Quarterly Journal of Government and Law,
Vol. 5, No. 1 (Serial 15), Spring 2024

Research Paper

Artificial Intelligence and the Challenges of Personal Data Protection Rules with a Control Approach; Alternative Legal Regime

Seyed Ali Hosseini*

Abstract

Artificial intelligence is built on technologies such as machine learning and deep learning neural networks, whose performance relies on a vast amount of high-quality data. Personal data is an indispensable resource for the development of artificial intelligence and the improvement of the efficiency of AI algorithms. Personal data is attributed to individuals and part of an individual's rights and obligations in the analog space can, depending on the case, have a close connection with its proper processing, which ensures the benefits for the data subject and prevents harm against them. Before the advent of artificial intelligence, the volume of personal data processing was relatively small and limited compared to AI; thus, the General Data Protection Regulations (2016) has mandated duties for each instance of personal data processing for the controller and has also determined rights for the data subject regarding each instance of personal data processing. However, considering the technical nature of artificial intelligence, the application of these rules to the algorithmic processing of personal data is fraught with difficulties. This article examines the challenges of the GDPR in protecting personal data under the processing of AI systems and analyzes legislative solutions for protecting personal data in the field of artificial intelligence. The major question of this article is, what is the legislative solution to overcome the challenge of personal data protection in algorithmic processes? This research is conducted using a descriptive-analytical method.

Keywords

Artificial Intelligence, Personal Data, GDPR, Fundamental Rights, Data Processing.

* PhD Candidate, Public Law, Imam Sadiq University, Tehran, Iran.
seyedalyhoseini@isu.ac.ir

Received: 2024/04/04 Accepted: 2024/06/19

فصلنامه «حقوق و دولت»، سال پنجم، شماره اول (پیاپی ۱۵)، بهار ۱۴۰۳، صص. ۱۲۲-۹۹

حقوق حفاظت از داده‌های شخصی در پردازش الگوریتمی، چالش‌ها و راهکارها

سیدعلی حسینی*

نوع مقاله: علمی- پژوهشی

چکیده

هوش مصنوعی بر فناوری‌هایی مانند یادگیری ماشین و شبکه‌های عصبی یادگیری عمیق بنا شده است که عملکرد هریک از آن‌ها وابسته به حجم عظیمی از داده‌های باکیفیت است. داده‌های شخصی منبعی اجتناب‌ناپذیر برای توسعه هوش مصنوعی و بهبود کارایی الگوریتم‌های هوش مصنوعی است. داده‌های شخصی منتسب به اشخاص است و بخشی از حقوق و تکالیف شخص در فضای آنالوگ، حسب مورد می‌تواند ارتباط وثیقی با پردازش صحیح آن داشته باشد که منافع شخص موضوع داده را تأمین کند و آسیبی علیه وی ایجاد نکند. پیش از ظهور هوش مصنوعی حجم پردازش داده‌های شخصی به نسبت هوش مصنوعی بسیار کم و محدود بود؛ به‌گونه‌ای که مقررات عمومی حفاظت از داده‌های شخصی اتحادیه اروپا (۲۰۱۶)، تکالیفی را برای هر مورد از پردازش داده‌های شخصی برای کنترلگر الزام کرده و نیز حقوقی را برای پردازش هریک از داده‌های شخصی برای شخص موضوع داده پیش‌بینی کرده است (رویکرد کنترلی)، اما با در نظرگرفتن ماهیت فنی هوش مصنوعی، امکان اعمال قواعد کنترلی بر پردازش الگوریتمی داده‌های شخصی با مشکلاتی همراه است. در این مقاله ضمن بررسی چالش‌های مقررات عمومی حفاظت از داده‌های شخصی در حفاظت از داده‌های شخصی (به‌عنوان مشهورترین نماینده این رویکرد) تحت پردازش سامانه‌های هوش مصنوعی، راهکار تقنینی حفاظت از داده شخصی در حوزه هوش مصنوعی مورد تحلیل قرار می‌گیرد. پرسش اصلی مقاله حاضر این است که قانون‌گذاری حفاظت از داده شخصی در پردازش الگوریتمی با چه چالش‌هایی مواجه است و رژیم حقوقی جایگزین برای حل این چالش‌ها چیست؟ این پژوهش به روش توصیفی- تحلیلی انجام شده است.

واژگان کلیدی

هوش مصنوعی، داده شخصی، مقررات عمومی حفاظت از داده‌های شخصی، حقوق اساسی، پردازش داده.

* دانشجوی دکتری حقوق عمومی، دانشگاه امام‌صادق علیه‌السلام، تهران، ایران. seyedalyhoseini@isu.ac.ir

تاریخ دریافت: ۱۴۰۳/۰۱/۱۵ تاریخ پذیرش: ۱۴۰۳/۰۳/۳۰

مقدمه

سیستم‌های هوش مصنوعی نیاز به تغذیه با حجم زیادی از داده‌ها دارند تا به‌درستی آموزش ببینند و نتایج دقیقی تولید کنند. اساساً داده به‌عنوان سوخت اقتصاد دیجیتال شناخته می‌شود و عدم دسترسی شرکت‌های فعال فناوری اطلاعات به آن، رشد و توسعه آنان را غیرممکن می‌سازد. این واقعیت که برخی از این داده‌ها شامل داده‌های شخصی هستند و بسیاری از سیستم‌های هوش مصنوعی دارای ویژگی‌هایی مانند مشکل جعبه سیاه هستند، نگرانی‌هایی را در مورد حفاظت از حقوق و آزادی‌های مشروع و اساسی هنگام استفاده از چنین سیستم‌هایی به وجود می‌آورد. در این زمینه، قانون باید بتواند از اشخاص در برابر آثار سوء هوش مصنوعی بر داده‌های شخصی محافظت کند و درعین‌حال، مانعی برای توسعه فناوری هوش مصنوعی نباشد.

در سال‌های اخیر، کشورهایی مانند آمریکا و چین به دلیل سیاست‌های داده باز، رشد معناداری را در حوزه اقتصاد دیجیتال و ازجمله هوش مصنوعی کسب کردند؛ به‌طوری‌که سهم اقتصاد دیجیتال آمریکا فاصله زیادی با دیگر کشورها و حتی کل کشورهای اتحادیه اروپا دارد (Bureau of Economic Analysis, 2022). این موضوع سبب شد که در سال‌های اخیر اتحادیه اروپا نیز به‌منظور جبران عقب‌ماندگی‌های خود، قوانینی مانند داده باز[1] و حکمرانی داده[2] را به‌منظور تسهیل دسترسی شرکت‌های اروپایی حوزه فناوری اطلاعات به داده‌ها به تصویب برساند، اما به نظر برخی صاحب‌نظران، یکی از علل زمینه‌ای عقب‌ماندگی اتحادیه اروپا در این رقابت جهانی، قوانین سخت‌گیرانه‌ای است که به‌عنوان مانعی برای جریان اطلاعات و استفاده مجدد از داده‌ها توسط پلتفرم‌های اروپایی در مقررات عمومی حفاظت از داده شخصی اتحادیه اروپا[3] وضع شده است (Ciriani, 2015: 45-48).

جمهوری اسلامی ایران در آستانه قانون‌گذاری در دو حوزه حمایت از داده‌های شخصی و هوش مصنوعی است. دور از انتظار نیست که مقررات عمومی حفاظت از داده شخصی اروپا به‌عنوان سندی تفصیلی و دارای استحکام شکلی قانونی، به‌عنوان مهم‌ترین الگو برای قانون‌گذاری در حوزه حمایت از داده‌های شخصی، مورد توجه کارشناسان و قانون‌گذاران کشور قرار گیرد، اما مقررات عمومی حفاظت از داده شخصی دارای نقایص و تعارضاتی با پیشرفت فناوری هوش مصنوعی است. به همین دلیل، در این تحقیق مقررات عمومی حفاظت از داده شخصی به‌عنوان الگوی غالب قانون‌گذاری و نماینده اصلی رویکرد کنترل فردی در قانون‌گذاری حفاظت از

1- EU, 2019: 1024 (Open Data and the Re-use of Public Sector Information)
2- EU, 2018: 1724 (Data Governance Act)
3- General Data Protection Regulation (GDPR)

داده‌های شخصی، مورد نقد و تحلیل قرار گرفته است. هدف از نگارش این مقاله واکاوی و تبیین ضعف‌ها و تعارضات چنین رویکرد قانون‌گذاری در حوزه حمایت از داده شخصی و ارائه راهکار پیشنهادی جایگزین منطبق با ویژگی‌های فنی رادیکال هوش مصنوعی است. برایندهای این تحقیق دیدگاه جامع‌تری را برای قانون‌گذاری در حوزه حمایت از داده شخصی ایجاد می‌کند تا ملاحظات فناورانه هوش مصنوعی را نیز تأمین کند.

پرسش اصلی تحقیق حاضر این است که راه‌حل تقنینی برون‌رفت از چالش حفاظت از داده‌های شخصی در پردازش‌های الگوریتمی چیست؟ برای پاسخ به این پرسش، نگارنده بخشی از این مقاله را به نقد سند مقررات عمومی حفاظت از داده شخصی اروپا اختصاص داده است تا فرضیه بی‌نقص بودن، خنثی بودن و انعطاف‌پذیری آن را در مقابل فناوری هوش مصنوعی به چالش بکشد. براین‌اساس، یکی از پرسش‌های فرعی این مقاله شکل می‌گیرد که قواعد کنترلی حفاظت از داده شخصی (در سطح مقررات عمومی حفاظت از داده شخصی) تا چه اندازه قابلیت تنظیم و حفاظت از پردازش داده‌های شخصی را در پردازش‌های الگوریتمی دارد؟ ضمن بررسی اجمالی اهم مفاهیم به‌کاررفته در این تحقیق در بخش نخست، پرسش اخیر در قالب بخش‌های دوم و سوم این مقاله به‌تفصیل بررسی شده است و ضمن بررسی ماهیت قاعده‌گریز هوش مصنوعی در حوزه داده، چالش‌های مقررات عمومی حفاظت از داده شخصی برای حفاظت از داده‌های شخصی در پردازش‌های الگوریتمی در سطح مبانی و اصول آن مورد ارزیابی قرار می‌گیرد. پرسش فرعی دیگر میزان انطباق تجویزهای احکام مقررات عمومی حفاظت از داده شخصی با برخی اصول کیفی و ماهوی قانون‌گذاری است. این موضوع در بخش چهارم مورد بررسی قرارگرفته است. درنهایت، راهکار تقنینی برای حفاظت از داده شخصی در پردازش‌های هوش مصنوعی در بخش پنجم ارائه شده است.

۱- مفاهیم

در ابتدا به دلیل جنبه‌های تطبیقی و فنی تحقیق حاضر، لازم است برخی مفاهیم به‌کاررفته در این سند را به‌اختصار توضیح دهیم.

۱-۱- هوش مصنوعی

در اصطلاح رایج، هوش مصنوعی «به طراحی سیستم‌های رایانه‌ای هوشمند» یا «به خودکارسازی رفتار هوشمند» می‌پردازد. ایده اولیه هوش مصنوعی توانمندسازی سیستم‌های رایانه‌ای برای شبیه‌سازی عملکرد مغز انسان و مدیریت هر وظیفه شناختی عمومی در هر شرایطی (هوش مصنوعی تقلیدکننده انسان) است (Meurisch & Mühlhäuser, 2021: 4). در سال‌های اخیر

تعاریف متعددی از هوش مصنوعی ارائه شده است که هریک بر جنبه‌ای از آن تأکید دارند (Kerrigan, 2022). یکی از مهم‌ترین و آخرین تعاریفی که از هوش مصنوعی ارائه شده است، مربوط به «قانون هوش مصنوعی اتحادیه اروپا»[1] می‌شود (مصوب ۱۳ مارس ۲۰۲۴). ماده ۱ قانون هوش مصنوعی اتحادیه اروپا «هوش مصنوعی» را این‌گونه تعریف می‌کند «سیستم هوش مصنوعی به معنای سیستمی مبتنی بر ماشین است که طراحی شده است تا دارای سطوحی از استقلال[2] باشد. سیستم ممکن است پس از به‌کارگیری دارای سازوکار خودتطبیقی[3] باشد و در راستای اهداف صریح یا ضمنی خود از ورودی‌هایی که دریافت می‌کند، نتیجه‌گیری کند و خروجی‌هایی مانند پیش‌بینی‌ها، محتوا، توصیه‌ها یا تصمیماتی را تولید کند که می‌توانند بر محیط‌های فیزیکی یا مجازی تأثیر بگذارند» (COM/2021/206 final). این تعریف بر جنبه‌هایی از هوش مصنوعی مانند استقلال و سازوکار خودتطبیقی تأکید دارد که در بخش‌های آتی بدان پرداخته می‌شود.

۲-۱- داده شخصی

داده شخصی به علت انتساب آن به یک شخص، ممکن است موضوع نقض و تعرض به حقوق و آزادی‌های فردی قرار گیرد. ازاین‌رو در اغلب کشورهای جهان قوانین خاصی درباره داده‌های شخصی تصویب شده که عمدتاً موضوع‌های منتسب به اشخاص حقیقی است (انصاری، ۱۴۰۰: ۹۰). در نظام حقوقی ایران، تاکنون قانونی به‌طور اختصاصی برای حمایت از داده‌های شخصی مانند مقررات حفاظت از داده شخصی اروپا (۲۰۱۶) و قانون حمایت از داده انگلستان (۲۰۱۸)، به تصویب نرسیده است، اما در میان قوانین مصوب مجلس به‌صورت پراکنده قواعدی دراین‌خصوص یافت می‌شود. داده شخصی در بند ر ماده ۱ قانون تجارت الکترونیکی ایران (مصوب ۱۳۸۲) چنین تعریف شده است «داده پیام‌های شخصی»[4] یعنی «داده پیام»های مربوط به یک شخص حقیقی (موضوع داده)[5] مشخص و معین. همچنین، در بند ب ماده ۱ قانون انتشار و دسترسی آزاد به اطلاعات (مصوب ۱۳۸۷) «اطلاعات شخصی» چنین تعریف شده است «اطلاعات شخصی: اطلاعات فردی مانند نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است». این تعریف به دلیل اینکه تنها به احصای مصادیق داده شخصی پرداخته است و معیاری برای تفکیک داده شخصی از دیگر انواع داده مانند داده‌های عمومی ارائه نمی‌دهد، دارای ضعف است

1- Artificial Intelligence Act
2- Autonomy
3- Adaptiveness
4. Private Data
5. Data Subject

(انصاری، ۱۴۰۰: ۹۱).

بند ۱ ماده ۴ مقررات حفاظت از داده شخصی اروپا، داده شخصی را این‌گونه تعریف کرده است «هر نوع اطلاعات مربوط به شخص حقیقی با هویت مشخص یا قابل شناسایی». در ادامه این بند، شخص قابل شناسایی نیز تعریف شده و مراد از آن شخصی قلمداد شدن هرگونه اطلاعاتی است که به‌صورت مستقیم مربوط به شخصی با هویت مشخص نباشد، اما با ارجاع داده به برخی دیگر از شناسه‌ها، قابلیت شناسایی شخص موضوع داده را امکان‌پذیر سازد (EU, 2016: 679).

۳-۱- حق‌های اساسی

حق‌های اساسی[1] یا بنیادین به دنبال همان ایده حقوق بشری مبنی بر حفاظت از ارزش‌های والای انسانی مانند کرامت، آزادی و عدالت در برابر تعدیات و تعرضات دولت‌ها شکل گرفت. بنیادین بودن برخی حقوق به‌خاطر این است که وجود آن مایه قوام و نبود آن موجب زوال شخص یا شخصیت انسان می‌شود (گرجی، ۱۳۸۳: ۹). حق‌های اساسی این تفاوت را با حق‌های بشری دارند که تضامین مؤثری برای حفاظت از آن‌ها در قالب نهادهای دادرسی اساسی کشورها ایجاد شده است و معمولاً توسط قانون اساسی یا اسنادی که به لحاظ جایگاه حقوقی بالاتر از قوانین موضوعه کشورهاست، تضمین می‌شوند (Gentili, 2020: 516). اتحادیه اروپا در منشور حقوق بنیادی[2] مجموعه‌ای از حق‌هایی را پیش‌بینی کرده است که از اصول انسانی مانند آزادی و امنیت، حریم خصوصی، منع تبعیض، ممنوعیت تفتیش عقیده و آزادی بیان و ... حمایت می‌کند و از طریق دیوان دادگستری اروپایی[3] بر اجرای این اصول توسط دولت‌های عضو نظارت می‌کند. ماده ۸ منشور حقوق بنیادی اروپا، حق حفاظت از داده شخصی را به‌عنوان حقی اساسی به رسمیت شناخته است. ماده ۸ ضمن تعریف داده شخصی، تأکید کرده است که این‌گونه داده‌ها باید به‌طور منصفانه و برای اهداف مشخص و بر اساس رضایت شخص مربوط یا هر مبنای قانونی دیگری که توسط قانون تعیین شده است، پردازش شوند. منشور همچنین، حق دسترسی شخص موضوع داده به داده‌های شخصی وی و اصلاح آن‌ها را شناسایی کرده است (European Union, 2012: 8).

۴-۱- مقررات عمومی حفاظت از داده‌های شخصی

قانون‌گذاری اتحادیه اروپا در حوزه حفاظت از داده‌های شخصی ریشه در اسناد و معاهدات حقوق بشری و بنیادین اتحادیه اروپا دارد که پیش از این بیان شد. نخستین‌بار اتحادیه اروپا در

1- Fundamental Rights
2- Charter of Fundamental Rights of the European Union
3- European Court of Justice (ECJ)

دستورالعمل حفاظت از داده شخصی در سال ۱۹۹۵، قواعدی را برای یکپارچه‌سازی قوانین ملی کشورهای عضو در حوزه حمایت از داده‌های شخصی به تصویب رساند (Directive 95/46/EC)، اما ازآنجاکه این مصوبه در قالب «دستورالعمل»[1] به تصویب رسید، توفیق چندانی در اجرا در کشورهای اروپایی به دست نیاورد؛ زیرا دستورالعمل، کشورهای عضو را تنها به تحصیل نتایج مشخصی الزام می‌کند؛ ضمن اینکه اتخاذ ابزارهای قانونی را به کشورهای عضو واگذار می‌کند. همین موضوع و برخی دیگر از ضعف‌های ماهوی دستورالعمل ۱۹۹۵، مانع اجرایی شدن آن شد. پس از آن در سال ۲۰۱۶، قواعد حفاظت از داده در قالب مقررات[2] به تصویب رسید که مقررات عمومی حفاظت از داده شخصی نامیده شد (EU, 2016: 679). مقررات در تعریف کمیسیون اروپا، «قوانین حقوقی هستند که به‌محض لازم‌الاجرا شدن بدون نیاز به تبدیل شدن به قانون ملی، به‌صورت خودکار و یکسان در تمام کشورهای اتحادیه اروپا اعمال می‌شوند. این مقررات به‌طور کامل برای تمام کشورهای اتحادیه اروپا الزام‌آور هستند»[3]. مقررات، غیر از استثنائاتی که در مقرره پیش‌بینی شده است، باید عیناً توسط کشورهای عضو اجرا شوند.

مقررات عمومی حفاظت از داده شخصی از سال ۲۰۱۸ در تمام کشورهای عضو لازم‌الاجرا شد. مواد تشکیل‌دهنده این مقررات را می‌توان در دو دسته کلی تقسیم‌بندی کرد (ورابک، ۱۴۰۲: ۴۰).

الف- تکالیف کنترلگرها و پردازشگران داده و قواعدی که برای نظارت بر آنان و تعیین مسئولیت‌های آنان وضع شده است.

ب- مقررات اعطای کنترل که با هدف شناسایی حقوقی برای اشخاص موضوع داده در راستای کنترل مستقیم پردازش داده وضع شده است.

دسته نخست از قواعد، مبتنی بر اصولی هستند که در ماده ۵ مقررات عمومی حفاظت از داده‌های شخصی بیان شده است و در بخش سوم این نوشتار توضیح داده خواهد شد. این اصول باید از سوی کنترلگرها و پردازشگران رعایت شوند و نهادهای تخصصی ناظر بر حمایت از داده‌های شخصی نیز باید رأساً یعنی صرف‌نظر از اینکه شخص خاصی از نقض این اصول شکایت کرده باشد، بر رعایت آن‌ها نظارت کنند (انصاری، ۱۴۰۲: ۱۴).

دسته دوم حقوق اشخاص موضوع داده است که در مواد ۱۲ تا ۲۳ مقررات عمومی حفاظت از داده شخصی پیش‌بینی شده است و به اشخاص موضوع داده این توانایی را می‌دهد که رأساً بر پردازش داده‌های شخصی خود توسط کنترلگرها و پردازشگران داده نظارت کنند. اهم این حق‌ها شامل حق دسترسی، حق اصلاح، حق حذف (فراموش شدن)، حق محدود کردن پردازش، حق

1- Directive
2- Regulation
3- https://commission.europa.eu/law/law-making-process/types-eu-law_en.

انتقال‌پذیری داده‌ها و حق اعتراض به پردازش می‌شود (EU, 2016: 679).

۲- چالش‌های فنی هوش مصنوعی

هوش مصنوعی از حیث ماهیت فنی آن دارای ویژگی‌هایی است که در موضوع حفاظت از داده‌های شخصی منشأ چالش خواهد بود. این ویژگی‌ها در بخش‌های آتی در نقد مقررات حمایت از داده شخصی اروپا مبنای ارزیابی قرار می‌گیرد.

۲-۱- ابهام[1]

مشکل ابهام در هوش مصنوعی که از آن به‌عنوان جعبه سیاه نیز یاد می‌شود، به ویژگی‌های سیستم‌های هوش مصنوعی اشاره دارد که باعث می‌شود فرایندهای درونی و چگونگی تصمیم‌گیری آن‌ها برای انسان‌ها نامفهوم و توضیح‌ناپذیر باشد. این مشکل به‌ویژه در الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی عمیق دیده می‌شود که به دلیل پیچیدگی و حجم بالای داده‌های مورد استفاده، نتایج آن‌ها قابل توضیح نیست. فناوری هوش مصنوعی با سازوکارهای خودآموز[2] هدایت می‌شود. این سازوکارها می‌توانند الگوریتم‌های برنامه‌ریزی‌شده خود را بر اساس داده‌های ورودی سازگار کنند (Allen, 2022: 149). بعد از آموزش اولیه ماشین، ممکن است الگوریتم برای طراحان آن شفاف باشد، اما پس از اینکه سیستم صدها، هزاران یا حتی میلیون‌ها الگوی خودبرنامه‌ریزی تکراری را طی کرد، حتی برنامه‌نویسان سیستم نیز دیگر اطلاعی از داده‌های پردازش‌شده، چگونگی پردازش، استنتاج‌ها، ضریب‌های هم‌بستگی و نحوه وزن‌دهی به داده‌ها نخواهند داشت.

۲-۲- پیچیدگی[3]

هوش مصنوعی مستقیماً با خود و با محیط خود در تعامل است. سیستم‌های هوش مصنوعی برای تعامل با محیط خود و تطبیق با تغییرات طراحی شده‌اند. سیستم پیوسته در حال یادگیری و تغییر رفتار بر اساس داده‌های جدید است (Kerrigan, 2022: 9). برخلاف نرم‌افزارهای سنتی، هوش مصنوعی در محیط ثابت عمل نمی‌کند، بلکه با دریافت داده‌های جدید، به‌طور مداوم تکامل می‌یابد. در برخی سیستم‌های هوش مصنوعی مانند خودروهای خودران، داده‌های جدید دائم در حال جمع‌آوری است و سیستم با ترکیب داده‌های قبلی باید به‌صورت درلحظه تصمیم‌گیری کند.

1- Opacity
2- Self-Learning Mechanisms
3- Complexity

عملکردهای سادشده هوش مصنوعی بر پایه دو فناوری یادگیری ماشین و شبکه‌های عصبی میسر شده است. سیستم‌های هوش مصنوعی، به‌ویژه آن‌هایی که از الگوریتم‌های یادگیری ماشین استفاده می‌کنند، از تجربیات پیشین خود یاد می‌گیرند و به‌مرور زمان بهبود می‌یابند. این تعامل با خود، جایی که خروجی‌های قبلی سیستم به‌عنوان ورودی برای پردازش‌های آینده استفاده می‌شوند، یک پیچیدگی تصاعدی ایجاد می‌کند (Rab, 2022: 362). در شبکه‌های عصبی به‌ویژه مدل‌های یادگیری عمیق، تعامل میان لایه‌های متعدد نورون‌ها به پیچیدگی بالایی منجر می‌شود. هر لایه داده‌ها را پردازش و به لایه بعدی منتقل می‌کند که باعث می‌شود رفتار کلی سیستم سخت‌تر پیش‌بینی و درک شود.

۳-۲- استقلال[1]

استقلال در هوش مصنوعی به معنای توانایی سیستم برای عملیات و تصمیم‌گیری به‌طور مستقل از دخالت انسانی است. این استقلال به این معناست که نتایج حاصل از عملیات کد به‌جای نیت برنامه‌نویس، از خود عملکرد کد نشئت می‌گیرد (Petrin, 2022: 65-66). خودمختاری به سیستم‌ها اجازه می‌دهد تا در محیط‌های پویا و پیچیده به‌طور مؤثر عمل کنند و با شرایط غیرمنتظره سازگار شوند. رفتار خودتطبیقی[2] در برخی از انواع فناوری‌های هوش مصنوعی منجر به کاهش شفافیت می‌شود.

۴-۲- پیش‌بینی‌ناپذیری[3]

پیش‌بینی‌ناپذیری یکی از ویژگی‌های اساسی سیستم‌های هوش مصنوعی است که آن‌ها را از برنامه‌نویسی سنتی که بر عملیات منطقی مبتنی است، متمایز می‌کند. در برنامه‌نویسی سنتی، خروجی سیستم به‌طور دقیق و پیش‌بینی‌پذیر بر اساس ورودی‌ها و منطق برنامه تعیین می‌شود، اما در هوش مصنوعی، به‌ویژه با استفاده از الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی عمیق، خروجی‌ها می‌توانند پیش‌بینی‌ناپذیر باشند (Trusilo, 2023: 2-1).

۳- چالش اعمال مقررات عمومی حفاظت از داده شخصی بر پردازش الگوریتمی

در میان بدنه کارشناسی حقوق فناوری اطلاعات در ایران، مقررات عمومی حفاظت از داده شخصی الگوی جامع و مطلوب قانون‌گذاری در حوزه هوش مصنوعی شناخته می‌شود. این در

1- Autonomous
2- Self-Adaptive
3- Unpredictability

حالی است که سند یادشده از حیث مبانی، اصول و قواعد واجد هنجارهایی است که اجرای آن‌ها منجر به ایستایی فناوری‌های داده‌محور مانند هوش مصنوعی خواهد شد. در این بخش، مقررات عمومی حفاظت از داده شخصی اروپا در دو بعد برخی مبانی حاکم و مواد ناظر بر اصول آن مورد نقد و بررسی قرار می‌گیرد.

۱-۳- مبنای کنترلی مقررات عمومی حفاظت از داده شخصی

مقررات حمایت از داده شخصی اروپا بر پایه دو ویژگی اساسی تنظیم شده که شناسایی آن دو، در فهم عمیق‌تر و تحلیل صحیح امکان اعمال و اجرای آن بر فناوری هوش مصنوعی بسیار ضروری است. این مبانی ریشه در اصول و قواعد سنتی حقوق اروپایی دارد و اعمال آن بر پردازش الگوریتمی هوش مصنوعی که دارای ماهیت منحصربه‌فرد و ابعاد پیچیده‌ای است، چالش‌هایی را به دنبال خواهد داشت.

۱-۱-۳- رویکرد کنترل فردی

قواعد سنتی حفاظت از داده شخصی بر مبنای رویکرد کنترل شخص موضوع داده بر داده‌های ایجادشده توسط وی شکل گرفته است (Purtova, 2011: 2-3). مقررات عمومی حفاظت از داده شخصی به استناد ماده ۸ منشور حقوق بشر اروپایی، حق حفاظت از داده شخصی را حقی اساسی دانسته و بر همین مبنا، حقوقی مانند حق اطلاع، حق فراموشی، حق اعتراض و... را به‌منظور ارتقای کنترل فردی شهروندان بر داده‌های شخصی وضع کرد. این رویکرد ریشه در مبانی دیگری در نظام حقوقی اتحادیه اروپا مانند حق تعیین سرنوشت اطلاعاتی، حق بر حریم خصوصی و حق مالکیت دارد (که در ادامه به آن‌ها می‌پردازیم). رویکرد کنترلی مقررات عمومی حفاظت از داده شخصی از نظر برخی صاحب‌نظران حقوق داده‌های شخصی ناکارآمد قلمداد می‌شود. ورابک، یکی از صاحب‌نظران حقوق فناوری اطلاعات، سه دلیل را برای این ناکارآمدی و عدم توفیق در نتیجه‌بخشی قواعد کنترلی مقررات عمومی حفاظت از داده شخصی بیان می‌کند (ورابک، ۱۴۰۲: ۲۰۳).

الف- دلیل نخست پیشرفت فناوری اطلاعات است. درحالی‌که قواعد کنترلی بیشتر به کنترل عملکردهای سطحی سیستم‌ها و فرایند و چگونگی پردازش داده شخصی می‌پردازد، پلتفرم‌های جدید با ویژگی‌های ماژولار بودن، بازنویسی مداوم و جریان یکپارچه داده در سیستم طراحی‌شده‌اند. در چنین سیستم‌هایی، روش‌های پردازش داده بسیار مبهم و امکان فهم آن برای نهادهای ناظر دشوار است.

ب- دلیل دوم عوامل روان‌شناختی است که اغلب افراد را از اعمال کنترل مؤثر بر داده‌ها بازمی‌دارد. قواعد سنتی حفاظت از داده شخصی متشکل از حقوقی برای شخص موضوع داده

است که باید به‌صورت ترافعی به شناسایی نقض، اعتراض و درنهایت، طرح دعوی در خصوص آن بپردازد درحالی‌که عمدتاً اشخاص موضوع داده فاقد توانایی و انگیزه کافی برای بررسی دقیق و جزئیات کلیدی چگونگی پردازش داده‌های شخصی برای تصمیم‌گیری آگاهانه در مورد داده‌های شخصی هستند.

پ- دلیل سوم نیز عوامل مسلط بر بازار است. پلتفرم‌های بزرگ مانند موتور جست‌وجوگر گوگل، مدل کسب‌وکار خود را بر اساس جمع‌آوری داده‌های شخصی و استفاده مجدد از داده‌های شخصی ایجاد کرده‌اند که این مدل به‌عنوان اسرار تجاری آنان شمرده و بسیار پیچیده است. ازاین‌رو استفاده مجدد از داده شخصی توسط الگوریتم‌های پیچیده این شرکت‌ها، امکان نظارت بر اعمال مقررات ناظر بر عملیات پردازش را دشوار می‌سازد.

۲-۱-۳- رویکرد مالکانه

مقررات عمومی حفاظت از داده شخصی بر مبنای رویکرد مالکانه شخص موضوع داده بر داده‌های شخصی خود استوار است. مقررات عمومی حفاظت از داده شخصی در ادامه تطوری تاریخی شکل گرفته است که منشأ آن در نظام حقوقی آلمان پدیدار شد (انصاری، ۱۴۰۲: ۲۳). نخستین آرای دادگاه قانون اساسی آلمان در زمینه داده‌های شخصی نشان می‌دهد که قضات «حق خودمختاری اطلاعات» را به حق مالکیت نسبت به داده‌ها پیوند داده‌اند. در یکی از آرای دادگاه قانون اساسی آلمان بیان شده است که هر فرد حق دارد تعیین کند که چه زمانی و در چه حدودی داده‌های شخصی‌اش منتشر شود درست مانند اینکه مالک حق دارد تعیین کند که چه زمانی به چه کسی اجازه استفاده از ملک خود را بدهد (Purtova, 2011: 215). مبنای مالکانه قواعد حمایت از داده‌های شخصی در دادگاه قانون اساسی آلمان، در سال‌های اخیر در سند حمایت از داده‌های شخصی اتحادیه اروپا (مصوب ۱۹۹۵) و سند مقررات عمومی حفاظت از داده شخصی مصوب ۲۰۱۶ نیز نفوذ کرده است. به همان ترتیبی که هرگونه استفاده بدون رضایت از ملک کسی توسط شخص دیگری به‌عنوان نقض حقوق مالکیت در نظر گرفته می‌شود، در حقوق داده‌های شخصی مقررات عمومی حفاظت از داده شخصی نیز هرگونه استفاده بدون رضایت از داده‌های شخصی اعم از جمع‌آوری، ذخیره‌سازی، پردازش و انتقال داده‌های شخصی به‌عنوان نقض حق حفاظت از داده‌ها تلقی می‌شود (European Parliament, 2020: 49). به‌رغم اینکه این رویکرد احتیاطی نسبت به حقوق اشخاص موضوع داده، حمایت حداکثری از حقوق اشخاص موضوع داده را در دستور کار خود دارد، اما چالش‌هایی که مقررات عمومی حفاظت از داده شخصی در مرحله اجرا با آن مواجه شده است، نشان از عدم انطباق آن با ماهیت فناوری و عدم هم‌بستگی آن با زندگی

اجتماعی دارد. در عصر برخط و دیجیتال کنونی که طیف وسیعی از داده‌های شخصی تقریباً همیشه و در همه سطوح منتشر و مبادله می‌شوند، قیاس اموال فیزیکی با داده‌های شخصی و تعمیم مالکیت سنتی به داده، صحیح به نظر نمی‌رسد (Schwartz, 2005: 2084). حجم عظیم داده‌های شخصی که روزانه کاربران در تعامل خود با شبکه اینترنت و وب ۲ ارائه می‌دهند، با اموال منقول و غیرمنقولی مانند خودرو و املاک قیاس‌ناپذیر است و علی‌القاعده نمی‌توان قواعد سنتی مالکیت اموال را بر داده‌های شخصی به کار بست. احکام مقررات حمایت از داده شخصی اروپا، واقع‌گرا نیست و مفهومی انتزاعی و آرمان‌گرایانه را ترسیم می‌کند. برای‌مثال، مطابق احکام مقررات عمومی حفاظت از داده شخصی اگر CPUهای شخصی یا سازمانی را در نظر بگیریم، روزانه میلیون‌ها نقض حقوق اشخاص موضوع داده رخ می‌دهد. بااین‌حال، به نظر می‌رسد که بنا به ضرورت‌ها و واقعیت‌های اجتماعی، دولت‌های اروپایی به‌ناچار از رویکرد مضیق قواعد مقررات عمومی حفاظت از داده شخصی در مواردی مانند مثال بالا که غیرقابل اجرایی شدن است، صرف‌نظر کرده‌اند.

۲-۳- اصول مقررات عمومی حفاظت از داده شخصی

در این بخش با توجه به خصوصیات و ویژگی‌هایی که برای هوش مصنوعی یاد شد، امکان اعمال اصول مقررات عمومی حفاظت از داده شخصی و به‌تبع، قواعد آن بر موقعیت‌های مختلف هوش مصنوعی مورد ارزیابی قرار می‌گیرد.

۱-۲-۳- شفافیت

مطابق ماده (a) (۱) ۵ مقررات عمومی حفاظت از داده شخصی، پردازش باید قانونی، منصفانه و شفاف باشد. اصل شفافیت الزام می‌کند که هرگونه اطلاعات و ارتباطات مربوط به پردازش داده‌های شخصی به‌راحتی و با زبانی ساده در دسترس شخص موضوع داده قرار گیرد. این اصل همچنین، حق اشخاص موضوع داده بر دریافت اطلاعات در خصوص هویت کنترلگر و اهداف پردازش و اطلاعات بیشتر را برای اطمینان از پردازش منصفانه و شفاف مورد تأکید قرار می‌دهد. الزامات کنترلگرها در خصوص اجرای اصل شفافیت به‌موجب احکام مندرج در مواد ۱۲ تا ۱۵ مقررات عمومی حفاظت از داده شخصی تعیین شده است (European Parliament, 2020: 44).

در پردازش‌های هوش مصنوعی، بیان و توجیه اهداف خاص تحلیل داده‌ها به‌صورت پیشینی دشوار است.کنترلگر ممکن است نتواند تأثیر پردازش داده‌های شخصی را که با ماشین انجام می‌شود، به‌صورت شفاف توضیح دهد؛ زیرا ماهیت خودآموز و خودمختار هوش مصنوعی که با متغیرهای ناشناخته (یا حتی توضیح‌ناپذیر) عمل می‌کند، در مقابل هرگونه تلاشی برای ارائه

اطلاعات شفاف مقاومت می‌کند. همچنین، ویژگی ابهام و جعبه سیاه هوش مصنوعی نیز در اجرای الزامات شفافیت مقررات عمومی حفاظت از داده شخصی، موانعی ایجاد می‌کند. شبکه‌های عصبی مصنوعی در لایه‌های پنهان خود ممکن است فرایندهای نرم‌افزاری مربوط را غیرقابل ردیابی یا حتی دسترسی به آن‌ها را ممنوع کنند (Church & Cumbley, 2022: 178).

۲-۲-۳- محدودیت هدف[1]

بر اساس اصل محدودیت هدف که در ماده (b) (۱) ۵ مقررات عمومی حفاظت از داده شخصی مقرر شده است، اهداف پردازش و جمع‌آوری داده‌های شخصی باید مشخص شده باشد و به‌طور دقیق به موضوع داده‌ها ارائه شود. این اصل بر هرگونه پردازش داده‌های اضافی نیز اعمال می‌شود. الزام به محدودیت پردازشگر به هدف از پیش تعیین‌شده، اساساً مغایر با کارکرد هوش مصنوعی است. هوش مصنوعی به‌صورت مستقل و خودمختار توسعه می‌یابد و معمولاً برای اهدافی که از پیش تعریف نشده‌اند، استفاده می‌شود. براین‌اساس، اصل محدودیت هدف مقررات عمومی حفاظت از داده شخصی منجر به تضعیف هوش مصنوعی خواهد شد. در بسیاری از سناریوهای هوش مصنوعی، پیش‌بینی اینکه الگوریتم چه چیزی یاد خواهد گرفت، تقریباً غیرممکن است. افزون‌براین، هدف از پردازش ممکن است در جریان توسعه خودکار هوش مصنوعی تغییر کند؛ به‌خصوص اینکه اهداف مربوط به پردازش داده‌ها در زمان جمع‌آوری داده‌ها ممکن است شناخته‌شده نباشند.

۳-۲-۳- حداقلی‌سازی داده‌ها[2]

ماده (c) (۱) ۵ مقرر می‌کند جمع‌آوری و ذخیره‌سازی داده‌های شخصی باید به‌اندازه کفایت مربوط به هدف پردازش و محدود به آنچه برای اهداف پردازش آن‌ها لازم است، باشد. مقررات عمومی حفاظت از داده شخصی، اجرای اصل حداقلی‌سازی داده‌ها را از مجرای الزامات محدودیت ذخیره‌سازی و پیاده‌سازی اقدامات فنی و حفاظت از داده‌ها پیش‌بینی کرده است. اصل محدودیت ذخیره‌سازی مقرر می‌کند که جایی که داده‌های شخصی ذخیره می‌شوند، شناسایی موضوع داده‌ها تنها برای زمانی که اهداف پردازش ایجاب می‌کند، مجاز است. مشابه اصول توضیح داده‌شده قبلی، اصل کاهش داده‌ها اغلب به‌طور مستقیم با ماهیت فناوری‌های هوش مصنوعی که نیاز به جمع‌آوری مقادیر زیادی داده دارد، در تضاد است. ماهیت هوش مصنوعی به‌گونه‌ای است که پیش‌بینی نوع و مقدار داده‌های لازم در شرایطی که هنوز توسط سیستم

1- Purpose Limitation
2- Data Minimization

مشخص نشده، بسیار دشوار است. این اصل در پردازش‌های هوش مصنوعی مشکلات زیادی ایجاد می‌کند؛ زیرا حذف یا محدودیت داده‌های شخصی پس از برآورده شدن هدف آن‌ها می‌تواند توسعه و استفاده از فناوری‌های هوش مصنوعی را به‌شدت محدود کند (Dogouli, 2023: 12). فرایند یادگیری ماشین بسیار پیچیده، زمان‌بر و نیازمند هزینه‌های زیادی است که انتزاع داده‌های شخصی از آن، از لحاظ فنی هزینه زیادی را برای توسعه‌دهنده هوش مصنوعی تحمیل می‌کند. بسیاری از اشکال هوش مصنوعی به‌شدت به آموزش بر حجم زیادی از داده‌های با کیفیت بالا به‌ویژه فناوری‌های یادگیری ماشین متکی هستند (انصاری، ۱۴۰۰: ۱۸۱).

۴-۲-۳- دقت[1]

اصل دیگری از قانون حفاظت از داده‌ها که ممکن است در هوش مصنوعی تحت تأثیر قرار گیرد، اصل دقت است که در ماده (d) (۱) ۵ مقرر شده است. به‌منظور حفاظت از شخص موضوع داده در برابر تمام زیان‌ها و مخاطرات ناشی از داده‌های نادرست منتسب به وی، اصل دقت کنترلگر را ملزم می‌کند تا اطمینان یابد که داده‌های شخصی جمع‌آوری‌شده به‌طور دقیق واقعیت را نشان می‌دهند (European Parliament, 2020: 48). پیش‌تر بیان شد که پیش‌بینی‌ناپذیری یکی از ویژگی‌های سامانه‌های هوش مصنوعی است. هوش مصنوعی که از فناوری شبکه‌های عمیق و یادگیری ماشین استفاده می‌کند، می‌تواند از داده‌های اولیه، داده‌های جدید و پیش‌بینی‌ناپذیر تولید کند. همچنین، حتی درصورتی‌که الگوریتم، داده‌های صحیحی ارائه دهد، داده‌های خروجی ممکن است در زمان کمی از اعتبار بیفتند یا به‌مرور زمان قدیمی و استنادناپذیر شوند و کنترلگر داده نیز توانایی لازم را برای شناسایی و تصحیح آن‌ها نداشته باشد.

۵-۲-۳- قانونی بودن[2]

بر اساس اصل قانونی بودن، پردازش داده‌ها نیاز به مبنایی قانونی دارد که پردازش داده‌ها را مجاز کند. مقررات عمومی حفاظت از داده شخصی، اصل را بر منع پردازش بنا نهاده است مگر اینکه کنترلگر دلیلی برای پردازش مطابق الزامات مقررات عمومی حفاظت از داده شخصی داشته باشد. مطابق ماده (a) (۱) ۶ مقررات عمومی حفاظت از داده شخصی، مبانی قانونی پردازش داده‌های شخصی شامل رضایت، اجرای قرارداد، اجرای تعهدات قانونی، حفاظت از منافع عمومی، اجرای وظایف عمومی یا اعمال اقتدار رسمی و حفاظت از منافع مشروع می‌شود.

مهم‌ترین مبنای قانونی برای پردازش داده‌های شخصی، رضایت شخص موضوع داده است.

1- Accuracy
2- Legitimacy

مطابق ماده (۱۴)۱۱مقررات عمومی حفاظت از داده شخصی، رضایت تنها زمانی معتبر است که به‌طور آزادانه، خاص، آگاهانه و صریح ابراز شود. بااین‌حال، یکی از ویژگی‌های ذاتی فناوری‌های هوش مصنوعی این است که ممکن است داده‌های استفاده‌شده برای آموزش خود را تغییر دهند، هم‌بستگی‌های جدیدی میان داده‌ها کشف کنند، آن‌ها را به روش‌های مختلف دسته‌بندی کنند و داده‌های جدیدی ایجاد کنند. این موارد ممکن است بدون نظارت یا آگاهی کنترلگر انجام شود. در چنین شرایطی رضایت نمی‌تواند «آگاهانه»، «خاص» و «صریح » تلقی شود؛ زیرا موضوع داده حتی نمی‌تواند بداند که این ویژگی‌های هوش مصنوعی چگونه در وضعیت فردی او عمل خواهند کرد و داده‌های ارائه‌شده چگونه مورد استفاده قرار خواهد گرفت. به‌این‌ترتیب، هدف از مفهوم رضایت که تضمین استقلال شخص موضوع داده است، محدود می‌شود (Paal, 2022: 296).

افزون‌براین، مطابق مقررات عمومی حفاظت از داده شخصی رضایت قابل رجوع است و شخص موضوع داده می‌تواند به‌سادگی از رضایت خود انصراف دهد. در پردازش الگوریتمی، رجوع از رضایت، استفاده از داده‌های شخص موضوع داده را برای توسعه الگوریتم متوقف می‌کند. عملاً حذف داده‌هایی که شخص از پردازش آن‌ها انصراف داده است، منجر به اختلال در سیستم هوش مصنوعی شود؛ زیرا اگر این حق برای اشخاص موضوع داده وجود داشته باشد که هر زمانی از رضایت خود رجوع کنند، داده‌های باقی‌مانده برای آموزش ماشین ناکافی و ممکن است نیاز به آموزش مجدد ماشین ایجاد شود. بنابراین، اجرای حق انصراف از رضایت در پردازش الگوریتمی، هزینه اقتصادی بالایی برای کنترلگر خواهد داشت.

۴- قانون‌گذاری حفاظت از داده شخصی در پردازش الگوریتمی

بنا بر بررسی‌هایی که در این مقاله ارائه شد، اجرای بخش زیادی از قواعد حمایت از داده‌های شخصی مقررات عمومی حفاظت از داده شخصی در پردازش‌های الگوریتمی از حیث فنی غیرممکن یا واجد هزینه‌های نامعقولی است که منجر به توقف توسعه هوش مصنوعی می‌شود. با در نظر گرفتن اینکه تدوین لوایح حمایت از داده شخصی در ایران مبتنی بر الگوی مقررات عمومی حمایت از داده شخصی اروپا شکل گرفته است، در این بخش، وضع قواعد (قانون یا مقرره) حمایت از داده شخصی کنترلی در موضوع هوش مصنوعی در پرتوی برخی از اصول کیفی قانون‌گذاری مورد تحلیل قرار می‌گیرد.

۴-۱- عدم مداخله

یکی از باورهای خطرناک در تنظیم‌گری، اعتقاد به لزوم قاعده‌گذاری دولت در مورد هر پدیده اجتماعی است. در مواردی که ریسک دخالت دولت در موضوعی محاسبه‌ناپذیر باشد یا ریسک

مداخله بسیار زیاد باشد، در این صورت باید به اصل عدم مداخله دولت رجوع کرد. همچنین، درصورتی‌که رابطه علی لازم و کافی میان رفتاری که بناست با دخالت دولت تنظیم شود و اهدافی که بناست از طریق تنظیم‌گری تأمین شود، وجود نداشته باشد یا رفتار تحت تنظیم‌گری دولت از تنوع و پیچیدگی زیادی برخوردار باشد، در این موارد نیز اصل بر عدم مداخله تقنینی دولت است (وکیلیان، ۱۴۰۲: ۶۵). با توجه به چالش‌هایی که در خصوص اعمال قواعد مقررات عمومی حفاظت از داده شخصی بر پردازش‌های الگوریتمی گفته شد، قدر متیقن این است که هرگونه قاعده‌گذاری کنترلی مشابه سند یادشده در حوزه هوش مصنوعی، ناقص و حصول به اهداف آن با شکست مواجه خواهد شد. وجود ویژگی‌های پیچیدگی، ابهام، پیش‌بینی‌ناپذیری و تطبیق‌پذیری در هوش مصنوعی، اراده کنترلگر داده را تحت شعاع قرار می‌دهد و اساساً وضع قواعد پیشگیرانه و کنترلی مانند مقررات عمومی حفاظت از داده شخصی اتحادیه اروپا، تکلیف به مالایطاق است. واضح است که وضع و الزام قواعد مشابه برای پردازش‌های الگوریتمی، با توجه به عدم امکان اجرایی شدن آن، تنها به ناکارآمدی قانون خواهد انجامید.

۲-۴- رویکرد هزینه‌فایده

تحلیل هزینه‌فایده می‌تواند ابزاری مؤثر برای ارزیابی دقیق‌تر ریسک‌ها و فواید پدیده‌های اجتماعی باشد. قانون‌گذاری نباید به‌صورت احساسی تنها در مخاطرات و آثار سوء یک موضوع تمرکز کند و از فوایدی که آن موضوع می‌تواند برای شهروندان داشته باشد، غفلت ورزد. قانون باید به‌گونه‌ای باشد که نه‌تنها از وقوع مخاطرات جلوگیری کند، بلکه جامعه را از فواید آن پدیده نیز محروم نسازد (Sunstein, 2005: 102). پردازش داده‌های شخصی با هوش مصنوعی، به‌خودی‌خود برای اشخاص موضوع داده خطرناک نیست. افزون‌براین، ایجاد تکالیفی در سطح قواعد مقررات عمومی حفاظت از داده شخصی برای کنترل پردازش داده‌های شخصی توسط هوش مصنوعی، به معنای بن‌بستی برای توسعه هوش مصنوعی خواهد بود. این در حالی است که هوش مصنوعی در بسیاری از حوزه‌های زندگی اجتماعی مانند آموزش، صنعت، حمل‌ونقل، سلامت و... می‌تواند در خدمت بشریت قرار گیرد. برای مثال، در کتاب معروف *عصر هوش مصنوعی و آینده انسان‌ها* نقل شده است که در سال ۲۰۲۰، پژوهشگران مؤسسه ام‌آی‌تی یک مدل هوش مصنوعی را آموزش دادند که با ارزیابی ویژگی‌های ۶۱ هزار مولکول، موفق به کشف آنتی‌بیوتیک باکتری‌ای شده که تا آن زمان در مقابل تمام آنتی‌بیوتیک‌های شناخته‌شده مقاوم بود (کسینجر و دیگران، ۱۴۰۱: ۸).

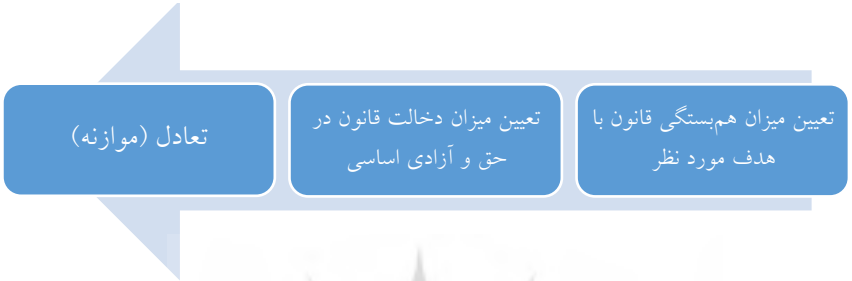
در دنیای آنالوگ (غیررقومی) نیز قانون‌گذار لزوماً در برابر هر خطری که اشخاص را تهدید

می‌کند، حکم به ممنوعیت نمی‌دهد. روزانه انسان‌ها در معرض مخاطرات مختلفی در زندگی اجتماعی خود هستند که به آن‌ها اعتنایی نمی‌کنند. برای مثال، روزانه اشخاص زیادی در تصادفات جاده‌ای کشته می‌شوند، اما این موضوع هیچ‌گاه سبب وضع قانون برای ممنوعیت مسافرت با وسایل نقلیه جاده‌ای نشده است یا قانون هیچ‌گاه برای کنترل تصادفات جاده‌ای، به ممنوعیت صدور گواهی‌نامه رانندگی نپرداخته است. همچنین، در مسابقات ورزشی حرفه‌ای، ورزش‌کاران صدمات جسمانی زیادی می‌بینند و حتی ممکن است در برخی رشته‌های ورزشی (برای مثال رزمی)، آن‌ها کشته شوند، اما این موضوع هیچ‌گاه سبب نشده است که آن رشته‌های رزمی ممنوع شود. در صورت وقوع مخاطره در هریک از مثال‌های فوق، موضوع به‌صورت ترافعی توسط دادگاه‌های کیفری یا مدنی مورد رسیدگی قرار می‌گیرد و جرائم ارتکابی رسیدگی می‌شود و زیان‌زننده محکوم به جبران خسارت می‌شود؛ البته قانون‌گذار می‌تواند برخی وجوه رفتارهای پرخطر را در مثال‌های فوق ممنوع کند یا مجازاتی را برای ارتکاب رفتارهای پرخطر یا قواعدی را برای جبران خسارت وضع کند.

۳-۴- اصل تناسب

در بند پیشین بر رویکرد هزینه‌فایده تأکید شد. در این بند به‌منظور کاربست اصل هزینه‌فایده در تحلیل موضوع پیش رو، از اصل تناسب که ابزاری ساختارمند برای تحلیل هنجارهای حقوقی به شمار می‌رود، استفاده می‌شود. اصل تناسب سال‌هاست که به‌عنوان یکی از اصول مهم قانون‌گذاری و نظارت قضایی در نظام حقوقی اتحادیه اروپا و کشورهای اروپایی، مورد استفاده مجالس قانون‌گذاری و دادگاه‌ها قرار می‌گیرد. اصل تناسب دارای آزمونی سه‌مرحله‌ای است که می‌توان هزینه‌ها و فواید قاعده‌گذاری حفاظت از داده‌های شخصی را در هوش مصنوعی با استفاده از آن مورد ارزیابی قرار داد. آزمون تناسب شامل سه مرحله مناسبت، ضرورت و تناسب به معنای خاص می‌شود (Clérico, 2018: 33). الکسی، حقوق‌دان و نویسنده آثار متعدد در زمینه اصل تناسب، مفهوم تناسب به مفهوم خاص (تعادل) را توسعه داده و آزمونی عینی و عملی از آن را برای سنجش تعارض حقوق اساسی و شهروندی ارائه کرده است. وی معتقد است که به کار گرفتن این روش، مقام ناظر را از دیگر مراحل آزمون تناسب بی‌نیاز می‌کند. الکسی قانون تعادل را این‌گونه تعریف می‌کند «هرچه درجه عدم امکان اجرای یک اصل یا ضرر ناشی از آن بیشتر باشد، باید اهمیت اجرای اصل دیگر بیشتر شود» (Alexy, 2010: 102). هر قانونی قابل تقسیم به سه مرحله مجزاست. اولاً، باید امکان اجرای قانون و اهمیت ناشی از آن مورد ارزیابی قرار گیرد. ثانیاً، باید دید که میزان عدم امکان اجرای یک حق یا آزادی بنیادین یا ضرر ناشی از اجرای آن چقدر

است. در مرحله سوم نیز به‌عنوان مرحله آخر باید دید که آیا اهمیت اجرای هدف قانون‌گذار، ضرر ناشی از نقض و تحدید حقوق و آزادی‌های بنیادین را توجیه می‌کند یا خیر. الکسی مدعی است که می‌توان به طرق عقلانی و عینی، فزونی مداخله دولت، درجه اهمیت یک حق و همچنین رابطه این دو با همدیگر را به‌طور کمّی محاسبه کرد (Alexy, 2005: 574).



شکل ۱- مراحل آزمون تعادل

مطابق آزمون تعادل می‌توان بررسی کرد که آیا قواعد حفاظت از داده شخصی کنترلی، اساساً در خصوص پردازش‌های هوش مصنوعی، اهداف مورد نظر قانون را برای حفاظت از اشخاص موضوع داده محقق می‌سازد یا خیر؟ بر اساس آنچه پیش‌تر بر اساس ویژگی‌های هوش مصنوعی و انطباق آن با قواعد کنونی مقررات عمومی حفاظت از داده شخصی اتحادیه اروپا بررسی شد، روشن شد که ابهام، پیچیدگی و خودتطبیقی هوش مصنوعی مانع اجرای اصول حفاظت از داده شخصی و حقوق اشخاص موضوع داده است. الکسی معتقد است درصورتی‌که در آزمون فوق، پاسخ به پرسش نخست منفی بود، آزمون متوقف و قانون یا اقدام عمومی اتخاذی مردود می‌شود.

۵- حمایت از داده شخصی بر بنیاد حق‌های اساسی

با در نظر گرفتن چالش‌های پیش روی قواعد کنترلی حفاظت از داده شخصی برای حفاظت از داده‌های شخصی در پردازش‌های الگوریتمی، وضع قواعد حقوقی نیز با توجه به وضعیت موضوع در دست قانون‌گذاری از حیث برخی اصول کیفی قانون‌گذاری دارای چالش‌هایی شناخته شد. در این بخش به‌عنوان نتایج حاصل از مباحثی که در نقد کارایی قواعد حفاظت از داده کنترلی گفته شد، راهکار نهایی نگارنده برای قانون‌گذاری حفاظت از داده‌های شخصی در حوزه هوش مصنوعی بیان می‌شود.

۵-۱- حفاظت از حق‌های اساسی

ابتدا ضروری است که اشتباه‌برداشت رایج را در خصوص مفهوم داده شخصی روشن کنیم.

بسیاری از مردم و حتی برخی کارشناسان تصور می‌کنند که داده‌های شخصی همان «حریم خصوصی» اشخاص یا بخشی از آن است و تفاوتی میان این دو مفهوم قائل نیستند. بنا بر این تصور رایج، داده شخصی نیز مانند حریم خصوصی جزئی از حقوق اساسی اشخاص تلقی می‌شود و مطلقاً باید مانع دخالت و تعرض دیگران به آن شد. در قانون اساسی جمهوری اسلامی ایران از حریم خصوصی یاد نشده، اما در اصل ۲۵ قانون اساسی، مصادیقی که آمده، مشمول حریم خصوصی اشخاص است و باید مورد حمایت قانون‌گذار قرار گیرد. حمایت از داده شخصی با حفظ حریم خصوصی متفاوت است. حریم خصوصی بخشی از زندگی شخص است که انتظار دارد دیگران به‌هیچ‌عنوان به آن تعرض نکنند مگر در مواردی که شخص رضایت به این موضوع داشته باشد یا دلیل قانونی برای این تعرض وجود داشته باشد. به‌هرحال، نقض حریم خصوصی اشخاص موضوعی استثنایی و خلاف اصل است، اما داده شخصی، آثار رقومی کنش‌ها و فعالیت‌های کاربران در فضای مجازی است که در بسیاری مواقع خارج از حریم خصوصی اشخاص قرار دارد. ازاین‌رو اگر حریم خصوصی را به‌عنوان یک حق اساسی در نظر بگیریم که درهرصورت مستلزم حمایت قانونی است، چنین ضرورتی برای داده شخصی وجود ندارد (ورابک، ۱۴۰۲: ۳۷).

حفاظت از داده شخصی معمولاً در مواردی ضرورت می‌یابد که با یکی از حق‌های اساسی شخص مرتبط شده است و نقض حقوق داده شخصی وی منجر به نقض یکی از حقوق اساسی یا بنیادی شخص شود. نویسنده یک مقاله، مثال‌ها و پرونده‌های متعددی را از انواع آسیب‌هایی که بر اثر جمع‌آوری داده‌های شخصی ایجاد شده، شرح داده است. این موارد شامل آزادی، نقض حقوق مالکیت و آزادی بیان، نقض حریم خصوصی، نقض دادرسی عادلانه و... می‌شود. در این مقاله، مثال‌ها و پرونده‌هایی آمده است که انتشار اطلاعات مالی شخصی منجر به نقض مالکیت شده است. همچنین، در پرونده‌های دیگر نقض داده‌های شخصی فرد، منجر به کشته شدن وی شده است مانند پرونده‌ای که مزاحم با یافتن نشانی قربانی خود که اداره‌ای به او داده بود، او را یافت و کشت (Solove, 2006: 154). مثال‌هایی که در این مقاله بیان شده است، نشان می‌دهد که داده شخصی را نمی‌توان تنها یک حق اساسی مستقل یا مشخصی مانند حق حریم خصوصی دانست؛ زیرا نقض داده شخصی حسب مورد ممکن است با بسیاری از حقوق و آزادی‌های اساسی شخص مرتبط شود و به اقتضای نقض همان حقوق اساسی باید میزان اهمیت نقض داده شخصی را مورد قضاوت قرار داد.

حقوق اساسی در برابر نقض بالفعل حقوق مرتبط اشخاص از آن‌ها محافظت می‌کنند. برای مثال، درصورتی‌که دولت، شخصی را بدون محاکمه قانونی زندانی کند، علیه اشخاص در

وضعیت‌های مشابه اعمال تبعیض کند، به‌صورت غیرقانونی مانع از تجمع و راه‌پیمایی اشخاص شود، مکالمات اشخاص را بدون حکم قضایی شنود کند، اموال اشخاص را بدون دلیل قانونی تصاحب کند و مواردی از این قبیل، حقوق اساسی شخص را نقض کرده است و در صورتی شخص می‌تواند در دادگاه یا مراجع صالح علیه نقض هریک از این حقوق شکایت کند که نقض این حقوق به‌صورت بالفعل تحقق یابد یا خطر واقعی و قریب‌الوقوع برای نقض آن حقوق وجود داشته باشد.

قوانین حمایت از داده شخصی مانند بسیاری از احکام مقررات عمومی حفاظت از داده شخصی اروپا، فارغ از اینکه پردازش داده‌های شخصی حقوق اشخاص را نقض کرده است یا خیر، تکالیفی را بر عهده پردازشگران قرار می‌دهد. به همین دلیل بسیاری از احکام مقررات عمومی حفاظت از داده شخصی در فضایی انتزاعی هستند و فهم ارتباط مواد آن با موقعیت‌های واقعی دشوار است. اساساً قواعد مقررات عمومی حفاظت از داده شخصی به‌صورت پیشگیرانه از حقوق اشخاص در ارتباط با جمع‌آوری، ذخیره‌سازی و پردازش داده‌های شخصی به‌صورت پیشینی محافظت می‌کند، اما باید اذعان داشت که جمع‌آوری، تجمیع و پردازش داده‌ها به‌خودی‌خود هیچ زیانی برای اشخاص موضوع داده ندارد مگر اینکه این داده‌ها برای اهداف نامشروع و غیرقانونی پردازش و تبدیل به اطلاعاتی شوند که ممکن است حقوق اساسی و مشروع شخص را نقض کند.

در دسته‌ای از داده‌های شخصی به دلیل حساسیت بسیار بالایی که دارند و سوءاستفاده از آن‌ها ممکن است منجر به نقض شدید حقوق و آزادی‌های شخص شود، حمایت پیشینی از این داده‌ها و صرف‌نظر کردن از منافع حاصل از پردازش آن‌ها بر اساس اصل احتیاط معقول و منطقی است. زمانی که شواهد علمی درباره خطر نامشخص است، اما آسیب احتمالی می‌تواند قابل توجه باشد، قانون‌گذاران ممکن است اصل احتیاط را اتخاذ کنند که از اقدامات پیشگیرانه حمایت می‌کند (Sunstein, 2005: 19) مانند داده‌های بیومتریک، داده‌های سلامت، اطلاعات مربوط به سوءپیشینه کیفری، عقاید سیاسی و مذهبی و... (که بسته به هر نظام اجتماعی برخی از موارد این دسته‌بندی می‌تواند متفاوت باشد) که افزون‌بر مقررات عمومی حفاظت از داده شخصی اتحادیه اروپا، در ماده ۵۸ قانون تجارت الکترونیکی ایران نیز مشمول حمایت‌های کنترلی ویژه‌ای قرار گرفته‌اند.

نگاهی به رویه دادگاه‌های کشورهای اروپایی در مورد حقوق حفاظت از داده‌های شخصی نشان می‌دهد که دادگاه‌ها حق حفاظت از داده‌های شخصی را به‌عنوان حق مستقل در نظر نمی‌گیرند، بلکه آن را حسب مورد با حقوق بنیادین دیگر مورد ارزیابی قرار می‌دهند. حتی در

سال‌های اولیه ظهور حق حفاظت از داده‌های شخصی در آلمان در رأی معروف «سرشماری»[1] (که بعدها سرمنشأ ظهور حق حفاظت از داده شخصی در سراسر اروپا شد)، دادگاه حق خودمختاری اطلاعاتی را با حقوق بنیادین دیگری مانند «حق تجمعات» مورد شناسایی قرار داد. در این رأی دادگاه قانون اساسی، دادگاه بر آثار سرکوبگرانه و رعب‌آور جمع‌آوری داده‌های شخصی افرادی که در تجمعات شرکت می‌کنند، تأکید کرد (BVerfG, Order of the First Senate of 15 December 1983 - 1 BvR 209/83 - paras. 1-214).

اگرچه ماده ۸ منشور حقوق بنیادین اتحادیه اروپا به‌صراحت حق حفاظت از داده‌ها را تضمین می‌کند، بااین‌حال، در رویه قضایی دادگاه عدالت اتحادیه اروپا، در آرای صادره، ماده ۸ همواره در کنار یک استناد قانونی دیگر در خصوص نقض حقوق بنیادین موضوع منشور حقوق بنیادین یاد شده است. اساساً به دلیل ذات انتزاعی حق حفاظت از داده شخصی، اجرایی شدن این حق نیازمند حق دیگری است تا از منفعتی عینی محافظت کند. این حق مکمل معمولاً حق حریم خصوصی است، اما حقوق دیگری نیز مانند حق مالکیت، حق آزادی و خودمختاری، حق تعیین سرنوشت، حق آزادی بیان و... ممکن است به اقتضای پرونده مورد استناد قرار گیرد. ازاین‌رو حتی در نظام حقوقی مانند نظام حقوقی اتحادیه اروپا که حق حمایت از داده شخصی به‌عنوان حق مستقل شناسایی شده است، به‌ناچار قضات در مقام صدور رأی به حقوق بنیادی دیگر تمسک می‌کنند.

حفاظت مطلق از داده‌های شخصی و قواعد حقوقی پیچیده‌ای که ناظر بر تمام عملیات پردازش داده‌های شخصی است، بر مبنای رویکرد احتیاطی بیش از حدی شکل گرفته است که بر اساس رویکرد هزینه‌فایده، فرصت‌های بسیاری را برای رشد فناوری هوش مصنوعی از بین می‌برد. هنجارهای قانونی حفاظت از داده باید ناظر بر کنترل مخاطرات واقعی و ناقض حق‌های اساسی اشخاص وضع شود. قواعد مضیق پیشگیرانه باید محدود به پردازش داده‌های حساس و مستعد مخاطرات بسیار خطرناک باشد و قواعد حقوقی عمدتاً باید ناظر بر رسیدگی به وضعیت‌های نقض حق‌های اساسی اشخاص و اعاده وضعیت شخص زیان‌دیده به حالت اولیه باشد.

۲-۵- آثار راه‌حل جایگزین

این رویکرد به ما اجازه می‌دهد که از بررسی تک‌تک پردازش داده‌های شخصی در میان انبوهی از جریان اطلاعات روزانه فاصله بگیریم. درصورتی‌که از حفاظت از داده‌ها در برابر خطرات انتزاعی و بالقوه فاصله گرفته شود، آنگاه قانون‌گذار یا تنظیم‌گر فرصت می‌یابد که به‌جای صرف

1- Volkszählungs-Urteil

وقت و هزینه زیاد برای شناسایی خیل تخلفات پردازش داده، بر سیستم پردازش داده و علل و زمینه‌های ایجاد مخاطرات واقعی آن علیه داده‌های شخصی تمرکز کند. برخلاف رویکرد سنتی، تمرکز بر خطرات واقعی و بالفعل برمبنای حق‌های اساسی که با فناوری‌های هوش مصنوعی مرتبط هستند، به شفافیت کامل سیستم هوش مصنوعی نیاز ندارد. در عوض، تکالیف قانونی بر ارزیابی خطر و اتخاذ اقدامات کاهش آثار نقض داده شخصی، اصلاح وضعیت مخاطره‌آمیز و جبران خسارت به‌مقتضای وضعیت تمرکز دارد. رویکرد سنتی حفاظت از داده شخصی تحت تأثیر علوم رایانه‌ای قرار دارد و همان‌طور که از مواد مقررات عمومی حفاظت از داده شخصی نیز مشخص است، قانون‌گذار احکام را بر مبنای عملکرد سیستم و چگونگی پردازش داده‌های شخصی وضع کرده است. رویکرد پیشنهادی بر مبنای ابهام سیستم هوش مصنوعی، مبنای تنظیم‌گری را بر ارزیابی خروجی سیستم‌های هوش مصنوعی قرار داده که این روش، واقع‌گرایانه‌تر است و سبب نتیجه‌بخشی قانون خواهد شد. قانون هوش مصنوعی در زمینه حفاظت از داده‌های شخصی باید به‌جای قاعده‌گذاری بر فرایند، بر رفتار سیستم و میزان نقض حق‌های اساسی شهروندان تمرکز کند.

نتیجه‌گیری

توسعه هوش مصنوعی در گروی وضع قانونی است که در عین حفاظت از داده‌های شخصی، بستر پردازش و استفاده دوباره از داده‌های شخصی را برای طراحی الگوریتم‌های دقیق فراهم کند. این سیاست، ضرورت قانون‌گذاری در حوزه هوش مصنوعی و حمایت از داده‌های شخصی برای جمهوری اسلامی ایران است که راهبرد قطعی آن، توسعه هوش مصنوعی و قرار گرفتن آن در میان قدرت‌های اول هوش مصنوعی تلقی می‌شود. بنا به ضرورت مطالعه تطبیقی به‌خصوص در حوزه‌های حقوق فناوری، الگو گرفتن از قوانین موجود حمایت از داده‌های شخصی مانند مقررات عمومی حفاظت از داده شخصی که در ایران مورد توجه کارشناسان حوزه‌های قانون‌گذاری قرارگرفته است، این سیاست را تأمین نمی‌کند؛ زیرا مقررات عمومی حفاظت از داده شخصی، نسخه اصلاحی قانون دستورالعمل حفاظت از داده شخصی سال ۱۹۹۵ در اتحادیه اروپا، بسیاری از الزامات ناظر بر ماهیت فنی هوش مصنوعی را نادیده می‌گیرد. اصول این دستورالعمل ریشه در قواعد سنتی اروپایی مانند حق کنترل فردی، حق تعیین سرنوشت اطلاعاتی و حق مالکیت نسبت به داده‌های شخصی دارد. به‌تبع، اصول مقررات عمومی حفاظت از داده شخصی نیز که تکالیف آن عمدتاً ناظر بر فرایند پردازش است، با بسیاری از ویژگی‌های فنی هوش مصنوعی ازجمله ماهیت جعبه سیاه آن همخوانی ندارد. از منظر قواعد کیفی ناظر بر ماهیت قانون، تأمین هدف حمایت از

داده‌های شخصی باید با محدودیتی که برای توسعه هوش مصنوعی ایجاد می‌شود، تناسب داشته باشد. بر اساس رویکرد هزینه‌فایده قانون‌گذار باید میان دو هدف حمایت از حقوق اشخاص موضوع داده و توسعه هوش مصنوعی تعادل معقولی را برقرار کند.

اساساً پردازش داده شخصی به‌خودی‌خود مغایرتی با حقوق اشخاص ندارد و زمانی این مغایرت تلقی می‌شود که پردازش به هر دلیلی و توسط هر سامانه‌ای ازجمله هوش مصنوعی، حقوق و آزادی‌های اشخاص را نقض کند. آنچه مهم است تحقق خطر و آسیب به حقوق اشخاص موضوع داده است. ازاین‌رو حفظ داده شخصی حق اساسی تلقی نمی‌شود که قانون با صرف‌نظر از هر مصلحت دیگری، درهرصورت به دفاع و حفاظت از آن بپردازد. آنچه باید معیار قانون‌گذاری برای حفاظت از داده شخصی در نظر گرفته شود، اولاً، نتیجه پردازش (تمرکز بر نتیجه پردازش با ماهیت ابهام و پیچیدگی هوش مصنوعی منطبق است) و ثانیاً، نقض حق اساسی است. قواعد قانون در موضوع حمایت از داده شخصی در حوزه هوش مصنوعی باید ناظر بر خروجی سامانه‌های هوش مصنوعی باشد تا درصورتی‌که نتیجه پردازش داده شخصی به نقض هریک از حقوق و آزادی‌های اساسی شخص مانند حق حریم خصوصی، حق آزادی بیان، حق مالکیت، حق آزادی فردی و منع تعرض و... بینجامد، بسته به میزان و اهمیت نقض حقوق اساسی، تضامین لازم اعمال شود.

کتابنامه

انصاری، باقر (۱۴۰۰). *حقوق داده‌ها و هوش مصنوعی*، تهران: سهامی انتشار.

انصاری، باقر (۱۴۰۲). *اصول پردازش داده‌های شخصی*، تهران: سهامی انتشار.

کیسینجر، هنری، اشمیت، اریک و هوتنلوچر، دانیل (۱۴۰۱). *عصر هوش مصنوعی و آینده ما انسان‌ها*، ترجمه علی پناهی، تهران: ذهن‌آویز.

گرجی، علی‌اکبر (۱۳۸۳). *مبنا و مفهوم حقوق بنیادین*، حقوق اساسی، ۲ (۲).

ورابک، هلنا یو (۱۴۰۲). *حقوق موضوع داده تحت مقررات عمومی حفاظت از اطلاعات اروپا*، ترجمه حسین صادقی و دیگران، تهران: حقوق‌یار.

وکیلیان، حسن (۱۴۰۲). *قانون‌گذاری خوب؛ مبانی، شاخص‌ها و ابعاد*، تهران: مرکز پژوهش‌های اتاق ایران.

Alexy, Robert (2010). A Theory of Constitutional Rights translate Julian Rivers, Oxford University Press.

Allen, J. G. (2022). AGENCY AND LIABILITY. In *Artificial Intelligence*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jun 19, 2024, from https://www.elgaronline.com/view/edcoll/9781800371712/97818003717

12.00020.xml.
Church, P., & Cumbley, R. (2022). "Chapter 10: DATA AND DATA PROTECTION". In *Artificial Intelligence*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jun 18, 2024, from https://www.elgaronline.com/view/edcoll/9781800371712/9781800371712.00021.xml.
Ciriani, Stephane, The Economic Impact of the European Reform of Data Protection (March 31, 2015). COMMUNICATIONS & STRATEGIES, no.97, 1st quarter 2015, Available at SSRN: https://ssrn.com/abstract=2674010.
Clérico, Laura (2018) Proportionality in Social Rights Adjudication; Making It Workable, In Proportionality in Law; an Analytical Perspective, Springer International.
Ding, Z., Zhou, Y., & Zhou, M. (2014). Modeling Self-Adaptive Software Systems With Learning Petri Nets. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 46. https://doi.org/10.1145/2591062.2591113.
Dogouli, Athanasia (2023). Examining Artificial Intelligence through the scope of the GDPR, Information Law Journal.
DOI:10.1007/978-3-030-58951-6_36.
European Parliament, Directorate-General for Parliamentary Research Services, Lagioia, F., Sartor, G. (2020). *The impact of the general data protection regulation on artificial intelligence*, (G.Sartor,edito) Publications Office. https://data.europa.eu/doi/10.2861/293.
Kerrigan, C. (2022). INTRODUCTORY ESSAY. In *Artificial Intelligence*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jun 19, 2024, from https://www.elgaronline.com/view/edcoll/9781800371712/9781800371712.00011.xml.
Kutyłowski, M., Lauks-Dutka, A., & Yung, M. (2020). Challenges for Reconciling Legal Rules with Technical Reality. European Symposium on Research in Computer Security.
Nivel, E., & Thórisson, K. (2009). Self-Programming: Operationalizing Autonomy. https://doi.org/10.2991/AGI.2009.45.
Petrin, M. (2022). CORPORATE GOVERNANCE". In *Artificial Intelligence*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jun 19, 2024, from https://www.elgaronline.com/view/edcoll/9781800371712/9781800371712.00016.xml.
Purtova, N. (2011). *Property rights in personal data: a European perspective*. Kluwer Law International.
Rab, S. (2022). Telecoms and Connectivity. In *Artificial Intelligence*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jun 19, 2024, from https://www.elgaronline.com/view/edcoll/9781800371712/9781800371712.00031.xml.
Robert Alexy (2005) Balancing, constitutional review and representation, International Journal of Constitutional Law, Volume 3, Issue 4.
S. Venkataramani *et al*.,(2020) "Efficient AI System Design With Cross-

Layer Approximate Computing," in *Proceedings of the IEEE*, vol. 108, no. 12, doi: 10.1109/JPROC.2020.3029453

Schwartz, Paul M. (2005) Property, Privacy, and Personal Data. Harvard Law Review, Available at SSRN: https://ssrn.com/abstract=721642 .

Srinivasan, R., & Chander, A. (2021). Biases in AI Systems. *Queue*, 19.

Sunstein, Cass R. (2005) Laws of Fear: Beyond the Precautionary Principle, Cambridge University Press.

Trusilo, D. (2023). Autonomous AI Systems in Conflict: Emergent Behavior and Its Impact on Predictability and Reliability. *Journal of Military Ethics*, 22. https://doi.org/10.1080/15027570.2023.2213985.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.https://doi.org/10.2307/40041279

Gentili, Aurelio (2020), 'Fundamental Rights as a Part of Contract Law', European Business Law Review, Volume, 31 Issue 3, https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.3/EULR2020021

(EU) 2016/679. General Data Protection Regulation. Retrieved from: https://gdpr-info.eu/

Meurisch, Christian ; Mühlhäuser, Max (2021) .Data Protection in AI Services: A Survey. A Survey. ACM Computing Surveys, 54(2), 40:1-40:38.

COM/2021/206 final, Artificial Intelligence Act (AI Act), Retrieved from https://ai-act-law.eu/

European Union. (2012). Charter of Fundamental Rights of the European Union: Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:C2012/326/02

BVerfG, Order of the First Senate of 15 December 1983 - 1 BvR 209/83 -, paras. 1-214, Retrieved from: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

Bureau of Economic Analysis, (2022), Retrieved from: https://www.bea.gov/system/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf

(EU) 2016/679 , General Data Protection Regulation, Retrieved from: https://gdpr-info.eu/