی یا تقصیر سنگین یا تقصیر سودآور واردکننده زیان باشد، به‌منظور تنبیه و مجازات مدنی وی، تعیین می‌کند و به زیان‌دیده پرداخت می‌شود. این نوع خسارت جنبه پیشگیرانه دارد که در کشورهای کامن‌لا به‌ویژه در ایالات متحده آمریکا رایج است (صفایی و رحیمی، ۱۳۹۷: ۵۱۵). چنین خسارتی در رویه قضایی اتحادیه اروپا نیز قابل مشاهده است که نمونه‌ای از آن در پرونده خانم Arjona Camacho علیه Securitas Seguridad España SA - شرکت امنیتی سوئدی - بیان شد.

در قوانین موضوعه ایران به جنبه تنبیهی خسارت و اثر بازدارندگی آن به‌عنوان قاعده عمومی اشاره نشده است و صرفاً در برخی مواد قانونی^۳ مصادیقی از خسارت

۱. مواد مختلفی از قانون مسئولیت مدنی.

2. Punitive Damages

۳. از مصادیق قانونی خسارت تنبیهی می‌توان به ماده (۵۵۵) قانون مجازات اسلامی مصوب ۱۳۹۲ اشاره کرد که مقرر می‌کند «هرگاه رفتار مرتکب و فوت مجنی‌علیه هر دو در ماه‌های حرام (محرم، رجب، ذی‌القعدة و ذی‌الحجه) یا در محدوده حرم مکه، واقع شود خواه جنایت عمدی خواه غیرعمدی باشد، علاوه بر دیه نفس، یک‌سوم دیه نیز افزوده می‌گردد. سایر مکان‌ها و زمان‌های مقدس و متبرک مشمول حکم تغلیظ دیه نیست». همچنین ماده (۳۱۴) قانون مدنی که مقرر می‌کند «اگر در نتیجه عمل غاصب قیمت مال مغضوب زیاد شود غاصب حق مطالبه قیمت زیادی را نخواهد داشت مگر اینکه آن زیادتی عین باشد که در این صورت عین زائد متعلق به خود غاصب است».

تنبیهی قابل مشاهده است (همان: ۲۵۷). البته به چنین خسارتی به صراحت در «قانون صلاحیت دادگستری جمهوری اسلامی ایران برای رسیدگی به دعاوی مدنی علیه دولت‌های خارجی» مصوب ۱۳۹۰ اشاره شده است. به موجب ماده (۴) این قانون، ملاک در میزان تقویم خسارت تنبیهی اصل عمل متقابل است. در عین حال به دلیل عدم عنایت کافی نظام حقوقی ایران به خسارت تنبیهی، جریان چنین خسارتی در نگاه اول نسبت به نقض داده‌های شخصی ممکن نیست. البته تعیین چنین خسارتی به دلیل تقویت اثر بازدارندگی خسارت، پیشنهاد می‌شود. در این راستا جریان آن در هر مورد، به اوضاع و احوال پرونده بستگی دارد و این وظیفه قاضی است که به تناسب هر پرونده در خصوص وجود چنین خسارتی تصمیم گیرد. مؤید برای مناسب بودن جریان خسارت تنبیهی در خصوص حفاظت از داده شخصی می‌تواند ماده (۶۴) پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» (ماده ۴۹) طرح «حمایت و حفاظت از داده و اطلاعات شخصی» باشد که بیان می‌کند «مرجع صلاحیت‌دار قضایی یا انتظامی می‌تواند متناسب با نوع و گستره آسیب حیثیتی وارده، میزان جبران‌پذیر و زیان‌های مادی ناشی از آن، مرتکب را به پرداخت جریمه تنبیهی یا محدودیت‌های اجتماعی در حق آسیب‌دیده محکوم نماید. شیوه‌نامه تعیین و تقویم زیان‌های مادی ناشی از پردازش غیرمجاز داده‌های شخصی و نحوه اعاده حیثیت ناشی از ورود آسیب‌های معنوی و جریمه به پیشنهاد کارگروه‌های تخصصی به تصویب کمیسیون می‌رسد».

همان‌طور که قابل ملاحظه است این ماده برای آسیب‌های ناشی از نقض داده شخصی، خسارت تنبیهی را پیشنهاد کرده است. البته اشاره به خسارت تنبیهی با پیش‌نویس مذکور بدون اشکال نیست. چنین اشکالی عدم اشاره مجزا به خسارت تنبیهی یا اشاره جزئی در ضمن یکی از مواد است. آخرین نکته درباره بند «۱» ماده

(۸۲) مقررات عمومی حفاظت از داده اتحادیه اروپا لزوم وجود رابطه سببیت بین نقض این مقررات و خسارت وارده است. در نظام حقوقی ایران نیز رابطه سببیت به عنوان یکی از ارکان جریان مسئولیت مدنی برای وجود حق جبران خسارت ضروری است (کاتوزیان، ۱۳۹۵، ج ۱: ۴۳۴؛ صفایی و رحیمی، ۱۳۹۸: ۲۰۴).

در خصوص بند «۲» ماده (۸۲) مقررات عمومی حفاظت از داده اتحادیه اروپا باید گفت، به موجب این بند و برخلاف سایر بسترهای قانونی سابق در اتحادیه اروپا، این مقررات پردازنده را مسئول تعهدات خود می‌داند و اشخاص موضوع داده می‌توانند مستقیماً با پردازنده روبه‌رو شوند و علیه وی اقامه دعوی کنند. رویه قانونی سابق در اتحادیه اروپا که مسئولیت نقض تعهدات پردازنده را نیز برعهده کنترل‌کننده می‌دانست، از منظر حقوق ایران خلاف اصل بود و این بند از مقررات عمومی حفاظت از داده اتحادیه اروپا موافق اصل است؛ زیرا اصل بر شخصی بودن مسئولیت بر مبنای قاعده وزر^۱ است (یزدانیان، ۱۳۹۵، ج ۲: ۱۸۷) و مسئولیت ناشی از فعل غیر، خلاف اصل است که جنبه حمایتی دارد و برای این است که زیانی بدون جبران باقی نماند (کاتوزیان، ۱۳۹۴، ج ۲: ۵). در حال حاضر اتحادیه اروپا مبنای خود را با مسئول دانستن پردازنده تغییر داده و موافق با اصل شخص بودن مسئولیت عمل کرده است که در راستای هدف این مقررات یعنی حمایت حداکثری از اشخاص موضوع داده است (در واقع حمایت حداکثری، با لحاظ این امر محقق شده است که کنترل‌کننده در حالت کلی مسئول است و علاوه بر کنترل‌کننده، پردازنده نیز به موجب مقررات عمومی حفاظت از داده اتحادیه اروپا مسئول شناخته می‌شود). در نظام حقوقی ایران از آنجایی که به کنترل‌کننده، پردازنده و مسئولیت آنها در بسترهای قانونی اشاره نشده باید مطابق با اصل یعنی شخصی بودن مسئولیت عمل کرد؛ بنابراین هر

۱. یکی از مبانی این قاعده، آیات قرآن کریم مانند آیه شریفه «وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَى» (انعام، ۱۶۴) است.

شخصی که داده‌های شخصی را پردازش می‌کند و موجب ورود ضرر به شخص موضوع داده می‌شود، مسئول جبران خسارت است. البته به دلیل لزوم حمایت حداکثری از اشخاص موضوع داده باید مسئولیت کنترل‌کننده همچنان وجود داشته باشد. این امر در مقررات عمومی حفاظت از داده اتحادیه اروپا نیز لحاظ شده است و با وجود مسئول دانستن پردازنده، همچنان کنترل‌کننده نیز مسئول است مبنای این تعهد جریان مسئولیت تجمعی بوده که جنبه‌ای از مسئولیت ناشی از فعل غیر است. به این موضوع در ماده (۶۱) پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» اشاره شده است. این ماده مقرر می‌کند «کنترل‌گر موظف است حسب درخواست زیان‌دیده تمامی ضرر و زیان وارده به شخص موضوع داده را جبران کند. در صورت عدم جبران ضرر و زیان، موضوع حسب شکایت زیان‌دیده از طریق مراجع قضایی پیگیری خواهد شد». هدف از وضع این مفاد حمایت از شخص موضوع داده و عدم خسارت بدون جبران است. همچنین در این خصوص تبیین رابطه بین کنترل‌کننده و پردازنده نیز می‌تواند راهگشا باشد. توضیح اینکه پردازنده^۱ به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که از جانب کنترل‌کننده، پردازش داده‌های شخصی را انجام می‌دهد (EUR-Lex, 2016: 33). پردازنده داده‌های شخصی را فقط به نمایندگی از کنترل‌کننده^۲ پردازش می‌کند و باید پردازش مطابق با استانداردهای مقررات عمومی حفاظت از داده اتحادیه اروپا باشد و حفاظت از حقوق افراد را تضمین کند. وظایف پردازنده نسبت به کنترل‌کننده باید در یک قرارداد یا با اقدام حقوقی

1. Processor

۲. کنترل‌کننده (Controller)، به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که به تنهایی یا به‌طور مشترک با دیگران، اهداف و ابزار پردازش داده‌های شخصی را تعیین می‌کند. بدین جهت در صورتی که شخصی - اعم از حقیقی یا حقوقی - یا مرجعی عمومی یا نهادی تصمیم گیرد که چرا و چگونه داده‌های شخصی باید پردازش شوند، کنترل‌کننده داده است (See. EUR-Lex, 2016: 33).

دیگری مشخص شود^۱ (European Commission, 2018). با توجه به آنچه بیان شد، روشن است که پردازنده به نمایندگی از کنترل کننده عمل می کند. بدین ترتیب به نظر می رسد بتوان در مورد جبران خسارت از ماده (۱۲) قانون مسئولیت مدنی^۲ نیز استفاده کرد. البته جریان ماده مذکور نسبت به کنترل کننده و پردازنده، زمانی صحیح است که رابطه بین کارگر و کارفرما نیز نمایندگی تلقی شود.^۳ با فرض جریان این ماده، به موجب حقوق ایران کنترل کننده، مسئول جبران خسارت است و زیان دیده نمی تواند مستقیماً به پردازنده مراجعه کند. در واقع صرفاً کنترل کننده حق مراجعه به پردازنده واردکننده زیان را دارد. البته این استنباط در جهت حمایت حداکثری از شخص موضوع داده (زیان دیده) نیست؛ چراکه حق مراجعه مستقیم به پردازنده را سلب می کند (فقدان وجود مسئولیت تضامنی بین کنترل کننده و پردازنده).

در خصوص بند «۳» ماده (۸۲) مقررات عمومی حفاظت از داده اتحادیه اروپا که مبین عدم مسئولیت اشخاص پردازش کننده داده در مواردی که ثابت کنند به هیچ وجه مسئول حادثه موجب خسارت نیستند، باید گفت در حقوق ایران این بند قابل تطبیق با بحث قوای قاهره و معاف شدن از مسئولیت با وجود قوه قاهره است. به موجب دکترین حقوقی، قوه قاهره حادثه خارجی، غیرقابل پیش بینی و احترازناپذیر است و ملاک جریان آن معیار نوعی است (کاتوزیان، ۱۳۹۵، ج ۱: ۴۷۹؛ صفایی و رحیمی، ۱۳۹۸: ۲۱۳). مصادیق این امر که در مواد قانونی نیز بدان اشاره شده است،^۴ در معنای عام خود حادثه

۱. در ماده (۲۶) مقررات عمومی حفاظت از داده اتحادیه اروپا به این وظیفه اشاره شده است.

۲. «کارفرمایی که مشمول قانون کار هستند مسئول جبران خساراتی می باشند که از طرف کارکنان اداری و یا کارگران آنان در حین انجام کار یا به مناسبت آن وارد شده است مگر اینکه محرز شود تمام احتیاطهایی که اوضاع و احوال قضیه ایجاب می نموده به عمل آورده و یا اینکه اگر احتیاطهای مزبور را به عمل می آورند باز هم جلوگیری از ورود زیان مقدور نمی بود کارفرما می تواند به واردکننده خسارت در صورتی که مطابق قانون مسئول شناخته شود مراجعه نماید».

۳. از دیدگاه برخی دکترین حقوقی، نماینده مأمور انجام اعمال حقوقی به نیابت است؛ در حالی که موضوع تعهد کارگر، اعمال مادی است (عراقی، ۱۳۸۹: ۱۸۵).

۴. این موارد از جمله ماده (۱۲) قانون مسئولیت مدنی و عموم مواد (۲۲۷) و (۲۲۹) قانون مدنی است.

۳۵۷ _____ بررسی تطبیقی ضمانت اجرای نقض حق بر داده در حقوق اتحادیه اروپا ...

طبیعی، فعل شخص ثالث و فعل متضرر است (ر.ک. صفایی و رحیمی، ۱۳۹۷: ۴۱۵-۴۱۲). با وجود این به نظر می‌رسد، صرف وجود هریک از مصادیق قوه قاهره براساس مقررات عمومی حفاظت از داده اتحادیه اروپا موجب معافیت از مسئولیت نیست؛ زیرا در خصوص این بند از مقررات بیان شده «در جایی که کنترل‌کننده و پردازنده بتواند تحقق تعهداتش را اثبات کند، اما این امر نتواند مانع از وقوع خسارت شود، معافیت اعمال نمی‌شود» (Voigt and Von Dem Bussche, 2017: 208).

درواقع نگاه این مقررات در خصوص مسئولیت سخت‌گیرانه است و از منظر مقررات عمومی حفاظت از داده اتحادیه اروپا انجام اقدام‌ها و تعهدهای اشخاص پردازش‌کننده داده باید برای جلوگیری از ضرر کافی باشد، در غیر این صورت معافیت وجود ندارد. مشابه این امر در حقوق ایران نیز وجود دارد. به‌عنوان نمونه در جایی که فعل شخص ثالث موجب خسارت است (که از مصادیق قوه قاهره است)؛ اما خواننده موظف به حفظ اموال خواهان بوده است، معافیت از مسئولیت وجود ندارد؛ مانند مستخدمی که موظف به قفل کردن در منزل است و با اجرا نکردن این کار، موجب ورود سارق به منزل و دزدیده شدن اموال می‌شود (همان: ۴۱۴-۴۱۳)؛ بنابراین با وجود ارزشمندی و مال بودن داده‌های شخصی می‌توان سخت‌گیری موجود در مقررات عمومی حفاظت از داده اتحادیه اروپا را برای حقوق ایران جاری دانست و گفت اشخاص پردازش‌کننده داده در شرایط مختلف، مسئول جبران خسارت هستند مگر اینکه به‌هیچ‌وجه مسئول وقوع حادثه موجب خسارت نبوده و اقدام‌های لازم و کافی را در جهت انجام تعهدات خود و عدم وقوع خسارت انجام داده باشد. البته ذکر این نکته مفید است که ید اشخاص پردازش‌کننده داده با توجه به نوع تصرف آنها در داده‌های شخصی، متفاوت است. توضیح اینکه اگر پردازش داده‌ها مجانی باشد (مانند پردازش داده‌های شخصی از سوی رسانه‌ها و شبکه‌های اجتماعی مجازی یا

موتورهای جستجو) رابطه بین شخص موضوع داده و اشخاص پردازش کننده داده، رابطه امانی است؛ زیرا در این موارد اذن ازسوی شخص موضوع داده و مجانی بودن برای جریان رابطه امانی موجود است. همچنین در صورتی که پردازش داده‌ها به موجب قرارداد باشد، ید امانی مالکی وجود دارد و در سایر موارد که پردازش به تجویز قانون است، می‌تواند ید امانی قانونی وجود داشته باشد (مانند پردازش داده‌های شخصی برای حفاظت از منافع حیاتی شخص موضوع داده یا دیگران یا پردازش به جهت منافع عمومی) (ر.ک. موسوی بجنوردی، ۱۳۷۹، ج ۱: ۲۱۴). در این موارد با تعدی و تفریط (تقصیر) ید اشخاص پردازش کننده داده به ضمانی مبدل خواهد شد. در مقابل اگر پردازش داده‌های شخصی مجانی نباشد (مانند پردازش داده‌های شخصی توسط بانک‌ها برای امور مالی) ید اشخاص پردازش کننده داده نسبت به شخص موضوع داده، ید ضمانی غیرعدوانی است؛ زیرا با وجود عناصر اذن و عدم مجانی بودن، ید ضمانی جریان دارد. در واقع اصل بر ضمانی بودن تصرف است و با فقدان یکی از عناصر ید امانی، به اصل رجوع می‌شود. بدین جهت در فرض ضمانی بودن رابطه، شخص پردازش کننده داده بدون تقصیر ضامن است (ر.ک. محقق داماد، ۱۳۸۴: ۱۰۲؛ نراقی، ۱۳۸۰، ج ۱: ۲۷).

درباره بندهای «۴» و «۵» مقررات عمومی حفاظت از داده اتحادیه اروپا که به مسئولیت تضامنی در مقابل شخص موضوع داده اشاره دارد، باید گفت مسئولیت تضامنی در حقوق ایران خلاف اصل است. این امر از مفهوم مخالف ماده (۴۰۳) قانون تجارت^۱ و اصل عدم که مبین عدم تضامن بوده قابل استنباط است. باین حال، در مواردی بر وجود مسئولیت تضامنی مانند مسئولیت غاصبان در مقابل مالک تصریح

۱. «در کلیه مواردی که به موجب قوانین یا موافق قراردادهای خصوصی ضمانت تضامنی باشد طلبکار می‌تواند به ضامن و مدیون اصلی مجتمعاً رجوع کرده یا پس از رجوع به یکی از آنها و عدم وصول طلب خود برای تمام یا بقیه طلب به دیگری رجوع نماید».

شده است. علت چنین امری این است که حق مالک در برابر غاصبانی تضمین شود که در استیلا نامشروع بر مال وضع مشترک دارند و مالک بتواند با انتخاب یک یا چند نفر از غاصبان با آسان‌ترین راه به حق خود دست یابد. همچنین از نظر منطقی امکان رجوع مالک به هریک از مسئولان موجب احیای مؤثر حق است (کاتوزیان، ۱۳۹۴، ج ۲: ۲۹۱). به نظر می‌رسد در بحث حفاظت از داده‌های شخصی نیز جریان مسئولیت تضامنی دور از انصاف و عدالت حقوقی نیست؛ زیرا داده‌های شخصی ارزشمند و در زمره اموال هستند^۱ و مسئولیت تضامنی موجب تضمین مؤثر حقوق شخص موضوع داده می‌شود. البته به دلیل خلاف اصل بودن مسئولیت تضامنی، جریان چنین مسئولیتی به تصریح قانونگذار نیاز دارد.

در خصوص بند «۶» ماده (۸۲) مقررات عمومی حفاظت از داده اتحادیه اروپا که به شخص موضوع داده اختیار می‌دهد به دادگاه مقرر اشخاص پردازش‌کننده داده (خواننده) یا به دادگاه‌های محل اقامت عادی خود (خواهان) رجوع کند، در حقوق ایران می‌توان به بحث صلاحیت محلی دادگاه‌ها اشاره کرد. به موجب ماده (۱۱) قانون آیین دادرسی مدنی مصوب ۱۳۷۹ اصل بر این است که دعوی در دادگاه محل اقامت خواننده طرح شود؛ لیکن بر این اصل استثنائاتی وارد است و قانونگذار می‌تواند دادگاه مشخصی را به عنوان دادگاه صالح اعلام کند^۲ یا به خواهان اختیار دهد که بین چند دادگاه، یکی را به عنوان مرجع صالح انتخاب کند.^۳ در خصوص بحث حاضر می‌توان گفت در صلاحیت محلی باید به اصل عمل کرد و دعوی باید در دادگاه محل اقامت

۱. در پاورقی مقدمه، به اهمیت اقتصادی داده‌ها و ابعاد مالی آنها اشاره شده است.

۲. مانند ماده (۱۲) قانون آیین دادرسی مدنی که مقرر می‌کند «دعوی مربوط به اموال غیرمنقول اعم از دعوی مالکیت مزاحمت ممانعت از حق تصرف عدوانی و سایر حقوق راجع به آن در دادگاه اقامه می‌شود که مال غیرمنقول در حوزه آن واقع است اگرچه خواننده در آن حوزه مقیم نباشد».

۳. ماده (۱۳) قانون آیین دادرسی مدنی «در دعوی بازرگانی و دعوی راجع به اموال منقول که از عقود و قراردادهای ناشی شده باشد خواهان می‌تواند به دادگاهی رجوع کند که عقد یا قرارداد در حوزه آن واقع شده است یا تعهد می‌بایست در آنجا انجام شود».

اشخاص پردازش‌کننده مطرح شود؛ اما قانونگذار ایران می‌تواند با وضع مقرره‌ای صریح، بر اصل یادشده استثنا وارد کند.

۲-۱. جبران خسارت در صورت پردازش با هوش مصنوعی به موجب مقررات

عمومی حفاظت از داده اتحادیه اروپا و بررسی آن در نظام حقوقی ایران

امروزه هوش مصنوعی در موارد بسیاری کاربرد دارد. هوش مصنوعی فرایند تقلید از تفکر انسانی است که با ماشین‌ها و دستگاه‌ها صورت می‌گیرد و در اصطلاح هوش ماشینی است (Čerka, Grigienė and Sirbikytė, 2017: 12). بسیاری از برنامه‌های هوش مصنوعی، داده‌های شخصی را پردازش می‌کنند. بدین توضیح که از یک سو، داده‌های شخصی می‌تواند داده‌های مورد استفاده برای دستگاه‌های ماشینی باشند و برای مدل‌های الگوریتمی از آنها استفاده شود و از سوی دیگر، چنین مدل‌هایی را می‌توان برای داده‌های شخصی به کار برد تا در مورد افراد خاص نتیجه‌گیری کنند؛ بنابراین به لطف هوش مصنوعی از داده‌های شخصی برای تجزیه و تحلیل و پیش‌بینی رفتارهای انسان‌ها استفاده می‌شود. استفاده از هوش مصنوعی و تصمیم‌گیری‌های خودکار با وجود مزایای بسیار، می‌تواند تأثیر منفی بر افراد موردنظر داشته باشد و نسبت به حقوق افراد خطراتی داشته باشد؛ بدین جهت بررسی جبران نقض حقوق افراد در زمان انجام پردازش با هوش مصنوعی به مسئله‌ای مهم تبدیل شده است (European Parliamentary Research Service, 2020: 1).

برای بررسی جبران خسارت در این فرض، ابتدا باید روشن شود که آیا اعطای شخصیت حقوقی مستقل با عنوان شخصیت الکترونیکی^۱ به هوش مصنوعی ممکن

۱. شخصیت الکترونیکی (Electronic Personality) اصطلاحی است که برای اولین بار کمیته امور حقوقی پارلمان اروپا در پیش‌نویس قوانین مربوط به رباتیک در تاریخ ۳۱ مه ۲۰۱۶ مطرح کرد. این اصطلاح برای توصیف وضعیت حقوقی پیشرفته‌ترین سیستم‌ها و ربات‌های خودمختار به کار می‌رود تا حقوق و تعهدات خاصی از جمله جبران خسارت وارده و استقلال در تعامل با اشخاص ثالث بررسی شود (European Law Blog, n.d).

است. مسئله مذکور در برخی از نظام‌های حقوقی محل بحث است. بحث در این است که گرچه هوش مصنوعی مؤلفه تصمیم‌گیری مستقل و تجزیه و تحلیل دارد - که از ویژگی‌های اعطای شخصیت مستقل است (Čerka, Grigienė and Sirbikytė, 2017: 12). لیکن اعطای شخصیت حقوقی مستقل و کامل برای هوش‌های مصنوعی ممکن نیست؛ زیرا برای اعطای چنین شخصیتی باید هوش مصنوعی قابلیت دارا شدن حقوق و تعهدات^۱ را داشته باشند که این امر در خصوص هوش‌های مصنوعی وجود ندارد (Andrade et al., 2007: 362). البته در برخی منابع به دلیل وجود تصمیم‌گیری مستقل از جانب هوش مصنوعی که به طور مستقیم بر زندگی اشخاص اثر دارد، برای هوش‌های مصنوعی، شخصیت حقوقی جزئی^۲ لحاظ شده است (Čerka, Grigienė and Sirbikytė, 2017: 12).

اتحادیه اروپا در مسیر پذیرش شخصیت الکترونیکی برای هوش‌های مصنوعی، معتقد است با توجه به اینکه مسئولیت مدنی و جبران خسارت با وجود شخصیت مستقل، مسئله حیاتی است؛ بسترهای قانونی آینده باید برای اعمال مسئولیت، وجود رابطه سببیت بین رفتار مضر هوش مصنوعی و آسیب برای طرف زیان‌دیده را کافی بدانند. همچنین به هیچ وجه نباید نوع یا میزان خسارت را تنها بدین دلیل که این خسارت را یک عامل غیرانسانی ایجاد کرده است، محدود کنند (European Parliament, 2015: 10). به رغم آنچه بیان شد، همچنان در مقام عمل جبران خسارت برعهده مالک هوش مصنوعی به جهت حفاظت مؤثر از منافع و حقوق افراد است (European Law Blog, n.d). از این رو همان‌طور که هیئت حفاظت از داده اتحادیه اروپا^۳ بیان کرده است هر زمان که هوش مصنوعی داده‌های شخصی را پردازش

1. The Capability of Being a Subject of Rights and Obligations

2. Partial Legal Personality

3. European Data Protection Board (EDPB)

می‌کند، همه الزامات مقررات عمومی حفاظت از داده اتحادیه اروپا قابل اعمال است (Centre for Information Policy Leadership (CIPL), 2020: 4)؛ اما مفاد مربوط به مسئولیت مدنی و جبران خسارت مذکور در این مقررات نسبت به مالک (اداره‌کننده) هوش مصنوعی^۱ جریان دارد. برای بررسی مسئله مذکور در نظام حقوقی ایران نیز با توجه به فقدان مقرره صریح در حقوق ایران، وجود شخصیت مستقل برای هوش‌های مصنوعی منتفی است چراکه شخصیت اعتباری است و قانونگذار با جعل شخصیت به آن رسمیت می‌دهد. بدین جهت در این مسئله، مبانی مسئولیت مالک و متصرف در خصوص مسئولیت ناشی از فعل اشیا مانند ماده (۳۳۴) قانون مدنی جریان دارد. به موجب این مبانی، مسئولیت نقض حقوق اشخاص موضوع داده با انجام پردازش از سوی هوش مصنوعی، برعهده مالک (اداره‌کننده) هوش مصنوعی است.

۲. جزای نقدی (ضمانت اجرای کیفری)

ضمانت اجرای دیگری که مقررات عمومی حفاظت از داده اتحادیه اروپا بدان تصریح کرده، جزای نقدی است. در این قسمت به چگونگی اعمال جزای نقدی به موجب این مقررات (۱-۲) و سپس بررسی این ضمانت اجرا در نظام حقوقی ایران پرداخته خواهد شد (۲-۲).

۲-۱. چگونگی اعمال جزای نقدی به موجب مقررات عمومی حفاظت از داده

اتحادیه اروپا

مراجع نظارتی حفاظت از داده اتحادیه اروپا، اختیارات تأدیبی (اصلاحی) متفاوتی دارند که می‌تواند در صورت نقض مقررات عمومی حفاظت از داده اتحادیه اروپا علیه کنترل‌کننده‌ها و پردازنده‌ها اعمال نمایند. یکی از این اختیارات، وضع جزای

1. Artificial Intelligence Manager

نقدی^۱ است. جزای نقدی مذکور از سوی دولت دریافت و برای منافع عمومی جامعه استفاده می‌شود (ماهیت مجازات کیفری دارد)^۲ (Afifi-Sabet, 2021). ماده (۸۳) این مقررات شرایط عمومی و میزان جزای نقدی را برای نقض این مقررات معین می‌کند. به موجب ماده (۸۳) بند «۴» برای تخلفات متفاوت جزای نقدی تا ۱۰ میلیون یورو یا در مورد سازمان‌های تجاری به میزان ۲٪ کل گردش مالی سالیانه جهانی در سال مالی گذشته، هر کدام که بیشتر باشد، مقرر شده است. همچنین تخلفات مهم‌تر نسبت به وضعیت اشخاص موضوع داده به موجب ماده (۸۳) بند «۵» مشمول جزای نقدی تا ۲۰ میلیون یورو یا در مورد سازمان‌های تجاری به میزان ۴٪ کل گردش مالی سالیانه جهانی در سال مالی گذشته، هر کدام که بیشتر باشد (EUR-Lex, 2016: 83).

میزان جزای نقدی برحسب مورد از سوی مراجع نظارتی تعیین خواهد شد. به موجب ماده (۸۳) بند «۱» این مقررات هر مرجع نظارتی باید اطمینان حاصل کند که اعمال جزای نقدی مؤثر، متناسب و منطقی در هر مورد خاص است. در مواردی که شخص باید جریمه شود، مراجع نظارتی باید سطح عمومی درآمد در کشور مربوطه عضو اتحادیه اروپا و نیز وضعیت اقتصادی شخص در لحاظ کردن مقدار مناسب جزای نقدی را در نظر گیرند (Hoofnagle et al., 2019: 93). همچنین هنگام تعیین میزان جزای نقدی، مراجع نظارتی باید عوامل مشدده یا مخففه مختلفی از جمله ماهیت، شدت و مدت تخلف با توجه به دامنه یا هدف پردازش، تعداد اشخاص آسیب‌دیده و میزان آسیب وارده به اشخاص؛ ماهیت عمدی بودن یا غیرعمدی بودن تخلف و

1. Administrative Fines: Administrative Penalty Means a Monetary Fine Imposed by the Division for Acts or Omissions Determined to Constitute Unprofessional or Unlawful Conduct in Accordance With a Fine Schedule Established by Rule and as a Result of an Adjudicative Proceeding Conducted in Accordance With Title 63G, Chapter 4, Administrative Procedures Act.

2. Criminal Penalty

هر اقدامی را لحاظ کند که کنترل کننده یا پردازنده برای کاهش آسیب به شخص موضوع داده انجام شده است (European Commission, n.d.-b).

۲-۲. بررسی جزای نقدی در نظام حقوقی ایران

برای بررسی ضمانت اجرای کیفری مذکور (جزای نقدی) در حقوق ایران، می‌توان به قوانین و مقررات مختلفی اشاره کرد که به مناسبت، به نقض حریم خصوصی اطلاعاتی و داده شخصی اشاره و برای آن جزای نقدی مقرر کرده‌اند. این موارد از قبیل مواد (۱)، (۳)، (۴)، (۸)، (۱۲) و (۱۷) قانون جرائم رایانه‌ای مصوب ۱۳۸۸؛ موادی از قانون مجازات اسلامی مصوب ۱۳۷۵ (تعزیرات و مجازات‌های بازدارنده) از قبیل ماده (۵۸۲) و (۶۴۸)؛ همچنین برخی مواد قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ مانند ماده (۶۶۰) است که جزای نقدی و میزان معینی برای آن مورد تصریح قرار گرفته است. در خصوص مواد پیش‌گفته چند نکته وجود دارد: اول اینکه دامنه شمول برخی از مواد محدود به افراد خاصی است و در مقابل برخی دیگر از مواد دامنه‌ای موسع دارند. به‌عنوان نمونه مخاطب ماده (۵۸۲) قانون مجازات اسلامی مصوب ۱۳۷۵^۱ همه اشخاصی است که در طیف حکومت مشغول به خدمت هستند و دامنه شمول این ماده از نظر شخصیت مرتکب، محدود است. بدین جهت مانع تعرض به داده‌های شخصی افراد از سوی غیرمستخدمان و مأموران دولتی نیست. این امر نسبت به ماده (۶۴۸) این قانون^۲ نیز وجود دارد.

۱. [جزای نقدی مقرر در ماده اصلاحی ۱۳۹۹/۱۱/۸] «هریک از مستخدمین و مأمورین دولتی، مراسلات یا مخابرات یا مکالمات تلفنی اشخاص را در غیر مواردی که قانون اجازه داده حسب مورد مفتوح یا توقیف یا معدوم یا بازرسی یا ضبط یا استراق سمع نماید یا بدون اجازه صاحبان آنها مطالب آنها را افشا نماید به حبس از یک سال تا سه سال و یا جزای نقدی از ۸۰,۰۰۰,۰۰۰ تا ۲۵۰,۰۰۰,۰۰۰ ریال محکوم خواهد شد».

۲. [جزای نقدی مقرر در ماده اصلاحی ۱۳۹۹/۱۱/۸] «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 چهل و پنج روز و دوازده ساعت تا شش ماه حبس و یا به ۲۰/۰۰۰/۰۰۰ تا ۶۰/۰۰۰/۰۰۰ ریال جزای نقدی محکوم می‌شوند».

شمول این ماده تنها نسبت به افرادی است که نوع شغل یا حرفه آنان موجب دسترسی به اسرار مردم - در بحث حاضر داده‌های شخصی^۱ - است، همچنین این افراد باید به مناسبت شغل و حرفه خود به اسرار دیگران آگاه باشند و به موجب قانون افشا نکنند (میرمحمد صادقی، ۱۳۹۲: ۵۳۸). در مقابل برخی مواد دیگر مانند مواد مربوطه از قانون جرائم رایانه‌ای^۲ صرف نظر از شخصیت مرتکب جرم‌انگاری کرده‌اند و در حمایت از داده‌های شخصی دامنه موسعی دارند (آقایی‌نیا، ۱۳۹۹: ۲۷۳-۲۷۱). نکته دیگر اینکه گرچه جزای نقدی مصرح در این مواد وجود دارد؛ اما از آنجایی که موضوع قوانین مذکور، خاص داده شخصی نیست، جریان مفاد مواد مربوطه نسبت به انواع پردازش داده شخصی با اشکال مواجه است. به عنوان نمونه قانون جرائم رایانه‌ای گرچه برای حالات مختلف نقض داده‌ها، جزای نقدی و ضمانت اجرا مقرر کرده است؛ لیکن به دلیل محدودیت دامنه این قانون در بستر موضوعی خود، اعمال آن نسبت به تمامی مصادیق پردازش داده‌های شخصی ممکن نیست. همچنین گفتنی است مواد پیش گفته علاوه بر جزای نقدی به مجازات حبس نیز اشاره کرده‌اند، در برخی مواد قانونی دیگر مانند ماده (۷۱) قانون تجارت الکترونیکی مصوب ۱۳۸۲ نیز صرفاً مجازات حبس برای نقض حریم خصوصی اطلاعاتی و داده‌های شخصی مقرر شده است. در مقابل به موجب حقوق اتحادیه اروپا وضع مجازات حبس به موجب اختیاری

۱. در خصوص سر تعلق شدن داده‌های شخصی می‌توان گفت، سر امری نسبی است و مصادیق آن با توجه به شرایط افراد و انگیزه آنها در پنهان کردن امری متفاوت می‌شود (قماش، ۱۳۸۵: ۴). از سوی دیگر 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 واقع 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 ایجاد نشدن بستری برای سوءاستفاده است. با توجه به آنچه بیان شد، در بسیاری از موارد می‌توان داده‌های شخصی را به نوعی سر دانست.

۲. از جمله ماده (۱) این قانون که به موجب آن [جزای نقدی مقرر در ماده اصلاحی ۱۳۹۹/۱۱/۸] «هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نودویک روز تا یک سال یا جزای نقدی از بیست میلیون (۲۰,۰۰۰,۰۰۰) ریال تا هشتاد میلیون (۸۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد».

است که در ماده (۸۴) مقررات عمومی حفاظت از داده اتحادیه اروپا به کشورهای عضو اتحادیه اعطا شده است. بدین جهت این مجازات در برخی از کشورهای عضو مانند آلمان نسبت به نقض حق بر داده در قوانین ملی وضع شده است و صراحتی در مقررات اروپایی حفاظت از داده در این خصوص وجود ندارد (Etteldorf, 2018: 374).

فارغ از مواد مذکور که به ضمانت اجرای کیفری (اعم از جزای نقدی و حبس) برای نقض حق بر داده‌های شخصی، به صورت موردی - در ضمن قوانین و مقررات مختلفی که به طور خاص برای حفاظت از داده شخصی تدوین نشده است - اشاره کرده‌اند؛ تصریح قانونگذار در خصوص این مسئله بسیار ضروری است. این ضرورت از آنجاست که برای تحقق جرم و جریان ضمانت اجرای کیفری عناصر سه‌گانه‌ای لازم است - رکن قانونی، مادی و روانی - که قانونی بودن مهم‌ترین رکن در تشکیل وصف کیفری است. به دلیل چنین اهمیتی، ارتباط آن با دو عنصر دیگر به صورت هم‌عرض و موازی نیست؛ بلکه مقدم و طولی است و برای تحقق جرم، تعیین عنوان مجرمانه از سوی قانونگذار بسیار مهم است (خبازی خادر و حسینی، ۱۳۹۹: ۳۰۱-۳۰۰).

در واقع عنصر قانونی بودن از سویی بر تعیین جرائم و از سوی دیگر بر تثبیت مجازات‌ها و کمیت آنها نظر دارد (اردبیلی، ۱۳۹۴، ج ۱: ۲۰۴).

همچنین پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» نیز در مواد ۶۵ الی ۷۰ به ضمانت اجرای کیفری اشاره کرده است - این امر از مواد ۵۰ الی ۵۲ طرح «حمایت و حفاظت از داده و اطلاعات شخصی» قابل دسترسی است. البته طرح در بخش مسئولیت‌ها و ضمانت اجراها مانند پیش‌نویس عمل نکرده که به صورت مجزا به ضمانت اجرای کیفری، مدنی و انتظامی اشاره کرده است و این به عنوان نقص طرح قابل اشاره است. لیکن در خصوص مواد مذکور دو نقد وجود دارد: اول اینکه مجازات در مفاد مذکور، معادل درجات مختلف تعزیرات قانون مجازات اسلامی لحاظ شده

۳۶۷ _____ بررسی تطبیقی ضمانت اجرای نقض حق بر داده در حقوق اتحادیه اروپا ...

است. گرچه مبالغ جزای نقدی تعزیرات قانون مجازات اسلامی به استناد ماده (۲۸) قانون مجازات اسلامی در تاریخ ۱۳۹۹/۱۱/۸ افزایش یافته است و به نظر می‌رسد تا حد زیادی جزای نقدی تعدیل شده است؛ اما بهتر است که مانند ماده (۸۳) مقررات عمومی حفاظت از داده اتحادیه اروپا به مجازات نقض حق بر داده شخصی، در خود بستر قانونی به‌طور خاص اشاره شود، به‌عنوان نمونه مبلغی معین شود که متناسب با تورم جامعه کافی باشد - البته ذکر مبلغ معین باید همراه با تعدیل متناسب با تورم باشد تا جنبه بازدارندگی حفظ شود - یا جزای نقدی براساس و به میزان ضرر وارده به شخص موضوع داده در جهت جبران هرچه بهتر خسارت و برگرداندن زیان دیده به حالت قبل از نقض داده، تعیین شود. این امر در ماده (۱) قانون تشدید مجازات مرتکبان ارتشا، اختلاس و کلاهبرداری مصوب ۱۳۶۷ مورد توجه قرار گرفته است.

نقد دوم نیز در خصوص مصادیقی است که مشمول ضمانت اجرای کیفری است که عمدتاً کلی است، مانند بند «پ» ماده (۶۸) پیش‌نویس (بند «پ» ماده (۵۱) طرح «حمایت و حفاظت از داده و اطلاعات شخصی») که بیان می‌کند «نقض تعهدات اعتبارپذیری، اعتمادپذیری یا استنادپذیر پردازش داده‌های شخصی، به یک یا هر دو مجازات درجه ۵» محکومیت دارد. به نظر می‌رسد مناسب‌تر این است که به نقض هریک از حقوق اشخاص موضوع داده یا اصول حاکم بر پردازش یا تکلیف اشخاص پردازش‌کننده داده به‌طور خاص اشاره شود و برای آنها مجازات لحاظ شود؛ زیرا با کلی بودن مصادیق ضمانت اجرای کیفری، هر تخلفی ممکن است مشمول ضمانت اجرای کیفری شود و از سوی دیگر به‌موجب اصل تفسیر مضیق به نفع متهم، متخلف از جزای کیفری معاف است. بدین جهت اگر قانونگذار در مقام بیان به‌طور خاص و جزئی به مصادیقی اشاره کند که مشمول ضمانت اجرای کیفری است، موجب رفع ابهام در رویه قضایی و عمل است. در مقابل رویکرد این اسناد (دو نقد

یادشده) می‌توان به پیش‌نویس طرح قانون «حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی» مورخ ۱۴۰۰/۴/۲۶ اشاره کرد. ماده (۲۷) این سند انواع تخلفات نسبت به تعهدات و تکالیف را مشخص کرده است، همچنین به موجب ماده (۲۸) چگونگی مجازات در خصوص تخلفات در خود سند مذکور مقرر شده است. این موارد می‌تواند گامی مثبت در جهت حمایت مناسب از اشخاص موضوع داده تلقی شود؛ بنابراین در خصوص اسناد مشابه پیشنهاد می‌شود.

۳. جمع‌بندی و نتیجه‌گیری

نقض حق بر داده شخصی، تجاوز به حقوق بشر و حقوق شهروندی اشخاص حقیقی است. بدین جهت باید برای این نقض، ضمانت‌اجراهای مختلفی وجود داشته باشد تا حمایت کامل از داده‌های شخصی حاصل شود. یکی از نظام‌های حقوقی که از عهده این مهم به خوبی برآمده است، اتحادیه اروپاست که با تصریح بر ضمانت‌اجراهای مختلف نسبت به نقض حق مذکور، بر حمایت جامع از داده‌های شخصی جامه عمل پوشانیده است. در این پژوهش ضمانت‌های مصرح در مقررات اروپایی حفاظت از داده تبیین شد و جریان آنها در نظام حقوق ایران به صورت تطبیقی مورد بررسی قرار گرفت و مشخص شد که به موجب حقوق اتحادیه اروپا، یکی از ضمانت‌اجراهای موجود، حق جبران خسارت است. این حق در دو وضعیت مورد توجه قرار گرفت؛ از یک سو در صورتی که پردازش را هوش انسانی انجام دهد و از سوی دیگر در زمانی که پردازش را هوش‌های مصنوعی و ماشین‌ها انجام می‌دهند. در صورتی که پردازش از سوی هوش انسانی باشد، حق جبران خسارت مقرر در ماده (۸۲) مقررات عمومی حفاظت از داده اتحادیه اروپا جریان دارد.

ماده (۸۲) جنبه‌های مختلفی را در خصوص جبران خسارت مورد توجه قرار داده

است تا از جبران خسارت مؤثر نسبت به شخص موضوع داده اطمینان حاصل شود. از سوی دیگر، در نظام حقوقی ایران نیز حق جبران خسارت به عنوان یکی از آثار مسئولیت مدنی در صورت نقض حق بر داده از طرف هوش انسانی مورد پذیرش است. همچنین مستنبط از منابع گوناگون جنبه های مختلف این حق در حقوق ایران قابل جریان است - همان طور که در مقررات اروپایی حفاظت از داده وجود دارد. با تبیین چگونگی وجود جبران خسارت در صورت پردازش با هوش انسانی، این امر در صورتی که هوش مصنوعی پردازش را انجام دهد، مورد بررسی قرار گرفت. در این خصوص مشخص شد که اتحادیه اروپا در مقام عمل، جبران خسارت را برعهده مالک (اداره کننده) هوش مصنوعی می داند، چنین مسئولیتی به جهت حفاظت مؤثر از منافع و حقوق افراد است. گفتنی است در حقوق ایران نیز به دلیل عدم ورود قانونگذار به مسئله امکان یا عدم امکان اعطای شخصیت به هوش های مصنوعی، وجود شخصیت مستقل برای هوش های مصنوعی منتفی است. بدین جهت به موجب حقوق موضوعه و مبانی حقوق ایران مسئولیت نقض حقوق اشخاص موضوع داده با وجود هوش مصنوعی، برعهده مالک (اداره کننده) هوش مصنوعی است.

ضمانت اجرای دیگر از نگاه مقررات عمومی حفاظت از داده اتحادیه اروپا، جزای نقدی است. به موجب مواد مربوطه یکی از اختیارات مراجع نظارتی وضع جزای نقدی است که ماهیت مجازات کیفری دارد. در ماده (۸۳) بندهای «۴» و «۵» این مقررات برای تخلفات گوناگون، به ترتیب جریمه نقدی بیست میلیون و ده میلیون یورو مقرر شده است. با تبیین چگونگی اعمال جزای نقدی در مقررات اروپایی، وجود این ضمانت اجرا در حقوق ایران جستجو شد. در این راستا گرچه قوانین و مقررات مختلفی وجود دارد که به نقض حریم خصوصی اطلاعاتی و داده شخصی اشاره کرده اند و برای این امر جزای نقدی مقرر کرده اند - بدین دلیل که حقوق ایران، قانونی

مستقل و بالتبع ضمانت اجراهایی ویژه برای نقض حق بر داده شخصی ندارد. اما از آنجایی که موضوع قوانین و مقررات مذکور، خاص داده شخصی نیست؛ جریان مفاد قانونی آنها، نسبت به انواع پردازش داده شخصی با اشکال مواجه است. در واقع مفاد مواد مربوطه نمی‌توانند نسبت به حمایت از داده‌های شخصی جامع باشند. بدین جهت تصریح قانونگذار در خصوص ضمانت اجرای کیفی بسیار ضروری است. همچنین از قانونگذار انتظار می‌رود با تصریح بر سایر ضمانت‌های اجراهی لازم در خصوص نقض حق مذکور، در مسیر حمایت کامل از اشخاص موضوع داده و تقویت حقوق بشر و حقوق شهروندی افراد، گام بردارد.



منابع و مأخذ

۱. آقای نیا، حسین (۱۳۹۹). حقوق کیفری اختصاصی، جرائم علیه اشخاص (شخصیت معنوی)، چاپ هفتم، تهران، نشر میزان.
۲. اردبیلی، محمدعلی (۱۳۹۴). حقوق جزای عمومی، تهران، نشر میزان.
۳. پیش‌نویس طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی ۱۴۰۰.
۴. پیش‌نویس لایحه صیانت و حفاظت از داده‌های شخصی منتشر شده در تیرماه ۱۳۹۷.
۵. خبازی خادر، سیده‌طاهره و سیدحسین حسینی (۱۳۹۹). «تبیین مدل توصیف کیفری اختصاصی: با نگاهی به بند «الف» ماده (۱) قانون مجازات اخلاص گران در نظام اقتصادی»، پژوهش‌های حقوقی، ۱۹ (۴۲).
۶. صفایی، سیدحسین و حبیب‌اله رحیمی (۱۳۹۷). مسئولیت مدنی تطبیقی، تهران، مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش.
۷. _____ (۱۳۹۸). مسئولیت مدنی (الزامات خارج از قرارداد)، چاپ دوازدهم، تهران، انتشارات سمت.
۸. عراقی، سیدعزت‌اله (۱۳۸۹). حقوق کار، چاپ یازدهم، تهران، انتشارات سمت.
۹. قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳.
۱۰. قانون آیین دادرسی کیفری مصوب ۱۳۹۲ با اصلاحات ۱۳۹۴.
۱۱. قانون آیین دادرسی مدنی مصوب ۱۳۷۹.
۱۲. قانون تجارت الکترونیکی مصوب ۱۳۸۲.
۱۳. قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری مصوب ۱۳۶۷.
۱۴. قانون جرائم رایانه‌ای مصوب ۱۳۸۸.
۱۵. قانون صلاحیت دادگستری جمهوری اسلامی ایران برای رسیدگی به دعاوی مدنی علیه دولت‌های خارجی مصوب ۱۳۹۰.
۱۶. قانون مجازات اسلامی مصوب ۱۳۷۵ و ۱۳۹۲.

۱۷. قماشی، سعید (۱۳۸۵). «بررسی جرم افشای اسرار حرفه‌ای»، مجله دادرسی، ش ۵۸.
۱۸. کاتوزیان، ناصر (۱۳۹۴). *الزام‌های خارج از قرارداد «مسئولیت‌های خاص و مختلط»*، چاپ دوازدهم، تهران، انتشارات دانشگاه تهران.
۱۹. _____ (۱۳۹۵). *الزام‌های خارج از قرارداد «قواعد عمومی»*، چاپ چهاردهم، تهران، انتشارات دانشگاه تهران.
۲۰. محقق داماد، مصطفی (۱۳۸۴). *قواعد فقه (بخش مدنی - مالکیت و مسئولیت)*، تهران، مرکز نشر علوم اسلامی.
۲۱. موسوی بجنوردی، محمد (۱۳۷۹). *قواعد فقهیه*، تهران، مؤسسه تنظیم و نشر آثار امام خمینی (ره)، مؤسسه چاپ و نشر عروج.
۲۲. میرمحمد صادقی، حسین (۱۳۹۲). *حقوق کیفری اختصاصی، جرائم علیه اشخاص*، چاپ یازدهم، تهران، نشر میزان.
۲۳. نراقی، احمدبن محمد مهدی (۱۳۸۰). *رسائل و مسائل، گردآورنده رضا استادی، قم، کنگره بزرگداشت محققان ملامهدی و ملااحمد نراقی*.
۲۴. یزدانیان، علیرضا (۱۳۹۵). *قواعد عمومی مسئولیت مدنی*، تهران، نشر میزان.
25. Afifi-Sabet, K. (2021). "GDPR Fines: Where does the Money Go?", <https://www.itpro.co.uk/general-data-protection-regulation-gdpr/who-benefits-from-gdpr-fines>
26. Andrade, F., P. Novais, J. MacHado and J. Neves (2007). "Contracting Agents: Legal Personality and Representation", *Artificial Intelligence and Law*, 15(4).
27. Bredin, P. and J. Riordan (2017). *GDPR: Judicial Remedies*.
28. Centre for Information Policy Leadership (CIPL) (2020). *Artificial Intelligence and Data Protection How the GDPR Regulates AI*.
29. Čerka, P., J. Grigienė and G. Sirbikytė (2017). "Is it Possible to Grant Legal Personality to Artificial Intelligence Software Systems?", *Computer Law and Security Review*, 33(5).

30. Council of Europe (1950). “European Convention on Human Rights”, In Vertical Judicial Dialogues in Asylum Cases, https://www.echr.coe.int/Documents/Convention_ENG.pdf
31. CURIA (2015). “María Auxiliadora Arjona Camacho v Securitas Seguridad España SA”, In Case C-407/14 (Issue December).
32. Etteldorf, C. (2018). “About Dashcams und Digital Estate - German Federal Court of Justice Weighs Up Data Protection Interests”, In *European Data Protection Law Review*, Vol. 4, Issue 3.
33. EUR-Lex (2012). “Charter of Fundamental Rights of the European Union (2012/C 326/02)”, *Official Journal of the European Union*, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>
34. 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*, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
35. European Commission (n.d.-a). *Can I Claim Compensation?*, Retrieved March 10, 2020, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/redress/can-i-claim-compensation_en
36. _____ (n.d.-b). *Questions and Answers – General Data Protection Regulation*, Retrieved February 13, 2020, from https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387
37. _____ (2018). “What is a Data Controller or a Data Processor?”, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en
38. European Data Protection Supervisor (n.d.). *Data Protection*. Retrieved June 17, 2020, from https://edps.europa.eu/data-protection/data-protection_en

39. European Law Blog (n.d.). Refusing to Award Legal Personality to AI: Why the European Parliament Got it Wrong – European Law Blog, Retrieved June 20, 2021, from <https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong/>
40. European Parliament (2015). Draft Report With Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).
41. European Parliamentary Research Service (2020). The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, In Panel for the Future of Science and Technology (STOA).
42. Hoofnagle, C.J., B. Van der Sloot and F.Z. Borgesius (2019). “The European Union General Data Protection Regulation: What it is and what it Means”, *Information and Communications Technology Law*, 28(1).
43. ICO. (n.d.-a). Taking your Case to Court and Claiming Compensation, Retrieved August 24, 2020, from <https://ico.org.uk/your-data-matters/data-protection-and-journalism/taking-your-case-to-court-and-claiming-compensation/>
44. _____ (n.d.-b). What is Criminal Offence Data?, Retrieved August 9, 2021, from <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/>
45. Ungureanu, C.T. (2018). “Legal Remedies for Personal Data Protection in European Union”, *Logos Universality Mentality Education Novelty: Law*, 6(2).
46. United Nations (2015). Universal Declaration of Human Rights , https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
47. Voigt, P. and A. Von Dem Bussche (2017). *The EU General Data Protection Regulation (GDPR)*, Springer International Publishing.