مجلهٔ حقوقی بین‌المللی/ ویژه‌نامه ترجمه/پاییز ۱۴۰۵/ صفحات ۶۰۸ـ۳۷۹

مقررات (اتحادیهٔ اروپا) شمارهٔ ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا ۱۳ ژوئن ۲۰۲۴ در مورد تدوین قوانین هماهنگ‌شده برای هوش مصنوعی و اصلاح مقررات «به شماره‌های ۳۰۰/۲۰۰۸، ۱۶۷/۲۰۱۳، ۱۶۸/۲۰۱۳، ۲۰۱۸/۸۵۸، ۲۰۱۸/۱۱۳۹، ۲۰۱۹/۲۱۴۴» و دستورالعمل‌های مرتبط «به شماره‌های ۲۰۱۴/۹۰، ۲۰۱۶/۷۹۷ و ۲۰۲۰/۱۸۲۸ (قانون هوش مصنوعی)»

قانون هوش مصنوعی اتحادیهٔ اروپا

(پژوهشی)

سینا نورانی مرنی*

میلاد فاتحی**

تاریخ دریافت: ۱۴۰۳/۱۲/۲۶ تاریخ پذیرش: ۱۴۰۵/۰۱/۳۱

مقدمه

(متن مرتبط با منطقهٔ اقتصادی اروپا)

پارلمان و شورای اروپا اتحادیهٔ اروپا،

با درنظرگرفتن معاهدهٔ عملکرد اتحادیهٔ اروپا، به‌ویژه مواد ۱۶ و ۱۱۴ آن،

با عنایت به پیشنهاد کمیسیون اروپا،

پس از ارسال پیش‌نویس مصوبه به پارلمان‌های ملی،

* دانشجوی دکتری حقوق بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران sina78ny@gmail.com

** مترجم مسئول، دانشجوی دکتری حقوق بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران milad67.fatehi@gmail.com

http://creativecommons.org/licenses/by/4.0/

با توجه به نظر کمیتهٔ اقتصادی و اجتماعی اروپا،[۱]
با توجه به نظر بانک مرکزی اروپا،[۲]
با توجه به نظر کمیتهٔ مناطق،[۳]
با رعایت رویهٔ قانونگذاری عادی،[۴]
با توجه به اینکه:

۱. هدف این مقررات، بهبود کارکرد بازار داخلی از طریق وضع چارچوب حقوقی یکنواخت است، به‌ویژه در زمینهٔ توسعه، عرضه در بازار، به‌بهره‌برداری‌رساندن و استفاده از سامانه‌های هوش مصنوعی در اتحادیه. این چارچوب باید مطابق ارزش‌های اتحادیهٔ اروپا باشد. این مقررات با هدف ترویج پذیرش هوش مصنوعی انسان‌محور و قابل اعتماد تدوین شده و هم‌زمان تضمین‌کنندهٔ سطح بالایی از حمایت از سلامت، ایمنی و حقوق بنیادین است؛ حقوقی که در منشور حقوق بنیادین اتحادیهٔ اروپا (منشور) تصریح شده‌اند. این حمایت، ازجمله، حوزه‌هایی همچون دموکراسی، حاکمیت قانون و حفاظت از محیط‌زیست را در بر می‌گیرد. همچنین این مقررات به منظور محافظت در برابر آثار زیان‌بار سامانه‌های هوش مصنوعی در اتحادیه و حمایت از نوآوری وضع شده است. مقررات حاضر، آزادی جابه‌جایی فرامرزی کالاها و خدمات مبتنی بر هوش مصنوعی را تضمین می‌کند و بدین وسیله از آن جلوگیری می‌کند که کشورهای عضو، محدودیت‌هایی بر توسعه، بازاریابی و استفاده از سامانه‌های هوش مصنوعی اعمال کنند، مگر در مواردی که این مقررات، صراحتاً چنین محدودیت‌هایی را مجاز دانسته باشد.

۲. این مقررات باید مطابق ارزش‌های اتحادیه که در منشور حقوق اساسی آن مورد حفاظت قرار گرفته است، اجرا شود و در عین تسهیل حفاظت از اشخاص حقیقی، بنگاه‌های اقتصادی، دموکراسی، حاکمیت قانون و حفاظت از محیط‌زیست، به تقویت نوآوری و اشتغال کمک کرده و اتحادیهٔ اروپا را به پیشگام پذیرش هوش مصنوعی قابل اعتماد تبدیل کند.

۳. سامانه‌های هوش مصنوعی به‌سادگی می‌توانند در بخش‌های متنوع اقتصادی و حوزه‌های متعدد اجتماعی، ازجمله در سطح فرامرزی به کار روند و در سراسر اتحادیه به گردش درآیند. شماری از کشورهای عضو نیز پیش‌تر اقدام به بررسی برای تصویب مقررات ملی به منظور تضمین توسعه و بهره‌برداری ایمن و قابل اعتماد از هوش مصنوعی، در انطباق با تعهدات مرتبط با حقوق اساسی اتحادیهٔ اروپا کرده‌اند. با این حال، ممکن است مقررات ملی ناهمگون، منجر به چندپارگی بازار داخلی شود و سطح اطمینان حقوقی را برای فعالانی که سامانه‌های هوش مصنوعی را توسعه و مورد استفاده قرار

1. OJ C 517, 22.12.2021, p. 56.
2. OJ C 115, 11.3.2022, p. 5.
3. OJ C 97, 28.2.2022, p. 60.
۴. نظر پارلمان اروپا در ۱۳ مارس ۲۰۲۴ (هنوز در روزنامهٔ رسمی منتشر نشده است) و تصمیم شورای اروپا در ۲۱ مه ۲۰۲۴.

می‌دهند یا وارد می‌کنند، کاهش دهد. بنابراین باید سطح بالایی از حفاظت به‌صورت منسجم در سرتاسر اتحادیه تضمین شود تا هوش مصنوعی قابل اعتماد حاصل شود. همچنین برای جلوگیری از اختلافات حقوقی که مانع گردش آزاد، نوآوری، استقرار و پذیرش سامانه‌های هوش مصنوعی و محصولات و خدمات مرتبط در بازار داخلی می‌شود، لازم است تعهدات یکنواختی برای فعالان اقتصادی تعیین شود و حمایت یکسانی از ملاحظات ضروری منافع عمومی و حقوق اشخاص در سرتاسر بازار داخلی، بر اساس ماده ۱۱۴ معاهدهٔ عملکرد اتحادیهٔ اروپا[5] تضمین شود. از آنجا که این مقررات شامل قواعد خاصی در خصوص حفاظت از افراد در زمینهٔ پردازش داده‌های شخصی و محدودیت‌های استفاده از سامانه‌های هوش مصنوعی برای شناسایی زیست‌سنجی از راه دور[6] به منظور اجرای قانون، ارزیابی ریسک اشخاص حقیقی در راستای اجرای قانون و طبقه‌بندی زیست‌سنجی برای مقاصد اجرای قانون است، مناسب خواهد بود که این مقررات، تا حدی که به این قواعد خاص مربوط می‌شود، بر اساس ماده ۱۶ معاهدهٔ عملکرد اتحادیهٔ اروپا تدوین شود. با توجه به این قواعد خاص و استناد به ماده ۱۶ معاهدهٔ عملکرد اتحادیهٔ اروپا، مشورت با هیئت حفاظت از داده‌های اروپا[7] نیز ضروری خواهد بود.

۴. هوش مصنوعی خانواده‌ای از فناوری‌ها است که به‌سرعت در حال تکامل است و به طیف گسترده‌ای از مزایای اقتصادی، زیست‌محیطی و اجتماعی در سرتاسر صنایع و فعالیت‌های اجتماعی کمک می‌کند. با بهبود پیش‌بینی، بهینه‌سازی عملکردها و تخصیص منابع، و شخصی‌سازی راه‌حل‌های دیجیتال برای افراد و سازمان‌ها، استفاده از هوش مصنوعی می‌تواند مزایای رقابتی مهمی را برای بنگاه‌های اقتصادی فراهم و از پیامدهای سودمند اجتماعی و زیست‌محیطی حمایت کند. برای مثال، هوش مصنوعی می‌تواند در حوزه‌هایی مانند بهداشت و درمان، کشاورزی، ایمنی مواد غذایی، آموزش و پرورش، رسانه، ورزش، فرهنگ، مدیریت زیرساخت‌ها، انرژی، حمل و نقل و تدارکات، خدمات عمومی، امنیت، عدالت، بهره‌وری منابع و انرژی، پایش محیط‌زیست، حفظ و احیاء تنوع زیستی و اکوسیستم‌ها، و کاهش و سازگاری با تغییرات اقلیمی نقش مؤثری ایفا کند.

۵. در عین حال، بسته به شرایط مربوط به کاربرد خاص، نحوهٔ استفاده و سطح توسعهٔ فناوری، ممکن است هوش مصنوعی مخاطراتی ایجاد کند و به منافع عمومی و حقوق اساسی که تحت حمایت حقوق اتحادیهٔ اروپا هستند، آسیب برساند. ممکن است این آسیب‌ها مادی یا غیرمادی باشند و شامل آسیب‌های فیزیکی، روانی، اجتماعی یا اقتصادی شوند.

---

5. Treaty on the Functioning of the European Union - TFEU

6. Remote Biometric Identification – RBI

زیست‌سنجی یا بیومتریک (Biometric) به مجموعهٔ فناوری‌ها و روش‌هایی گفته می‌شود که برای شناسایی یا تأیید هویت افراد بر اساس ویژگی‌های فیزیکی یا رفتاری منحصربه‌فردشان به کار می‌روند.

7. The European Data Protection Board - EDPB

۶. با توجه به تأثیر قابل‌توجهی که هوش مصنوعی می‌تواند در جامعه داشته باشد و ضرورت ایجاد اعتماد، توسعهٔ هوش مصنوعی و چارچوب مقرراتی آن باید مطابق ارزش‌های اتحادیه مندرج در مادهٔ ۲ معاهدهٔ اتحادیهٔ اروپا، حقوق و آزادی‌های اساسی مقرر در معاهدات و بر اساس مادهٔ ۶ منشور حقوق اساسی اتحادیهٔ اروپا انجام شود. به‌عنوان پیش‌نیاز، هوش مصنوعی باید فناوری انسان‌محور باشد. این فناوری باید به‌عنوان ابزاری در خدمت انسان عمل کند و هدف نهایی آن افزایش رفاه بشری باشد.

۷. به منظور تضمین سطح بالای حفاظت از منافع عمومی به‌صورت منسجم در زمینهٔ سلامت، ایمنی و حقوق اساسی، باید قواعد مشترکی برای سامانه‌های هوش مصنوعی پرخطر وضع شود. این قواعد باید با منشور حقوق اساسی اتحادیه سازگار، غیرتبعیض‌آمیز و همسو با تعهدات تجاری بین‌المللی اتحادیه باشند. همچنین این قواعد باید *اعلامیهٔ اروپایی حقوق و اصول دیجیتال برای دههٔ دیجیتال* و *رهنمودهای اخلاقی برای هوش مصنوعی قابل اعتماد* گروه کارشناسان بلندپایهٔ هوش مصنوعی[۸] را نیز مدنظر قرار دهند.

۸. بنابراین ایجاد چارچوب حقوقی در سطح اتحادیه که شامل قواعد هماهنگ‌شده‌ای در زمینهٔ هوش مصنوعی باشد، ضروری است تا توسعه، استفاده و پذیرش هوش مصنوعی در بازار داخلی تسهیل شود؛ در عین حال، این چارچوب باید سطح بالای حفاظت از منافع عمومی، مانند سلامت و ایمنی و حمایت از حقوق اساسی، ازجمله دموکراسی، حاکمیت قانون و حفاظت از محیط‌زیست را که در حقوق اتحادیه به رسمیت شناخته و حمایت شده‌اند، تضمین کند. برای دستیابی به این هدف، باید مقرراتی برای عرضه در بازار، بهره‌برداری و استفاده از برخی سامانه‌های هوش مصنوعی وضع شود تا عملکرد روان بازار داخلی تضمین شود و این سیستم‌ها بتوانند از اصل آزادی جابه‌جایی کالاها و خدمات بهره‌مند شوند. این مقررات باید روشن و قاطع در حفاظت از حقوق اساسی، حامی راه‌حل‌های نوآورانه، و تسهیل‌کنندهٔ ایجاد نظام اروپایی متشکل از بازیگران عمومی و خصوصی در حوزهٔ توسعهٔ سامانه‌های هوش مصنوعی مطابق ارزش‌های اتحادیه باشند و همچنین ظرفیت تحول دیجیتال را در تمامی مناطق اتحادیه فعال کنند. با تعیین این قواعد و اتخاذ تدابیری در حمایت از نوآوری، به‌ویژه با تمرکز بر بنگاه‌های اقتصادی کوچک و متوسط،[۹] ازجمله شرکت‌های نوپا، این مقررات با هدف ترویج رویکرد انسان‌محور اروپا به هوش مصنوعی و تبدیل‌شدن به رهبر جهانی در توسعهٔ هوش مصنوعی ایمن، قابل اعتماد و اخلاقی، مطابق آنچه شورای اروپا[۱۰] اعلام کرده است، حمایت می‌کند. همچنین مقررات حاضر، حفاظت از اصول اخلاقی را که به‌طور مشخص از

8. AI of the High-Level Expert Group on Artificial Intelligence - AI HLEG

9. Small and Medium Enterprises - SMEs

۱۰. شورای اروپا، جلسهٔ ویژهٔ شورای اروپا (۱ و ۲ اکتبر ۲۰۲۰)، نتایج در جلسهٔ EUCO ۲۰/۱۳، ۲۰۲۰، ص ۶

سوی پارلمان اروپا[۱۱] درخواست شده تضمین می‌کند.

۹. قواعد هماهنگ‌شده‌ای که برای عرضه در بازار، بهره‌برداری و استفاده از سامانه‌های هوش مصنوعی پرخطر اعمال می‌شوند، باید با مقررات شمارهٔ ۲۰۰۸/۷۶۵ پارلمان و شورای اروپا،[۱۲] تصمیم شمارهٔ ۲۰۰۸/۷۶۸ پارلمان و شورای اروپا[۱۳] و مقررات شمارهٔ ۲۰۱۹/۱۰۲۰ پارلمان و شورای اروپا[۱۴] (چارچوب قانونگذاری جدید) سازگار باشند. قواعد هماهنگ‌شده‌ای که در این مقررات وضع شده‌اند باید در تمامی بخش‌ها اعمال شوند و مطابق چارچوب قانونگذاری جدید، بدون خدشه به قوانین موجود اتحادیه، به‌ویژه در حوزه‌های حفاظت از داده‌ها، حمایت از مصرف‌کنندگان، حقوق اساسی، اشتغال و حمایت از کارگران و ایمنی محصولات اجرا شوند. مقررات حاضر در تکمیل قوانین مذکور عمل می‌کند. در نتیجه، تمامی حقوق و راهکارهای جبرانی که بر اساس قوانین اتحادیه برای مصرف‌کنندگان و سایر اشخاصی که ممکن است تحت تأثیر منفی سامانه‌های هوش مصنوعی قرار گیرند، ازجمله جبران خسارات احتمالی طبق دستورالعمل شمارهٔ ۸۵/۳۷۴ شورای اروپا[۱۵] پیش‌بینی شده‌اند، همچنان محفوظ و کاملاً قابل اجرا خواهند بود. افزون بر این، در زمینهٔ اشتغال و حمایت از کارگران، این مقررات نباید قوانین اجتماعی اتحادیه و قوانین ملی کار را که مطابق حقوق اتحادیه در مورد شرایط اشتغال و کار، ازجمله ایمنی و سلامت شغلی و روابط بین کارفرمایان و کارگران وضع شده‌اند، تحت تأثیر قرار دهد. همچنین این مقررات نباید بر اجرای حقوق اساسی که در کشورهای عضو و در سطح اتحادیه به رسمیت شناخته شده‌اند، تأثیر بگذارد، ازجمله حق یا آزادی اعتصاب، حق مذاکره، انعقاد و اجرای توافقات جمعی یا اقدام دسته‌جمعی مطابق قوانین ملی یا سایر اقداماتی که تحت نظام‌های خاص روابط صنعتی در کشورهای عضو قرار دارند. به‌علاوه، این مقررات نباید بر مقررات مربوط به بهبود شرایط کاری در مشاغل پلتفرمی که در دستورالعمل پارلمان و شورای اروپا دربارهٔ بهبود شرایط کاری در این حوزه آمده است، تأثیر بگذارد. هدف این مقررات، تقویت کارآیی این حقوق و راهکارهای جبرانی موجود از طریق وضع الزامات و تعهدات

۱۱. قطعنامهٔ پارلمان اروپا در ۲۰ اکتبر ۲۰۲۰، رهنمودهایی به کمیسیون اروپا دربارهٔ چارچوب جنبه‌های اخلاقی هوش مصنوعی، رباتیک و فناوری‌های مرتبط (۲۰۲۰/۲۰۱۲ INL).

۱۲. مقررات شمارهٔ ۲۰۰۸/۷۶۵ پارلمان و شورای اروپا، ۹ ژوئیهٔ ۲۰۰۸ که الزمات مربوط به اعتباربخشی را تعیین کرده است و مقررات شمارهٔ ۳۳۹/۹۳ را لغو کرده است. (روزنامهٔ رسمی ۲۱۸، ۲۰۰۸/۸/۱۳، ص ۳۰).

۱۳. مقررات شمارهٔ ۲۰۰۸/۷۶۸ پارلمان و شورای اروپا، ۹ ژوئیهٔ ۲۰۰۸ در مورد چارچوب مشترک برای بازاریابی محصولات و لغو تصمیم شورای اتحادیهٔ اروپا به شمارهٔ ۴۶۵/۹۳ (روزنامهٔ رسمی ۲۱۸، ۲۰۰۸/۸/۱۳، ص ۸۲).

۱۴. مقررات شمارهٔ ۲۰۱۹/۱۰۲۰ پارلمان و شورای اروپا، ۲۰ ژوئن ۲۰۱۹ در مورد نظارت بر بازار و تطابق محصولات و اصلاح دستورالعمل ۲۰۰۴/۴۲ و مقررات شمارهٔ ۲۰۰۸/۷۶۵ و شمارهٔ ۳۰۵ (روزنامهٔ رسمی ۱۶۹، ۲۰۱۹/۶/۲۵، ص ۱).

۱۵. دستورالعمل شمارهٔ ۸۵/۳۷۴ شورای اروپا در مورد هماهنگی قوانین و مقررات اداری کشورهای عضو در خصوص مسئولیت ناشی از محصولات معیوب (روزنامهٔ رسمی ۲۱۰، ۱۹۸۵/۸/۷، ص ۲۹).

خاص، ازجمله در زمینهٔ شفافیت، مستندات فنی و ثبت سوابق سامانه‌های هوش مصنوعی است. همچنین تعهداتی که این مقررات بر فعالان مختلف زنجیرهٔ ارزش هوش مصنوعی تحمیل می‌کند، باید بدون لطمه به قوانین ملی اعمال شوند و سازگار با قوانین اتحادیه باشند، به گونه‌ای که استفاده از برخی سامانه‌های هوش مصنوعی را محدود کند، در صورتی که چنین قانونی خارج از دامنهٔ این مقررات باشد یا اهداف و منافع مشروع عمومی دیگری غیر از اهداف دنبال‌شده توسط این مقررات را پیگیری کند. به‌عنوان مثال، قوانین ملی کار و قوانین حمایت از کودکان و نوجوانان افراد زیر ۱۸ سال که با درنظرگرفتن نظر عمومی شمارهٔ ۲۵ (سال ۲۰۲۱) کمیتهٔ حقوق کودک سازمان ملل متحد دربارهٔ حقوق کودکان در محیط دیجیتال تدوین شده‌اند، تا زمانی که مشخصاً مربوط به سامانه‌های هوش مصنوعی نبوده و اهداف و منافع مشروع عمومی دیگری را دنبال کنند، نباید تحت تأثیر این مقررات قرار گیرند.

۱۰. حق بنیادین حفاظت از داده‌های شخصی، به‌ویژه در مقررات شمارهٔ ۲۰۱۶/۶۷۹[۱۶] و ۲۰۱۸/۱۷۲۵[۱۷] پارلمان و شورای اروپا و دستورالعمل شمارهٔ ۲۰۱۶/۶۸۰ پارلمان و شورای اروپا[۱۸] تضمین شده است. افزون بر این، دستورالعمل EC/۲۰۰۲/۵۸ پارلمان و شورای اروپا[۱۹] از زندگی خصوصی و محرمانگی ارتباطات ازجمله به‌واسطهٔ تعیین شرایط ذخیره‌سازی داده‌های شخصی و غیرشخصی در تجهیزات پایانه‌ای (ارتباطات الکترونیک) و دسترسی به آن‌ها حمایت می‌کند. این اسناد قانونی اتحادیه ازجمله در مواردی که مجموعهٔ داده‌ها ترکیبی از داده‌های شخصی و غیرشخصی باشد، مبنای پردازش پایدار و مسئولانهٔ داده‌ها را فراهم می‌کنند. این مقررات در صدد اثرگذاری بر اجرای قوانین موجود اتحادیه در زمینهٔ پردازش داده‌های شخصی، ازجمله وظایف و اختیارات مراجع نظارتی مستقلِ مسئول نظارت بر رعایت آن اسناد نیست. همچنین این مقررات، تعهدات ارائه‌دهندگان

---

۱۶. مقررات شمارهٔ ۲۰۱۶/۶۷۹ پارلمان و شورای اروپا، ۲۷ آوریل ۲۰۱۶ در مورد حفاظت از افراد حقیقی در برابر پردازش داده‌های شخصی و جریان آزاد این داده‌ها و لغو دستورالعمل ۹۵/۴۶ (مقررات عمومی حفاظت از داده‌ها) (روزنامهٔ رسمی ۱۱۹، ۲۰۱۶/۵/۴، ص ۱).

۱۷. مقررات شمارهٔ ۲۰۱۸/۱۷۲۵ پارلمان و شورای اروپا، ۲۳ اکتبر ۲۰۱۸ در مورد حفاظت از افراد حقیقی در برابر پردازش داده‌های شخصی توسط نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیهٔ اروپا و جریان آزاد این داده‌ها و لغو مقررات ۲۰۰۵/۴۵ و تصمیم شمارهٔ ۲۰۰۲/۱۲۴۷ (روزنامهٔ رسمی ۲۹۵، ۲۰۱۸/۱۱/۲۱، ص ۳۹).

۱۸. مقررات شمارهٔ ۲۰۱۶/۶۸۰ پارلمان و شورای اروپا، ۲۷ آوریل ۲۰۱۶ در مورد حفاظت از افراد حقیقی در برابر پردازش داده‌های شخصی توسط مقامات ذی‌صلاح به منظور پیشگیری، تحقیق، شناسایی یا تعقیب جرائم یا اجرای مجازات‌های کیفری و جریان آزاد این داده‌ها و لغو تصمیم شورای اروپا به شمارهٔ ۲۰۰۸/۹۷۷ (JHA) (روزنامهٔ رسمی ۱۱۹، ۲۰۱۶/۵/۴، ص ۸۹).

۱۹. دستورالعمل شمارهٔ ۲۰۰۲/۵۸ پارلمان و شورای اروپا، ۱۲ ژوئیهٔ ۲۰۰۲ در مورد پردازش داده‌های شخصی و حفاظت از حریم خصوصی در بخش ارتباطات الکترونیکی (دستورالعمل در خصوص حریم خصوصی و ارتباطات الکترونیکی) (روزنامهٔ رسمی ۲۰۱، ۲۰۰۲/۷/۳۱، ص ۳۷).

و بهره‌برداران سامانه‌های هوش مصنوعی را در مقام متولی یا پردازشگر داده تغییر نمی‌دهد، مشروط بر آنکه قوانین اتحادیه یا قوانین ملی در زمینهٔ حمایت از داده‌های شخصی و نیز طراحی، توسعه یا به‌کارگیری این سیستم‌ها مستلزم پردازش داده‌های شخصی باشد. بنابراین شایسته است تا روشن شود که اشخاص موضوع داده، همچنان از تمامی حقوق و تضمین‌های مقرر در قوانین اتحادیه، ازجمله حقوق مربوط به تصمیم‌گیری خودکار فردی و نمایه‌سازی[۲۰] برخوردارند. همچنین قواعد هماهنگ برای عرضه، بهره‌برداری و استفاده از سامانه‌های هوش مصنوعی باید اجرای مؤثر این حقوق و سایر راهکارهای جبرانی تضمین‌شده در قوانین اتحادیه در زمینهٔ حمایت از داده‌های شخصی و دیگر حقوق بنیادین را تسهیل کند.

۱۱. این مقررات نباید بر مفاد مربوط به مسئولیت ارائه‌دهندگان خدمات واسطه‌ای که در مقررات شمارهٔ ۲۰۲۲/۲۰۶۵ پارلمان و شورای اروپا[۲۱] آمده است، خدشه وارد کند.

۱۲. *سامانهٔ هوش مصنوعی* در این مقررات باید به‌طور روشن تعریف شود. این تعریف باید با فعالیت سازمان‌های بین‌المللی مرتبط، هماهنگ باشد تا قطعیت حقوقی تضمین و پذیرش و همگرایی جهانی نیز تسهیل شود. در عین حال، لازم است انعطاف کافی برای همراهی با تحولات سریع فناوری حفظ شود. تعریف سامانهٔ هوش مصنوعی باید بر ویژگی‌های اساسی آن استوار باشد که آن را از نرم‌افزارها یا رویکردهای سنتی برنامه‌نویسی متمایز می‌کند. این تعریف نباید شامل سیستم‌هایی شود که تنها بر اساس قواعد تعیین‌شده توسط انسان برای اجرای خودکار عملیات ساخته شده‌اند. ویژگی کلیدی سامانه‌های هوش مصنوعی قابلیت استنباط آن‌ها است. این قابلیت استنباط به فرآیند به‌دست‌آوردن خروجی‌هایی مانند پیش‌بینی‌ها، محتوا، توصیه‌ها یا تصمیم‌ها اشاره دارد که می‌تواند بر محیط‌های فیزیکی و مجازی تأثیر بگذارد، و به قابلیتی از سامانه‌های هوش مصنوعی اشاره دارد که مدل‌ها یا الگوریتم‌ها، یا هر دو را از ورودی‌ها یا داده‌ها استخراج می‌کند. تکنیک‌هایی که امکان استنباط را در هنگام ساخت سامانهٔ هوش مصنوعی فراهم می‌آورند شامل رویکردهای یادگیری ماشین هستند که از داده‌ها می‌آموزند چگونه به اهداف مشخص دست یابند و همچنین رویکردهای مبتنی بر منطق و دانش که از طریق دانش رمزگذاری‌شده یا نمایش نمادین وظیفهٔ موردنظر، به استنباط می‌پردازند. ظرفیت سامانهٔ هوش

---

۲۰. نمایه‌سازی یا پروفایلینگ (Profiling)، فرآیندی است که طی آن اطلاعاتی دربارهٔ یک فرد، شیء یا موضوع جمع‌آوری و سازماندهی می‌شود تا یک تصویر کلی یا *نمایه* از آن ایجاد شود. این فرآیند می‌تواند برای اهداف مختلفی ازجمله شناسایی الگوها، پیش‌بینی رفتارها، یا دسته‌بندی اطلاعات به کار رود. در واقع، نمایه‌سازی کمک می‌کند تا با استفاده از داده‌ها، اطلاعاتی استخراج شود که به‌راحتی قابل دسترس نبودند.

۲۱. مقررات شمارهٔ ۲۰۲۲/۲۰۶۵ پارلمان و شورای اروپا، ۱۹ اکتبر ۲۰۲۲ ، با موضوع بازار واحد برای خدمات دیجیتال و اصلاح دستورالعمل شمارهٔ ۳۱/ ۲۰۰۰ (قانون خدمات دیجیتال) (روزنامهٔ رسمی ۲۷۷، ۲۰۲۲/۱۰/۲۷، ص ۱).

مصنوعی برای استنباط از پردازش داده‌های ساده فراتر می‌رود و به سیستم این امکان را می‌دهد که یاد بگیرد، استدلال یا مدل‌سازی کند. اصطلاح *ماشین‌محور* یا *مبتنی بر ماشین* به این واقعیت اشاره دارد که سامانه‌های هوش مصنوعی بر روی ماشین‌ها اجرا می‌شوند. این اصطلاح ضمن اشاره به اهداف صریح یا ضمنی تأکید می‌کند که سامانه‌های هوش مصنوعی می‌توانند بر اساس اهداف تعریف‌شدهٔ صریح یا ضمنی عمل کنند. ممکن است اهداف سامانهٔ هوش مصنوعی با هدف اصلی سامانهٔ هوش مصنوعی در زمینهٔ خاص متفاوت باشد. برای اهداف مقررات حاضر، محیط‌ها باید به‌عنوان زمینه‌هایی درک شوند که سامانه‌های هوش مصنوعی در آن‌ها عمل می‌کنند، در حالی که خروجی‌های تولیدشده توسط سامانهٔ هوش مصنوعی نشان‌دهندهٔ عملکردهای مختلفی هستند که توسط سامانه‌های هوش مصنوعی انجام می‌شوند و شامل پیش‌بینی‌ها، محتوا، توصیه‌ها یا تصمیم‌ها هستند. سامانه‌های هوش مصنوعی با درجات متفاوتی از خودمختاری طراحی می‌شوند؛ به این معنا که می‌توانند تا حدی مستقل از مداخلهٔ انسان عمل کنند و حتی بدون دخالت مستقیم انسان به کار خود ادامه دهند. ویژگی سازگاری در این سیستم‌ها که پس از استقرار بروز می‌یابد، به توانایی یادگیری خودکار آن‌ها اشاره دارد و امکان تغییر در حین استفاده را فراهم می‌کند. سامانه‌های هوش مصنوعی می‌توانند به‌صورت مستقل یا به‌عنوان بخشی از یک محصول به کار گرفته شوند؛ چه به‌طور فیزیکی در محصول ادغام شده باشند (تعبیه‌شده) و چه بدون ادغام، صرفاً کارکرد محصول را پشتیبانی کنند (غیرتعبیه‌شده).

۱۳. مفهوم *استفاده‌کننده* که در این مقررات به آن اشاره شده است باید به‌عنوان هر شخص حقیقی یا حقوقی، ازجمله یک مقام عمومی، آژانس یا نهاد دیگر که از سامانهٔ هوش مصنوعی تحت اختیار خود استفاده می‌کند، تفسیر شود، مگر اینکه سامانهٔ هوش مصنوعی در جریان فعالیت شخصی غیرحرفه‌ای مورد استفاده گیرد. بر اساس نوع سامانهٔ هوش مصنوعی، ممکن است استفاده از این سیستم بر افرادی غیر از استفاده‌کننده تأثیر بگذارد.

۱۴. مفهوم *داده‌های زیست‌سنجی* که در این مقررات بیان شده است باید در پرتو مفهوم داده‌های زیست‌سنجی که در بند ۱۴ ماده ۴ مقررات شورای اروپا به شمارهٔ ۶۷۹/ ۲۰۱۶ و بند ۱۸ ماده ۳ مقررات شورای اروپا به شمارهٔ ۱۷۲۵/ ۲۰۱۸ و بند ۱۳ ماده ۳ دستورالعمل شورای اروپا به شمارهٔ ۶۸۰/ ۲۰۱۶ تعریف شده است، تفسیر شود. داده‌های زیست‌سنجی می‌توانند برای تأیید هویت، شناسایی یا دسته‌بندی اشخاص حقیقی و برای شناسایی احساسات اشخاص حقیقی استفاده شوند.

۱۵. مفهوم *شناسایی زیست‌سنجی* که در این مقررات به آن اشاره شده است باید به‌عنوان شناسایی خودکار ویژگی‌های فیزیکی، فیزیولوژیکی و رفتاری انسان مانند چهره، حرکت چشم،

شکل بدن، صدا، لحن، راه‌رفتن، وضعیت بدن، ضربان قلب، فشار خون، بوی بدن، ویژگی‌های تایپ‌کردن کلیدها، برای هدف شناسایی هویت فرد از طریق مقایسهٔ داده‌های زیست‌سنجی آن فرد با داده‌های زیست‌سنجی ذخیره‌شدهٔ افراد در پایگاه داده تعریف شود، بدون توجه به اینکه فرد رضایت خود را اعلام کرده است یا خیر. این تعریف سامانه‌های هوش مصنوعی که برای تأیید زیست‌سنجی به کار می‌روند، ازجمله سامانه‌های احراز هویت را شامل نمی‌شود. هدف این سیستم‌ها (تأیید زیست‌سنجی) صرفاً تأیید این است که شخص حقیقی همان شخصی است که ادعا می‌کند و برای تأیید هویت یک شخص به منظور دسترسی به یک خدمت، بازکردن دستگاه یا دسترسی امنیتی به مکان‌ها به کار گرفته می‌شود.

۱۶. مفهوم *دسته‌بندی زیست‌سنجی* که در این مقررات به آن اشاره شده است باید به‌صورت قراردادن اشخاص حقیقی در دسته‌های خاص بر اساس داده‌های زیست‌سنجی آن‌ها تعریف شود. این دسته‌بندی‌های خاص می‌تواند به جنبه‌هایی مانند جنسیت، سن، رنگ مو، رنگ چشم، تتوها، ویژگی‌های رفتاری یا شخصیتی، زبان، مذهب، عضویت در اقلیت ملی، گرایش جنسی یا سیاسی مرتبط باشد. این مفهوم شامل سیستم‌های دسته‌بندی زیست‌سنجی نمی‌شود که کارکردی کاملاً فرعی دارند که ذاتاً به یک خدمت تجاری دیگر وابسته هستند؛ به این معنا که ویژگی مذکور به دلایل فنی عینی نمی‌تواند بدون خدمت اصلی مورد استفاده قرار گیرد و ادغام آن ویژگی یا عملکرد با خدمت اصلی، به‌عنوان وسیله‌ای برای دورزدن قواعد این مقررات محسوب نمی‌شود. به‌عنوان مثال، فیلترهایی که ویژگی‌های صورت یا بدن را در بازارهای برخط دسته‌بندی می‌کنند می‌توانند به‌عنوان ویژگی جانبی محسوب شوند زیرا صرفاً در چارچوب خدمت اصلی (مانند فروش محصول) قابل استفاده هستند و به مصرف‌کننده این امکان را می‌دهند که پیش‌نمایش محصول را بر روی خود مشاهده کند و به او در تصمیم‌گیری برای خرید کمک می‌کنند. همچنین فیلترهایی که در خدمات شبکه‌های اجتماعی برخط برای دسته‌بندی ویژگی‌های صورت یا بدن به منظور اضافه‌کردن یا ویرایش تصاویر یا ویدیوها استفاده می‌شوند نیز می‌توانند به‌عنوان ویژگی جانبی محسوب شوند، چرا که چنین فیلترهایی بدون خدمت اصلی شبکهٔ اجتماعی که شامل اشتراک‌گذاری برخط محتوا است، قابل استفاده نیستند.

۱۷. مفهوم *سیستم شناسایی زیست‌سنجی از راه دور* در این مقررات باید بر اساس عملکرد آن تعریف شود. این سیستم، یک سامانهٔ هوش مصنوعی است که برای شناسایی اشخاص حقیقی بدون دخالت فعال آن‌ها معمولاً از فاصله‌ای دور و از طریق مقایسهٔ داده‌های زیست‌سنجی یک شخص با داده‌های زیست‌سنجی موجود در پایگاه داده، بدون توجه به فناوری خاص، فرآیندها یا انواع داده‌های زیست‌سنجی طراحی شده است. این سیستم‌های شناسایی زیست‌سنجی از راه دور،

معمولاً برای شناسایی همزمان چند نفر یا رفتارهای آن‌ها به کار می‌روند و به‌طور قابل‌توجهی تشخیص هویت افراد واقعی را بدون نیاز به مداخلهٔ فعال آن‌ها تسهیل می‌کنند. این تعریف شامل سامانه‌های هوش مصنوعی که برای تأیید زیست‌سنجی، ازجمله احراز هویت طراحی شده‌اند، نمی‌شود. هدف این سیستم‌ها صرفاً تأیید این است که شخص حقیقی همان شخصی است که ادعا می‌کند و برای تأیید هویت یک شخص به منظور دسترسی به یک خدمت، بازکردن دستگاه یا دسترسی امنیتی به مکان‌ها به کار گرفته می‌شود. این استثنا با این واقعیت توجیه می‌شود که چنین سیستم‌هایی (تأیید زیست‌سنجی)، در مقایسه با سیستم‌های شناسایی زیست‌سنجی از راه دور که ممکن است داده‌های زیست‌سنجی تعداد زیادی از افراد را بدون دخالت فعال آن‌ها پردازش کند، تأثیر کمی بر حقوق بنیادی اشخاص حقیقی دارند. در مورد سیستم‌های *زمان واقعی*[۲۲] ثبت داده‌های زیست‌سنجی، مقایسه و شناسایی به‌صورت آنی یا بدون تأخیر محسوس انجام می‌شود. در این زمینه، نباید راهی برای دورزدن قواعد این مقررات در استفادهٔ *زمان واقعی* از سامانه‌های هوش مصنوعی مربوطه، با اعمال تأخیرهای جزئی، وجود داشته باشد. سیستم‌های *زمان واقعی* از داده‌های *زنده* یا *نزدیک به زنده* استفاده می‌کنند، مانند تصاویر ویدئویی که توسط دوربین یا دستگاهی با عملکرد مشابه تولید می‌شوند. در مقابل، در سیستم‌های *پساپردازشی*، داده‌های زیست‌سنجی پیش از آن ضبط شده‌اند و مقایسه و شناسایی تنها پس از تأخیر قابل‌توجه انجام می‌شود. این فرآیند شامل داده‌هایی مانند تصاویر یا فیلم‌های ویدیویی است که توسط دوربین‌های مداربسته یا دستگاه‌های خصوصی تولید شده‌اند و قبل از به‌کارگیری این سیستم در مورد اشخاص حقیقی موردنظر ایجاد شده است.

۱۸. مفهوم *سیستم شناسایی احساسات* که در این مقررات به آن اشاره شده است باید به‌طور مشخص به‌عنوان سامانهٔ هوش مصنوعی برای شناسایی یا استنباط احساسات یا نیت‌های اشخاص حقیقی بر اساس داده‌های زیست‌سنجی آن‌ها تعریف شود. این مفهوم به احساسات یا نیت‌هایی مانند شادی، غم، عصبانیت، تعجب، انزجار، شرمندگی، هیجان، شرم، تحقیر، رضایت و سرگرمی اشاره دارد. این مفهوم شامل حالات فیزیکی مانند درد یا خستگی نمی‌شود. برای مثال، سیستم‌هایی که برای تشخیص خستگی خلبانان یا رانندگان حرفه‌ای به منظور پیشگیری از حوادث استفاده می‌شوند، مشمول این تعریف نیستند. همچنین این شامل تشخیص صرف حالات، حرکات یا ژست‌های آشکار نمی‌شود، مگر آنکه برای شناسایی یا استنتاج احساسات به کار روند. این حالات می‌توانند

22. Real-time

زمان واقعی (Real-time) به حالتی گفته می‌شود که یک سیستم یا برنامه، داده‌ها و اطلاعات را بلافاصله و بدون تأخیر پردازش کرده و نمایش می‌دهد. در واقع، وقتی چیزی به‌صورت زمان واقعی انجام می‌شود، واکنش آن به اتفاقات یا ورودی‌ها آنی و هم‌زمان با وقوع آن‌هاست.

شامل حالات سادهٔ چهره مانند اخم یا لبخند، ژست‌هایی مانند حرکت دست، بازو یا سر، یا ویژگی‌های صدای فرد مانند بلندشدن صدا یا نجواکردن باشند.

۱۹. برای اهداف این مقررات، مفهوم *محیط عمومی قابل دسترس* باید به‌عنوان هر فضای فیزیکی که برای تعداد نامعینی از اشخاص حقیقی قابل دسترسی است در نظر گرفته شود، بدون توجه به اینکه آیا فضای مذکور، تحت مالکیت خصوصی یا عمومی است و بدون توجه به نوع فعالیتی که ممکن است در آن فضا انجام شود. این فضاها می‌توانند شامل موارد زیر باشند: فضاهای تجاری (برای مثال فروشگاه‌ها، رستوران‌ها، کافه‌ها)، خدماتی (مانند بانک‌ها، فعالیت‌های حرفه‌ای و صنعت هتل‌داری)، ورزشی (مانند استخرها، باشگاه‌های ورزشی و استادیوم‌ها)، حمل و نقل (مانند ایستگاه‌های اتوبوس، مترو و قطار، فرودگاه‌ها و وسایل حمل و نقل عمومی)، تفریحی و فرهنگی (مانند سینماها، تئاترها، موزه‌ها، سالن‌های کنسرت و کنفرانس)، تفریحی یا سایر اهداف (مانند خیابان‌ها و میدان‌های عمومی، پارک‌ها، جنگل‌ها و زمین‌های بازی). همچنین یک فضا حتی در صورت داشتن محدودیت ظرفیت یا الزامات امنیتی، چنانچه دسترسی به آن منوط به شرایط از پیش تعیین‌شده‌ای باشد که تعداد نامشخصی از افراد بتوانند آن را برآورده کنند، همچنان فضای عمومی محسوب می‌شود، مانند خرید بلیط یا داشتن مجوز حمل و نقل، ثبت‌نام قبلی یا داشتن حداقل سن معین. در مقابل، اگر دسترسی به یک فضا محدود به اشخاص حقیقی خاص و تعریف‌شده بر اساس قوانین اتحادیهٔ اروپا یا قوانین ملی مرتبط با ایمنی یا امنیت عمومی یا از طریق ابراز ارادهٔ صریح فرد صاحب اختیار قانونی بر آن فضای مربوطه باشد، آن فضا نباید به‌عنوان فضای عمومی قابل دسترسی در نظر گرفته شود. امکان دسترسی فیزیکی صرف به یک فضا، مانند درب باز یا دروازه‌ای که قفل نیست، به‌تنهایی نشان‌دهندهٔ عمومی‌بودن و قابل دسترسی‌بودن فضا نیست اگر نشانه‌ها یا شرایطی که خلاف آن را نشان دهند، مانند نصب تابلوهای ممنوعیت یا محدودیت دسترسی. محوطه‌های شرکت‌ها و کارخانه‌ها و به‌طور کلی دفاتر و محل‌های کاری که تنها برای کارکنان و ارائه‌دهندگان خدمات مربوطه قابل دسترسی هستند، فضاهایی هستند که قابل دسترسی برای عموم نیستند. فضاهای عمومی قابل دسترسی نباید شامل زندان‌ها یا کنترل مرزی باشند. ممکن است برخی فضاهای دیگر، ترکیبی از فضاهای عمومی قابل دسترسی و غیرقابل دسترسی باشند، مانند راهروهای ساختمان مسکونی خصوصی که برای دسترسی به مطب پزشک یا بخش‌هایی از فرودگاه مورد استفاده قرار می‌گیرد. فضاهای برخط شامل مفهوم موردنظر نمی‌شوند زیرا فضاهای فیزیکی نیستند. با این حال، اینکه آیا فضای خاصی برای عموم مردم قابل دسترسی است یا نه باید به‌صورت موردی و با توجه به ویژگی‌های خاص هر وضعیت تعیین شود.

۲۰. برای بهره‌برداری بهینه از سامانه‌های هوش مصنوعی همراه با صیانت از حقوق اساسی، سلامت و ایمنی و برای تضمین امکان کنترل دموکراتیک (آن)، سواد هوش مصنوعی باید فراهم‌کنندگان، استفاده‌کنندگان و افراد متأثر را به مفاهیم لازم برای اتخاذ تصمیمات آگاهانه در مورد سامانه‌های هوش مصنوعی مجهز کند. این مفاهیم می‌تواند بسته به زمینهٔ مربوطه متفاوت باشد و شامل درک به‌کارگیری صحیح عناصر فنی در مرحلهٔ توسعهٔ سامانهٔ هوش مصنوعی، تدابیری که باید در زمان استفاده از آن رعایت شوند، شیوه‌های مناسب تفسیر خروجی‌های سامانهٔ هوش مصنوعی، و در مورد اشخاص متأثر، دانشی باشد که برای درک تأثیر تصمیمات اتخاذشده با کمک هوش مصنوعی بر آنان ضروری است. در زمینهٔ اجرای این مقررات، سواد هوش مصنوعی باید بینش لازم را در اختیار همهٔ بازیگران مربوطه در زنجیرهٔ ارزشی هوش مصنوعی قرار دهد تا رعایت مناسب مقررات و اجرای صحیح آن تضمین شود. افزون بر این، اجرای گستردهٔ تدابیر (مربوط به) سواد هوش مصنوعی و ارائهٔ اقدامات پیگیری مناسب می‌تواند شرایط کاری را بهبود بخشیده و در نهایت، مسیر تحکیم و نوآوری هوش مصنوعی قابل اعتماد را در اتحادیهٔ اروپا استمرار بخشد. هیئت هوش مصنوعی اروپایی (هیئت) باید به کمیسیون در زمینهٔ ترویج ابزارهای سواد هوش مصنوعی و افزایش آگاهی و درک عمومی از مزایا، ریسک‌ها، اقدامات حفاظتی، حقوق و تعهدات مربوط به استفاده از سامانه‌های هوش مصنوعی مساعدت کند. کمیسیون و دولت‌های عضو باید با همکاری ذی‌نفعان مرتبط، تهیه، تدوین و اجرای دستورالعمل‌های داوطلبانه را برای پیشبرد سواد هوش مصنوعی در میان افرادی که در توسعه، طرز کار و استفاده از هوش مصنوعی نقش دارند تسهیل کنند.

۲۱. برای اطمینان از ایجاد شرایط برابر و حفاظت مؤثر از حقوق و آزادی‌های افراد در سرتاسر اتحادیهٔ اروپا، قواعد تعیین‌شده در این مقررات باید به‌صورت غیرتبعیض‌آمیز نسبت به تأمین‌کنندگان سامانه‌های هوش مصنوعی، بدون توجه به اینکه در اتحادیه مستقر هستند یا در کشورهای ثالث، و نسبت به استفاده‌کنندگان سامانه‌های هوش مصنوعی که در اتحادیه مستقر هستند، اعمال شود.

۲۲. با توجه به ماهیت دیجیتالی برخی از سامانه‌های هوش مصنوعی، این سامانه‌ها باید تحت پوشش مقررات حاضر قرار گیرند حتی اگر در بازار اتحادیهٔ اروپا عرضه نشود، به بهره‌برداری نرسد یا در اتحادیه مورد استفاده قرار نگیرد. به‌عنوان مثال، در صورتی که اپراتور مستقر در اتحادیه، خدماتی را به اپراتور مستقر در کشور ثالث واگذار کند که مرتبط با فعالیتی باشد که سامانهٔ هوش مصنوعی آن به‌عنوان سیستم پرخطر شناخته می‌شود، در این شرایط، سامانهٔ هوش مصنوعی که در کشور ثالث توسط اپراتور استفاده می‌شود، می‌تواند داده‌های جمع‌آوری‌شده به‌طور قانونی از اتحادیه را پردازش کند و خروجی آن را به اپراتور قراردادی در اتحادیه ارائه دهد، بدون اینکه آن سیستم به بازار عرضه شود، به بهره‌برداری برسد یا در اتحادیه مورد استفاده قرارگیرد. برای جلوگیری

از دورزدن این مقررات و تضمین حفاظت مؤثر از افراد مقیم اتحادیهٔ اروپا، این مقررات باید شامل تأمین‌کنندگان و استفاده‌کنندگان سامانه‌های هوش مصنوعی مستقر در کشورهای ثالث نیز باشد، به شرطی که خروجی تولیدشده توسط این سیستم‌ها در اتحادیه مورد استفاده قرارگیرند. با این حال، برای درنظرگرفتن ترتیبات موجود و نیازهای خاص همکاری‌های آینده با شرکای خارجی که اطلاعات و شواهد مبادله می‌کنند، این مقررات نباید نسبت به مقامات عمومی کشورهای ثالث و سازمان‌های بین‌المللی که در چارچوب همکاری یا توافق‌های بین‌المللی منعقده در سطح اتحادیه یا ملی برای همکاری در زمینهٔ اجرای قانون و همکاری قضائی با اتحادیه یا کشورهای عضو فعالیت می‌کنند، اعمال شود، به شرطی که کشور ثالث یا سازمان بین‌المللی مزبور، تدابیر حفاظتی مناسبی در زمینهٔ حفاظت از حقوق و آزادی‌های بنیادین افراد فراهم کند. در صورت لزوم، این ممکن است شامل فعالیت‌های نهادهایی باشد که از سوی کشورهای ثالث به انجام وظایف خاصی در حمایت از چنین همکاری‌های اجرایی و قضائی منصوب شده‌اند. چنین چارچوب‌هایی برای همکاری یا توافق‌ها به‌صورت دوجانبه میان کشورهای عضو و کشورهای ثالث یا بین اتحادیهٔ اروپا، یوروپل و سایر آژانس‌های اتحادیه و کشورهای ثالث و سازمان‌های بین‌المللی برقرار شده است. مراجع صلاحیت‌دار مسئول نظارت بر مقامات اجرایی و قضائی در چارچوب این مقررات باید ارزیابی کنند که آیا این چارچوب‌های همکاری یا توافق‌های بین‌المللی، تدابیر حفاظتی کافی برای حفاظت از حقوق و آزادی‌های بنیادین افراد را شامل می‌شوند یا خیر. مراجع ملی دریافت‌کننده و نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه که از چنین خروجی‌هایی در اتحادیه استفاده می‌کنند، مسئولیت دارند تا اطمینان حاصل کنند که استفاده از آن‌ها با قوانین اتحادیه مطابقت دارد. زمانی که این توافق‌های بین‌المللی اصلاح و توافق‌های جدیدی در آینده منعقد می‌شوند، طرفین متعهد باید حداکثر تلاش خود را برای هم‌راستاکردن این توافق‌ها با الزامات مقررات حاضر به کار گیرند.

۲۳. همچنین این مقررات باید نسبت به نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه، زمانی که به‌عنوان تأمین‌کننده یا استفاده‌کنندهٔ سامانهٔ هوش مصنوعی عمل می‌کنند، اعمال شود.

۲۴. مقررات حاضر باید نسبت به نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه، زمانی که به‌عنوان تأمین‌کننده یا بهره‌بردار سامانه‌های هوش مصنوعی عمل می‌کنند، اعمال شود، اگر و تا زمانی که سامانه‌های هوش مصنوعی برای اهداف نظامی، دفاعی یا امنیت ملی عرضه می‌شود، مورد استفاده قرار می‌گیرد یا بدون تغییر در چنین سیستم‌هایی، باید از دامنهٔ مقررات حاضر مستثنا شوند، صرف‌نظر از اینکه چه نوع نهادی این فعالیت‌ها را انجام می‌دهد، مانند اینکه آیا این نهاد دولتی یا خصوصی است. در خصوص اهداف نظامی و دفاعی، این استثنا به دلیل ماده ۴(۲) معاهدهٔ اتحادیهٔ اروپا و ویژگی‌های خاص سیاست دفاعی مشترک اتحادیهٔ اروپا که در فصل ۲ از بخش پنج معاهدهٔ

اتحادیهٔ اروپا قرار دارد و مرتبط با حقوق بین‌الملل عمومی است، توجیه می‌شود. تنظیم سامانه‌های هوش مصنوعی در زمینهٔ استفاده از نیروی کشنده و دیگر سامانه‌های هوش مصنوعی در فعالیت‌های نظامی و دفاعی باید به‌طور کامل تحت قوانین حقوق بین‌الملل عمومی قرار باشد. به‌طور مشابه، در خصوص اهداف امنیت ملی، این استثنا به دلیل این که امنیت ملی مسئولیت انحصاری کشورهای عضو است و همچنین بر اساس ماده ۴(۲) معاهدهٔ اتحادیهٔ اروپا به دلیل ماهیت خاص و نیازهای عملیاتی فعالیت‌های امنیت ملی و قوانین خاص ملی مربوط به این فعالیت‌ها توجیه می‌شود. با این حال، اگر سیستمی برای اهداف نظامی، دفاعی یا امنیت ملی توسعه یابد و در بازار عرضه شود، به کار گرفته یا مورد استفاده قرارگیرد و بعدها به‌طور موقت یا دائمی برای اهداف دیگری، مانند اهداف غیرنظامی، بشردوستانه، اجرای قانون یا امنیت عمومی استفاده شود، باید تحت شمول مقررات حاضر قرار گیرد. در این صورت، نهادی که از سامانهٔ هوش مصنوعی برای اهدافی غیر از اهداف نظامی، دفاعی یا امنیت ملی استفاده می‌کند باید اطمینان حاصل کند که سامانهٔ هوش مصنوعی با این مقررات سازگار است، مگر اینکه سیستم قبلاً با این مقررات سازگار باشد. سامانه‌های هوش مصنوعی که به منظور اهدافی که از دامنهٔ مقررات حاضر مستثنا هستند، یعنی اهداف نظامی، دفاعی یا امنیت ملی، در بازار قرار گرفته یا به‌کار گرفته می‌شوند و در عین حال برای اهداف غیرمستثناشده، مانند اهداف غیرنظامی یا اجرای قانون، مورد استفاده قرار می‌گیرند، باید تحت شمول این مقررات قرار گیرند و تأمین‌کنندگان این سیستم‌ها باید اطمینان حاصل کنند که سیستم‌ها با مقررات حاضر سازگار هستند. در این موارد، اینکه سامانهٔ هوش مصنوعی ممکن است تحت شمول مقررات حاضر قرار گیرد نباید تأثیری بر امکان استفاده از سامانه‌های هوش مصنوعی توسط نهادهایی که فعالیت‌های امنیت ملی، دفاعی و نظامی را انجام می‌دهند، صرف‌نظر از نوع نهادی که این فعالیت‌ها را به کار می‌گیرند، داشته باشد. این سیستم‌ها برای اهداف نظامی، دفاعی یا امنیت ملی، که از دامنهٔ شمول مقررات حاضر مستثنا هستند، همچنان می‌توانند به کار روند. سامانه‌های هوش مصنوعی که به منظور اهداف غیرنظامی یا اجرای قانون در بازار قرار گرفته‌اند و برای اهداف نظامی، دفاعی یا امنیت ملی به کار می‌روند، صرف‌نظر از نوع نهادی که این فعالیت‌ها را انجام می‌دهند، نباید تحت شمول مقررات حاضر قرار گیرند.

۲۵. این مقررات باید از نوآوری حمایت کند، آزادی علم را محترم بشمارد و فعالیت‌های تحقیق و توسعه را تضعیف نکند. بنابراین لازم است سیستم‌ها و مدل‌های هوش مصنوعی که به‌طور خاص برای اهداف تحقیق و توسعهٔ علمی طراحی و به کار گرفته شده‌اند، از دامنهٔ شمول این مقررات مستثنا شوند. همچنین ضروری است اطمینان حاصل شود که این مقررات، فعالیت‌های تحقیق و توسعهٔ علمی بر سیستم‌ها یا مدل‌های هوش مصنوعی قبل از عرضه به بازار یا قرارگرفتن در خدمت

عمومی را تحت تأثیر قرار ندهد. در خصوص فعالیت‌های تحقیق، آزمایش و توسعهٔ محصول‌محور بر سیستم‌ها یا مدل‌های هوش مصنوعی، مفاد این مقررات نیز نباید قبل از آنکه این سیستم‌ها و مدل‌ها به کار گرفته شوند یا به بازار عرضه شوند، اعمال شود. این استثنا به این معناست که رعایت این مقررات، همچنان برای سامانه‌های هوش مصنوعی که تحت شمول این مقررات قرار دارند و در نتیجهٔ فعالیت‌های تحقیق و توسعه، وارد بازار یا به کار گرفته می‌شوند، الزامی است؛ همچنین شامل کاربرد مفاد مربوط به *سندباکس نظارتی هوش مصنوعی*[۲۳] و آزمایش در شرایط واقعی نیز می‌شود. علاوه بر این، بدون خدشه به استثنای سامانه‌های هوش مصنوعی که صرفاً برای تحقیق و توسعهٔ علمی طراحی و به کار گرفته شده‌اند، هر سامانهٔ هوش مصنوعی دیگری که ممکن است برای انجام هر گونه فعالیت تحقیق و توسعه به کار رود، همچنان مشمول مفاد این مقررات خواهد بود. در هر صورت، هر فعالیت تحقیق و توسعه باید مطابق استانداردهای اخلاقی و حرفه‌ای شناخته‌شده برای تحقیق علمی انجام شود و با قوانین قابل اجرای اتحادیه هماهنگ باشد.

۲۶. برای معرفی مجموعه‌ای از قواعد الزام‌آور متناسب و مؤثر برای سامانه‌های هوش مصنوعی، بی‌تردید باید از رویکرد مبتنی بر ریسک پیروی شود. این رویکرد باید نوع و محتوای این قواعد را با توجه به شدت و دامنهٔ ریسک‌هایی که سامانه‌های هوش مصنوعی می‌توانند ایجاد کنند، تنظیم کند. بنابراین لازم است که برخی از عملکردها یا روش‌های غیرقابل قبول هوش مصنوعی ممنوع شوند، الزامات مربوط به سامانه‌های هوش مصنوعی پرخطر و وظایف مربوط به اپراتورهای مرتبط تعیین شوند و الزامات شفافیت برای برخی از سامانه‌های هوش مصنوعی وضع شود.

۲۷. در حالی که رویکرد مبتنی بر ریسک، مبنایی برای مجموعه‌ای متناسب و مؤثر از قواعد الزام‌آور فراهم می‌کند، مهم است به *راهنمای اصول اخلاقی برای هوش مصنوعی قابل اعتماد* سال ۲۰۱۹ اشاره شود که توسط گروه کارشناسان مستقل هوش مصنوعی منصوب‌شده توسط کمیسیون تدوین شده است. گروه کارشناسان در این رهنمودها، هفت اصل اخلاقی غیرالزام‌آور برای هوش مصنوعی تدوین کرده است که هدف از آن‌ها تضمین قابل اعتمادبودن و سازگاری اخلاقی هوش مصنوعی است. این هفت اصل، شامل عاملیت و نظارت انسانی، استحکام فنی و ایمنی، حریم خصوصی و حاکمیت داده‌ها، شفافیت، تنوع، عدم تبعیض و انصاف، رفاه اجتماعی و محیط‌زیست و پاسخگویی هستند. با رعایت الزامات قانونی مقررات حاضر و سایر قوانین قابل اعمال اتحادیه، این رهنمودها به طراحی هوش مصنوعی منسجم، قابل اعتماد و انسان‌محور مطابق منشور و ارزش‌های بنیادین اتحادیه کمک می‌کنند.

---

23. AI Regulatory Sandboxes

سندباکس نظارتی، محیطی کنترل‌شده است که به شرکت‌های نوپا و نوآور اجازه می‌دهد محصولات یا خدمات جدید خود را در مقیاس محدود و تحت نظارت قانونگذار آزمایش کنند، بدون اینکه الزاماً تمام قوانین موجود را رعایت کنند. این ابزار به آشنایی با فناوری‌های جدید جهت تدوین قوانین مناسب کمک می‌کند.

بر اساس رهنمودهای گروه کارشناسان، عاملیت و نظارت انسانی به این معناست که سامانه‌های هوش مصنوعی به‌عنوان ابزاری برای خدمت به انسان‌ها، احترام به کرامت انسانی و خودمختاری فردی توسعه می‌یابند و مورد استفاده می‌گیرند و به‌طور مناسب، تحت کنترل و نظارت انسان‌ها قرار دارند. استحکام فنی و ایمنی به این معناست که سامانه‌های هوش مصنوعی باید به نحوی توسعه یابند و به کار گرفته شوند که در صورت مواجهه با مشکلات، مقاوم باشند و در برابر تلاش‌ها برای تغییر کاربری یا عملکرد آن‌ها به منظور استفادهٔ غیرقانونی توسط اشخاص ثالث، از خود مقاومت نشان دهند و آسیب‌های ناخواسته را به حداقل برسانند. حریم خصوصی و حاکمیت داده‌ها به این معناست که سامانه‌های هوش مصنوعی مطابق قوانین حریم خصوصی و حفاظت از داده‌ها توسعه یابند و به کار روند و داده‌های مورد پردازش از استانداردهای بالای کیفیت و یکپارچگی برخوردار باشند. شفافیت به این معناست که سامانه‌های هوش مصنوعی به گونه‌ای توسعه یابند و به کار روند که قابلیت ردیابی و توضیح‌پذیری مناسب را فراهم کنند به نحوی که انسان‌ها از تعامل یا ارتباط خود با سامانهٔ هوش مصنوعی آگاه باشند و همچنین استقراردهندگان از قابلیت‌ها و محدودیت‌های آن سیستم و اشخاص متأثر، از حقوق خود آگاه شوند. تنوع، عدم تبعیض و انصاف به این معناست که سامانه‌های هوش مصنوعی به گونه‌ای توسعه یابند و به کار روند که شامل بازیگران متنوع شوند و دسترسی برابر، برابری جنسیتی و تنوع فرهنگی را ارتقاء دهند، در حالی که از آثار تبعیض‌آمیز و تعصبات ناعادلانه که طبق قوانین اتحادیه یا قوانین ملی ممنوع هستند، اجتناب شود. رفاه اجتماعی و محیط‌زیست به این معناست که سامانه‌های هوش مصنوعی به گونه‌ای توسعه یافته و به کار روند که به‌صورت پایدار و دوستدار محیط‌زیست و در راستای بهره‌مندی تمام انسان‌ها باشد، در حالی که اثرات بلندمدت آن‌ها بر فرد، جامعه و دموکراسی تحت نظارت و ارزیابی قرار گیرد. اعمال این اصول باید در طراحی و استفاده از مدل‌های هوش مصنوعی مدنظر قرار گیرد، هرچند در هر صورت باید به‌عنوان مبنای تدوین کدهای رفتاری در چارچوب این مقررات عمل شود. تمامی ذی‌نفعان، ازجمله صنعت، دانشگاه، جامعهٔ مدنی و سازمان‌های استانداردسازی، ترغیب می‌شوند که اصول اخلاقی را در توسعهٔ بهترین شیوه‌ها و استانداردهای داوطلبانه مدنظر قرار دهند.

۲۸. علاوه بر کاربردهای مفید فراوان هوش مصنوعی، این فناوری می‌تواند مورد سوءاستفاده قرار گیرد و ابزارهای جدید و قدرتمندی برای روش‌های دستکاری، استثمار و کنترل اجتماعی فراهم آورد. چنین روش‌هایی به‌ویژه زیان‌بار و سوءاستفاده‌آمیز هستند و باید ممنوع شوند زیرا با ارزش‌های اتحادیهٔ اروپا مبنی بر احترام به کرامت انسانی، آزادی، برابری، دموکراسی و حاکمیت قانون و حقوق بنیادین مندرج در منشور حقوق اساسی اتحادیهٔ اروپا، ازجمله حق عدم تبعیض، حفاظت از داده‌ها، حریم خصوصی و حقوق کودک، مغایرت دارند.

۲۹. روش‌های دستکاری‌شده مبتنی بر هوش مصنوعی می‌توانند برای متقاعدکردن افراد به انجام رفتارهای ناخواسته یا فریب‌دادن آن‌ها از طریق راه‌هایی که خودآگاهی، تصمیم‌گیری و انتخاب‌های آزاد آن‌ها را تضعیف می‌کند، به کار روند. عرضه، به‌کارگیری یا استفاده از برخی سامانه‌های هوش مصنوعی که هدف یا تأثیر آن‌ها، تغییر رفتارهای انسان باشد، به‌طوری که منجر به آسیب‌های قابل‌توجهی، به‌ویژه آثار نامطلوب مهم بر سلامت جسمی، روانی یا منافع مالی شود، به‌طور خاص، خطرناک و ممنوع است. چنین سامانه‌های هوش مصنوعی از اجزای نامحسوس مانند محرک‌های صوتی، تصویری و ویدئویی استفاده می‌کنند که افراد قادر به درک آن‌ها نیستند زیرا این محرک‌ها فراتر از ادراک انسان هستند، یا از سایر تکنیک‌های دستکاری‌کننده یا فریبنده بهره می‌برند که خودمختاری، تصمیم‌گیری یا انتخاب آزاد افراد را تضعیف یا مختل می‌کنند به روشی که افراد از این تکنیک‌ها آگاه نیستند یا در صورت آگاهی، همچنان فریب خورده‌اند یا قادر به کنترل یا مقاومت در برابر آن‌ها نیستند. این امر می‌تواند مثلاً با استفاده از رابط‌های مغز و ماشین یا واقعیت مجازی تسهیل شود زیرا آن‌ها امکان کنترل بالاتری از آنچه به افراد ارائه می‌شود، فراهم می‌کنند، به‌طوری که ممکن است به‌طور قابل‌توجهی رفتار آن‌ها را به روش مضر تحریف کنند. علاوه بر این، ممکن است سامانه‌های هوش مصنوعی از آسیب‌پذیری‌های فرد یا گروه خاصی از افراد به دلیل سن، معلولیت (طبق دستورالعمل ۲۰۱۹/۸۸۲ اتحادیهٔ اروپا)[۲۴] یا وضعیت اجتماعی یا اقتصادی خاصی که احتمالاً این افراد را در برابر بهره‌کشی آسیب‌پذیرتر می‌کند، مانند افرادی که در فقر شدید زندگی می‌کنند یا اقلیت‌های قومی یا مذهبی سوءاستفاده کند. ممکن است چنین سامانه‌های هوش مصنوعی با هدف یا اثری به کار گرفته یا استفاده شوند که منجر به تغییر اساسی رفتار فرد شود و به او یا سایر افراد یا گروه‌ها، آسیب‌های قابل‌توجهی وارد کند، ازجمله آسیب‌هایی که ممکن است در طول زمان رخ دهد؛ بنابراین باید ممنوع شوند. در مواردی که تحریف ناشی از عواملی خارجی و خارج از کنترل ارائه‌دهنده یا به‌کارگیرندهٔ سامانهٔ هوش مصنوعی باشد، یعنی عواملی که ممکن است به‌طور معقول قابل پیش‌بینی نباشند و بنابراین امکان کاهش آن‌ها برای ارائه‌دهنده یا به‌کارگیرندهٔ سامانهٔ هوش مصنوعی وجود نداشته باشد، ممکن است نتوان فرض کرد که قصد تغییر یا سوءاستفاده از رفتار وجود دارد. با این حال، لزومی ندارد که ارائه‌دهنده یا بهره‌بردار، قصد واردکردن آسیب قابل‌توجه را داشته باشد، بلکه صرف وقوع چنین آسیبی در نتیجهٔ شیوه‌های سوءاستفاده‌آمیز یا دستکاری‌کننده مبتنی بر هوش مصنوعی برای ممنوعیت این اقدامات کافی است. قصد ممنوعیت‌های مربوط به این شیوه‌های

۲۴. دستورالعمل شمارهٔ ۲۰۱۹/۸۸۲ پارلمان و شورای اروپا، ۱۷ آوریل ۲۰۱۹ در مورد الزامات دسترسی برای محصولات و خدمات (روزنامهٔ رسمی ۱۵۱، ۲۰۱۹/۶/۷، ص ۷۰).

هوش مصنوعی مکمل مقررات موجود در دستورالعمل شمارهٔ ۲۰۰۵/۲۹ پارلمان و شورای اروپا[۲۵] است که به‌ویژه شیوه‌های تجاری غیرمنصفانه که منجر به آسیب‌های اقتصادی یا مالی به مصرف‌کنندگان می‌شود، در تمامی شرایط ممنوع است، فارغ از اینکه این شیوه‌ها از طریق سامانه‌های هوش مصنوعی یا به‌طور دیگری اعمال شوند. ممنوعیت‌های شیوه‌های دستکاری و استثماری در این مقررات نباید بر شیوه‌های قانونی در زمینهٔ درمان پزشکی، مانند درمان بیماری‌های روانی یا توان‌بخشی فیزیکی تأثیر بگذارد، به شرط آنکه این شیوه‌ها مطابق قانون و استانداردهای پزشکی انجام شوند، مانند رضایت صریح افراد یا نمایندگان قانونی آن‌ها. علاوه بر این، شیوه‌های تجاری رایج و مشروع، مانند تبلیغات، که مطابق قوانین قابل اجرا هستند، نباید به‌طور خودکار به‌عنوان شیوه‌های دستکاری مضر مبتنی بر هوش مصنوعی تلقی شوند.

۳۰. سیستم‌های دسته‌بندی‌کنندهٔ زیست‌سنجی که مبتنی بر داده‌های زیست‌سنجی اشخاص حقیقی، مانند صورت یا اثر انگشت یک فرد، برای استنتاج یا استنباط عقاید سیاسی او، عضویت‌اش در اتحادیه‌های کارگری، باورهای مذهبی یا فلسفی، نژاد، زندگی جنسی یا گرایش جنسی افراد هستند، باید ممنوع شوند. این ممنوعیت شامل برچسب‌گذاری، فیلترکردن یا دسته‌بندی قانونی مجموعهٔ داده‌های زیست‌سنجی که طبق قوانین اتحادیه یا قوانین ملی به دست آمده‌اند نمی‌شود، مانند مرتب‌سازی تصاویر بر اساس رنگ مو یا رنگ چشم، که به‌عنوان مثال در حوزهٔ اجرای قانون قابل استفاده است.

۳۱. سامانه‌های هوش مصنوعی که برای ارزیابی اجتماعی افراد حقیقی توسط نهادهای عمومی یا خصوصی به کار می‌روند، می‌توانند منجر به نتایج تبعیض‌آمیز و حذف گروه‌های خاص شوند. ممکن است این سیستم‌ها حق کرامت و عدم تبعیض و همچنین ارزش‌های برابری و عدالت را نقض کنند. سامانه‌های هوش مصنوعی، افراد حقیقی یا گروه‌هایی از آن‌ها را بر اساس داده‌های مختلف مربوط به رفتار اجتماعی‌شان در زمینه‌های مختلف یا ویژگی‌های شخصی و شخصیتی شناخته‌شده، استنباط‌شده یا پیش‌بینی‌شده در دوره‌های زمانی خاص، ارزیابی یا طبقه‌بندی می‌کنند. ممکن است امتیاز اجتماعی به‌دست‌آمده از این سامانه‌های هوش مصنوعی به رفتار نامطلوب یا تبعیض‌آمیز علیه اشخاص حقیقی یا گروه‌هایی از آن‌ها در زمینه‌های اجتماعی منجر شود که هیچ ارتباطی با زمینه‌ای که داده‌ها در آن تولید یا جمع‌آوری شده‌اند، ندارد یا به رفتار نامطلوبی بینجامد که به‌طور نامتناسب یا غیرموجه، شدیدتر از رفتار اجتماعی آن‌ها ارزیابی شود. بنابراین سامانه‌های هوش مصنوعی که به چنین شیوه‌های ارزیابی غیرقابل قبول و به نتایج منفی یا نامساعد منجر می‌شوند

۲۵. دستورالعمل شمارهٔ ۲۰۰۵/۲۹ پارلمان و شورای اروپا، ۱۱ مه ۲۰۰۵ در مورد شیوه‌های تجاری ناعادلانهٔ بنگاه‌ها در قبال مصرف‌کنندگان در بازار داخلی و اصلاح دستورالعمل ۸۴/۴۵۰ شورای اروپا، دستورالعمل‌های ۹۷/۷ و ۹۸/۲۷ و۶۵/ ۲۰۰۲ پارلمان و شورای اروپا و همچنین مقررات شمارهٔ ۲۰۰۶/۲۰۰۴ پارلمان و شورای اروپا (دستورالعمل شیوه‌های تجاری ناعادلانه) (روزنامهٔ رسمی ۱۴۹، ۲۰۰۵/۶/۱۱، ص ۲۲).

باید ممنوع شوند. نباید این ممنوعیت بر ارزیابی‌های قانونی افراد حقیقی که برای هدف خاصی مطابق قوانین اتحادیه و قوانین ملی انجام می‌شوند، تأثیر بگذارد.

۳۲. استفاده از سامانه‌های هوش مصنوعی برای شناسایی زیست‌سنجی از راه دور و *زمان واقعی* اشخاص در فضاهای عمومی در راستای اجرای قانون، به‌ویژه به حقوق و آزادی‌های افراد آسیب می‌زند؛ تا جایی که می‌تواند زندگی خصوصی بخش بزرگی از جمعیت را تحت تأثیر قرار دهد، احساس نظارت دائمی ایجاد کند و به‌طور غیرمستقیم، افراد را از اعمال آزادی تجمع و سایر حقوق بنیادین بازدارد. ممکن است نارسایی‌های فنی سامانه‌های هوش مصنوعی که برای شناسایی زیست‌سنجی از راه دور اشخاص طراحی شده‌اند، به نتایج جانبدارانه منجر شود و آثار تبعیض‌آمیز داشته باشد. این نتایج جانبدارانه و آثار تبعیض‌آمیز به‌ویژه در ارتباط با سن، قومیت، نژاد، جنسیت یا ناتوانی‌ها اهمیت پیدا می‌کند. افزون بر این، آنی‌بودن آثار چنین سیستم‌هایی و محدودبودن امکان بررسی یا اصلاح پسینی در کاربرد سیستم‌هایی که به‌صورت زمان واقعی عمل می‌کنند، خطرات بیشتری برای حقوق و آزادی‌های اشخاص ذی‌ربط در بستر یا در نتیجهٔ فعالیت‌های اجرای قانون به همراه دارد.

۳۳. به‌طور کلی باید استفاده از این سیستم‌ها به منظور اجرای قانون ممنوع باشد، مگر در مواردی که به‌طور دقیق و محدود تعریف شده و استفاده از آن‌ها به‌طور قطعی برای دستیابی به منافع عمومی قابل‌توجهی ضروری باشد که اهمیت آن منافع از خطرات ناشی از آن بیشتر باشد. این موارد شامل جستجو برای قربانیان خاص جرایم ازجمله افراد مفقودشده، تهدیدات خاص به جان یا ایمنی جسمانی افراد یا تهدیدات تروریستی و شناسایی یا تعیین موقعیت مرتکبین یا مظنونین به جرایم ذکرشده در پیوست این مقررات است؛ جایی که این جرایم در دولت عضو مربوطه قابل مجازات با حکم حبس یا دستور بازداشت به مدت حداقل چهار سال باشند؛ همان طور که در قانون آن دولت عضو تعریف شده است. چنین آستانه‌ای برای حکم حبس یا دستور بازداشت طبق قوانین ملی کمک می‌کند تا اطمینان حاصل شود که جرم باید به اندازهٔ کافی جدی باشد تا استفاده از سیستم‌های شناسایی زیست‌سنجی از راه دور در زمان واقعی را به‌طور بالقوه توجیه کند. علاوه بر این، فهرست جرایم موجود در پیوست این مقررات بر اساس ۳۲ جرم مندرج در تصمیم چارچوبی شورای JHA/۲۰۰۲/۵۸۴[۲۶] است؛ با این توجه که برخی از این جرایم در عمل احتمالاً اهمیت بیشتری خواهند داشت، به‌طوری که استفاده از شناسایی زیست‌سنجی از راه دور در زمان واقعی می‌تواند برای شناسایی یا تعیین موقعیت مرتکب یا مظنون به این جرایم به‌طور معقول و متناسب ضروری باشد. همچنین تهدید فوری به جان یا ایمنی جسمانی افراد می‌تواند از اختلال جدی در زیرساخت‌های حیاتی ناشی شود، همان طور که در ماده ۲،

۲۶. تصمیم چارچوب شورا JHA/۵۸۴/۲۰۰۲ در ۱۳ ژوئن ۲۰۰۲ در مورد دستور جلب اروپایی و روش‌های استرداد بین کشورهای عضو (نشریهٔ رسمی اتحادیهٔ اروپا L 190، ۱۸.۷.۲۰۰۲، ص ۱).

بند (۴) از دستورالعمل ۲۵۵۷/۲۰۲۲ از پارلمان و شورای اروپا تعریف شده است؛[۲۷] جایی که اختلال یا تخریب چنین زیرساخت‌هایی می‌تواند تهدید فوری به جان یا ایمنی یک فرد ایجاد کند. همچنین باید این مقررات، توانایی مقامات اجرای قانون، کنترل مرزی، مهاجرت یا پناهندگی را برای انجام بررسی هویت در حضور شخص مربوطه، طبق شرایط تعیین‌شده در قوانین ملی و اتحادیه برای چنین بررسی‌هایی حفظ کند. به‌ویژه، مقامات اجرای قانون، کنترل مرزی، مهاجرت یا پناهندگی باید قادر باشند از سیستم‌های اطلاعاتی مطابق قوانین ملی یا اتحادیه برای شناسایی افرادی که در حین بررسی هویت از شناسایی خود امتناع می‌کنند یا قادر به اثبات هویت خود نیستند، استفاده کنند، بدون اینکه طبق این مقررات، مجبور به دریافت مجوز پیشین شوند. این مورد می‌تواند شامل فردی باشد که در جرم درگیر است و به دلایل مختلف ازجمله تصادف یا شرایط پزشکی قادر به افشای هویت خود به مقامات اجرای قانون نیست.

۳۴. برای اطمینان از اینکه این سیستم‌ها به شکل مسئولانه و متناسب استفاده شوند، لازم است روشن باشد که در هر یک از شرایط محدود و دقیقی که به‌طور جامع فهرست شده‌اند، باید عناصر خاصی در نظر گرفته شوند؛ ازجمله ماهیت موقعیتی که موجب درخواست شده، پیامدهای استفاده از سیستم برای حقوق و آزادی‌های افراد ذی‌ربط، و تضمین‌ها و شرایطی که برای این استفاده پیش‌بینی شده است. علاوه بر این، استفاده از سیستم‌های شناسایی زیست‌سنجی از راه دور و زمان واقعی در فضاهای عمومی برای مقاصد اجرای قانون باید صرفاً به تأیید هویت فرد مشخص و هدف‌گذاری‌شده محدود شود. این استفاده باید تنها به میزانی انجام گیرد که کاملاً ضروری است؛ چه از نظر بازهٔ زمانی، چه از نظر دامنهٔ جغرافیایی و شخصی، با توجه ویژه به شواهد یا نشانه‌های مربوط به تهدیدها، قربانیان یا مرتکبان. به‌کارگیری چنین سیستمی در فضاهای عمومی تنها زمانی مجاز است که مقام صلاحیت‌دار اجرای قانون، *ارزیابی اثرات بر حقوق بنیادین* انجام داده باشد مگر آنکه در این مقررات، خلاف آن پیش‌بینی شده باشد و سیستم در پایگاه داده‌ای که این مقررات مقرر کرده، ثبت شده باشد. همچنین پایگاه داده‌ای که افراد در آن مرجع قرار دارند، باید متناسب با هر مورد استفاده و در هر یک از شرایط یادشده باشد.

۳۵. هر بار استفاده از سیستم شناسایی زیست‌سنجی از راه دور و *زمان واقعی* در فضاهای عمومی برای مقاصد اجرای قانون باید منوط به صدور مجوز صریح و مشخص از سوی مرجع قضایی یا مرجع اداری مستقل در دولت عضو باشد؛ تصمیم این مراجع الزام‌آور است. در اصل، این مجوز باید پیش از به‌کارگیری سامانهٔ هوش مصنوعی برای شناسایی فرد یا افراد اخذ شود.

۲۷. دستورالعمل (اتحادیهٔ اروپا) ۲۵۵۷/۲۰۲۲ پارلمان اروپا و شورا در ۱۴ دسامبر ۲۰۲۲ در مورد تاب‌آوری نهادهای حیاتی و لغو دستورالعمل شورا EC/۱۱۴/۲۰۰۸ (نشریهٔ رسمی اتحادیهٔ اروپا L 333، ۲۷.۱۲.۲۰۲۲، ص ۱۶۴).

با این حال، استثناهایی در شرایط ضروری که به‌طور موجه توجیه شوند، یعنی در مواردی که نیاز به استفاده از سیستم‌ها به حدی فوری باشد که اخذ مجوز پیش از شروع استفاده عملاً ناممکن شود مجاز است. در چنین شرایطی، استفاده از سیستم باید به حداقل لازم محدود شود و تحت تضمین‌ها و شرایط مناسب قرار گیرد؛ این شرایط در قوانین ملی تعیین می‌شوند و در هر مورد فوری مشخص توسط خود مرجع اجرای قانون تبیین می‌شوند. علاوه بر این، مرجع اجرای قانون باید در چنین شرایطی، بدون تأخیر غیرموجه و حداکثر ظرف ۲۴ ساعت، ضمن بیان دلایل عدم امکان درخواست زودتر، تقاضای صدور مجوز را ارائه کند. اگر درخواست مجوز رد شود، استفاده از سیستم شناسایی زیست‌سنجی زمان واقعی که به آن مجوز وابسته است باید فوراً متوقف شود و تمام داده‌های مرتبط با آن استفاده حذف و نابود شود. این داده‌ها شامل داده‌های ورودی است که سامانهٔ هوش مصنوعی در جریان استفاده مستقیماً جمع‌آوری کرده و همچنین نتایج و خروجی‌های به‌دست‌آمده در ارتباط با آن مجوز. اما شامل داده‌های ورودی نمی‌شود که به‌طور قانونی مطابق قوانین اتحادیه یا قوانین ملی دیگر به دست آمده باشند. در هر حال، هیچ تصمیمی که برای فرد، اثر حقوقی منفی ایجاد کند نباید صرفاً بر مبنای خروجی سیستم شناسایی زیست‌سنجی از راه دور اتخاذ شود.

۳۶. به منظور اجرای وظایف مراجع ذی‌صلاح نظارت بر بازار و مراجع ملی حفاظت از داده‌ها، مطابق الزامات مقرر در این قانون و نیز قواعد ملی، باید هر مورد استفاده از سامانهٔ شناسایی زیست‌سنجی آنی به این مراجع اطلاع داده شود. مراجع مذکور که از چنین استفاده‌ای مطلع شده‌اند، باید گزارش سالانه‌ای دربارهٔ به‌کارگیری سامانه‌های شناسایی زیست‌سنجی آنی به کمیسیون ارائه کنند.

۳۷. علاوه بر این، بر اساس چارچوب کامل و مشخص مقرر در این قانون، چنین استفاده‌ای در قلمرو دولت عضو، مطابق این قانون، صرفاً در صورتی امکان‌پذیر خواهد بود که دولت عضو ذی‌ربط تصمیم گرفته باشد در مقررات تفصیلی حقوق ملی خود، به‌صراحت امکان صدور مجوز چنین استفاده‌ای را پیش‌بینی کند. بر این اساس، دولت‌های عضو، بر پایهٔ این قانون آزادند که اساساً چنین امکانی را پیش‌بینی نکنند یا آن را صرفاً در خصوص برخی از اهدافی که در این قانون به‌عنوان مبانی موجه صدور مجوز استفاده ذکر شده‌اند، مجاز بدانند. چنین قواعد ملی باید حداکثر ظرف ۳۰ روز پس از تصویب به کمیسیون ابلاغ شوند.

۳۸. استفاده از سامانه‌های هوش مصنوعی برای شناسایی زیست‌سنجی آنی و از راه دورِ اشخاص حقیقی در اماکن عمومی با هدف اجرای قانون، اساساً مستلزم پردازش داده‌های زیست‌سنجی است. مقررات این قانون که چنین استفاده‌ای را جز در موارد استثنایی ممنوع می‌کند و مبتنی بر ماده ۱۶

معاهدهٔ عملکرد اتحادیهٔ اروپا است، باید به‌عنوان قانون خاص[۲۸] نسبت به مقررات پردازش داده‌های زیست‌سنجی مندرج در ماده ۱۰ *دستورالعمل (اتحادیهٔ اروپا) ۶۸۰/۲۰۱۶* اعمال شود و به این ترتیب، استفاده از این سامانه و پردازش داده‌های زیست‌سنجی مربوطه را به‌صورت کامل و جامع تنظیم کند. بنابراین چنین استفاده و پردازشی تنها در صورتی ممکن است که با چارچوب مقرر در این قانون سازگار باشد و خارج از این چارچوب، مقامات صلاحیت‌دار (در زمانی که با هدف اجرای قانون اقدام می‌کنند) نتوانند صرفاً بر مبنای دلایل مندرج در ماده ۱۰ دستورالعمل ۶۸۰/۲۰۱۶ اتحادیهٔ اروپا، از این سامانه‌ها استفاده یا داده‌های مربوط را پردازش کنند. در این راستا، این قانون به منزلهٔ ایجاد مبنای قانونی برای پردازش داده‌های شخصی به موجب ماده ۸ دستورالعمل ۶۸۰/۲۰۱۶ اتحادیهٔ اروپا در نظر گرفته نمی‌شود. با این حال، به‌کارگیری سامانه‌های شناسایی زیست‌سنجی آنی و از راه دور در اماکن عمومی، زمانی که هدف آن اجرای قانون نباشد، حتی اگر توسط مقامات صلاحیت‌دار انجام شود، تحت شمول چارچوب ویژه‌ای که این قانون برای اجرا مقرر کرده، قرار نمی‌گیرد. از این رو استفاده از این سامانه‌ها برای اهدافی غیر از اجرای قانون، نیازی به دریافت مجوز طبق این قانون و مقررات ملی مربوط به آن مجوز ندارد.

۳۹. هر گونه پردازش داده‌های زیست‌سنجی و سایر داده‌های شخصی مرتبط با استفاده از سامانه‌های هوش مصنوعی برای شناسایی زیست‌سنجی، بجز در موارد استفاده از سامانه‌های شناسایی زیست‌سنجی آنی و از راه دور در اماکن عمومی به منظور اجرای این قانون، باید همچنان تمام الزامات مندرج در ماده ۱۰ *دستورالعمل (اتحادیهٔ اروپا) ۶۸۰/۲۰۱۶* را رعایت کند. برای اهدافی غیر از اجرای قانون، بند ۱ ماده ۹ *دستورالعمل (اتحادیهٔ اروپا) ۶۷۹/۲۰۱۶* و بند ۱ ماده ۱۰ *دستورالعمل (اتحادیهٔ اروپا) ۱۷۲۵/۲۰۱۸* پردازش داده‌های زیست‌سنجی را بجز در موارد استثنایی محدودشده در همین مواد، ممنوع اعلام کرده‌اند. در اجرای بند ۱ماده ۹ دستورالعمل (اتحادیهٔ اروپا) ۶۷۹/۲۰۱۶، استفاده از شناسایی زیست‌سنجی از راه دور برای مقاصد غیر از اجرای قانون، پیش‌تر با ممنوعیت صادرشده از سوی مراجع ملی حفاظت از داده‌ها مواجه شده است.

۴۰. مطابق قسمت (الف) ماده ۶ *پروتکل شمارهٔ ۲۱* دربارهٔ *جایگاه بریتانیا و ایرلند در حوزهٔ آزادی، امنیت و عدالت* که به *معاهدهٔ اتحادیهٔ اروپا* و *معاهدهٔ عملکرد اتحادیهٔ اروپا* پیوست شده است، ایرلند موظف به رعایت مواد زیر از معاهدات مذکور نیست: بند ۱ ماده ۵، بند نخست، جزء (چ) تا آنجا که به استفاده از سامانه‌های دسته‌بندی زیست‌سنجی برای فعالیت‌های مرتبط با همکاری‌های پلیسی و قضایی در امور کیفری مربوط می‌شود؛ بند ۱ ماده ۵، بند نخست، جزء (ت)

۲۸. بارت lex specialis در حقوق به معنای *قانون خاص* یا *قاعدهٔ خاص* است. در اصطلاح حقوقی، این واژه بیان می‌کند در صورت تعارض بین یک قانون با قاعدهٔ عام و یک قانون با قاعدهٔ خاص، قانون یا قاعدهٔ خاص باید بر قانون عام (lex generalis) ارجحیت داشته باشد.

تا آنجا که شامل استفاده از سامانه‌های هوش مصنوعی موضوع آن حکم است؛ جزء (ح) همان بند؛ بندهای ۲ تا ۶ ماده ۵؛ و بند ۱۰ ماده ۲۶. این مواد بر اساس ماده ۱۶ معاهدهٔ عملکرد اتحادیهٔ اروپا تصویب شده و به پردازش داده‌های شخصی توسط دولت‌های عضو و انجام فعالیت‌هایی مربوط می‌شوند که ذیل فصل چهارم یا پنجم، عنوان V بخش سوم معاهدهٔ عملکرد اتحادیهٔ اروپا معاهده قرار دارند. اما در مواردی که ایرلند طبق معاهده ملزم به رعایت مقررات مربوط به انواع همکاری قضایی در امور کیفری یا همکاری پلیسی که مستلزم تبعیت از مقررات مبتنی بر ماده ۱۶ معاهدهٔ عملکرد اتحادیهٔ اروپا هستند نباشد، تعهدی به اجرای این مواد نیز نخواهد داشت.

۴۱. مطابق بند ۲ و بند (الف) ماده ۲ *پروتکل شمارهٔ ۲۲* دربارهٔ *جایگاه دانمارک* که به *معاهدهٔ اتحادیهٔ اروپا* و *معاهدهٔ عملکرد اتحادیهٔ اروپا* پیوست شده است، دانمارک موظف به رعایت مواد زیر از معاهدات مذکور نیست: بند ۱ ماده ۵، بند نخست، جزء (g) تا آنجا که به استفاده از سامانه‌های دسته‌بندی زیست‌سنجی برای فعالیت‌های مرتبط با همکاری‌های پلیسی و قضایی در امور کیفری مربوط می‌شود؛ بند ۱ ماده ۵، بند نخست، جزء (d) تا آنجا که شامل استفاده از سامانه‌های هوش مصنوعی موضوع آن حکم است؛ جزء (h) همان بند؛ بندهای ۲ تا ۶ ماده ۵؛ و بند ۱۰ ماده ۲۶. این مواد بر اساس ماده ۱۶ معاهدهٔ عملکرد اتحادیهٔ اروپا تصویب شده و به پردازش داده‌های شخصی توسط دولت‌های عضو و انجام فعالیت‌هایی مربوط می‌شوند که ذیل فصل چهارم یا پنجم، عنوان V بخش سوم معاهدهٔ عملکرد اتحادیهٔ اروپا معاهده قرار دارند.

۴۲. با رعایت اصل *برائت*، اشخاص حقیقی در اتحادیه باید همواره بر اساس رفتار واقعی خود قضاوت شوند. اشخاص حقیقی نباید صرفاً بر مبنای رفتار پیش‌بینی‌شده توسط هوش مصنوعی، که تنها بر پایهٔ نمایه‌سازی (پروفایلینگ)، ویژگی‌های شخصیتی یا خصایص آنان مانند تابعیت، محل تولد، محل اقامت، تعداد فرزندان، میزان بدهی یا نوع خودرو، بدون وجود ظنّ معقول نسبت به مشارکت آنان در فعالیت مجرمانه مبتنی بر حقایق عینی و قابل تأیید و بدون ارزیابی انسانی قضاوت شوند. از این رو انجام ارزیابی‌های ریسک در مورد اشخاص حقیقی با هدف سنجش احتمال ارتکاب جرم یا پیش‌بینی وقوع جرم بالفعل یا بالقوه که صرفاً بر اساس نمایه‌سازی یا ارزیابی ویژگی‌ها و خصایص شخصیتی آنان صورت گیرد، باید ممنوع باشد. در هر حال، این ممنوعیت شامل ارزیابی‌های ریسکی که بر مبنای نمایه‌سازی افراد یا ویژگی‌ها و خصایص شخصیتی آنان انجام نمی‌شود، نمی‌شود؛ ازجمله، سامانه‌های هوش مصنوعی که از تحلیل ریسک برای ارزیابی احتمال وقوع تقلب مالی توسط مؤسسات بر اساس تراکنش‌های مشکوک استفاده می‌کنند، یا ابزارهای تحلیل ریسک که با اتکا بر مسیرهای شناخته‌شدهٔ قاچاق، احتمال شناسایی محل مواد مخدر یا کالاهای غیرقانونی را توسط مقامات گمرکی پیش‌بینی می‌کنند.

۴۳. عرضه در بازار، به بهره‌برداری‌رساندن برای آن هدف خاص یا استفاده از سامانه‌های هوش مصنوعی که از طریق گردآوری غیرهدفمند تصاویر چهره از اینترنت یا تصاویر دوربین‌های مداربسته به ایجاد یا گسترش پایگاه‌های دادهٔ شناسایی چهره می‌پردازند، باید ممنوع شود زیرا چنین رویه‌ای موجب تشدید احساس نظارت همگانی شده و می‌تواند به نقض فاحش حقوق بنیادین ازجمله حق بر حریم خصوصی منجر شود.

۴۴. از آنجا که ابراز احساسات در فرهنگ‌ها و موقعیت‌های مختلف و حتی در فرد واحد، تفاوت‌های چشمگیری دارد، دربارهٔ مبنای علمی سامانه‌های هوش مصنوعی که با هدف شناسایی یا استنباط احساسات طراحی شده‌اند، نگرانی‌های جدی وجود دارد. از مهم‌ترین ضعف‌های این سامانه‌ها می‌توان به قابلیت اعتماد محدود، فقدان دقت کافی و تعمیم‌پذیری پایین اشاره کرد. بنابراین سامانه‌های هوش مصنوعی که بر اساس داده‌های زیست‌سنجی به شناسایی یا استنباط احساسات یا نیت‌های افراد حقیقی می‌پردازند، می‌توانند منجر به نتایج تبعیض‌آمیز شوند و حقوق و آزادی‌های افراد را نقض کنند. با توجه به عدم توازن قدرت در محیط‌های کاری یا آموزشی و ماهیت مداخله‌گرایانهٔ این سامانه‌ها، استفاده از آن‌ها ممکن است باعث رفتار زیان‌بار یا ناعادلانه نسبت به برخی افراد یا گروه‌ها شود. بنابراین باید عرضه در بازار، به‌کارگیری یا استفاده از سامانه‌های هوش مصنوعی که برای تشخیص وضعیت عاطفی افراد در محیط‌های کاری و آموزشی طراحی شده‌اند، ممنوع شود. این ممنوعیت شامل سامانه‌هایی نمی‌شود که صرفاً به دلایل پزشکی یا ایمنی مانند کاربردهای درمانی عرضه می‌شوند.

۴۵. نباید رویه‌هایی که مطابق قوانین اتحادیهٔ اروپا ازجمله قوانین حفاظت از داده‌ها، مقابله با تبعیض، حمایت از مصرف‌کننده و رقابت ممنوع شده‌اند، مشمول تأثیر این مقررات قرار گیرند.

۴۶. سامانه‌های هوش مصنوعی پرخطر باید تنها در صورتی در بازار اتحادیه عرضه، به‌کار گرفته یا مورد استفاده قرار گیرند که با مجموعه‌ای از الزامات اجباری مطابقت داشته باشند. این الزامات باید تضمین کنند که سامانه‌های هوش مصنوعی پرخطر موجود در اتحادیه یا خروجی آن‌ها که به هر نحو در اتحادیه به کار می‌روند، برای منافع عمومی مهم اتحادیه، همان گونه که توسط قوانین اتحادیه به رسمیت شناخته شده و حمایت می‌شوند، خطری غیرقابل قبول ایجاد نکنند. بر اساس چارچوب قانونگذاری جدید، همان گونه که در اطلاعیهٔ کمیسیون با عنوان *راهنمای آبی رنگ برای اجرای قوانین محصول اتحادیهٔ اروپا ۲۰۲۲*[۲۹] تشریح شده است، قاعدهٔ کلی این است که امکان دارد بیش

۲۹. (روزنامهٔ رسمی ۲۴۷، ۲۰۲۲/۶/۲۹، ص ۱).

از یک متن قانونی از قوانین هماهنگ ساز اتحادیه، مانند مقررات ۷۴۵ / ۲۰۱۷[۳۰] و ۷۴۶ / ۲۰۱۷[۳۱] و دستورالعمل ۴۲ /۲۰۱۶[۳۲] پارلمان و شورای اروپا برای یک محصول قابل اعمال باشد زیرا عرضه یا به‌کارگیری محصول، تنها زمانی امکان‌پذیر است که محصول با تمام قوانین هماهنگ‌ساز اتحادیه که بر آن اعمال می‌شود، مطابقت داشته باشد. برای تضمین همخوانی و اجتناب از مسئولیت‌های اداری یا هزینه‌های غیرضروری، ارائه‌دهندگان محصولی که شامل یک یا چند سامانهٔ هوش مصنوعی پرخطر و مشمول الزامات این مقررات و قوانین هماهنگ‌ساز اتحادیه مندرج در پیوست این مقررات هستند، باید در تصمیم‌گیری‌های عملیاتی خود دربارهٔ نحوهٔ تضمین مطابقت محصول با تمام الزامات قوانین هماهنگ ساز اتحادیه، انعطاف داشته باشند و این امر به شیوه‌ای بهینه انجام شود. سامانه‌های هوش مصنوعی که به‌عنوان پرخطر شناخته می‌شوند، باید محدود به آن‌هایی باشند که تأثیر زیان‌بار قابل‌توجهی بر سلامت، ایمنی و حقوق بنیادین افراد در اتحادیه دارند و این محدودیت باید هر گونه محدودیت احتمالی در تجارت بین‌المللی را به حداقل برساند.

۴۷. سامانه‌های هوش مصنوعی به‌ویژه هنگامی که به‌عنوان اجزای ایمنی محصولات به کار گرفته می‌شوند، می‌توانند تأثیرات نامطلوبی بر سلامت و ایمنی افراد داشته باشند. در راستای اهداف قوانین هماهنگ‌ساز اتحادیهٔ اروپا در زمینهٔ تسهیل گردش آزاد کالا در بازار داخلی و تضمین آن که تنها کالاهای ایمن و منطبق با الزامات وارد بازار شوند، اهمیت دارد که از مخاطرات ایمنی ناشی از محصول به‌طور کلی و به شکل خاص در اثر اجزای دیجیتال آن ازجمله سامانه‌های هوش مصنوعی، به‌درستی پیشگیری شود و کاهش یابد. برای مثال، *روبات‌های خودمختار روزافزون*[۳۳] در حوزهٔ تولید و در زمینهٔ کمک و مراقبت شخصی باید قادر باشند در محیط‌های پیچیده به‌طور ایمن فعالیت کنند و وظایف خود را انجام دهند. همچنین در بخش سلامت که اهمیت حفظ جان و سلامت افراد به‌طور خاص برجسته است، سیستم‌های تشخیصی پیشرفته و سیستم‌هایی که از تصمیم‌گیری انسانی پشتیبانی می‌کنند، باید قابل اعتماد و دقیق باشند.

---

۳۰. «مقررات شمارهٔ ۷۴۵/۲۰۱۷ پارلمان اروپا و شورای اروپا در ۵ آوریل ۲۰۱۷ در خصوص تجهیزات پزشکی، با اصلاح دستورالعمل شمارهٔ EC/۸۳/۲۰۰۱، مقررات کمیسیون اروپا به شمارهٔ ۲۰۰۲/۱۷۸ و ۲۰۰۹/۱۲۲۳ و با لغو دستورالعمل‌های شورا به شماره‌های EEC/۳۸۵/۹۰ و EEC/۴۲/۹۳» (روزنامهٔ رسمی ۱۱۷، ۲۰۱۷/۵/۵، ص ۱).

۳۱. «مقررات شمارهٔ ۷۴۶/۲۰۱۷ پارلمان اروپا و شورای اروپا در ۵ آوریل ۲۰۱۷ در خصوص تجهیزات پزشکی تشخیصی IVD (آزمایش‌های ترکیبی) و با لغو دستورالعمل EC/۷۹/۹۸ و تصمیم کمیسیون EU/۲۲۷/۲۰۱۰ » (روزنامهٔ رسمی ۱۱۷، ۲۰۱۷/۵/۵، ص ۱۷۶).

۳۲. «دستورالعمل EC/۴۲/۲۰۰۶ پارلمان اروپا و شورای اروپا در ۱۷ مه ۲۰۰۶ در خصوص ماشین‌آلات و با اصلاح دستورالعمل EC/۱۶/۹۵» (روزنامهٔ رسمی ۱۵۷، ۲۰۰۶/۶/۹، ص ۲۴).

33. Increasingly autonomous robots

۴۸. میزان تأثیرات زیان‌آور ناشی از سامانهٔ هوش مصنوعی بر حقوق بنیادینی که منشور اتحادیهٔ اروپا از آن‌ها حمایت می‌کند اهمیت ویژه‌ای دارد، به‌ویژه هنگامی که قرار باشد که سامانهٔ هوش مصنوعی به‌عنوان سیستم *پرخطر* طبقه‌بندی شود. این حقوق شامل حق کرامت انسانی، احترام به زندگی خصوصی و خانوادگی، حمایت از داده‌های شخصی، آزادی بیان و دسترسی به اطلاعات، آزادی تجمع و انجمن‌سازی، حق برابری و عدم تبعیض، حق آموزش، حمایت از مصرف‌کننده، حقوق کارگران، حقوق افراد دارای معلولیت، برابری جنسیتی، حقوق مالکیت فکری، حق برخورداری از روش‌های مؤثر جبران خسارت و محاکمهٔ عادلانه، حق دفاع و اصل برائت، و حق مدیریت شایسته می‌شود. علاوه بر این حقوق، لازم است به حقوق ویژهٔ کودکان نیز توجه شود که در ماده ۲۴ منشور و همچنین در *کنوانسیون حقوق کودک سازمان ملل متحد* تصریح شده‌اند و در *نظر تفسیری شمارهٔ ۲۵ کمیتهٔ حقوق کودک* در خصوص محیط دیجیتال، به‌طور ویژه توسعه یافته‌اند. این اسناد به آسیب‌پذیری‌های کودکان و فراهم‌کردن حمایت و مراقبت‌های لازم برای رفاه آن‌ها تأکید و توجه دارند. همچنین حق بنیادین برخورداری از سطح بالای حفاظت از محیط‌زیست که در منشور به رسمیت شناخته شده و در سیاست‌های اتحادیه به اجرا درآمده است، باید هنگام ارزیابی شدت زیان احتمالی سامانهٔ هوش مصنوعی به‌ویژه در ارتباط با سلامت و ایمنی افراد مورد توجه قرار گیرد.

۴۹. در مورد سامانه‌های هوش مصنوعی پرخطر که به‌عنوان یکی از اجزای ایمنی محصولات یا سیستم‌ها عمل می‌کنند، یا خودشان محصول یا سیستمی محسوب می‌شوند که تحت پوشش مقررات و دستورالعمل‌های پارلمان و شورای اروپا به شماره‌های ۲۰۰۸/۳۰۰[۳۴]، ۲۰۱۳ /۱۶۷[۳۵] ۲۰۱۳/ ۱۶۸[۳۶]

۳۴. «مقررات شمارهٔ ۲۰۰۸/۳۰۰ پارلمان اروپا و شورای اروپا در ۱۱ مارس ۲۰۰۸ دربارهٔ قواعد مشترک در حوزهٔ امنیت هوانوردی غیرنظامی و با لغو مقررات کمیسیون اروپا به شمارهٔ ۲۰۰۲/۲۳۲۰» (روزنامهٔ رسمی ۹۷، ۲۰۰۸/۴/۹، ص ۷۲).

۳۵. «مقررات شمارهٔ ۲۰۱۳/۱۶۷ پارلمان اروپا و شورای اروپا در ۵ فوریهٔ ۲۰۱۳ در خصوص تأیید و نظارت بر بازار وسایل نقلیهٔ کشاورزی و جنگل‌داری» (روزنامهٔ رسمی ۶۰، ۲۰۱۳/۳/۲، ص ۱).

۳۶. «مقررات شمارهٔ ۲۰۱۳/۱۶۸ پارلمان اروپا و شورای اروپا در ۱۵ ژانویهٔ ۲۰۱۳ در خصوص تأیید و نظارت بر بازار وسایل نقلیهٔ دو یا سه چرخ و چهارچرخ‌های کوچک» (روزنامهٔ رسمی ۶۰، ۲۰۱۳/۳/۲، ص ۵۲).

۲۰۱۴ /۹۰،[۳۷] ۲۰۱۶ /۷۹۷،[۳۸] ۲۰۱۸ /۸۵۸،[۳۹] ۲۰۱۸ /۱۱۳۹،[۴۰] ۲۰۱۹ /۲۱۴۴[۴۱] قرار می‌گیرند، مناسب است که این مقررات اصلاح شوند تا اطمینان حاصل شود که کمیسیون، با توجه به ویژگی‌های فنی و مقرراتی هر بخش و بدون تداخل با ساختارهای موجود حکمرانی، ارزیابی انطباق، مکانیزم‌ها و نهادهای اجرای تعیین‌شده در آن‌ها، الزامات اجباری مربوط به سامانه‌های هوش مصنوعی پرخطر مندرج در این مقررات را هنگام تصویب هر گونه مصوبات تفویضی یا اجرایی مرتبط در چارچوب آن مقررات مدنظر قرار می‌دهد.

۵۰. در خصوص سامانه‌های هوش مصنوعی که به‌عنوان اجزای ایمنی محصولات عمل می‌کنند یا خودشان محصولی هستند که مشمول برخی قوانین هماهنگ‌ساز اتحادیه هستند و در پیوست این مقررات فهرست شده‌اند، مناسب است که طبق این مقررات به‌عنوان سیستم‌های پرخطر طبقه‌بندی شوند، مشروط بر آنکه محصول مربوطه تحت فرآیند ارزیابی انطباق با نهاد ثالث ارزیابی انطباق، مطابق آن قوانین هماهنگ‌ساز قرار گیرد. به‌طور مشخص، چنین محصولاتی شامل ماشین‌آلات، اسباب‌بازی‌ها، آسانسورها، تجهیزات و سیستم‌های حفاظتی برای استفاده در محیط‌های دارای خطر انفجار، تجهیزات رادیویی، تجهیزات تحت فشار، تجهیزات قایق‌های تفریحی، تأسیسات تله‌کابین، وسایل سوزانندهٔ سوخت‌های گازی، تجهیزات پزشکی، تجهیزات پزشکی تشخیصی IVD (آزمایش‌های ترکیبی)،

۳۷. «دستورالعمل شمارهٔ EU/۹۰/۲۰۱۴ پارلمان اروپا و شورای اروپا در ۲۳ ژوئیهٔ ۲۰۱۴ در خصوص تجهیزات دریایی و با لغو دستورالعمل شورای اوپا به شمارهٔ EC/۹۸/۹۶» (روزنامهٔ رسمی ۲۵۷، ۲۰۱۴/۸/۲۸، ص ۱۴۶).

۳۸. «دستورالعمل EU/۷۹۷/۲۰۱۶ پارلمان اروپا و شورای اروپا در ۱۱ مه ۲۰۱۶ دربارهٔ قابلیت تعامل سیستم ریلی درون اتحادیهٔ اروپا» (روزنامهٔ رسمی ۱۳۸، ۲۰۱۶/۵/۲۶، ص ۴۴).

۳۹. «مقررات شمارهٔ ۸۵۸/۲۰۱۸ پارلمان اروپا و شورای اروپا در ۳۰ مه ۲۰۱۸ در خصوص تأیید و نظارت بر بازار وسایل نقلیهٔ موتوری و تریلرهای آن‌ها، و همچنین سیستم‌ها، قطعات و واحدهای فنی مستقل مورد نظر برای چنین وسایلی، با اصلاح مقررات شمارهٔ ۲۰۰۷/۷۱۵ و شمارهٔ ۲۰۰۹/۵۹۵ و با لغو دستورالعمل EC/۴۶/۲۰۰۷» (روزنامهٔ رسمی ۱۵۱، ۲۰۱۸/۶/۱۴، ص ۱).

۴۰. «مقررات شمارهٔ ۱۱۳۹/۲۰۱۸ پارلمان اروپا و شورای اروپا در ۴ ژوئیهٔ ۲۰۱۸ دربارهٔ قواعد مشترک در حوزهٔ هوانوردی غیرنظامی و تأسیس آژانس ایمنی هوانوردی اتحادیهٔ اروپا، با اصلاح مقررات شمارهٔ ۲۰۰۵/۲۱۱۱ (EC)، شمارهٔ ۲۰۰۸/۱۰۰۸، شمارهٔ ۲۰۱۰/۹۹۶، شمارهٔ ۲۰۱۴/۳۷۶ و دستورالعمل‌های EU/۳۰/۲۰۱۴ و EU/۵۳/۲۰۱۴ پارلمان و شورای اروپا و با لغو مقررات شمارهٔ ۲۰۰۴/۵۵۲ و شمارهٔ ۲۰۰۸/۲۱۶ پارلمان و شورای اروپا و مقررات شورای شمارهٔ ۹۱/۳۹۲۲» (روزنامهٔ رسمی ۲۱۲، ۲۰۱۸/۸/۲۲، ص ۱).

۴۱. «مقررات شمارهٔ ۲۱۴۴/۲۰۱۹ پارلمان اروپا و شورای اروپا در ۲۷ نوامبر ۲۰۱۹ دربارهٔ الزامات تأیید نوع برای وسایل نقلیهٔ موتوری و تریلرهای آن‌ها، و سیستم‌ها، قطعات و واحدهای فنی مستقل مورد نظر برای چنین وسایلی، با توجه به ایمنی عمومی و حفاظت از سرنشینان وسایل نقلیه و کاربران آسیب‌پذیر جاده، با اصلاح مقررات شمارهٔ ۸۵۸/۲۰۱۸ پارلمان و شورای اروپا و با لغو مقررات شمارهٔ ۲۰۰۹/۷۸، شمارهٔ ۲۰۰۹/۷۹ و شمارهٔ ۲۰۰۹/۶۶۱ پارلمان و شورای اروپا و مقررات کمیسیون شمارهٔ ۲۰۰۹/۶۳۱، شمارهٔ ۲۰۱۰/۴۰۶، شمارهٔ ۲۰۱۰/۶۷۲، شمارهٔ ۲۰۱۰/۱۰۰۳، شمارهٔ ۲۰۱۰/۱۰۰۵، شمارهٔ ۲۰۱۰/۱۰۰۸، شمارهٔ ۲۰۱۰/۱۰۰۹، شمارهٔ ۲۰۱۱/۱۹، شمارهٔ ۲۰۱۱/۱۰۹، شمارهٔ ۲۰۱۱/۴۵۸، شمارهٔ ۲۰۱۲/۶۵، شمارهٔ ۲۰۱۲/۱۳۰، شمارهٔ ۲۰۱۲/۳۴۷، شمارهٔ ۲۰۱۲/۳۵۱، شمارهٔ ۲۰۱۲/۱۲۳۰ و شمارهٔ ۱۶۶/۲۰۱۵» (روزنامهٔ رسمی ۳۲۵، ۲۰۱۹/۱۲/۱۶، ص ۱).

وسایل نقلیهٔ موتوری و هواپیماها می‌شوند.

۵۱. طبقه‌بندی یک سامانهٔ هوش مصنوعی به‌عنوان سامانهٔ *پرخطر* طبق این قانون، الزاماً به این معنا نیست که محصولی که هوش مصنوعی بخشی از ایمنی آن است یا خودِ سامانه به‌عنوان محصول شناخته می‌شود، طبق معیارهای مقررات هماهنگ‌ساز اتحادیهٔ اروپا نیز *پرخطر* محسوب شود. این موضوع به‌ویژه در مورد مقررات ۷۴۵ /۲۰۱۷ و ۷۴۶ /۲۱۰۷ صدق می‌کند زیرا در این مقررات، برای محصولات با ریسک متوسط و پرخطر، انجام ارزیابی انطباق توسط نهاد مستقل، الزامی شده است.

۵۲. در خصوص سامانه‌های هوش مصنوعی مستقل یعنی سامانه‌های پرخطری که نه جزء ایمنی محصولات به‌شمار می‌روند و نه خود به‌عنوان محصول شناخته می‌شوند، مناسب است آن‌ها در صورتی جزء سامانه‌های *پرخطر* طبقه‌بندی شوند که با توجه به هدف موردنظر از به‌کارگیری‌شان، خطر بالایی از حیث واردآوردن آسیب به سلامت و ایمنی اشخاص یا حقوق بنیادین آنان ایجاد کنند. در این ارزیابی باید هم شدتِ آسیب احتمالی و هم احتمال وقوع آن مورد توجه قرار گیرد. چنین سامانه‌هایی تنها در حوزه‌های مشخص و از پیش تعریف‌شده‌ای که در این قانون ذکر شده‌اند، پرخطر محسوب می‌شوند. شناسایی این سامانه‌ها بر مبنای همان روش‌شناسی و معیارهایی انجام می‌گیرد که برای هر گونه اصلاح آتی فهرست سامانه‌های پرخطر نیز پیش‌بینی خواهد شد. این اصلاح به اختیار کمیسیون باید از طریق تصویب *اعمال تفویضی*[۴۲] و به منظور همگام‌سازی با سرعت بالای تحولات فناورانه و نیز تغییرات احتمالی در کاربرد سامانه‌های هوش مصنوعی انجام گیرد.

۵۳. می‌بایست به این نکته توجه شود که در برخی موارد، سامانه‌های هوش مصنوعی در حوزه‌های از پیش تعیین‌شدهٔ این قانون ممکن است خطر قابل‌توجهی برای منافع حقوقی محافظت‌شده ایجاد نکنند، چرا که تأثیر چشمگیری بر تصمیم‌گیری ندارند یا به این منافع آسیبی جدی نمی‌رسانند. به موجب این قانون، سامانه‌ای که تأثیر قابل‌توجهی بر نتیجهٔ تصمیم‌گیری ندارد، به معنای آن است که خروجی تصمیم‌گیری، چه انسانی و چه خودکار، تحت تأثیر ماهیت سامانه قرار نمی‌گیرد. ممکن است چنین سامانه‌ای زمانی وجود داشته باشد که یکی از شرایط زیر برقرار باشد: شرط اول این است که سامانه برای انجام وظایف رویه‌ای و محدود طراحی شده باشد، مانند تبدیل داده‌های ساختارنیافته به داده‌های ساختاریافته، دسته‌بندی اسناد ورودی در گروه‌های مشخص، یا شناسایی موارد تکراری در میان تعداد زیادی درخواست. این نوع وظایف به دلیل محدودیت دامنهٔ‌شان، تنها خطرات اندکی ایجاد می‌کنند و حتی در صورت استفاده در

۴۲. عبارت Delegated acts یا *اعمال تفویضی* در نظام حقوقی اتحادیهٔ اروپا، به تصمیمات حقوقی الزام‌آوری گفته می‌شود که توسط کمیسیون اروپا بر اساس اختیاری که از سوی قانونگذار اتحادیه (پارلمان و شورای اتحادیهٔ اروپا) به آن تفویض شده است، تصویب می‌شوند. این ابزار به کمیسیون اجازه می‌دهد تا برخی از مقررات غیراساسی یک سند قانونی (مانند قانون یا دستورالعمل) را تکمیل یا اصلاح کند، بدون آنکه لازم باشد کل فرآیند قانونگذاری مجدد طی شود.

زمینه‌ای که در پیوست این قانون به‌عنوان کاربرد پرخطر فهرست شده است، میزان خطر آن‌ها افزایش نمی‌یابد. شرط دوم این است که وظیفه‌ای که سامانهٔ هوش مصنوعی انجام می‌دهد، به منظور بهبود نتیجهٔ فعالیت انسانی قبلی طراحی شده باشد؛ فعالیتی که ممکن است با اهداف و کاربردهای پرخطر ذکرشده در پیوست این قانون مرتبط باشد. با توجه به این ویژگی‌ها، سامانهٔ هوش مصنوعی صرفاً یک لایهٔ کمکی به فعالیت انسانی ارائه می‌دهد و در نتیجه، خطر آن کاهش می‌یابد. این شرط، برای مثال، شامل سامانه‌هایی می‌شود که هدف آن‌ها بهبود زبان به‌کاررفته در اسناد از قبل تهیه‌شده است، مانند بهبود لحن حرفه‌ای، سبک زبان علمی یا هماهنگی متن با پیام‌دهی یک برند خاص. شرط سوم این است که سامانهٔ هوش مصنوعی برای شناسایی الگوهای تصمیم‌گیری یا انحراف از الگوهای پیشین تصمیم‌گیری طراحی شده باشد. در این حالت، خطر کاهش می‌یابد زیرا سامانهٔ هوش مصنوعی بر اساس ارزیابی انسانی قبلی عمل می‌کند و قرار نیست آن را جایگزین یا تحت تأثیر قرار دهد و از این رو بررسی انسانی مناسب انجام می‌شود. نمونه‌ای از چنین سامانه‌هایی، آن‌هایی هستند که با توجه به الگوی نمره‌دهی یک معلم، می‌توانند پس از آن بررسی کنند که آیا معلم از الگوی نمره‌دهی منحرف شده است و حتی در صورت لزوم، ناهماهنگی‌ها یا خطاهای احتمالی را شناسایی کنند. شرط چهارم این است که سامانهٔ هوش مصنوعی برای انجام وظیفه‌ای صرفاً مقدماتی طراحی شده باشد که برای ارزیابی بعدی مرتبط با سامانه‌های هوش مصنوعی ذکرشده در پیوست این قانون به کار می‌رود. بنابراین تأثیر خروجی سامانه بر ارزیابی نهایی بسیار پایین است و ریسک قابل‌توجهی ایجاد نمی‌کند. این شرط شامل راهکارهای هوشمند مدیریت پرونده‌ها است که عملکردهایی مانند فهرست‌بندی، جستجو، پردازش متن و گفتار یا اتصال داده‌ها به منابع دیگر را پوشش می‌دهد و همچنین سامانه‌های هوش مصنوعی که برای ترجمهٔ اسناد اولیه به کار می‌روند. در هر صورت، سامانه‌های هوش مصنوعی که در موارد استفادهٔ پرخطر مندرج در پیوست این قانون به‌کار می‌روند، باید در صورتی‌که مستلزم *نمایه‌سازی* به مفهوم مندرج در بند (۴) ماده ۴ مقررات ۶۷۹/۲۰۱۶ (اتحادیهٔ اروپا) یا بند (۴) ماده ۳ دستورالعمل ۶۸۰/۲۰۱۶ (اتحادیهٔ اروپا) یا بند (۵) ماده ۳ مقررات ۱۷۲۵/۲۰۱۸ (اتحادیهٔ اروپا) باشند، به‌عنوان سامانه‌هایی تلقی شوند که خطرات جدی برای سلامت، ایمنی یا حقوق بنیادین ایجاد می‌کنند. برای تضمین قابلیت رهگیری و شفافیت، ارائه‌دهنده‌ای که تشخیص می‌دهد یک سامانهٔ هوش مصنوعی بر اساس شرایط فوق، پرخطر محسوب نمی‌شود، باید پیش از عرضهٔ آن سامانه به بازار یا بهره‌برداری از آن، مستندات ارزیابی خود را تنظیم کند و در صورت درخواست، این مستندات را در اختیار مقامات صلاحیت‌دار ملی قرار دهد. همچنین چنین ارائه‌دهنده‌ای ملزم است سامانهٔ هوش مصنوعی مربوطه را در پایگاه دادهٔ اتحادیهٔ اروپا که بر اساس این قانون ایجاد شده، به ثبت برساند. به منظور ارائهٔ راهنمایی

بیشتر برای اجرای عملی شرایطی که بر اساس آن‌ها سامانه‌های هوش مصنوعی مندرج در پیوست این قانون به‌طور استثنایی غیرپرخطر تلقی می‌شوند، کمیسیون باید پس از مشورت با هیئت مربوطه، دستورالعمل‌هایی صادر کند که هم شیوهٔ اجرای عملی این شرایط را مشخص کند و هم شامل فهرست جامعی از نمونه‌های کاربردی سامانه‌های هوش مصنوعی اعم از موارد پرخطر و موارد غیرپرخطر باشد.

۵۴. از آنجا که داده‌های زیست‌سنجی در زمرهٔ دسته‌بندی ویژه‌ای از داده‌های شخصی قرار می‌گیرند، شایسته است چندین مورد استفادهٔ حیاتی از سامانه‌های زیست‌سنجی تا جایی که استفاده از آن‌ها تحت حقوق اتحادیه و قوانین ملی مربوطه مجاز باشد، به‌عنوان موارد پرخطر طبقه‌بندی شوند. نارسایی‌های فنی سامانه‌های هوش مصنوعی که برای شناسایی از راه دور اشخاص حقیقی به کار می‌روند، می‌توانند به نتایج جانبدارانه منجر شده و آثار تبعیض‌آمیز داشته باشند. خطر بروز چنین نتایج جانبدارانه و آثار تبعیض‌آمیز به‌ویژه در ارتباط با سن، قومیت، نژاد، جنسیت یا ناتوانی‌های جسمی و ذهنی اهمیت دارد. از این رو سامانه‌های شناسایی زیست‌سنجی از راه دور باید با توجه به خطراتی که ایجاد می‌کنند، در زمرهٔ سامانه‌های پرخطر طبقه‌بندی شوند. این طبقه‌بندی شامل آن دسته از سامانه‌های هوش مصنوعی نمی‌شود که برای *تأیید هویت زیست‌سنجی* ازجمله احراز هویت طراحی شده‌اند زیرا تنها هدف آن تأیید این است که شخص حقیقی معین همان فردی است که ادعا می‌کند و تأیید هویت وی تنها برای دسترسی به یک خدمت، بازگشایی یک دستگاه یا دسترسی ایمن به اماکن به کار می‌رود. علاوه بر این، سامانه‌های هوش مصنوعی که برای *دسته‌بندی زیست‌سنجی* بر اساس ویژگی‌ها یا خصایص حساسِ مشمول حمایت بند (۱) ماده ۹ مقررات ۶۷۹/۲۰۱۶ (اتحادیهٔ اروپا) و بر مبنای داده‌های زیست‌سنجی طراحی شده‌اند، تا آنجا که طبق این قانون ممنوع نباشند و نیز سامانه‌های تشخیص احساسات که تحت این قانون ممنوع نشده‌اند، باید در ردیف سامانه‌های پرخطر قرار گیرند. در مقابل، سامانه‌های زیست‌سنجی که صرفاً با هدف تسهیل اقدامات امنیت سایبری و تدابیر حمایت از داده‌های شخصی به کار می‌روند، نباید به‌عنوان سامانه‌های هوش مصنوعی، پرخطر تلقی شوند.

۵۵. در خصوص مدیریت و بهره‌برداری از زیرساخت‌های حیاتی، شایسته است سامانه‌های هوش مصنوعی که به‌عنوان اجزای ایمنی در مدیریت و بهره‌برداری از زیرساخت‌های دیجیتال حیاتی مندرج در بند (۸) پیوست دستورالعمل ۲۵۵۷/۲۰۲۲ (اتحادیهٔ اروپا) در مورد ترافیک جاده‌ای و تأمین آب، گاز، گرمایش و برق به کار می‌روند، در زمرهٔ سامانه‌های پرخطر طبقه‌بندی شوند زیرا ممکن است بروز اختلال یا نقص عملکرد در آن‌ها جان و سلامت اشخاص را در مقیاس گسترده به مخاطره اندازد و موجب اخلال قابل‌توجه در جریان عادی فعالیت‌های اجتماعی و اقتصادی شود. اجزای ایمنی زیرساخت‌های حیاتی، ازجمله زیرساخت‌های دیجیتال حیاتی، سامانه‌هایی هستند که

به‌طور مستقیم از تمامیت فیزیکی زیرساخت‌های حیاتی یا از سلامت و ایمنی اشخاص و اموال حفاظت می‌کنند، اما وجود آن‌ها برای عملکرد کلی سامانه ضرورت ندارد. ممکن است بروز نقص یا اختلال در چنین اجزایی مستقیماً منجر به ایجاد خطراتی برای تمامیت فیزیکی زیرساخت‌های حیاتی و در نتیجه برای سلامت و ایمنی اشخاص و اموال شود. اجزایی که صرفاً برای اهداف امنیت سایبری طراحی شده‌اند، نباید در زمرهٔ اجزای ایمنی محسوب شوند. نمونه‌هایی از اجزای ایمنی این گونه زیرساخت‌های حیاتی می‌تواند شامل سامانه‌های پایش فشار آب یا سامانه‌های کنترل هشدار آتش‌سوزی در مراکز رایانش ابری باشد.

۵۶. به‌کارگیری سامانه‌های هوش مصنوعی در آموزش، نقشی اساسی در ارتقاء آموزش و تربیت باکیفیت دیجیتال ایفا می‌کند و این امکان را فراهم می‌کند که همهٔ یادگیرندگان و معلمان، مهارت‌ها و صلاحیت‌های دیجیتال لازم ازجمله سواد رسانه‌ای و تفکر انتقادی را کسب و به اشتراک گذارند تا بتوانند در اقتصاد، جامعه و فرآیندهای دموکراتیک مشارکت فعال داشته باشند. با این حال، سامانه‌های هوش مصنوعیِ مورد استفاده در آموزش یا آموزش حرفه‌ای به‌ویژه برای تعیین دسترسی یا پذیرش، اختصاص افراد به مؤسسات یا برنامه‌های آموزشی و حرفه‌ای در همهٔ سطوح، ارزیابی نتایج یادگیری اشخاص، سنجش سطح آموزشی مناسب برای فرد و تأثیرگذاری اساسی بر سطح آموزش و تربیتی که افراد دریافت می‌کنند یا قادر به دسترسی به آن هستند، یا برای نظارت و شناسایی رفتارهای ممنوعه دانشجویان در طول آزمون‌ها به‌کار می‌روند باید در زمرهٔ سامانه‌های هوش مصنوعی پرخطر طبقه‌بندی شوند زیرا این سامانه‌ها می‌توانند مسیر آموزشی و حرفه‌ای زندگی یک فرد را تعیین کنند و به تبع آن، توانایی وی برای تأمین معیشت را تحت تأثیر قرار دهند. چنانچه این سامانه‌ها به نحو نامناسب طراحی و استفاده شوند، ممکن است به‌ویژه ماهیتی مداخله‌گرانه بیابند و منجر به نقض حق بر آموزش و تربیت و همچنین حق بر عدم تبعیض شوند و الگوهای تاریخی تبعیض ازجمله علیه زنان، گروه‌های سنی خاص، اشخاص دارای معلولیت یا افرادی با منشأ نژادی یا قومی یا گرایش جنسی معین را تداوم بخشند.

۵۷. سامانه‌های هوش مصنوعی مورد استفاده در حوزهٔ اشتغال، مدیریت کارگران و دسترسی به خوداشتغالی، به‌ویژه آن‌هایی که در فرآیند جذب و گزینش افراد، تصمیم‌گیری‌های مؤثر بر شرایط روابط کاری، ارتقاء یا خاتمهٔ روابط قراردادی کاری، تخصیص وظایف بر اساس رفتار فردی، ویژگی‌ها یا خصایص شخصی و همچنین در امر نظارت یا ارزیابی افراد در روابط قراردادی کاری به‌کار می‌روند نیز باید در زمرهٔ سامانه‌های پرخطر طبقه‌بندی شوند زیرا این سامانه‌ها می‌توانند تأثیر چشمگیری بر چشم‌اندازهای شغلی آینده، معیشت افراد و حقوق کارگران داشته باشند. روابط قراردادی کاری مربوطه باید به‌طور معناداری شامل کارکنان و اشخاصی باشد که از طریق پلتفرم‌ها

خدمات ارائه می‌دهند، آن گونه که در *برنامهٔ کاری کمیسیون ۲۰۲۱* ذکر شده است. در سرتاسر فرآیند جذب و نیز در ارزیابی، ارتقا یا حفظ اشخاص در روابط قراردادی کاری، ممکن است چنین سامانه‌هایی الگوهای تاریخی تبعیض را تداوم بخشند، ازجمله علیه زنان، گروه‌های سنی خاص، اشخاص دارای معلولیت یا افرادی با منشأ نژادی یا قومی یا گرایش جنسی معین. همچنین سامانه‌های هوش مصنوعی مورد استفاده برای نظارت بر عملکرد و رفتار این اشخاص می‌توانند حقوق بنیادین آنان در زمینهٔ حمایت از داده‌ها و حریم خصوصی را تضعیف کنند.

۵۸. حوزهٔ دیگری که استفاده از سامانه‌های هوش مصنوعی در آن شایسته توجه ویژه است، دسترسی و بهره‌مندی از خدمات و مزایای اساسی خصوصی و عمومی است. این خدمات و مزایا برای مشارکت کامل افراد در جامعه یا ارتقاء سطح زندگی آنان ضروری هستند. اشخاص حقیقی که برای دریافت یا در حال دریافت مزایا و خدمات عمومی اساسی از مقامات دولتی هستند ازجمله خدمات بهداشتی، مزایای تأمین اجتماعی، خدمات اجتماعی حمایتی در مواردی همچون بارداری، بیماری، حوادث کار، وابستگی یا کهولت سن و بیکاری، همچنین خدمات اجتماعی و کمک‌های مسکن، عموماً به این خدمات و مزایا وابسته‌اند و در برابر مقامات مسئول در موقعیتی آسیب‌پذیر قرار دارند.

چنانچه از سامانه‌های هوش مصنوعی برای تعیین این موضوع استفاده شود که آیا این مزایا و خدمات باید اعطا، رد، کاهش، لغو یا استرداد شوند ازجمله برای تشخیص اینکه ذی‌نفعان به‌طور قانونی مستحق چنین خدمات یا مزایایی هستند یا خیر، این سامانه‌ها می‌توانند تأثیر قابل‌توجهی بر معیشت اشخاص داشته باشند و حقوق بنیادین آنان از قبیل حق بر حمایت اجتماعی، برابری و عدم تبعیض، کرامت انسانی و حق بر جبران مؤثر را نقض کنند. از این رو باید در زمرهٔ سامانه‌های پرخطر طبقه‌بندی شوند. با این حال، این قانون نباید مانعی در برابر توسعه و استفاده از رویکردهای نوآورانه در مدیریت عمومی ایجاد کند؛ رویکردهایی که می‌توانند از به‌کارگیری گستردهٔ سامانه‌های ایمن و منطبق با مقررات منتفع شوند، مشروط بر آنکه چنین سامانه‌هایی خطری جدی برای اشخاص حقیقی و حقوقی به همراه نداشته باشند. علاوه بر این، سامانه‌های هوش مصنوعی مورد استفاده برای ارزیابی اعتبار مالی یا توان بازپرداخت اشخاص حقیقی باید در زمرهٔ سامانه‌های پرخطر قرار گیرند، چرا که دسترسی این اشخاص به منابع مالی یا خدمات ضروری مانند مسکن، برق و خدمات مخابراتی را تعیین می‌کنند. استفاده از این سامانه‌ها می‌تواند به تبعیض میان افراد یا گروه‌ها بینجامد و الگوهای تاریخی تبعیض مانند تبعیض مبتنی بر منشأ نژادی یا قومی، جنسیت، ناتوانی، سن یا گرایش جنسی را تداوم بخشد یا اشکال جدیدی از آثار تبعیض‌آمیز ایجاد کند. با وجود این، سامانه‌های هوش مصنوعیِ پیش‌بینی‌شده در حقوق اتحادیهٔ اروپا برای مقاصد تشخیص تقلب در ارائهٔ خدمات

مالی و نیز برای اهداف احتیاطی جهت محاسبهٔ الزامات سرمایه‌ای مؤسسات اعتباری و شرکت‌های بیمه، نباید در زمرهٔ سامانه‌های پرخطر ذیل این قانون قرار گیرند. علاوه بر این، سامانه‌های هوش مصنوعی که برای ارزیابی ریسک و قیمت‌گذاری بیمهٔ سلامت و عمر در مورد اشخاص حقیقی به کار می‌روند نیز می‌توانند تأثیر چشمگیری بر معیشت افراد داشته باشند و چنانچه به‌درستی طراحی، توسعه یافته و استفاده نشوند، قادرند حقوق بنیادین اشخاص را نقض کنند و پیامدهای جدی برای زندگی و سلامت آنان ازجمله محرومیت مالی و تبعیض به بار آورند. در نهایت، سامانه‌های هوش مصنوعی مورد استفاده برای ارزیابی و طبقه‌بندی تماس‌های اضطراری اشخاص حقیقی یا برای اعزام و تعیین اولویت در اعزام خدمات اضطراری اولیه ازجمله پلیس، آتش‌نشانی، امداد پزشکی و نیز سامانه‌های اولویت‌بندی بیماران در فوریت‌های درمانی نیز باید در زمرهٔ سامانه‌های پرخطر قرار گیرند زیرا این سامانه‌ها در شرایط بسیار حساس و بحرانی برای زندگی، سلامت و اموال اشخاص تصمیم‌گیری می‌کنند.

۵۹. با توجه به نقش و مسئولیت مراجع اجرای قانون، استفادهٔ این مراجع از برخی سامانه‌های هوش مصنوعی با سطح چشمگیری از عدم توازن قدرت همراه است و می‌تواند به نظارت، بازداشت یا سلب آزادی اشخاص حقیقی و نیز به دیگر آثار نامطلوب بر حقوق بنیادین تضمین‌شده در منشور بینجامد. به‌ویژه در مواردی که یک سامانهٔ هوش مصنوعی با داده‌های باکیفیت آموزش ندیده باشد، یا از حیث عملکرد، دقت یا استحکام، الزامات مناسب را برآورده نکند، یا پیش از عرضه به بازار یا به‌کارگیری به نحو دیگری به‌درستی طراحی و آزمایش نشده باشد، ممکن است اشخاص را به گونه‌ای تبعیض‌آمیز یا به شکلی نادرست یا ناعادلانه شناسایی و هدف‌گذاری کند. افزون بر این، ممکن است اعمال برخی حقوق بنیادین مهم آیین دادرسی مانند حق برخورداری از جبران مؤثر و دادرسی عادلانه، و نیز حق دفاع و اصل برائت، با مانع مواجه شود. این امر به‌ویژه در شرایطی صادق است که چنین سامانه‌های هوش مصنوعی از شفافیت، توضیح‌پذیری و مستندسازی کافی برخوردار نباشند. از این رو شایسته است شماری از سامانه‌های هوش مصنوعی که برای استفاده در بستر اجرای قانون طراحی شده‌اند، تا جایی که استفاده از آن‌ها طبق حقوق اتحادیه و قوانین ملی مربوطه مجاز است، به‌عنوان سامانه‌های پرخطر طبقه‌بندی شوند زیرا در این زمینه، دقت، قابلیت اعتماد و شفافیت اهمیتی ویژه‌ای دارد تا از آثار نامطلوب جلوگیری، اعتماد عمومی حفظ و پاسخگویی و جبران مؤثر تضمین شود. با توجه به ماهیت فعالیت‌ها و خطرات مرتبط با آن‌ها، این سامانه‌های هوش مصنوعی پرخطر باید به‌ویژه شامل سامانه‌هایی باشند که قرار است توسط مقامات مجری قانون یا از سوی آن‌ها، یا توسط نهادها، ارکان، دفاتر یا آژانس‌های اتحادیهٔ اروپا در حمایت از مقامات مجری قانون به کار روند. ازجملهٔ این موارد می‌توان به سامانه‌هایی

اشاره کرد که برای ارزیابی خطر قربانی‌شدن یک شخص حقیقی در برابر جرایم کیفری به کار می‌روند؛ ابزارهایی مانند دستگاه‌های دروغ‌سنج (پُلی‌گراف) و ابزارهای مشابه، سامانه‌های ارزیابی قابلیت اعتماد ادله در جریان تحقیق یا تعقیب کیفری و نیز ـ تا آنجا که بر اساس این مقرره ممنوع نشده باشد ـ سامانه‌هایی که برای ارزیابی خطر ارتکاب یا تکرار جرم توسط شخص حقیقی به کار می‌روند، مشروط بر آنکه این ارزیابی صرفاً مبتنی بر پروفایل‌سازی اشخاص حقیقی یا سنجش ویژگی‌ها و خصایص شخصیتی یا رفتار کیفری گذشتهٔ اشخاص یا گروه‌ها نباشد. همچنین این سامانه‌ها می‌توانند برای پروفایل‌سازی در جریان کشف، تحقیق یا تعقیب جرایم کیفری به کار روند. با این حال، سامانه‌های هوش مصنوعی که به‌طور خاص برای استفاده در روندهای اداری توسط مقامات مالیاتی و گمرکی و همچنین توسط واحدهای اطلاعات مالی که وظایف اداری تحلیل اطلاعات را طبق حقوق اتحادیه در زمینهٔ مبارزه با پولشویی انجام می‌دهند، طراحی شده‌اند، نباید به‌عنوان سامانه‌های پرخطرِ مورد استفاده توسط مراجع اجرای قانون برای مقاصد پیشگیری، کشف، تحقیق و تعقیب جرایم کیفری تلقی شوند. استفاده از ابزارهای هوش مصنوعی توسط مراجع اجرای قانون و سایر مقامات ذی‌ربط نباید به عاملی برای نابرابری یا طردشدن تبدیل شود. همچنین تأثیر استفاده از این ابزارها بر حقوق دفاعی متهمان نباید نادیده گرفته شود. به‌ویژه دشواری در دسترسی به اطلاعات معنادار دربارهٔ نحوهٔ عملکرد این سامانه‌ها و در نتیجه دشواری در به‌چالش‌کشیدن نتایج آن‌ها در دادگاه خصوصاً برای اشخاص حقیقی تحت تعقیب اهمیت ویژه دارد.

۶۰. سامانه‌های هوش مصنوعی که در حوزه‌های مدیریت مهاجرت، پناهندگی و کنترل مرزها به کار گرفته می‌شوند، بر اشخاصی اثر می‌گذارند که غالباً در موقعیتی به‌ویژه آسیب‌پذیر قرار دارند و سرنوشت آن‌ها به نتایج اقدامات مقامات عمومی صلاحیت‌دار وابسته است. از این رو دقت، ماهیت غیرتبعیض‌آمیز و شفافیت سامانه‌های هوش مصنوعی مورد استفاده در این زمینه‌ها، برای تضمین احترام به حقوق بنیادین اشخاص متأثر از آن‌ها اهمیتی ویژه دارد، به‌ویژه حقوق آن‌ها در زمینهٔ آزادی رفت و آمد، منع تبعیض، حمایت از زندگی خصوصی و داده‌های شخصی، حمایت بین‌المللی و ادارهٔ مطلوب؛ لذا شایسته است مادامی که استفاده از آن‌ها در چارچوب حقوق اتحادیه و قوانین ملی مربوط مجاز باشد، سامانه‌های هوش مصنوعی مورد استفاده توسط یا به نمایندگی از مراجع عمومی صلاحیت‌دار یا نهادها، ارگان‌ها، دفاتر یا آژانس‌های اتحادیه که مأمور انجام وظایف در زمینهٔ مهاجرت، پناهندگی و مدیریت کنترل مرزها هستند، در زمرهٔ سامانه‌های پرخطر طبقه‌بندی شوند. این امر به‌ویژه شامل سامانه‌هایی مانند دستگاه‌های دروغ‌سنج (پُلی‌گراف) و ابزارهای مشابه است که برای ارزیابی برخی خطرات منتسب به اشخاص حقیقیِ واردشونده به

قلمرو دولت عضو، یا متقاضیان روادید یا پناهندگی به کار می‌روند. همچنین این طبقه‌بندی شامل سامانه‌هایی می‌شود که به منظور یاری‌رساندن به مقامات عمومی صلاحیت‌دار در رسیدگی به درخواست‌های پناهندگی، روادید و مجوز اقامت، ازجمله ارزیابی‌های مرتبط با قابلیت اعتماد ادله و نیز رسیدگی به شکایات مرتبط، با هدف احراز شرایط احراز وضعیت حقوقی مورد درخواستِ اشخاص حقیقی به کار می‌روند. افزون بر این، سامانه‌های هوش مصنوعی که برای کشف، شناسایی یا احراز هویت اشخاص حقیقی در بستر مدیریت مهاجرت، پناهندگی و کنترل مرزها به کار می‌روند نیز در زمرهٔ سامانه‌های پرخطر قرار می‌گیرند؛ با این استثنا که سامانه‌های مربوط به راستی‌آزمایی اسناد مسافرتی از این حکم خارج‌اند. سامانه‌های هوش مصنوعی در حوزهٔ مهاجرت، پناهندگی و مدیریت کنترل مرزها که مشمول این قانون هستند باید با الزامات شکلی و آیین دادرسی مندرج در مقررات ۲۰۰۹/۸۱۰[۴۳] پارلمان و شورای اروپا و دستورالعمل ۳۲/۲۰۱۳[۴۴] پارلمان و شورای اروپا و دیگر مقررات مرتبط اتحادیه مطابقت داشته باشند. استفاده از سامانه‌های هوش مصنوعی در این حوزه‌ها تحت هیچ شرایطی نباید وسیله‌ای برای کشورهای عضو یا نهادها، ارگان‌ها، دفاتر یا آژانس‌های اتحادیه جهت دورزدن تعهدات بین‌المللی آن‌ها بر پایهٔ کنوانسیون ۱۹۵۱ ژنو دربارهٔ وضعیت پناهندگان (با اصلاحات پروتکل ۱۹۶۷) باشد. همچنین نباید به هیچ وجه ناقض اصل عدم اخراج[۴۵] یا مانعی در برابر دسترسی ایمن و مؤثر به مسیرهای قانونی ورود به قلمرو اتحادیه ازجمله حق برخورداری از حمایت بین‌المللی شود.

۶۱. برخی سامانه‌های هوش مصنوعی که برای ادارهٔ عدالت و فرآیندهای دموکراتیک طراحی شده‌اند، باید به‌عنوان سامانه‌های پرخطر طبقه‌بندی شوند زیرا می‌توانند تأثیر قابل‌توجهی بر دموکراسی، حاکمیت قانون، آزادی‌های فردی و همچنین حق بر جبران مؤثر و دادرسی منصفانه داشته باشند، به‌ویژه برای مقابله با خطرات ناشی از سوگیری‌های احتمالی، خطاها و عدم شفافیت، شایسته است سامانه‌های هوش مصنوعی که برای استفاده توسط مراجع قضایی یا به نمایندگی از آن‌ها طراحی شده‌اند و به مراجع قضایی در تحقیق و تفسیر واقعیت‌ها و قوانین و اعمال قانون به مجموعه‌ای مشخص از واقعیت‌ها کمک می‌کنند، به‌عنوان سامانه‌های پرخطر شناخته شوند. سامانه‌های

۴۳. مقررات شمارهٔ ۲۰۰۹/۸۱۰ پارلمان و شورای اتحادیهٔ اروپا (۱۳ ژوئیهٔ ۲۰۰۹) همان چیزی است که به‌عنوان *کد روادید جامعه* (Visa Code) شناخته می‌شود (روزنامهٔ رسمی ۲۴۳، ۲۰۰۹/۹/۱۵، ص ۱).

۴۴. دستورالعمل ۳۲/۲۰۱۳ پارلمان و شورای اتحادیهٔ اروپا (۲۶ ژوئن ۲۰۱۳) با عنوان *دستورالعمل مربوط به رویه‌های مشترک برای اعطا و لغو حمایت بین‌المللی* تنظیم شده است (روزنامهٔ رسمی ۱۸۰، ۲۰۱۳/۶/۲۹، ص ۶۰).

۴۵. عبارت non-refoulement یا *عدم اخراج* یک اصل عرفی بین‌المللی و بدین معناست که «هیچ دولتی نباید پناهنده‌ای را به سرزمینی که جان یا آزادی او به علت نژاد، دین، تابعیت، عضویت در گروه اجتماعی معین یا عقیده سیاسی در معرض تهدید باشد» بازگرداند یا اخراج کند. در مقررات و دستورالعمل‌های پناهندگی اتحادیه، اصل عدم اخراج نه‌تنها برای پناهندگان، بلکه نسبت به همهٔ اشخاص در معرض خطر شکنجه یا رفتار غیرانسانی اعمال می‌شود.

هوش مصنوعی مورد استفاده توسط مرجع حل اختلاف جایگزین نیز زمانی که نتایج رسیدگی‌های آن‌ها آثار حقوقی برای طرفین ایجاد می‌کند، باید در زمرهٔ سامانه‌های پرخطر قرار گیرند. استفاده از ابزارهای هوش مصنوعی می‌تواند قدرت تصمیم‌گیری قضات یا استقلال قضایی را تقویت کند اما نباید جایگزین آن شود زیرا تصمیم نهایی باید همواره توسط انسان اتخاذ شود. با این حال، طبقه‌بندی سامانه‌های هوش مصنوعی به‌عنوان پرخطر، نباید شامل سامانه‌هایی شود که صرفاً برای فعالیت‌های اداری جانبی طراحی شده‌اند؛ ضمن اینکه بر ادارهٔ واقعی عدالت در پرونده‌های فردی تأثیری ندارند، مانند ناشناس‌سازی یا شبه‌ناشناس‌سازی تصمیمات قضایی، اسناد یا داده‌ها، ارتباطات بین کارکنان و وظایف اداری.

۶۲. بدون لطمه به قواعد موجود در مقررات ۹۰۰ /۲۰۲۴[۴۶] پارلمان و شورای اروپا و به منظور شناسایی مخاطرات ناشی از مداخلهٔ ناروای خارجی با حق رأی مندرج در ماده ۳۹ منشور و جهت جلوگیری از آثار نامطلوب آن بر دموکراسی و حاکمیت قانون، سامانه‌های هوش مصنوعی که برای تأثیرگذاری بر نتیجهٔ انتخابات یا همه‌پرسی یا رفتار رأی‌دهی اشخاص حقیقی در جریان اعمال حق رأی آنان در انتخابات یا همه‌پرسی طراحی شده‌اند، باید به‌عنوان سامانه‌های پرخطر طبقه‌بندی شوند. البته این استثنا وجود دارد که سامانه‌هایی که خروجی آن‌ها مستقیماً در معرض اشخاص حقیقی قرار نمی‌گیرند، مانند ابزارهایی که برای سازماندهی، بهینه‌سازی و ساختاربندی پویش‌های سیاسی از منظر اداری و لجستیکی استفاده می‌شوند شامل این طبقه‌بندی نمی‌شوند.

۶۳. این که یک سامانهٔ هوش مصنوعی بر اساس این قانون به‌عنوان سامانهٔ پرخطر طبقه‌بندی می‌شود، به این معنا نیست که استفاده از آن تحت سایر قوانین اتحادیهٔ اروپا یا قوانین ملی منطبق با حقوق اتحادیه، ازجمله قوانین مربوط به حفاظت از داده‌های شخصی، استفاده از دروغ‌سنج‌ها و ابزارهای مشابه یا سایر سامانه‌ها برای تشخیص وضعیت عاطفی اشخاص حقیقی، مشروع در نظر گرفته می‌شود. هر گونه استفاده از این سامانه‌ها باید صرفاً مطابق الزامات مندرج در منشور حقوق بنیادین و قوانین ثانویهٔ اتحادیه و قوانین ملی قابل اعمال انجام شود. این قانون نباید به گونه‌ای تفسیر شود که موجبی برای مشروعیت پردازش داده‌های شخصی ازجمله دسته‌بندی‌های خاص داده‌های شخصی ایجاد کند، مگر آنکه صراحتاً در خود قانون پیش‌بینی شده باشد.

۶۴. به منظور کاهش ریسک‌های ناشی از سامانه‌های هوش مصنوعی پرخطر که در بازار عرضه یا به خدمت گرفته می‌شوند و تضمین سطح بالایی از اعتمادپذیری باید برخی الزامات اجباری بر این سامانه‌ها اعمال شود؛ البته با توجه به هدف موردنظر و زمینهٔ استفاده از سامانهٔ هوش مصنوعی و

---

۴۶. مقررات ۹۰۰ /۲۰۲۴ پارلمان و شورای اروپا که در ۱۳ مارس ۲۰۲۴ تصویب شد، به منظور افزایش شفافیت و کنترل هدف‌گیری در تبلیغات سیاسی برخط طراحی شده است (روزنامهٔ رسمی ۲۰۲۴/۹۰۰، ۲۰۲۴/۳/۲۰).

مطابق سیستم مدیریت ریسک که توسط ارائه‌دهنده ایجاد می‌شود. اقدامات اتخاذشده توسط ارائه‌دهندگان برای رعایت الزامات اجباری این قانون باید با وضعیت فنی و علمی پذیرفته‌شده در زمینهٔ هوش مصنوعی همخوانی داشته و متناسب و مؤثر باشد و اهداف این قانون را محقق کند. بر اساس *چارچوب قانونی نوین اتحادیه*[۴۷] و همان طور که در اطلاعیهٔ کمیسیون با عنوان *راهنمای آبی‌رنگ* برای اجرای قوانین محصول اتحادیهٔ اروپا ۲۰۲۲ مشخص و به‌عنوان قاعدهٔ کلی شناخته شده است، بیش از یک مصوبهٔ قانونی هماهنگ‌شدهٔ اتحادیه ممکن است برای یک محصول قابل اعمال باشد زیرا عرضه یا به‌خدمت‌گرفتن محصول، تنها زمانی ممکن است که محصول با تمام قوانین هماهنگ‌شدهٔ قابل اعمال اتحادیه مطابقت داشته باشد. خطرات سامانه‌های هوش مصنوعی تحت پوشش الزامات این قانون، ابعاد متفاوتی از خطرات قوانین هماهنگ‌شدهٔ اتحادیه را در بر می‌گیرند و بنابراین الزامات این قانون، تکمیل‌کنندهٔ چارچوب قانونی هماهنگ‌شدهٔ موجود خواهند بود. به‌عنوان مثال، ممکن است محصولات ماشین‌آلات یا تجهیزات پزشکی که دارای سامانهٔ هوش مصنوعی هستند، خطراتی داشته باشند که در الزامات سلامت و ایمنی مندرج در قوانین هماهنگ‌شدهٔ بخش مربوطه پوشش داده نشده‌اند زیرا آن قوانین، بخشی را به خطرات ویژهٔ سامانه‌های هوش مصنوعی اختصاص نداده‌اند. این امر، لزوم اجرای همزمان و مکمل قوانین مختلف را مطرح می‌کند. برای تضمین هماهنگی و جلوگیری از بار اداری و هزینه‌های غیرضروری، ارائه‌دهندگان محصولاتی که شامل یک یا چند سامانهٔ هوش مصنوعی پرخطر هستند و الزامات این قانون و قوانین هماهنگ‌شدهٔ اتحادیه مبتنی بر چارچوب قانونی نوین و مندرج در پیوست این قانون بر آن‌ها اعمال می‌شود، باید انعطاف‌پذیری در تصمیمات عملیاتی در زمینهٔ نحوهٔ تضمین مطابقت محصول با تمام الزامات قابل اعمال داشته باشند. این انعطاف‌پذیری می‌تواند به‌عنوان مثال، شامل تصمیم ارائه‌دهنده برای ادغام بخشی از فرآیندهای لازم تست و گزارش‌دهی، اطلاعات و مستندات مورد نیاز این قانون در مستندات و رویه‌های موجود بر اساس قوانین هماهنگ‌شدهٔ اتحادیه باشد. این امر به هیچ وجه تعهد ارائه‌دهنده برای رعایت تمام الزامات قابل اعمال را تضعیف نمی‌کند.

۶۵. سامانهٔ مدیریت ریسک باید متشکل از فرآیندی مستمر و تکرارشونده باشد که در سرتاسر چرخهٔ عمر یک سامانهٔ هوش مصنوعی پرخطر طراحی و اجرا می‌شود. هدف این فرآیند، شناسایی و کاهش ریسک‌های مرتبط با سامانه‌های هوش مصنوعی بر سلامت، ایمنی و حقوق بنیادین است. سامانهٔ مدیریت ریسک باید به‌طور منظم مورد بازبینی و به‌روزرسانی قرار گیرد تا اثربخشی آن استمرار یابد و تصمیمات و اقدامات مهم اتخاذشده، مستند و توجیه‌پذیر شوند. این فرآیند باید تضمین کند که تأمین‌کننده، ریسک‌ها یا آثار زیان‌بار را شناسایی و برای ریسک‌های شناخته‌شده و به‌طور معقول قابل پیش‌بینی سامانه‌های هوش مصنوعی نسبت به سلامت،

47. New Legislative Framework

ایمنی و حقوق بنیادین، متناسب با هدف پیش‌بینی‌شده و سوءاستفاده‌های معقول قابل پیش‌بینی، تدابیر کاهنده ازجمله اتخاذ ریسک‌های احتمالی ناشی از تعامل میان سامانه و محیط عمل اتخاذ می‌کند. سامانهٔ مدیریت ریسک باید مناسب‌ترین تدابیر مدیریت ریسک را در پرتو پیشرفته‌ترین وضعیت دانش فنی در حوزهٔ هوش مصنوعی اتخاذ کند. هنگام شناسایی مناسب‌ترین تدابیر مدیریت ریسک، تأمین‌کننده باید تصمیمات خود را مستند و تبیین کند و در صورت لزوم از متخصصان و ذی‌نفعان بیرونی بهره گیرد. در شناسایی سوءاستفاده‌های معقول قابل پیش‌بینی از سامانه‌های هوش مصنوعی پرخطر، تأمین‌کننده باید کاربردهایی را نیز در نظر بگیرد که گرچه به‌طور مستقیم در هدف پیش‌بینی‌شده و در دستورالعمل استفاده ذکر نشده‌اند، می‌توانند به‌طور معقول از رفتار انسانی قابل پیش‌بینی در پرتو ویژگی‌ها و کارکردهای خاص یک سامانه ناشی شوند. هر گونه وضعیت شناخته‌شده یا معقول قابل پیش‌بینی در ارتباط با استفاده از سامانهٔ هوش مصنوعی پرخطر، خواه مطابق هدف پیش‌بینی‌شده یا در شرایط سوءاستفادهٔ معقول قابل پیش‌بینی که ممکن است منجر به ریسک‌های سلامت، ایمنی یا حقوق بنیادین شود، باید در دستورالعمل‌های استفادهٔ ارائه‌شده از سوی تأمین‌کننده درج شود. هدف این است که بهره‌بردار هنگام استفاده از سامانهٔ هوش مصنوعی پرخطر از این ریسک‌ها آگاه باشد و آن‌ها را مدنظر قرار دهد. شناسایی و اجرای تدابیر کاهش ریسک برای سوءاستفاده‌های معقول قابل پیش‌بینی بر اساس این قانون نباید مستلزم آموزش اضافی خاص برای سامانهٔ هوش مصنوعی پرخطر از سوی تأمین‌کننده باشد. با این حال، از تأمین‌کنندگان خواسته می‌شود در صورت ضرورت و تناسب، آموزش‌های تکمیلی را نیز مدنظر قرار دهند تا سوءاستفاده‌های معقول قابل پیش‌بینی به نحو بهتری کاهش یابد.

۶۶. الزامات باید در خصوص سامانه‌های هوش مصنوعی پرخطر ناظر بر مدیریت ریسک، کیفیت و ارتباط داده‌های مورد استفاده، مستندسازی فنی و نگهداری سوابق، شفافیت و ارائهٔ اطلاعات به بهره‌برداران، نظارت انسانی، استحکام و نیز دقت و امنیت سایبری اعمال شوند. این الزامات برای کاهش مؤثر ریسک‌های مربوط به سلامت، ایمنی و حقوق بنیادین ضروری‌اند. از آنجا که هیچ اقدام دیگری با محدودیت تجاری کمتر به‌طور معقول در دسترس نیست، این الزامات به‌عنوان محدودیت‌های ناموجه بر تجارت تلقی نمی‌شوند.

۶۷. داده‌های باکیفیت و دسترسی به داده‌های باکیفیت، نقش حیاتی در ساختاردهی و تضمین کارآیی بسیاری از سامانه‌های هوش مصنوعی دارند؛ به‌ویژه در مواردی که از شیوه‌های مبتنی بر آموزش مدل‌ها استفاده می‌شود، تا اطمینان حاصل شود که سامانهٔ هوش مصنوعی پرخطر مطابق هدف تعیین‌شده و به‌طور ایمن عمل می‌کند و به منبع تبعیض ممنوع‌شده در حقوق

اتحادیه تبدیل نمی‌شود. مجموعهٔ داده‌های باکیفیت برای آموزش، اعتبارسنجی و آزمون نیازمند اجرای شیوه‌های مناسب حاکمیت و مدیریت داده است. این مجموعهٔ داده‌ها ازجمله برچسب‌ها باید متناسب، به‌قدر کافی گویای واقعیت و با توجه به هدف موردنظر سامانه تا حد امکان، عاری از خطا و کامل باشند. برای تسهیل رعایت حقوق اتحادیه در زمینهٔ حفاظت از داده‌ها، مانند مقررات ۶۷۹/۲۰۱۶ (اتحادیهٔ اروپا)، شیوه‌های حاکمیت و مدیریت داده باید در صورت پردازش داده‌های شخصی شامل شفافیت دربارهٔ هدف اولیهٔ گردآوری داده‌ها باشند. همچنین مجموعهٔ داده‌ها باید دارای ویژگی‌های آماری مناسب باشند، به‌ویژه در خصوص اشخاص یا گروه‌هایی که سامانهٔ هوش مصنوعی پرخطر در ارتباط با آنان به کار می‌رود. ممکن است این سامانه‌ها با تمرکز خاص بر کاهش سوگیری‌های احتمالی موجود در داده‌ها بر سلامت و ایمنی افراد اثر گذارند و آثار منفی بر حقوق بنیادین داشته یا به تبعیض ممنوع‌شده تحت حقوق اتحادیه بینجامند، به‌ویژه هنگامی که خروجی‌های داده بر ورودی‌های عملیات آتی (چرخه‌های بازخورد)[۴۸] اثرگذار باشند. سوگیری‌ها می‌توانند به‌طور مثال، در داده‌ها مبنایی ذاتی باشند، به‌ویژه هنگام استفاده از داده‌های تاریخی یا در زمان به‌کارگیری سامانه‌ها در محیط‌های واقعی ایجاد شوند. نتایج ارائه‌شده از سوی سامانه‌های هوش مصنوعی می‌تواند تحت تأثیر چنین سوگیری‌های ذاتی قرار گیرد، که تمایل به افزایش تدریجی داشته و بدین‌ترتیب تبعیض موجود را تداوم بخشیده و تشدید می‌کنند، به‌ویژه علیه افراد متعلق به گروه‌های آسیب‌پذیر خاص، ازجمله گروه‌های نژادی یا قومی. الزام به کامل‌بودن و عاری‌بودن از خطا در مجموعهٔ داده‌ها تا حد امکان، نباید مانع استفاده از روش‌های حفظ حریم خصوصی در فرآیند توسعه و آزمون سامانه‌های هوش مصنوعی شود. به‌طور خاص، مجموعهٔ داده‌ها باید تا حدی که هدف موردنظر ایجاب می‌کند، ویژگی‌ها، خصوصیات یا عناصری را در نظر گیرند که مختص محیط جغرافیایی، زمینه‌ای، رفتاری یا کارکردی خاصی است که سامانهٔ هوش مصنوعی برای آن طراحی شده است. می‌توان الزامات مربوط به حاکمیت داده را از طریق توسل به اشخاص ثالثی که خدمات ممیزی دارای گواهی رسمی ارائه می‌دهند ازجمله در زمینهٔ راستی‌آزمایی حاکمیت داده، یکپارچگی مجموعهٔ داده‌ها، شیوه‌های آموزش، اعتبارسنجی و آزمون داده رعایت کرد، مشروط بر آنکه انطباق با الزامات داده‌ای این قانون تضمین شود.

۶۸. برای توسعه و ارزیابی سامانه‌های هوش مصنوعی پرخطر، برخی بازیگران مانند تأمین‌کنندگان، نهادهای اطلاع‌رسان و سایر اشخاص ذی‌ربط ازجمله مراکز نوآوری دیجیتال اروپایی، مراکز آزمایش، آزمون و پژوهشگران باید بتوانند به مجموعهٔ داده‌های باکیفیت در حوزه‌های فعالیت مرتبط

48. feedback loops

با این قانون دسترسی یافته و از آن‌ها استفاده کنند. فضاهای دادهٔ مشترک اروپایی که توسط کمیسیون تأسیس می‌شوند و نیز تسهیل اشتراک‌گذاری داده میان کسب‌وکارها و با کمک دولت در جهت منافع عمومی، نقش اساسی در فراهم‌کردن دسترسی مبتنی بر اعتماد، پاسخگویی و غیرتبعیض‌آمیزبودن داده‌های باکیفیت برای آموزش و اعتبارسنجی سامانه‌های هوش مصنوعی خواهند داشت. برای نمونه، در حوزهٔ سلامت، فضای دادهٔ سلامت اروپا دسترسی غیرتبعیض‌آمیز به داده‌های سلامت و آموزش الگوریتم‌های هوش مصنوعی بر پایهٔ این داده‌ها را تسهیل خواهد کرد، آن هم به نحوی که حفظ حریم خصوصی، امنیت، شفافیت، اعتمادپذیری و زمان‌بندی مناسب تضمین و حاکمیت نهادی مقتضی برقرار باشد. همچنین مراجع ذی‌صلاح مرتبط، ازجمله مراجع بخشی که ارائه یا پشتیبانی دسترسی به داده‌ها را بر عهده دارند، می‌توانند در تأمین داده‌های باکیفیت برای آموزش و اعتبارسنجی سامانه‌های هوش مصنوعی نیز ایفای نقش کنند.

۶۹. حق بر حریم خصوصی و حمایت از داده‌های شخصی باید در سرتاسر چرخهٔ عمر سامانهٔ هوش مصنوعی تضمین شود. در این راستا، اصول کاهش حداقل داده‌ها و حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض، همان گونه که در حقوق حفاظت از داده‌های اتحادیه مقرر شده است در موارد پردازش داده‌های شخصی قابل اعمال است. اقداماتی که از سوی تأمین‌کنندگان برای تضمین رعایت این اصول اتخاذ می‌شود، می‌تواند شامل نه‌تنها ناشناس‌سازی و رمزنگاری، بلکه بهره‌گیری از فناوری‌هایی باشد که امکان می‌دهند الگوریتم‌ها نزد داده‌ها آورده شوند و آموزش سامانه‌های هوش مصنوعی بدون انتقال میان طرفین یا کپی‌برداری از داده‌های خام یا ساختاریافته صورت گیرد، بی‌آنکه به الزامات مربوط به حاکمیت دادهٔ مقرر در این قانون، لطمه‌ای وارد آید.

۷۰. به منظور حمایت از حق دیگران در برابر تبعیضی که ممکن است از انحراف تبعیض‌آمیز در سامانه‌های هوش مصنوعی ناشی شود، تأمین‌کنندگان باید بتوانند به‌طور استثنایی و صرفاً در حدی که برای شناسایی و اصلاح انحرافات تبعیض‌آمیز در سامانه‌های هوش مصنوعی پرخطر به‌طور دقیق ضروری باشد، به پردازش دسته‌های خاصی از داده‌های شخصی نیز مبادرت ورزند. این امر باید همراه با تضمین‌های مقتضی برای حمایت از حقوق بنیادین و آزادی‌های اشخاص حقیقی و با رعایت تمامی شرایط مقرر در این قانون، همچنین شرایط مقرر در مقررات اتحادیهٔ اروپا به شماره‌های ۶۷۹ /۲۰۱۶ و ۱۷۲۵/ ۲۰۱۸ و دستورالعمل ۶۸۰ / ۲۰۱۶ انجام پذیرد. چنین پردازشی به‌عنوان امری مرتبط با منافع عمومی اساسی در معنای بند ۲ (g) ماده ۹ مقررات ۶۷۹ / ۲۰۱۶ و بند ۲ (g) ماده ۱۰ مقررات ۱۷۲۵ / ۲۰۱۸ تلقی خواهد شد.

۷۱. داشتن اطلاعات روشن و قابل فهم در خصوص نحوهٔ توسعهٔ سامانه‌های پرخطر هوش مصنوعی و چگونگی عملکرد آن‌ها در سرتاسر چرخهٔ عمرشان برای تضمین قابلیت ردیابی این سامانه‌ها، احراز انطباق با الزامات این قانون و نیز نظارت بر عملیات و پایش پس از عرضه به بازار ضروری است. این امر مستلزم نگهداری سوابق و فراهم‌بودن مستندات فنی است که باید حاوی اطلاعات لازم برای ارزیابی انطباق سامانهٔ هوش مصنوعی با الزامات مربوطه و تسهیل‌کنندهٔ پایش پس از عرضه به بازار باشند. این اطلاعات باید شامل ویژگی‌های کلی، توانمندی‌ها و محدودیت‌های سامانه، الگوریتم‌ها، داده‌ها، فرآیندهای آموزش، آزمون و اعتبارسنجی مورد استفاده و همچنین مستندات مربوط به نظام مدیریت ریسک ذی‌ربط باشد و در قالبی روشن و جامع تنظیم شود. مستندات فنی باید به‌روزرسانی مستمر داشته و در سرتاسر چرخهٔ عمر سامانهٔ هوش مصنوعی به‌طور مقتضی نگهداری شوند. افزون بر این، سامانه‌های پرخطر هوش مصنوعی باید از حیث فنی این قابلیت را داشته باشند که ثبت خودکار رویدادها (از طریق گزارش‌نگاری/لاگ‌ها)[۴۹] را در طول مدت چرخهٔ عمر خود امکان‌پذیر کنند.

۷۲. به منظور رسیدگی به نگرانی‌ها، ابهامات و پیچیدگی‌های مرتبط با سامانه‌های هوش مصنوعی و کمک به کاربران این سامانه‌ها و همچنین برای رعایت تعهدات خود طبق این قانون، شفافیت برای سامانه‌های هوش مصنوعی پرخطر پیش از عرضه به بازار یا قرارگرفتن در وضعیت استفاده الزامی است. سامانه‌های هوش مصنوعی پرخطر باید به گونه‌ای طراحی شوند که کاربران بتوانند نحوهٔ عملکرد سامانه را درک و کارکرد آن را ارزیابی کنند و توانمندی‌ها و محدودیت‌های آن را بشناسند. این سامانه‌ها باید همراه با اطلاعات مناسب در قالب دستورالعمل‌های استفاده ارائه شوند. چنین اطلاعاتی باید شامل موارد زیر باشد: ویژگی‌ها، توانمندی‌ها و محدودیت‌های عملکرد سامانه، اطلاعات دربارهٔ شرایط شناخته‌شده و پیش‌بینی‌شده مرتبط با استفاده از سامانه‌های پرخطر ازجمله اقدامات کاربران که ممکن است بر رفتار و عملکرد سامانه تأثیر بگذارد و شرایطی که ممکن است سامانه منجر به خطر برای سلامت، ایمنی و حقوق بنیادین شود، تغییرات از پیش‌تعیین‌شده و ارزیابی‌شده برای انطباق توسط تأمین‌کننده و اقدامات نظارت انسانی مرتبط ازجمله اقداماتی برای تسهیل تفسیر خروجی‌های سامانه توسط کاربران. همچنین شفافیت نیز شامل دستورالعمل‌های همراه باید به کاربران در استفادهٔ صحیح و آگاهانه از سامانه کمک کند. کاربران باید ازجمله در انتخاب درست سامانهٔ موردنظر با توجه به تعهدات خود، در آگاهی از کاربردهای مجاز و ممنوع و

۴۹. عبارت گزارش‌نگاری لاگ (Log recording / Logging) یعنی سامانه به‌طور خودکار، تمام رویدادها، تغییرات و عملیات مهمی را که در طول فعالیتش رخ می‌دهد ثبت و ذخیره کند. این گزارش‌ها که به آن‌ها لاگ (Log) گفته می‌شود، معمولاً شامل اطلاعات زیر هستند: زمان دقیق وقوع رویداد، نوع فعالیت یا عملیات انجام‌شده، تغییرات داده یا معیارهای سامانه، هویت کاربری یا سامانه‌ای که تغییر را انجام داده است.

در استفادهٔ صحیح و مناسب از سامانه در موقعیت بهتری قرار داشته باشند. برای افزایش خوانایی و دسترسی‌پذیری اطلاعات موجود در دستورالعمل‌ها در صورت مقتضی باید نمونه‌های مصور مانند محدودیت‌ها و کاربردهای مجاز و ممنوع سامانه درج شوند. تأمین‌کنندگان باید اطمینان حاصل کنند که تمام مستندات ازجمله دستورالعمل‌های استفاده، حاوی اطلاعات معنادار، جامع، قابل دسترس و قابل فهم باشد و نیازها و دانش پیش‌بینی‌شدهٔ کاربران هدف را مدنظر قرار دهد. دستورالعمل‌ها باید به زبانی قابل فهم برای کاربران هدف مطابق کشور عضو مربوطه ارائه شود.

۷۳. سامانه‌های هوش مصنوعی پرخطر باید به گونه‌ای طراحی شده و توسعه یابند که اشخاص حقیقی بتوانند عملکرد آن‌ها را نظارت کنند و اطمینان حاصل نمایند که این سامانه‌ها طبق اهداف تعیین‌شده به‌کارگیری می‌شوند و در سرتاسر چرخهٔ عمر سامانه‌ها به آثار آن‌ها رسیدگی می‌شود. برای این منظور، اقدامات نظارت انسانی مناسب باید توسط تأمین‌کنندهٔ سامانه پیش از عرضه به بازار یا قرارگرفتن در وضعیت استفاده شناسایی شوند. این اقدامات باید به‌طور خاص، تضمین‌کنندهٔ موارد زیر باشند: سامانه دارای محدودیت‌های عملیاتی تعبیه‌شده است و خودبه‌خود نمی‌تواند این محدودیت‌ها را نادیده بگیرد؛ سامانه پاسخگوی عملکرد اپراتور انسانی است و اشخاص حقیقی که مسئول نظارت انسانی هستند از صلاحیت، آموزش و اختیار لازم برای انجام این نقش برخوردارند. همچنین ضروری است در موارد مقتضی که سامانه‌های پرخطر شامل مکانیزم‌هایی برای راهنمایی و اطلاع‌رسانی به اشخاص حقیقی مسئول نظارت انسانی باشند تا آن‌ها بتوانند تصمیمات آگاهانه دربارهٔ زمان و نحوهٔ مداخله برای جلوگیری از پیامدها یا خطرات منفی اتخاذ کنند یا در صورتی که سامانه طبق هدف عمل نمی‌کند، آن را متوقف کنند. با توجه به پیامدهای مهم برای افراد در صورت تشخیص نادرست برخی سامانه‌های شناسایی زیست‌سنجی، مناسب است که الزامات نظارت انسانی تقویت‌شده برای این سامانه‌ها پیش‌بینی شود به‌طوری که هیچ اقدام یا تصمیمی توسط کاربر سامانه بر اساس تشخیص سامانه اتخاذ نشود، مگر اینکه حداقل دو شخص حقیقی جداگانه آن را تأیید کرده باشند. این اشخاص می‌توانند یک یا چند نهاد و شامل اپراتور یا کاربر سامانه نیز باشند. این الزام نباید باعث تحمیل و تأخیر غیرضروری شود و کافی است که تأییدهای جداگانه توسط اشخاص مختلف به‌طور خودکار در لاگ‌ها یا گزارش‌های تولیدشده توسط سامانه ثبت شود. با توجه به ویژگی‌های خاص حوزه‌های اجرای قانون، مهاجرت، کنترل مرز و پناهندگی، این الزام، زمانی که قانون اتحادیه یا قوانین ملی اعمال آن را نامتناسب بداند، قابل اجرا نیست.

۷۴. سامانه‌های هوش مصنوعی پرخطر باید در طول چرخهٔ عمر خود عملکردی پایدار داشته باشند و سطح مناسبی از دقت، پایداری و امنیت سایبری را با توجه به هدف تعیین‌شده و مطابق استانداردهای شناخته‌شدهٔ علمی و فنی رعایت کنند. کمیسیون و سازمان‌ها و ذی‌نفعان ذی‌ربط،

تشویق می‌شوند تا کاهش ریسک‌ها و آثار منفی سامانه‌های هوش مصنوعی را به‌دقت مدنظر قرار دهند. سطح مورد انتظار شاخص‌های عملکرد باید در دستورالعمل‌های استفاده اعلام شود. تأمین‌کنندگان تشویق می‌شوند تا این اطلاعات را به کاربران سامانه به‌صورت واضح، قابل فهم و بدون ابهام یا اطلاعات گمراه‌کننده ارائه کنند. قوانین اتحادیه دربارهٔ استانداردسازی قانونی اندازه‌گیری‌ها،[۵۰] ازجمله دستورالعمل‌های ۳۱ / ۲۰۱۴[۵۱] و ۳۲ / ۲۰۱۴[۵۲] پارلمان و شورای اروپا، با هدف تضمین دقت اندازه‌گیری‌ها و شفافیت و انصاف در معاملات تجاری تدوین شده‌اند. کمیسیون باید در همکاری با سازمان‌ها و ذی‌نفعان ذی‌ربط در این زمینه مانند مراجع سنجش و پایش استانداردها در صورت مقتضی توسعهٔ معیارها و روش‌های اندازه‌گیری برای سامانه‌های هوش مصنوعی را تشویق کند. در انجام این کار، کمیسیون باید به اقدامات شرکای بین‌المللی فعال در زمینهٔ سنجش و شاخص‌های مرتبط با هوش مصنوعی توجه و با آن‌ها همکاری کند.

۷۵. پایداری فنی یکی از الزامات کلیدی برای سامانه‌های هوش مصنوعی پرخطر است. این سامانه‌ها باید در برابر رفتارهای مضر یا نامطلوب ناشی از محدودیت‌های درون سامانه یا محیطی که در آن فعالیت می‌کنند (مثلاً خطاها، نقص‌ها، ناسازگاری‌ها یا شرایط غیرمنتظره) مقاوم باشند. بنابراین اقدامات فنی و سازمانی لازم است تا پایداری سامانه‌های هوش مصنوعی پرخطر تضمین شود؛ برای مثال از طریق طراحی و توسعهٔ راهکارهای فنی مناسب برای جلوگیری یا کاهش رفتارهای مضر یا نامطلوب. این راهکارهای فنی می‌توانند شامل مکانیزم‌هایی باشند که اجازه می‌دهند سامانه در صورت بروز برخی ناهنجاری‌ها یا فعالیت خارج از مرزهای از پیش تعیین‌شده به‌طور ایمن عملیات خود را متوقف کند (برنامه‌های ایمنی خودکار).[۵۳] عدم محافظت در برابر این خطرات می‌تواند منجر به تأثیرات منفی بر ایمنی یا حقوق بنیادین شود، مثلاً به دلیل تصمیمات نادرست یا خروجی‌های اشتباه یا جانبدارانهٔ تولیدشده توسط سامانهٔ هوش مصنوعی.

۷۶. امنیت سایبری نقش اساسی در تضمین مقاومت سامانه‌های هوش مصنوعی در برابر تلاش‌ها برای تغییر کاربری، رفتار، عملکرد یا مختل‌سازی ویژگی‌های امنیتی آن‌ها توسط اشخاص ثالث مخرب دارد که از آسیب‌پذیری‌های سامانه سوءاستفاده می‌کنند. حملات سایبری علیه سامانه‌های

---

۵۰. *استانداردسازی قانونی اندازه‌گیری‌ها* به مجموعه قوانین، مقررات و چارچوب‌های فنی گفته می‌شود که دقت، صحت و قابل اعتمادبودن اندازه‌گیری‌ها را در زمینه‌های مختلف، به‌ویژه در تجارت، سلامت، ایمنی و حفاظت از مصرف‌کننده تضمین می‌کند.

۵۱. دستورالعمل ۳۱/۲۰۱۴ پارلمان و شورای اروپا ۲۶ فوریهٔ ۲۰۱۴ دربارهٔ همسان‌سازی قوانین کشورهای عضو در ارتباط با عرضهٔ ابزارهای اندازه‌گیری غیرخودکار در بازار (روزنامهٔ رسمی ۹۶، ۲۰۱۴/۳/۲۹، ص ۱۰۷).

۵۲. دستورالعمل ۳۲/۲۰۱۴ پارلمان و شورای اروپا در ۲۶ فوریهٔ ۲۰۱۴ دربارهٔ همسان‌سازی قوانین کشورهای عضو در ارتباط با عرضهٔ ابزارهای اندازه‌گیری در بازار (روزنامهٔ رسمی ۹۶، ۲۰۱۴/۳/۲۹، ص ۱۴۹).

53. fail-safe plans

هوش مصنوعی می‌توانند بر دارایی‌های خاص این سامانه‌ها متمرکز شوند، مانند مجموعه داده‌های آموزشی (برای نمونه، آلوده‌سازی یا دستکاری مخرب داده‌ها)[۵۴] یا مدل‌های آموزش‌دیده (برای مثال، حملات متخاصم الگوریتمی[۵۵] یا تشخیص عضویت داده)[۵۶] یا از طریق بهره‌برداری از آسیب‌پذیری‌های موجود در دارایی‌های دیجیتال سامانه یا زیرساخت‌های فناوری اطلاعات و ارتباطات زیربنایی انجام شوند. برای تضمین سطحی از امنیت سایبری متناسب با مخاطرات، لازم است که تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر، تدابیر مناسب ازجمله کنترل‌های امنیتی را به کار گیرند و در صورت لزوم، زیرساخت زیربنایی را نیز مدنظر قرار دهند.

۷۷. بدون خدشه به الزامات مرتبط و مقرر در این قانون، سامانه‌های هوش مصنوعی پرخطر که در قلمرو شمول مقررات پارلمان و شورای اروپا در خصوص الزامات عام امنیت سایبری برای محصولات دارای عناصر دیجیتال قرار می‌گیرند، می‌توانند با رعایت الزامات اساسی امنیت سایبری مقرر در آن مقررات، انطباق خود را با الزامات امنیت سایبری مندرج در این قانون احراز کنند. هر گاه سامانه‌های هوش مصنوعی پرخطر، الزامات اساسی مندرج در مقررات پارلمان و شورای اروپا در زمینهٔ الزامات عام امنیت سایبری برای محصولات دارای عناصر دیجیتال را برآورده کنند، متعاقباً باید با الزامات امنیت سایبری پیش‌بینی‌شده در این قانون نیز منطبق باشند مشروط بر آنکه تحقق این الزامات در اعلامیهٔ انطباق اتحادیهٔ اروپا یا بخش‌های مربوط به آن که بر اساس مقررات مزبور صادر شده است، اثبات شود. بدین منظور، ارزیابی مخاطرات امنیت سایبری مرتبط با یک محصول دارای عناصر دیجیتال که طبق این مقررات به‌عنوان سامانهٔ هوش مصنوعی پرخطر طبقه‌بندی شده است و تحت مقررات پارلمان و شورای اروپا در خصوص الزامات عام امنیت سایبری برای محصولات دارای عناصر *دیجیتال* انجام می‌شود، باید به خطرات مربوط به پایداری سایبری سامانهٔ هوش مصنوعی در برابر تلاش اشخاص ثالث غیرمجاز برای تغییر در کاربری، رفتار یا عملکرد آن ازجمله آسیب‌پذیری‌های خاص هوش مصنوعی نظیر *دستکاری مخرب داده‌ها* یا *حملات متخاصم الگوریتمی* و همچنین در صورت اقتضا، به خطرات مربوط به حقوق بنیادین، مطابق الزامات این قانون توجه کند.

---

۵۴. عبارت Data Poisoning نوعی حمله است که در آن مهاجم به داده‌های آموزشی یک مدل هوش مصنوعی دسترسی پیدا کرده و آن‌ها را تغییر می‌دهد یا داده‌های جعلی به آن اضافه می‌کند.

۵۵. عبارت Adversarial Attacks نوعی حمله است که در آن مهاجم ورودی‌هایی طراحی می‌کند که از نظر انسان، طبیعی یا بی‌ضرر به نظر می‌رسند اما موجب خطا در تصمیم‌گیری مدل می‌شوند.

۵۶. عبارت membership inference معمولاً به این معناست که مهاجم می‌خواهد تشخیص دهد آیا دادهٔ خاصی در مجموعهٔ آموزشی یک مدل هوش مصنوعی وجود داشته است یا خیر.

۷۸. رویهٔ ارزیابی انطباق مقرر در این قانون باید در ارتباط با الزامات اساسی امنیت سایبری یک محصول دارای عناصر دیجیتال که مشمول مقررات پارلمان و شورای اروپا در خصوص الزامات عام امنیت سایبری برای محصولات دارای عناصر دیجیتال بوده و تحت این قانون به‌عنوان سامانهٔ هوش مصنوعی پرخطر طبقه‌بندی شده است، اعمال شود. با این حال، نباید این قاعده، سطح لازم اطمینان را برای محصولات حیاتی دارای عناصر دیجیتال که مشمول مقررات پارلمان و شورای اروپا در خصوص الزامات عام امنیت سایبری برای محصولات دارای عناصر دیجیتال هستند، کاهش دهد. بنابراین به‌عنوان استثنا از این قاعده، سامانه‌های هوش مصنوعی پرخطری که در قلمرو شمول این قانون قرار می‌گیرند و همچنین بر اساس مقررات پارلمان و شورای اروپا در زمینهٔ الزامات عام امنیت سایبری برای محصولات دارای عناصر دیجیتال به‌عنوان محصولات مهم و حیاتی دارای عناصر دیجیتال محسوب می‌شوند و نسبت به آن‌ها رویهٔ ارزیابی انطباق مبتنی بر کنترل داخلی مندرج در یکی از پیوست‌های این قانون اعمال می‌شود، صرفاً از حیث الزامات اساسی امنیت سایبری مشمول مقررات ارزیابی انطباق مقرر در مقررات پارلمان و شورای اروپا در زمینهٔ الزامات عام امنیت سایبری برای محصولات دارای عناصر دیجیتال خواهند بود. در این حالت، در خصوص سایر جنبه‌هایی که تحت پوشش این قانون قرار دارند، احکام مربوط به ارزیابی انطباق مبتنی بر کنترل داخلی مندرج در یکی از پیوست‌های همین قانون اعمال می‌شود. کمیسیون، با بهره‌گیری از دانش و تخصص *آژانس اتحادیهٔ اروپا برای امنیت سایبری*[۵۷] در زمینهٔ سیاست امنیت سایبری و وظایف محوله به آن بر اساس مقررات ۸۸۱ / ۲۰۱۹[۵۸] پارلمان و شورای اروپا باید در موضوعات مرتبط با امنیت سایبری سامانه‌های هوش مصنوعی با آژانس یادشده همکاری کند.

۷۹. شایسته است شخص معین حقیقی یا حقوقی که به‌عنوان *تأمین‌کننده* تعریف می‌شود، مسئولیت عرضه در بازار یا به‌کارگیری سامانهٔ هوش مصنوعی پرخطر را بر عهده گیرد، صرف‌نظر از آنکه آن شخص حقیقی یا حقوقی، طراح یا توسعه‌دهندهٔ سامانه باشد یا خیر.

۸۰. به‌عنوان امضاکنندگان کنوانسیون حقوق افراد دارای معلولیت، سازمان ملل متحد، اتحادیه و کشورهای عضو از نظر حقوقی موظف به حفاظت از افراد دارای معلولیت در برابر تبعیض و ارتقاء برابری آن‌ها هستند، به گونه‌ای که اطمینان حاصل شود افراد دارای معلولیت بر پایهٔ برابری با دیگران، به فناوری‌ها و سامانه‌های اطلاعات و ارتباطات دسترسی داشته باشند و همچنین حریم خصوصی آنان رعایت شود. با توجه به اهمیت فزاینده و کاربرد گستردهٔ سامانه‌های هوش مصنوعی،

57. European Union Agency for Cybersecurity (ENISA)

۵۸. مقررات شمارهٔ ۸۸۱/۲۰۱۹ پارلمان و شورای اروپا در ۱۷ آوریل ۲۰۱۹ دربارهٔ آژانس اتحادیهٔ اروپا برای امنیت سایبری و در خصوص صدور گواهی امنیت سایبری در حوزهٔ فناوری‌های اطلاعات و ارتباطات و لغو مقررات پیشین (روزنامهٔ رسمی ۱۵۱، ۲۰۱۹/۶/۷، ص ۱۵).

اعمال اصول طراحی جهانی در تمامی فناوری‌ها و خدمات جدید باید دسترسی کامل و برابر را برای تمامی کسانی که ممکن است تحت تأثیر استفاده از فناوری‌های هوش مصنوعی قرار می‌گیرند، ازجمله افراد دارای معلولیت فراهم آورد به نحوی که به‌طور کامل به کرامت ذاتی و تنوع آن‌ها توجه شود. بنابراین ضروری است که تأمین‌کنندگان اطمینان حاصل کنند که الزامات دسترس‌پذیری ازجمله دستورالعمل ۲۰۱۶/۲۱۰۲[۵۹] و دستورالعمل ۲۰۱۹/۸۸۲ پارلمان و شورای اروپا به‌طور کامل رعایت می‌شود. همچنین تأمین‌کنندگان باید از طریق طراحی اطمینان حاصل کنند که این الزامات رعایت می‌شوند. از این رو اقدامات لازم باید تا حد امکان در طراحی سامانهٔ هوش مصنوعی پرخطر مدنظر قرار گیرد.

۸۱. تأمین‌کننده باید سامانهٔ مدیریت کیفیت مستحکم برقرار و اطمینان حاصل کند که فرآیند ارزیابی انطباق مورد نیاز به‌درستی انجام شده است. مستندات مربوطه را تهیه و یک سامانهٔ پایش مستحکم پس از عرضه به بازار ایجاد کند. تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر که مشمول تعهدات مرتبط با سامانه‌های مدیریت کیفیت طبق قوانین اتحادیهٔ اروپا هستند، باید امکان داشته باشند عناصر سامانهٔ مدیریت کیفیت پیش‌بینی‌شده در این قانون را با بخشی از سامانهٔ مدیریت کیفیت موجود خود در آن قوانین اتحادیه ادغام کنند. همچنین باید در فعالیت‌های آتی استانداردسازی یا رهنمودهایی که توسط کمیسیون اتخاذ می‌شوند، تکمیل این قانون و قوانین موجود اتحادیه مدنظر قرار گیرند. مقامات عمومی که سامانه‌های هوش مصنوعی پرخطر را برای استفادهٔ داخلی خود به‌کار می‌گیرند، می‌توانند قوانین مربوط به سامانهٔ مدیریت کیفیت را به‌عنوان بخشی از سامانهٔ مدیریت کیفیت پذیرفته‌شده در سطح ملی یا منطقه‌ای با توجه به مقتضیات و با درنظرگرفتن ویژگی‌های خاص آن بخش، صلاحیت‌ها و سازمان‌دهی مرجع عمومی مربوطه اتخاذ و اجرا کنند.

۸۲. برای امکان اجرای این قانون و ایجاد شرایط یکسان برای بهره‌برداران و با درنظرگرفتن شکل‌های مختلف عرضهٔ محصولات دیجیتال، مهم است که تحت هر شرایطی، شخصی که در اتحادیه مستقر است بتواند تمام اطلاعات لازم را دربارهٔ انطباق سامانهٔ هوش مصنوعی به مراجع ذی‌ربط ارائه کند. بنابراین پیش از آنکه تأمین‌کنندگان مستقر در کشورهای ثالث، سامانه‌های هوش مصنوعی خود را در اتحادیه عرضه کنند، باید با وکالتنامهٔ کتبی یک نمایندهٔ مجاز مستقر در اتحادیه را تعیین کنند. این نمایندهٔ مجاز، نقش محوری در اطمینان از انطباق سامانه‌های هوش مصنوعی پرخطر عرضه‌شده یا به‌کارگرفته‌شده در بازار اتحادیه توسط تأمین‌کنندگانی که در اتحادیه

۵۹. دستورالعمل شمارهٔ ۲۰۱۶/۲۱۰۲ پارلمان و شورای اروپا در ۲۶ اکتبر ۲۰۱۶ دربارهٔ دسترس‌پذیری وب‌سایت‌ها و برنامه‌های کاربردی موبایل نهادهای بخش عمومی (روزنامهٔ رسمی ۳۲۷، ۲۰۱۶/۱۲/۲، ص ۱).

مستقر نیستند ایفا می‌کند و همچنین به‌عنوان شخص مسئول ارتباطات آنان مستقر در اتحادیه عمل می‌کند.

۸۳. در پرتو ماهیت و پیچیدگی زنجیرهٔ ارزشی سامانه‌های هوش مصنوعی و مطابق چارچوب قانونگذاری جدید، تضمین اطمینان حقوقی و تسهیل رعایت این مقررات ضروری است. از این رو لازم است نقش و تعهدات مشخص متصدیان ذی‌ربط در طول این زنجیرهٔ ارزشی ازجمله واردکنندگان و توزیع‌کنندگان که ممکن است در توسعهٔ سامانه‌های هوش مصنوعی نقش داشته باشند، روشن شود. در برخی موارد، ممکن است این بهره‌برداران همزمان در بیش از یک نقش عمل کنند و بنابراین باید به‌صورت تجمیعی تمام تعهدات مربوط به آن نقش‌ها را ایفا کنند. برای مثال، یک متصدی می‌تواند همزمان به‌عنوان توزیع‌کننده و واردکننده فعالیت کند.

۸۴. تحت شرایط خاص و مشخص و برای تضمین اطمینان حقوقی لازم است روشن شود که هر توزیع‌کننده، واردکننده، بهره‌بردار یا شخص ثالث دیگر باید به‌عنوان تأمین‌کنندهٔ سامانهٔ هوش مصنوعی پرخطر محسوب شود و بنابراین تمام تعهدات مرتبط را بر عهده گیرد. این وضعیت، زمانی رخ می‌دهد که آن طرف بدون خدشه به ترتیبات قراردادی که تعهدات را به نحو دیگری مشخص می‌کنند، نام یا علامت تجاری خود را بر سامانهٔ هوش مصنوعی پرخطر که قبلاً در بازار عرضه یا به کار گرفته شده است، قرار دهد. همچنین این وضعیت، زمانی صدق می‌کند که آن طرف تغییر قابل‌ملاحظه‌ای در یک سامانهٔ هوش مصنوعی پرخطر که قبلاً در بازار عرضه یا به کار گرفته شده ایجاد کند به نحوی که سامانه همچنان طبق این قانون سامانهٔ هوش مصنوعی پرخطر باقی بماند. وضعیت دیگر اینکه هدف موردنظر یک سامانهٔ هوش مصنوعی ازجمله سامانهٔ هوش مصنوعی عمومی را که تا کنون به‌عنوان سامانهٔ پرخطر طبقه‌بندی نشده و قبلاً در بازار عرضه یا به کار گرفته شده است تغییر دهد، به نحوی که آن سامانه طبق این قانون تبدیل به سامانهٔ هوش مصنوعی پرخطر شود. این احکام باید بدون خدشه به مقررات خاص مندرج در برخی قوانین هماهنگ‌شدهٔ اتحادیه مبتنی بر چارچوب قانونگذاری جدید اعمال شوند و این قانون باید همراه با آن‌ها اجرا شود. برای مثال، بند (۲) ماده ۱۶ از مقررات ۲۰۱۷/۷۴۵ که مقرر می‌دارد برخی تغییرات نباید به‌عنوان اصلاحات دستگاهی تلقی شوند که بر انطباق آن با الزامات قابل اجرا اثر می‌گذارد بلکه باید نسبت به سامانه‌های هوش مصنوعی پرخطری که به‌عنوان دستگاه‌های پزشکی طبق همان مقررات شناخته می‌شوند نیز اعمال شود.

۸۵. ممکن است سامانه‌های *هوش مصنوعی عمومی*[۶۰] به‌تنهایی به‌عنوان سامانه‌های هوش مصنوعی پرخطر به کار روند یا به‌عنوان اجزای دیگر سامانه‌های هوش مصنوعی پرخطر عمل کنند. از این رو با توجه به ماهیت خاص این سامانه‌ها و به منظور تضمین تقسیم عادلانهٔ مسئولیت‌ها

60. General-purpose AI systems

در طول زنجیرهٔ ارزش هوش مصنوعی، تأمین‌کنندگان چنین سامانه‌هایی صرف‌نظر از اینکه آیا ممکن است سامانه‌ها توسط سایر تأمین‌کنندگان به‌عنوان سامانه‌های هوش مصنوعی پرخطر مستقل یا به‌عنوان اجزای سامانه‌های هوش مصنوعی پرخطر به کار روند، باید با تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر ذی‌ربط همکاری نزدیک داشته باشند تا امکان رعایت تعهدات مربوطه طبق این قانون و تعامل مؤثر با مراجع ذی‌صلاح مستقر طبق این قانون فراهم شود، مگر آنکه در این قانون پیش‌بینی دیگری شده باشد.

۸۶. در مواردی که طبق شرایط مقرر در این قانون، تأمین‌کننده‌ای در ابتدا سامانهٔ هوش مصنوعی را در بازار عرضه کرده یا به کار گرفته باشد، دیگر به‌عنوان تأمین‌کننده برای اهداف این قانون محسوب نمی‌شود و زمانی که آن تأمین‌کننده صراحتاً تغییر سامانهٔ هوش مصنوعی به سامانهٔ پرخطر را مستثنا نکرده باشد، تأمین‌کنندهٔ پیشین باید همکاری نزدیک داشته باشد و اطلاعات لازم را در دسترس قرار دهد و دسترسی فنی و سایر کمک‌های معقول مورد انتظار را که برای اجرای تعهدات مقرر در این قانون لازم است به‌ویژه در خصوص رعایت الزامات ارزیابی انطباق سامانه‌های هوش مصنوعی پرخطر فراهم کند.

۸۷. علاوه بر این، اگر یک سامانهٔ هوش مصنوعی پرخطر که به‌عنوان جزء ایمنی یک محصول شناخته می‌شود و تحت قوانین هماهنگ‌شدهٔ اتحادیه مبتنی بر چارچوب قانونگذاری جدید قرار دارد، به‌صورت مستقل از محصول عرضه یا به کار گرفته نشود، تولیدکنندهٔ آن محصول موظف است تمام تعهدات تأمین‌کننده طبق این قانون را رعایت کند و به‌ویژه اطمینان دهد که سامانهٔ هوش مصنوعی تعبیه‌شده در محصول نهایی، مطابق الزامات این قانون عمل می‌کند.

۸۸. در طول زنجیرهٔ ارزش هوش مصنوعی غالباً چندین طرف مختلف سامانه‌ها، ابزارها و خدمات هوش مصنوعی و همچنین اجزا یا فرآیندهایی را تأمین می‌کنند که توسط تأمین‌کننده در سامانهٔ هوش مصنوعی ادغام می‌شوند و اهداف مختلفی را دنبال می‌کنند، ازجمله آموزش مدل، بازآموزی مدل، آزمون و ارزیابی مدل، ادغام در نرم‌افزار یا سایر جنبه‌های توسعهٔ مدل. این طرف‌ها نقش مهمی در زنجیرهٔ ارزش در قبال تأمین‌کنندهٔ سامانهٔ هوش مصنوعی پرخطر که سامانه‌ها، ابزارها، خدمات، اجزا یا فرآیندهای آن‌ها در آن ادغام شده است، ایفا می‌کنند و باید بر اساس توافقنامهٔ کتبی، اطلاعات، امکانات، دسترسی فنی و سایر کمک‌های لازم را مطابق وضعیت شناخته‌شده و متداول فناوری در اختیار تأمین‌کننده قرار دهند تا تأمین‌کننده بتواند به‌طور کامل به تعهدات مقرر در این قانون عمل کند، بدون آنکه حقوق مالکیت فکری یا اسرار تجاری خود طرف‌ها به خطر بیفتد.

۸۹. اشخاص ثالثی که ابزارها، خدمات، فرآیندها یا اجزای هوش مصنوعی بجز مدل‌های هوش مصنوعی عمومی را در دسترس عموم قرار می‌دهند، البته زمانی که این ابزارها، خدمات، فرآیندها یا اجزا به‌صورت مجوز آزاد و متن‌باز در دسترس قرار گرفته باشند، وظیفه‌ای برای رعایت الزامات مربوط به مسئولیت‌ها در طول زنجیرهٔ ارزش هوش مصنوعی به‌ویژه در قبال تأمین‌کننده‌ای که از آن‌ها استفاده کرده یا آن‌ها را ادغام کرده است ندارند. البته توسعه‌دهندگان ابزارها، خدمات، فرآیندها یا اجزای هوش مصنوعی آزاد و متن‌باز بجز مدل‌های هوش مصنوعی عمومی باید تشویق شوند تا شیوه‌های مستندسازی رایج و پذیرفته‌شده مانند *کارت‌های مدل*[۶۱] و *برگه‌های داده*[۶۲] را با هدف تسریع اشتراک‌گذاری اطلاعات در طول زنجیرهٔ ارزش هوش مصنوعی و ارتقاء سامانه‌های هوش مصنوعی قابل اعتماد در اتحادیهٔ اروپا اجرا کنند.

۹۰. کمیسیون می‌تواند شرایط قراردادی داوطلبانه میان تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر و اشخاص ثالث تأمین‌کنندهٔ ابزارها، خدمات، اجزا یا فرآیندها را که در سامانه‌های هوش مصنوعی پرخطر استفاده یا ادغام می‌شوند به منظور تسهیل همکاری در طول زنجیرهٔ ارزش، تدوین و توصیه کند. همچنین هنگام تدوین این شرایط قراردادی داوطلبانه، کمیسیون باید الزامات قراردادی ممکن در بخش‌ها یا موارد تجاری خاص را نیز مدنظر قرار دهد.

۹۱. با توجه به ماهیت سامانه‌های هوش مصنوعی و خطراتی که استفاده از آن‌ها ممکن است برای ایمنی و حقوق بنیادین ایجاد کند ازجمله ضرورت اطمینان از پایش مناسب عملکرد سامانهٔ هوش مصنوعی در محیط واقعی، شایسته است که مسئولیت‌های مشخصی برای بهره‌برداران تعیین شود. بهره‌برداران باید به‌ویژه اقدامات فنی و سازمانی مناسبی اتخاذ کنند تا اطمینان حاصل کنند که سامانه‌های هوش مصنوعی پرخطر مطابق دستورالعمل‌های استفاده به کار گرفته می‌شوند و برخی تعهدات دیگر نیز باید در خصوص پایش عملکرد سامانه‌های هوش مصنوعی و نگهداری سوابق حسب مقتضی پیش‌بینی شود. افزون بر این، بهره‌برداران باید اطمینان حاصل کنند که افرادی که مأمور اجرای دستورالعمل‌های استفاده و نظارت انسانی طبق این قانون شده‌اند، دارای صلاحیت لازم ازجمله سطح کافی سواد هوش مصنوعی، آموزش و اختیارات لازم برای انجام صحیح وظایف خود باشند. این تعهدات بدون خدشه به سایر تعهدات بهره‌برداران در رابطه با سامانه‌های هوش مصنوعی پرخطر طبق قوانین اتحادیه یا قوانین ملی اعمال می‌شود.

---

۶۱. عبارت *کارت مدل* (Model Card) مستند رسمی و استانداردشده است که اطلاعات کلیدی دربارهٔ یک مدل هوش مصنوعی ارائه می‌دهد، مانند هدف مدل، داده‌های آموزشی، معیارهای عملکرد، ملاحظات اخلاقی و شرایط استفادهٔ مناسب.

۶۲. عبارت *برگهٔ داده* (Data Sheet) مستندی است که اطلاعات کامل دربارهٔ مجموعهٔ داده‌ها را ارائه می‌دهد، مانند مشخصات داده، روش جمع‌آوری و پردازش، محدودیت‌ها و ملاحظات، مجوزها و حقوق استفاده از داده.

۹۲. این قانون بدون خدشه نسبت به تعهدات کارفرمایان برای اطلاع‌رسانی و مشورت با کارگران یا نمایندگان آن‌ها طبق قوانین و رویه‌های اتحادیه یا قوانین ملی ازجمله دستورالعمل۱۴ /۲۰۰۲[۶۳] پارلمان و شورای اروپا در خصوص تصمیمات به‌کارگیری یا استفاده از سامانه‌های هوش مصنوعی اعمال می‌شود. همچنین در مواردی که شرایط لازم برای تعهدات اطلاع‌رسانی و مشورت در سایر متون قانونی فراهم نشده باشد، ضروری است که اطلاع‌رسانی به کارگران و نمایندگان آن‌ها در مورد استقرار برنامه‌ریزی‌شدهٔ سامانه‌های هوش مصنوعی پرخطر در محیط کار تضمین شود. علاوه بر این، چنین حق اطلاع‌رسانی، حق فرعی و ضروری برای تحقق هدف حفاظت از حقوق بنیادین است که اساس این قانون را تشکیل می‌دهد. بنابراین الزام برای اطلاع‌رسانی در این خصوص باید در این قانون پیش‌بینی شود، بدون آنکه حقوق موجود کارگران تحت تأثیر قرار گیرد.

۹۳. در حالی که ممکن است خطرات مرتبط با سامانه‌های هوش مصنوعی ناشی از نحوهٔ طراحی این سامانه‌ها باشد، همچنین ممکن است خطرات از نحوهٔ استفاده از این سامانه‌ها نیز ناشی شوند. بنابراین بهره‌برداران سامانه‌های هوش مصنوعی پرخطر، نقش حیاتی در تضمین حفاظت از حقوق بنیادین ایفا می‌کنند و مکمل تعهدات تأمین‌کننده در مرحلهٔ توسعهٔ سامانهٔ هوش مصنوعی هستند. بهره‌برداران بهترین موقعیت را برای درک نحوهٔ استفادهٔ عملی از سامانهٔ هوش مصنوعی پرخطر دارند زیرا دانش دقیق‌تری از زمینهٔ استفاده، اشخاص یا گروه‌های احتمالی متأثر ازجمله گروه‌های آسیب‌پذیر دارند و بنابراین می‌توانند خطرات بالقوه‌ای را که در مرحلهٔ توسعه پیش‌بینی نشده‌اند شناسایی کنند. بهره‌برداران سامانه‌های هوش مصنوعی پرخطری که در پیوست این قانون فهرست شده‌اند، همچنین نقش حیاتی در اطلاع‌رسانی به افراد حقیقی دارند و باید زمانی که تصمیم‌گیری می‌کنند یا در تصمیم‌گیری مرتبط با افراد حقیقی مشارکت دارند، در صورت مقتضی، افراد حقیقی را مطلع کنند که آن‌ها تحت استفاده از سامانهٔ هوش مصنوعی پرخطر قرار دارند. این اطلاع‌رسانی باید شامل هدف موردنظر و نوع تصمیماتی که سامانه اتخاذ می‌کند باشد. همچنین بهره‌بردار باید افراد حقیقی را از حق خود برای دریافت توضیح طبق این قانون آگاه کند. در خصوص سامانه‌های هوش مصنوعی پرخطری که برای اهداف اجرای قانون به‌کار گرفته می‌شوند، این تعهد باید طبق ماده ۱۳ دستورالعمل ۲۰۱۶/۶۸۰ پارلمان و شورای اروپا اجرا شود.

۹۴. هر گونه پردازش داده‌های زیست‌سنجی در چارچوب استفاده از سامانه‌های هوش مصنوعی برای شناسایی زیست‌سنجی به منظور اجرای قانون باید مطابق ماده ۱۰ دستورالعمل ۲۰۱۶/۶۸۰ انجام

۶۳. دستورالعمل ۱۴/۲۰۰۲ پارلمان و شورای اروپا در ۱۱ مارس ۲۰۰۲ در خصوص ایجاد چارچوب کلی برای اطلاع‌رسانی و مشورت با کارمندان در جامعهٔ اروپایی (روزنامهٔ رسمی ۲۰۰۲/۳/۸۰۲۳، ص ۲۹).

شود که چنین پردازشی را تنها در صورتی مجاز می‌داند که به‌طور کاملاً ضروری و تحت ضمانت‌های مناسب برای حقوق و آزادی‌های شخص و با مجوز قانون اتحادیه یا کشور عضو باشد. همچنین این استفاده، زمانی مجاز است که اصول مقرر در بند ۱ماده ۴ دستورالعمل ۲۰۱۶/۶۸۰ را رعایت کند، ازجمله قانون‌مندی، انصاف و شفافیت، محدودیت هدف، دقت و محدودیت نگهداری داده‌ها.

۹۵. بدون خدشه به قوانین قابل اجرا در اتحادیهٔ اروپا، ازجمله مقررات ۲۰۱۶/۶۷۹ و دستورالعمل ۲۰۱۶/۶۸۰ پارلمان و شورای اروپا، با توجه به ماهیت مداخله‌جویانهٔ *سامانه‌های شناسایی زیست‌سنجی پس از ضبط از راه دور*،[۶۴] استفاده از این سامانه‌ها باید مشروط به اتخاذ تدابیر حفاظتی مناسب باشد. سامانه‌های شناسایی زیست‌سنجی پس از ضبط از راه دور باید همواره به گونه‌ای استفاده شوند که تناسب، مشروعیت و ضرورت مطلق رعایت شود و باید به شناسایی افراد، مکان و محدودهٔ زمانی بپردازد و مبتنی بر مجموعه‌ای از تصاویر ویدئویی قانونی و هدفمند باشند. در هر صورت، سامانه‌های شناسایی زیست‌سنجی پس از ضبط از راه دور نباید در چارچوب اجرای قانون به منظور نظارت غیرمتمایز و گسترده به کار گرفته شوند. شرایط استفاده از سامانه‌های شناسایی زیست‌سنجی پس از ضبط از راه دور نیز نباید به گونه‌ای باشد که امکان دورزدن مقررات ممنوعیت و استثنائات سختگیرانهٔ مربوط به *شناسایی زیست‌سنجی در زمان واقعی از راه دور*[۶۵] را فراهم کند.

۹۶. به منظور تضمین مؤثر حمایت از حقوق بنیادین، استفاده‌کنندگان از سامانه‌های پرخطر هوش مصنوعی که نهادهای تابع حقوق عمومی هستند یا اشخاص خصوصی که خدمات عمومی ارائه می‌دهند و نیز استفاده‌کنندگان از برخی سامانه‌های پرخطر مندرج در پیوست این قانون نظیر نهادهای بانکی یا بیمه‌ای، باید پیش از بهره‌برداری از سامانه، *ارزیابی تأثیر بر حقوق بنیادین* را انجام دهند. خدماتی که برای افراد، ماهیتی عمومی دارند ممکن است توسط نهادهای خصوصی نیز ارائه شوند. این نهادهای خصوصی که خدمات عمومی ارائه می‌دهند، به وظایفی در راستای منافع عمومی ازجمله در حوزه‌های آموزش، بهداشت و درمان، خدمات اجتماعی، مسکن و دادگستری مرتبط هستند. هدف از ارزیابی تأثیر بر حقوق بنیادین آن است که استفاده‌کننده، خطرات مشخصی را که ممکن است حقوق افراد یا گروه‌های خاصی را تحت تأثیر قرار دهد شناسایی کرده و تدابیر مقتضی برای مواجهه با تحقق این خطرات را تعیین کند. این ارزیابی باید

---

۶۴. عبارت *سامانه‌های شناسایی زیست‌سنجی پس از ضبط از راه دور*(Post-remote biometric identification systems) به معنای تشخیص هویت افراد با استفاده از داده‌های زیست‌سنجی (مانند چهره یا اثر انگشت) که قبلاً از راه دور جمع‌آوری و ضبط شده‌اند است، بدون اینکه شناسایی در همان لحظهٔ جمع‌آوری داده‌ها انجام شود.

۶۵. عبارت *شناسایی زیست‌سنجی در زمان واقعی از راه دور* (real time remote biometric identification) به معنای تشخیص هویت افراد به‌صورت زنده و لحظه‌ای، با استفاده از داده‌های زیست‌سنجیِ جمع‌آوری‌شده از فاصلهٔ دور (مانند تصاویر ویدئویی یا حسگرهای دوربین) بدون نیاز به حضور فیزیکی فرد است.

پیش از به‌کارگیری سامانهٔ پرخطر انجام شود و در صورت تغییر عوامل مؤثر، به‌روزرسانی شود. در این ارزیابی باید فرآیندهای مرتبط استفاده‌کننده و مطابقت سامانهٔ پرخطر با هدف پیش‌بینی‌شده مشخص شود و همچنین شامل توضیحاتی دربارهٔ مدت‌زمان و دفعات استفاده از سامانه و نیز دسته‌های مشخصی از اشخاص حقیقی یا گروه‌هایی باشد که در بستر استفادهٔ معین، احتمالاً متأثر خواهند شد. افزون بر این، ارزیابی باید به شناسایی خطرات و آسیب‌های خاصی بپردازد که می‌تواند بر حقوق بنیادین این افراد یا گروه‌ها اثرگذار باشد. در انجام این ارزیابی، استفاده‌کننده باید اطلاعات مرتبط با ارزیابی صحیح ازجمله (اما محدود به این مورد نیست) اطلاعاتی را که از سوی تأمین‌کنندهٔ سامانهٔ پرخطر هوش مصنوعی در دستورالعمل‌های بهره‌برداری ارائه می‌شود در نظر گیرد. با توجه به خطرات شناسایی‌شده، استفاده‌کنندگان باید تدابیری را برای مواجهه با تحقق احتمالی آن خطرات اتخاذ کنند، مانند سازوکارهای حکمرانی در بستر استفادهٔ خاص، ترتیبات نظارت انسانی طبق دستورالعمل‌های بهره‌برداری یا رویه‌های رسیدگی به شکایات و جبران خسارت. این موارد می‌توانند در کاهش خطرات تهدیدکنندهٔ حقوق بنیادین در موقعیت‌های مشخص، نقش مؤثری ایفا کنند. پس از انجام ارزیابی، استفاده‌کننده باید مقام ناظر ذی‌ربط در بازار را مطلع کند. در صورت اقتضا، به منظور گردآوری اطلاعات لازم برای انجام ارزیابی تأثیر، استفاده‌کنندگان سامانه‌های پرخطر به‌ویژه هنگامی که این سامانه‌ها در بخش عمومی به کار گرفته می‌شوند می‌توانند ذی‌نفعان ذی‌ربط ازجمله نمایندگان گروه‌های افرادی که احتمالاً تحت تأثیر سامانه قرار می‌گیرند، کارشناسان مستقل و سازمان‌های جامعهٔ مدنی را در فرآیند انجام این ارزیابی‌ها و طراحی تدابیر مقابله با تحقق خطرات دخالت دهند. دفتر اروپایی هوش مصنوعی باید یک الگوی پرسش‌نامه تدوین کند تا رعایت الزامات را تسهیل و بار مسئولیت را برای استفاده‌کنندگان کاهش دهد.

۹۷. مفهوم مدل‌های هوش مصنوعی با مقاصد عام باید به‌روشنی تعریف و از مفهوم *سامانه‌های هوش مصنوعی* متمایز شود تا قطعیت حقوقی تضمین شود. تعریف مزبور باید بر ویژگی‌های عملکردی اساسی یک مدل هوش مصنوعی با مقاصد عام به‌ویژه بر جنبه‌های عمومیت و توانایی انجام شایستهٔ طیف گسترده‌ای از وظایف متمایز مبتنی باشد. این مدل‌ها به‌طور معمول بر اساس کلان‌داده‌ها و در مقیاس وسیع مورد آموزش قرار گرفته و از روش‌های متنوعی مانند یادگیری خودنظارتی، یادگیری بدون نظارت یا یادگیری تقویتی بهره می‌گیرند. ممکن است مدل‌های هوش مصنوعی با مقاصد عام به طرق مختلف در بازار عرضه شوند، ازجمله از طریق کتابخانه‌ها، رابط‌های برنامه‌نویسی کاربردی،[۶۶] دانلود مستقیم یا نسخه‌های فیزیکی. این مدل‌ها می‌توانند در ادامه تغییر یافته یا از طریق تنظیمات تکمیلی به مدل‌های جدید تبدیل شوند. با این حال، مدل‌های هوش مصنوعی، اجزای اساسی

66. Application programming interfaces (APIs)

سامانه‌های هوش مصنوعی را تشکیل می‌دهند و به خودی خود *سامانهٔ هوش مصنوعی* محسوب نمی‌شوند. برای آنکه یک مدل هوش مصنوعی به سامانه‌ای کامل تبدیل شود، نیازمند افزودن اجزای دیگری همچون رابط کاربری است. بنابراین مدل‌های هوش مصنوعی معمولاً درون سامانه‌های هوش مصنوعی ادغام شده و بخشی از آن‌ها را تشکیل می‌دهند. این قانون قواعد خاصی را برای مدل‌های هوش مصنوعی با مقاصد عام و همچنین برای مدل‌های هوش مصنوعی با مقاصد عام که دارای خطرات نظام‌مند هستند پیش‌بینی کرده است؛ قواعدی که حتی اگر این مدل‌ها در سامانه‌های هوش مصنوعی ادغام شوند یا بخشی از آن‌ها شوند نیز لازم‌الاجرا خواهند بود. باید دانست که تعهدات مقرر برای ارائه‌دهندگان مدل‌های هوش مصنوعی با مقاصد عام، از زمان عرضهٔ این مدل‌ها به بازار اعمال می‌شود. هر گاه ارائه‌دهندهٔ یک مدل هوش مصنوعی با مقاصد عام، آن مدل را در سامانهٔ هوش مصنوعی خود ادغام کند و سامانهٔ مزبور در بازار عرضه یا به کار گرفته شود، چنین مدلی در حکم *عرضه‌شده به بازار*[۶۷] تلقی می‌شود و در نتیجه تعهدات مقرر در این قانون نسبت به مدل‌ها، علاوه بر تعهدات مربوط به سامانه‌های هوش مصنوعی همچنان اعمال خواهد شد. با این حال، تعهدات مقرر برای مدل‌ها در هیچ موردی شامل وضعیتی نمی‌شود که مدلی صرفاً برای فرآیندهای داخلی به‌کار گرفته شود؛ فرآیندهایی که برای ارائهٔ محصول یا خدمت به اشخاص ثالث ضروری نیستند و بر حقوق اشخاص حقیقی نیز تأثیری ندارند. با توجه به امکان بروز آثار منفی قابل‌ملاحظه، مدل‌های هوش مصنوعی با مقاصد عام و دارای خطر نظام‌مند باید همواره مشمول تعهدات مربوط در این قانون باشند. تعریف ارائه‌شده نباید شامل مدل‌های هوش مصنوعی‌ای شود که پیش از عرضه به بازار، صرفاً برای مقاصد پژوهش، توسعه و فعالیت‌های نمونه‌سازی به کار گرفته می‌شوند. البته این امر، خدشه‌ای به الزام به رعایت قانون حاضر وارد نمی‌کند زیرا پس از پایان این فعالیت‌ها و عرضهٔ مدل به بازار، تعهدات قانونی مزبور لازم‌الاجرا خواهند بود.

۹۸. با این حال، عمومیت یک مدل می‌تواند بر اساس شمار مؤلفه‌های تنظیمی آن تعیین شود. مدل‌هایی که دست‌کم دارای یک میلیارد مؤلفه بوده و با بهره‌گیری از حجم عظیمی از داده‌ها و از طریق یادگیری خودنظارتی در مقیاس وسیع آموزش دیده‌اند، باید به گونه‌ای تلقی شوند که از سطح قابل‌توجهی از عمومیت برخوردارند و توانایی انجام شایستهٔ طیف گسترده‌ای از وظایف متمایز را دارند.

۹۹. مدل‌های بزرگ هوش مصنوعی مولد،[۶۸] نمونه‌ای از مدل‌های هوش مصنوعی با مقاصد عام به‌شمار می‌روند زیرا امکان تولید انعطاف‌پذیر محتوا را فراهم می‌کنند؛ محتوایی که می‌تواند در قالب متن، صوت، تصویر یا ویدئو ارائه شود و به‌آسانی طیف گسترده‌ای از وظایف متمایز را پوشش

67. placed on the market
68. Large generative AI models

دهد.

۱۰۰. هر گاه یک مدل هوش مصنوعی با مقاصد عام در یک سامانهٔ هوش مصنوعی ادغام شود یا بخشی از آن را تشکیل دهد و هر گاه به دلیل این ادغام، توانایی خدمت‌رسانی به مقاصد متنوع را پیدا کند، آن سامانه باید در حکم سامانهٔ هوش مصنوعی با مقاصد عام تلقی شود. سامانهٔ هوش مصنوعی با مقاصد عام می‌تواند به‌طور مستقیم مورد استفاده قرار گیرد یا ممکن است در سامانه‌های هوش مصنوعی دیگر ادغام شود.

۱۰۱. ارائه‌دهندگان مدل‌های هوش مصنوعی با مقاصد عام، نقش و مسئولیت ویژه‌ای در طول زنجیرهٔ ارزش هوش مصنوعی دارند زیرا مدل‌هایی که ارائه می‌دهند ممکن است مبنایی برای طیف گسترده‌ای از *سامانه‌های پایین‌دستی*[۶۹] باشند. این سامانه‌ها اغلب توسط ارائه‌دهندگان پایین‌دستی ارائه می‌شوند و نیازمند درک کافی از مدل‌ها و قابلیت‌های آن‌ها به منظور ادغام این مدل‌ها در محصولات خود و برای اجرای تعهدات قانونی خود طبق این قانون یا سایر مقررات هستند. بنابراین اقدامات شفاف‌سازی متناسب باید تدوین شود ازجمله تهیه و به‌روزنگه‌داشتن مستندات و فراهم‌کردن اطلاعات مربوط به مدل هوش مصنوعی با مقاصد عام برای استفادهٔ ارائه‌دهندگان پایین‌دستی. مستندات فنی باید توسط ارائه‌دهندهٔ مدل‌های هوش مصنوعی با مقاصد عام تهیه و به‌روز نگه داشته شود تا در صورت درخواست در اختیار دفتر هوش مصنوعی و مقامات ملی ذی‌صلاح قرار گیرد. حداقل مجموعهٔ عناصری که باید در این مستندات گنجانده شود، باید در پیوست‌های خاص این قانون مشخص شود. همچنین کمیسیون باید اختیار داشته باشد که با استفاده از اقدامات تفویضی و با توجه به تحولات فناوری، این پیوست‌ها را اصلاح کند.

۱۰۲. نرم‌افزار و داده‌ها ازجمله مدل‌ها که تحت یک مجوز آزاد و متن‌باز منتشر می‌شوند، مجوزی که امکان اشتراک‌گذاری آزادانه را فراهم می‌آورد و به کاربران اجازه می‌دهد آزادانه به آن‌ها دسترسی داشته، استفاده کنند، تغییر دهند و نسخه‌های تغییریافتهٔ آن‌ها را بازتوزیع کنند، می‌توانند در پژوهش و نوآوری در بازار سهم داشته و فرصت‌های رشد چشمگیری برای اقتصاد اتحادیه فراهم کنند. مدل‌های هوش مصنوعی با مقاصد عام که تحت مجوزهای آزاد و متن‌باز منتشر می‌شوند باید به گونه‌ای تلقی شوند که سطوح بالایی از شفافیت و دسترس پذیری را تضمین کنند، مشروط بر اینکه مؤلفه‌های تنظیمی (ازجمله مقادیر)، اطلاعات مربوط به معماری مدل و اطلاعات مربوط به نحوهٔ استفاده از مدل به‌صورت عمومی در دسترس قرار گیرد. مجوز نیز باید آزاد و متن‌باز محسوب شود، حتی زمانی که به کاربران اجازه دهد نرم‌افزار و داده‌ها (ازجمله مدل‌ها) را اجرا، کپی، توزیع، مطالعه، تغییر و ارتقاء دهند مشروط بر اینکه نام ارائه‌دهندهٔ اصلی مدل ذکر شود و شرایط یکسان

69. Downstream systems

یا قابل مقایسه در توزیع رعایت شود.

۱۰۳. بخش‌های آزاد و متن‌باز هوش مصنوعی شامل نرم‌افزارها، داده‌ها (ازجمله مدل‌ها و مدل‌های هوش مصنوعی با مقاصد عام) و ابزارها، جزو خدمات یا فرآیندهای یک سامانهٔ هوش مصنوعی محسوب می‌شوند. اجزای آزاد و متن‌باز هوش مصنوعی می‌توانند از طریق کانال‌های مختلف ازجمله توسعهٔ آن‌ها در پایگاه‌های متن‌باز ارائه شوند. برای مقاصد این قانون، اجزای هوش مصنوعی که در برابر پرداخت هزینه عرضه می‌شوند یا به هر شکل دیگری تجاری‌سازی می‌شوند ازجمله از طریق ارائهٔ پشتیبانی فنی یا خدمات دیگر (حتی از طریق یک سکوی نرم‌افزاری) مرتبط با جزء هوش مصنوعی، یا از طریق استفاده از داده‌های شخصی برای مقاصدی غیر از صرفاً بهبود امنیت، سازگاری یا قابلیت همکاری نرم‌افزار نباید از معافیت‌های پیش‌بینی‌شده برای اجزای آزاد و متن‌باز هوش مصنوعی بهره‌مند شوند. استثنا در این زمینه تنها شامل معاملات میان *بنگاه‌های* خرد[۷۰] خواهد بود. همچنین صرفِ در دسترس قراردادن اجزای هوش مصنوعی از طریق پایگاه‌های متن‌باز، به‌خودی‌خود تجاری‌سازی محسوب نمی‌شود.

۱۰۴. ارائه‌دهندگان مدل‌های هوش مصنوعی با مقاصد عام که تحت مجوز آزاد و متن‌باز منتشر می‌شوند و مؤلفه‌های تنظیمی آن‌ها (ازجمله مقادیر)، اطلاعات مربوط به معماری و نحوهٔ استفاده از مدل به‌صورت عمومی در دسترس قرار گرفته است، باید از استثنائات مرتبط با الزامات شفافیت مقرر در مورد مدل‌های هوش مصنوعی با مقاصد عام بهره‌مند شوند، مگر آنکه مدل مذکور در زمرهٔ مدل‌های دارای خطر نظام‌مند قرار گیرد. در این صورت، صرفِ شفاف‌بودن مدل و انتشار آن تحت یک مجوز متن‌باز، به‌تنهایی دلیل کافی برای معافیت از رعایت تعهدات مقرر در این قانون محسوب نمی‌شود. در هر حال، با توجه به اینکه انتشار مدل‌های هوش مصنوعی با مقاصد عام تحت یک مجوز آزاد و متن‌باز، لزوماً اطلاعات اساسی دربارهٔ مجموعهٔ داده‌های مورد استفاده برای آموزش یا تنظیم دقیق مدل و نیز دربارهٔ چگونگی رعایت الزامات حقوق مؤلف را آشکار نمی‌کند، استثنای پیش‌بینی‌شده برای مدل‌های هوش مصنوعی با مقاصد عام از رعایت الزامات شفافیت، نباید شامل تعهد به ارائهٔ خلاصه از محتوای به‌کاررفته در آموزش مدل و نیز تعهد به تدوین یک سیاست برای رعایت حقوق مؤلف در اتحادیه باشد. این امر به‌ویژه شامل شناسایی و رعایت حق محفوظداشتن مطابق ماده ۴(۳) دستورالعمل ۷۹۰ /۲۰۱۹ [۷۱] پارلمان و شورای اروپا است.

۱۰۵. مدل‌های هوش مصنوعی با مقاصد عام، به‌ویژه مدل‌های بزرگ هوش مصنوعی مولد که قادر به تولید متن، تصویر و دیگر انواع محتوا هستند، فرصت‌های نوآوری منحصربه‌فردی

70. Microenterprises

۷۱. دستورالعمل شمارهٔ ۲۰۱۹/۷۹۰ پارلمان اروپا و شورای اروپا در ۱۷ آوریل ۲۰۱۹ در خصوص حق مؤلف و حقوق مرتبط در بازار واحد دیجیتال و اصلاح برخی دستورالعمل‌های آن EC/۹/۹۶ و EC/۲۹/۲۰۱۱ (روزنامهٔ رسمی ۲۰۱۹/۵/۱۳۰۱۷، ص ۹۲).

فراهم می‌آورند اما هم‌زمان چالش‌هایی برای هنرمندان، نویسندگان و سایر خالقان محتوا ایجاد می‌کنند و بر نحوهٔ خلق، توزیع، استفاده و مصرف محتوای خلاقانهٔ آن‌ها تأثیر می‌گذارند. توسعه و آموزش چنین مدل‌هایی مستلزم دسترسی به حجم عظیمی از متن، تصویر، ویدئو و داده‌های دیگر است. در این زمینه، فناوری‌های استخراج *متن و داده*[۷۲] می‌توانند به‌طور گسترده برای بازیابی و تحلیل این محتوا به کار روند. ممکن است این محتوا تحت حقوق مؤلف و حقوق مرتبط محافظت شده باشد. هر گونه استفاده از محتوای محافظت‌شده توسط کپی‌رایت، مستلزم اخذ اجازه از دارندهٔ حقوق مربوطه است، مگر آنکه استثناها و محدودیت‌های مرتبط با کپی‌رایت اعمال شوند. دستورالعمل شمارهٔ ۲۰۱۹/۷۹۰ استثناها و محدودیت‌هایی را معرفی کرده است که اجازهٔ تکثیر و استخراج آثار یا دیگر موضوعات را به منظور استخراج متن و داده تحت شرایط مشخص فراهم می‌آورد. بر اساس این قوانین، دارندگان این حقوق می‌توانند حق خود بر آثار یا دیگر موضوعات را محفوظ نگه دارند تا از انجام استخراج متن و داده جلوگیری کنند، مگر آنکه این فعالیت‌ها برای اهداف پژوهش علمی انجام شود.

۱۰۶. ارائه‌دهندگان مدل‌های هوش مصنوعی با مقاصد عام که این مدل‌ها را در بازار اتحادیهٔ اروپا عرضه می‌کنند، باید رعایت تعهدات مرتبط مندرج در این قانون را تضمین کنند. برای این منظور، ارائه‌دهندگان مدل‌های هوش مصنوعی با مقاصد عام باید برای رعایت قوانین اتحادیهٔ اروپا در زمینهٔ حق مؤلف و حقوق مرتبط به‌ویژه به منظور شناسایی و رعایت حقوق محفوظ اعلام‌شده توسط دارندگان اثر مطابق ماده ۴(۳) دستورالعمل شمارهٔ ۲۰۱۹/۷۹۰، سیاستی را تدوین کنند. هر ارائه‌دهنده‌ای که یک مدل هوش مصنوعی با مقاصد عام را در بازار اتحادیه ارائه می‌دهد باید این تعهد را رعایت کند، فارغ از حوزهٔ قضایی که اعمال مرتبط با کپی‌رایت برای آموزش آن مدل‌ها در آنجا انجام شده است. این الزام لازم است تا رقابت عادلانه میان ارائه‌دهندگان مدل‌های هوش مصنوعی با مقاصد عام در بازار اتحادیه تضمین شود به گونه‌ای که هیچ ارائه‌دهنده‌ای نتواند با اعمال استانداردهای پایین‌تر کپی‌رایت نسبت به آنچه در اتحادیه مقرر شده است، مزیت رقابتی غیرمنصفانه کسب کند. در مواردی که حق خودداری از استخراج متن و داده به‌طور صریح و مناسب محفوظ نگه داشته شده باشد، اگر ارائه‌دهندگان مدل‌های هوش مصنوعی با مقاصد عام، بخواهند بر روی چنین آثار یا موضوعاتی استخراج متن و داده انجام دهند، لازم است مجوز دارندهٔ حقوق را دریافت کنند.

---

۷۲. عبارت *استخراج متن و داده‌ها* (Text and Data Mining – TDM) به مجموعه‌ای از فناوری‌ها و روش‌های خودکار گفته می‌شود که برای بازیابی، تحلیل و کشف الگوها در متون و داده‌های دیجیتال استفاده می‌شوند.

۱۰۷. به منظور افزایش شفافیت در خصوص داده‌هایی که در پیش‌آموزش و آموزش مدل‌های هوش مصنوعی با مقاصد عام به کار گرفته می‌شوند ازجمله متن و داده‌های محافظت‌شده توسط قوانین کپی‌رایت، کافی است که ارائه‌دهندگان چنین مدل‌هایی یک خلاصهٔ کافی و تا حد لازم دقیق از محتوای مورد استفاده برای آموزش مدل تهیه و به‌صورت عمومی در دسترس قرار دهند. با درنظرگرفتن لزوم حفاظت از اسرار تجاری و اطلاعات محرمانهٔ کسب‌وکار، این خلاصه باید به‌طور کلی جامع باشد و از لحاظ فنی بسیار جزئی‌نگرانه نباشد تا به طرف‌های دارای منافع مشروع ازجمله دارندگان حقوق مؤلف امکان دهد حقوق خود را تحت قوانین اتحادیهٔ اروپا اعمال و اجرایی کنند. برای مثال، ارائهٔ خلاصه می‌تواند شامل فهرست مجموعه‌ها یا پایگاه‌های دادهٔ اصلی مورد استفاده در آموزش مدل مانند پایگاه‌های دادهٔ خصوصی یا عمومی بزرگ، یا آرشیوهای داده‌ای و همچنین توضیحی روایی دربارهٔ سایر منابع داده مورد استفاده باشد. شایسته است که دفتر هوش مصنوعی یک الگوی استاندارد برای تهیهٔ این خلاصه ارائه دهد به گونه‌ای که ساده و مؤثر باشد و امکان ارائهٔ خلاصه به شکل توصیفی توسط ارائه‌دهنده را فراهم کند.

۱۰۸. در خصوص تعهداتی که بر عهدهٔ ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی گذاشته شده است، مبنی بر تدوین سیاستی برای رعایت حقوق مالکیت فکری اتحادیه و انتشار عمومی خلاصه‌ای از محتوای آموزشی، *دفتر هوش مصنوعی* باید نظارت کند که آیا تأمین‌کننده این تعهدات را ایفا کرده است یا خیر. این دفتر نباید بررسی جزئی و موردیِ پایبندی داده‌های آموزشی به حقوق مؤلف را انجام دهد. این قانون به اجرای قواعد حقوق مؤلف در حقوق اتحادیه آسیبی وارد نمی‌کند.

۱۰۹. رعایت تعهدات مربوط به ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی باید متناسب با نوع ارائه‌دهنده باشد. توسعه‌دهندگان یا کاربران غیرحرفه‌ای و پژوهشگران علمی، از این الزامات معاف هستند، هرچند به رعایت داوطلبانهٔ آن تشویق می‌شوند. این تعهدات باید با توجه به اندازهٔ ارائه‌دهنده اعمال شود و برای بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا، روش‌های ساده‌شده‌ای پیش‌بینی شود تا هزینه‌های سنگین ایجاد نکند و مانع استفاده از این مدل‌ها نشود. در صورت تغییر یا تنظیم دقیق یک مدل، تعهدات ارائه‌دهنده صرفاً به همان تغییر یا تنظیم محدود خواهد بود. برای نمونه، تکمیل مستندات فنی موجود و افزودن اطلاعات مربوط به تغییرات، ازجمله منابع جدید داده‌های آموزشی می‌تواند راهی برای رعایت الزامات زنجیرهٔ ارزش در این قانون باشد.

۱۱۰. مدل‌های هوش مصنوعی عمومی می‌توانند خطرات نظام‌مند ایجاد کنند، ازجمله آثار منفی بالفعل یا قابل پیش‌بینی بر حوادث بزرگ، اختلال در بخش‌های حیاتی و پیامدهای جدی برای

سلامت و ایمنی عمومی. این خطرات همچنین می‌توانند بر فرآیندهای دموکراتیک، امنیت عمومی و اقتصادی اثر بگذارند و به انتشار محتوای غیرقانونی، نادرست یا تبعیض‌آمیز بینجامند. شدت این خطرات که با افزایش توانمندی‌ها و دامنهٔ دسترسی مدل‌ها بیشتر می‌شود، می‌تواند در کل چرخهٔ عمر مدل بروز یابد و تحت تأثیر عواملی مانند سوءاستفاده، قابلیت اطمینان، انصاف، امنیت، میزان خودمختاری مدل، دسترسی آن به ابزارها و شیوه‌های نوین یا ترکیبی، روش‌های انتشار، امکان حذف حفاظ‌ها و سایر عوامل قرار دارد. در سطح بین‌المللی، توجه ویژه‌ای به خطرات ناشی از سوءاستفادهٔ عمدی یا مشکلات پیش‌بینی‌نشده در هم‌سویی با مقاصد انسانی شده است. این خطرات شامل تهدیدات شیمیایی، زیستی، رادیولوژیک و هسته‌ای (از طریق کاهش موانع ورود به توسعه، طراحی، دستیابی یا استفاده از سلاح‌ها)، قابلیت‌های تهاجمی سایبری (در کشف و بهره‌برداری یا استفادهٔ عملیاتی از آسیب‌پذیری‌ها)، امکان کنترل سامانه‌های فیزیکی و زیرساخت‌های حیاتی، خودتکثیری مدل‌ها یا آموزش مدل‌های دیگر، بروز سوگیری و تبعیض زیان‌بار، تسهیل انتشار اطلاعات نادرست، نقض حریم خصوصی و تهدید ارزش‌های دموکراتیک و حقوق بشر است. حتی یک رویداد منفرد می‌تواند زنجیره‌ای از پیامدهای منفی ایجاد کند که دامنهٔ آن تا سطح یک شهر، یک حوزهٔ فعالیت یا کل یک جامعه گسترش یابد.

۱۱۱. برای شناسایی مدل‌های هوش مصنوعی عمومی که دارای خطرات نظام‌مند هستند، باید یک روش‌شناسی مشخص تدوین شود. چنین مدلی زمانی در این دسته قرار می‌گیرد که دارای *توانمندی‌های با اثرگذاری بالا* باشد (بر اساس ابزارها و روش‌های فنی مناسب) یا به دلیل گسترهٔ استفاده، تأثیر قابل‌توجهی بر بازار داخلی داشته باشد. توانمندی‌های با اثرگذاری بالا به قابلیت‌هایی اطلاق می‌شود که با پیشرفته‌ترین مدل‌ها برابری می‌کند یا از آن‌ها فراتر می‌رود. ممکن است این توانمندی‌ها پس از عرضه به بازار یا در تعامل با استفاده‌کنندگان، بهتر نمایان شوند. بر اساس سطح فناوری موجود در زمان لازم‌الاجراشدن این قانون، میزان *تجمعی محاسبات آموزشی*[۷۳] (بر حسب عملیات ممیز شناور)[۷۴] معیاری مهم برای سنجش توانمندی مدل است. میزان تجمعی محاسبات آموزشی شامل همهٔ محاسباتی است که در فعالیت‌ها و روش‌هایی صرف می‌شود که هدف آن‌ها تقویت توانایی‌هایی مانند پیش‌آموزش، تولید داده‌های مصنوعی و تنظیم دقیق مدل پیش از به‌کارگیری آن است. بدین جهت باید یک آستانهٔ اولیه برای این محاسبات تعیین شود که در صورت رسیدن مدل به آن، فرض شود که مدل دارای خطرات

73. the Cumulative Amount of Computation Used for the Training

74. Floating Point Operation

عملیات ممیز شناور به محاسباتی گفته می‌شود که با اعداد اعشاری (اعداد با ممیز شناور) انجام می‌شوند. این اعداد در رایانه‌ها به شکلی ذخیره می‌شوند که ممیز اعشار در موقعیت‌های مختلفی قرار می‌گیرد و می‌تواند مقادیر بسیار بزرگ یا بسیار کوچک را نمایش دهد. کاربرد آن در محاسبات علمی و مهندسی، شبیه‌سازی‌ها و مدل‌سازی‌ها، پردازش تصویر و ویدئو، هوش مصنوعی، یادگیری ماشین، بازی‌های ویدیویی زیاد است. (ن.ک: بند ۶۷ ماده سه همین قانون).

نظام‌مند است. این آستانه باید متناسب با تغییرات فناوری و صنعت (مانند بهبود الگوریتم‌ها یا افزایش بهره‌وری سخت‌افزاری) اصلاح شود و با شاخص‌ها و آزمون‌های معیار برای ارزیابی توانمندی مدل تکمیل شود. برای این منظور، *دفتر هوش مصنوعی* باید با جامعهٔ علمی، صنعت، جامعهٔ مدنی و سایر متخصصان همکاری کند. ابزارها، آستانه‌ها و آزمون‌های معیار ارزیابی باید به گونه‌ای طراحی شوند که پیش‌بینی‌کنندهٔ قابل اعتمادی برای سنجش میزان عمومیت، توانمندی‌ها و خطرات نظام‌مند مدل‌های هوش مصنوعی عمومی باشند و می‌توانند عواملی مانند نحوهٔ عرضهٔ مدل به بازار یا شمار کاربران بالقوهٔ آن را نیز در نظر گیرند. علاوه بر این، کمیسیون می‌تواند در موارد خاص، یک مدل را، حتی اگر دقیقاً به آستانه نرسیده باشد، به‌عنوان مدل دارای خطرات نظام‌مند تعیین کند، در صورتی که توانمندی‌ها یا اثر آن معادل معیارهای مقرر باشد. این تصمیم بر اساس ارزیابی کلی معیارهای مندرج در پیوست این قانون اتخاذ می‌شود، مانند کیفیت یا حجم دادهٔ آموزشی، تعداد استفاده‌کنندگان تجاری و نهایی، نحوهٔ ورودی و خروجی مدل، سطح خودمختاری و مقیاس‌پذیری آن، یا ابزارهای در دسترس مدل. در صورت ارائهٔ درخواست مستدل از سوی ارائه‌دهندهٔ مدل دارای خطرات نظام‌مند، کمیسیون باید این درخواست را بررسی کرده و در صورت لزوم، دوباره ارزیابی کند که آیا این مدل همچنان باید در دستهٔ خطرات نظام‌مند قرار گیرد یا خیر.

۱۱۲. ضروری است که رویه‌ای برای طبقه‌بندی مدل‌های هوش مصنوعی عمومی دارای خطرات نظام‌مند روشن شود. هر مدل هوش مصنوعی عمومی که به آستانهٔ مقرر برای توانمندی‌های با اثرگذاری بالا برسد، باید به‌طور پیش‌فرض *دارای خطرات نظام‌مند* تلقی شود. ارائه‌دهنده باید حداکثر ظرف دو هفته پس از تحقق الزامات، یا زمانی که مطمئن می‌شود مدل او به این الزامات خواهد رسید، موضوع را به *دفتر هوش مصنوعی* اطلاع دهد. این امر به‌ویژه در مورد آستانهٔ عملیات ممیز شناور اهمیت دارد زیرا آموزش مدل‌های هوش مصنوعی عمومی مستلزم برنامه‌ریزی گسترده است و تخصیص پیشینی منابع پردازشی می‌شود. بنابراین ارائه‌دهندگان چنین مدل‌هایی می‌توانند پیش از اتمام آموزش، پیش‌بینی کنند که آیا مدل آن‌ها به آستانه خواهد رسید یا خیر. در چارچوب این اطلاع‌رسانی، ارائه‌دهنده باید بتواند نشان دهد که مدل او به دلیل ویژگی‌های خاص، استثنائاً فاقد خطرات نظام‌مند است و در نتیجه نباید به‌عنوان مدل دارای خطرات نظام‌مند طبقه‌بندی شود. این اطلاعات برای *دفتر هوش مصنوعی* ارزشمند است تا بتواند عرضهٔ مدل‌های دارای خطرات نظام‌مند به بازار را پیش‌بینی کرده و امکان تعامل زودهنگام ارائه‌دهندگان با دفتر فراهم شود. این اطلاعات به‌ویژه در مورد مدل‌هایی که قرار است به‌صورت *متن‌باز*[۷۵] منتشر شوند، اهمیت دارد زیرا پس از انتشار متن‌باز، ممکن است اجرای اقدامات لازم برای تضمین رعایت تعهدات، ذیل این قانون دشوارتر شود.

75. Open-source

۱۱۳. چنانچه کمیسیون آگاه شود که یک مدل هوش مصنوعی عمومی واجد شرایط طبقه‌بندی به‌عنوان مدل دارای خطرات نظام‌مند است، ولی پیش‌تر این موضوع ناشناخته بوده یا ارائه‌دهندهٔ مربوطه آن را به کمیسیون اطلاع نداده است، کمیسیون باید اختیار داشته باشد که آن مدل را به این عنوان تعیین کند. برای این منظور، سامانه‌ای از *هشدارهای واجد شرایط* باید تضمین کند که *دفتر هوش مصنوعی* علاوه بر فعالیت‌های نظارتی خود، از سوی *هیئت علمی* نیز در مورد مدل‌های هوش مصنوعی عمومی که احتمالاً باید به‌عنوان مدل‌های دارای خطرات نظام‌مند طبقه‌بندی شوند، مطلع شود.

۱۱۴. ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی که دارای خطرات نظام‌مند هستند، علاوه بر تعهدات مقرر برای کلیهٔ ارائه‌دهندگان این مدل‌ها، باید به تعهداتی پایبند باشند که هدف آن شناسایی و کاهش این خطرات و تضمین سطح مناسب حفاظت امنیت سایبری است. این تعهدات بدون توجه به مستقل‌بودن مدل یا ادغام آن در یک سامانهٔ هوش مصنوعی یا محصول دیگر اعمال می‌شود. برای تحقق این اهداف، قانون حاضر باید ارائه‌دهندگان را ملزم کند تا پیش از نخستین عرضه به بازار، ارزیابی‌های لازم را انجام دهند، ازجمله اجرا و مستندسازی آزمون‌های چالش‌برانگیز بر روی مدل که می‌تواند حسب مورد از طریق آزمون‌های داخلی یا آزمون‌های مستقل خارجی صورت گیرد. افزون بر این، ارائه‌دهندگان چنین مدل‌هایی باید به‌طور مستمر خطرات نظام‌مند را ارزیابی و کاهش دهند. این امر می‌تواند با ایجاد سیاست‌های مدیریت ریسک (مانند فرآیندهای پاسخ‌گویی و حکمرانی)، اجرای پایش پس از عرضه، اتخاذ تدابیر مناسب در سراسر چرخهٔ عمر مدل و همکاری با بازیگران ذی‌ربط در زنجیرهٔ ارزش هوش مصنوعی محقق شود.

۱۱۵. ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی دارای خطرات نظام‌مند باید این خطرات را ارزیابی کنند و کاهش دهند. چنانچه با وجود تلاش‌ها برای شناسایی و پیشگیری از خطرات مرتبط با چنین مدلی، توسعه یا استفاده از آن موجب وقوع حادثهٔ جدی شود، ارائه‌دهنده باید بی‌درنگ آن حادثه را ثبت کرده و هر گونه اطلاعات مرتبط و اقدامات اصلاحی محتمل را به کمیسیون و مقامات صلاحیت‌دار ملی گزارش دهد. همچنین ارائه‌دهندگان باید سطح مناسبی از حفاظت امنیت سایبری را برای مدل و زیرساخت فیزیکی آن و حسب مورد در سراسر چرخهٔ عمر مدل، تضمین کنند. حفاظت امنیت سایبری مرتبط با خطرات نظام‌مند ناشی از سوءاستفاده یا حملات مخرب، باید به‌طور مقتضی ملاحظاتی چون نشت تصادفی مدل، انتشار غیرمجاز، دورزدن تدابیر ایمنی و دفاع در برابر حملات سایبری، دسترسی غیرمجاز یا سرقت مدل را در بر گیرد. چنین حفاظتی می‌تواند از طریق ایمن‌سازی معیارهای مدل، الگوریتم‌ها، سرورها و مجموعه‌داده‌ها تسهیل شود؛ برای مثال می‌تواند با تدابیر عملیاتی امنیت اطلاعات، سیاست‌های خاص امنیت سایبری، راهکارهای فنی مناسب و کنترل‌های دسترسی سایبری و فیزیکی متناسب با شرایط و سطح خطر تحقق یابد.

۱۱۶. دفتر هوش مصنوعی باید تدوین، بازبینی و تطبیق *آیین‌نامه‌های رفتاری*[۷۶] را با درنظرگرفتن رویکردهای بین‌المللی، تشویق و تسهیل کند. تمامی ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی می‌توانند برای مشارکت دعوت شوند. برای تضمین آن که آیین‌نامه‌های رفتاری بازتاب‌دهندهٔ پیشرفته‌ترین سطح دانش و فناوری باشند و دیدگاه‌های متنوع را پوشش دهند، دفتر هوش مصنوعی باید با مقامات ملی صلاحیت‌دار همکاری و در صورت لزوم با سازمان‌های جامعهٔ مدنی، سایر ذی‌نفعان و کارشناسان، ازجمله *هیئت علمی* مشورت کند. آیین‌نامه‌های رفتاری باید تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی و نیز مدل‌های دارای خطرات نظام‌مند را پوشش دهند. در زمینهٔ خطرات نظام‌مند این آیین‌نامه‌ها باید به ایجاد یک طبقه‌بندی از نوع و ماهیت این خطرات در سطح اتحادیه، ازجمله منابع آن‌ها کمک کنند. همچنین آیین‌نامه‌ها باید بر اقدامات مشخصی جهت ارزیابی و کاهش خطر متمرکز باشند.

۱۱۷. آیین‌نامه‌های رفتاری باید ابزار اصلی برای اطمینان از رعایت صحیح تعهدات مقرر در این قانون برای ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی باشند. ارائه‌دهندگان باید بتوانند به این آیین‌نامه‌ها استناد کنند تا انطباق خود با تعهدات را اثبات کنند. کمیسیون می‌تواند از طریق اقدامات اجرایی، تصمیم به تصویب آیین‌نامهٔ رفتاری و اعطای اعتبار عمومی به آن بگیرد؛ یا در عوض اگر تا زمان لازم‌الاجراشدن این آیین‌نامه، آیین‌نامهٔ اجرایی نهایی نشده باشد یا توسط دفتر هوش مصنوعی کافی تشخیص داده نشود، قواعد مشترکی را برای اجرای تعهدات مربوطه ارائه دهد. پس از انتشار *استاندارد هماهنگ‌شده* که دفتر هوش مصنوعی آن را برای پوشش تعهدات مربوط مناسب ارزیابی کند، رعایت آن استاندارد برای ارائه‌دهندگان، فرض انطباق ایجاد خواهد کرد. با این حال، اگر آیین‌نامهٔ رفتاری یا استاندارد هماهنگ‌شده در دسترس نباشد یا ارائه‌دهندگان نخواهند به آن اتکا کنند، می‌توانند با استفاده از روش‌های مناسب جایگزین، انطباق خود را نشان دهد.

۱۱۸. قانون حاضر، سامانه‌ها و مدل‌های هوش مصنوعی را با تحمیل الزامات و تعهدات خاص بر بازیگران تجاری که آن‌ها را در بازار عرضه می‌کنند، به خدمت می‌گیرند یا در اتحادیه مورد استفاده قرار می‌دهند، تنظیم می‌کند. در نتیجه، تعهدات ارائه‌دهندگان خدمات واسطه‌ای که این سامانه‌ها یا مدل‌ها را در خدمات خود ادغام می‌کنند (مطابق قانون ۲۰۶۵/۲۰۲۲ (اتحادیهٔ اروپا)) تکمیل می‌شود. در مواردی که چنین سامانه‌ها یا مدل‌هایی در *سکوهای برخط بسیار بزرگ* یا *موتورهای جستجوی برخط بسیار بزرگ* تعیین‌شده ادغام شوند، مشمول چارچوب مدیریت ریسک مقرر در ۲۰۶۵/۲۰۲۲ (اتحادیهٔ اروپا) خواهند بود؛ لذا تعهدات متناظر این قانون به‌طور پیش‌فرض انجام‌شده تلقی می‌شود؛

76. The Codes of Practice

مگر اینکه خطرات نظام‌مند مهمی که قانون مزبور پوشش نداده است در این مدل‌ها شناسایی شود. در این چارچوب، ارائه‌دهندگان سکوهای برخط بسیار بزرگ و موتورهای جستجوی برخط بسیار بزرگ موظف‌اند خطرات نظام‌مند بالقوهٔ ناشی از طراحی، عملکرد و استفاده از خدمات خود را ارزیابی کنند؛ ازجمله چگونگی مشارکت طراحی سامانه‌های الگوریتمیِ مورد استفاده در خدمت در ایجاد چنین خطراتی و نیز خطرات نظام‌مند ناشی از سوءاستفاده‌های احتمالی. این ارائه‌دهندگان همچنین مکلف‌اند با رعایت حقوق بنیادین، تدابیر مناسب جهت کاهش خطر را اتخاذ کنند.

۱۱۹. با توجه به سرعت بالای نوآوری و تحول فناوری در حوزهٔ خدمات دیجیتال که تحت شمول ابزارهای گوناگون حقوق اتحادیه قرار می‌گیرند و با درنظرداشتن شیوهٔ استفاده و برداشت کاربران از این خدمات، سامانه‌های هوش مصنوعی مشمول این قانون می‌توانند به‌عنوان *خدمات میانجی* یا بخشی از آن‌ها به معنای مندرج در قانون (اتحادیهٔ اروپا) ۲۰۶۵/۲۰۲۲ ارائه شوند. این قانون باید به‌صورت *فناوری خنثی* تفسیر شود. به‌عنوان نمونه، ممکن است سامانه‌های هوش مصنوعی برای ارائهٔ موتورهای جستجوی برخط به کار گرفته شوند، به‌ویژه زمانی که یک سامانهٔ هوش مصنوعی مثلاً یک ربات گفتگو که تمامی وب‌سایت‌ها را جستجو کرده، نتایج را در پایگاه دانش خود وارد می‌کند و با بهره‌گیری از داده‌های به‌روز، خروجی واحدی ایجاد می‌کند که منابع مختلف اطلاعاتی را با یکدیگر ترکیب می‌کند.

۱۲۰. برخی تعهدات این قانون، ارائه‌دهندگان و بهره‌برداران سامانه‌های خاص هوش مصنوعی را ملزم می‌کند امکان شناسایی و افشای این موضوع را فراهم کنند که خروجی‌های سامانه به‌صورت مصنوعی تولید یا دستکاری شده‌اند. این الزامات برای اجرای مؤثر قانون (اتحادیهٔ اروپا) ۲۰۶۵/۲۰۲۲ اهمیت ویژه دارند. این موضوع، به‌ویژه در مورد تعهدات ارائه‌دهندگان *سکوهای برخط بسیار بزرگ* یا *موتورهای جستجوی برخط بسیار بزرگ* برجسته است زیرا آنان باید خطرات نظام‌مند ناشی از انتشار محتوای تولید یا دستکاری‌شدهٔ مصنوعی را شناسایی کنند و کاهش دهند. این خطرات شامل آثار منفی بالفعل یا قابل پیش‌بینی بر فرآیندهای دموکراتیک، گفتمان مدنی و فرآیندهای انتخاباتی از طریق انتشار اطلاعات نادرست است.

۱۲۱. استانداردسازی باید نقش کلیدی در ارائهٔ راه‌حل‌های فنی به ارائه‌دهندگان ایفا کند تا بتوانند با رعایت سطح فناوری روز، الزامات این قانون را اجرا کنند. این فرآیند همچنین باید به ترویج نوآوری، رقابت‌پذیری و رشد در بازار واحد کمک کند. این فرآیند همچنین باید نوآوری، رقابت‌پذیری و رشد در بازار واحد را ترویج دهد. رعایت *استانداردهای هماهنگ*، طبق تعریف بند

(۱)(ج) ماده ۲ قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۲/۱۰۲۵ پارلمان و شورای اروپا اتحادیه[۷۷] که عموماً منعکس‌کنندهٔ سطح فناوری روز هستند، باید وسیله‌ای برای اثبات انطباق ارائه‌دهندگان با الزامات این قانون محسوب شود. ارائهٔ متعادل منافع با مشارکت تمامی ذی‌نفعان در توسعهٔ استانداردها، به‌ویژه بنگاه‌های کوچک و متوسط، سازمان‌های مصرف‌کننده و ذی‌نفعان زیست‌محیطی و اجتماعی، مطابق مواد ۵ و ۶ قانون شمارهٔ ۲۰۱۲/۱۰۲۵ باید مورد حمایت قرار گیرد. به منظور تسهیل انطباق، کمیسیون باید بدون تأخیر غیرموجه درخواست‌های استانداردسازی را صادر کند و در این فرآیند با *انجمن مشورتی* و *هیئت* مشورت کند تا دانش تخصصی لازم جمع‌آوری شود. با این حال، در صورت فقدان ارجاعات مرتبط به استانداردهای هماهنگ، کمیسیون می‌تواند از طریق *اقدامات اجرایی* و پس از مشورت با انجمن مشورتی، *مشخصات مشترک* برای برخی الزامات مقرر را تدوین کند. این مشخصات مشترک باید راهکاری استثنایی تلقی شود و تنها در مواردی اعمال شود که درخواست استانداردسازی از سوی سازمان‌های اروپایی پذیرفته نشده، یا استانداردهای هماهنگ، نگرانی‌های مربوط به حقوق بنیادین را به اندازهٔ کافی پوشش نداده‌اند، یا با درخواست مطابقت نداشته‌اند، یا در تصویب آن‌ها تأخیر ایجاد شده است. اگر این تأخیر ناشی از پیچیدگی فنی استاندارد باشد، کمیسیون باید پیش از تصمیم به تدوین مشخصات مشترک آن را در نظر بگیرد. همچنین در فرآیند تدوین مشخصات مشترک، همکاری با شرکای بین‌المللی و نهادهای استانداردسازی بین‌المللی توصیه می‌شود.

۱۲۲. بدون خدشه به استفاده از استانداردهای هماهنگ و مشخصات مشترک، بهتر است که ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر، در صورتی که این سامانه‌ها بر اساس داده‌هایی آموزش و آزمون شده باشند که بازتاب‌دهندهٔ شرایط جغرافیایی، رفتاری، زمینه‌ای یا کارکردی خاص محل استفادهٔ موردنظر آن‌هاست، فرض بر رعایت الزامات حاکمیت دادهٔ مقرر در این قانون گذاشته شود.

بدون خدشه به کاربرد استانداردهای هماهنگ و مشخصات مشترک، بهتر است ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر از یک فرض قانونی بهره‌مند شوند. این فرض، زمانی برقرار است که سامانه‌های آن‌ها بر پایهٔ داده‌هایی آموزش و آزمون شده باشند که شرایط جغرافیایی، رفتاری، زمینه‌ای یا کارکردی محل استفادهٔ موردنظر را بازتاب می‌دهند. در این صورت، رعایت الزامات حاکمیت دادهٔ مقرر در این قانون، مفروض خواهد بود.

---

۷۷. مقررات اتحادیهٔ اروپا به شمارهٔ ۲۰۱۲/۱۰۲۵ پارلمان اروپا و شورا در ۲۵ اکتبر ۲۰۱۲ در مورد استانداردسازی اروپایی، اصلاحیهٔ دستورالعمل‌های شورا EEC/۶۸۶/۸۹ و EEC/۱۵/۹۳ و دستورالعمل‌های EC/۹/۹۴، EC/۲۵/۹۴، EC/۱۶/۹۵، EC/۲۳/۹۷، EC/۳۴/۹۸، EC/۲۲/۲۰۰۴، EC/۲۳/۲۰۰۷، EC/۲۳/۲۰۰۹ و EC/۱۰۵/۲۰۰۹ پارلمان اروپا و شورا و لغو تصمیم شورا EEC/۹۵/۸۷ و تصمیم شمارهٔ EC/۲۰۰۶/۱۶۷۳ پارلمان اروپا و شورا (روزنامهٔ رسمی ۳۱۶، ۲۰۱۲/۱۱/۱۴، ص ۱۲).

همچنین بدون خدشه به الزامات مرتبط با استحکام و دقت مندرج در این قانون، طبق ماده ۵۴(۳) قانون (اتحادیهٔ اروپا) ۸۸۱/۲۰۱۹ سامانه‌های هوش مصنوعی پرخطر که دارای گواهی یا بیانیهٔ انطباق تحت یک طرح امنیت سایبری باشند و مرجع آن در روزنامهٔ رسمی اتحادیهٔ اروپا منتشر شده باشد، فرض بر رعایت الزامات امنیت سایبری این قانون گذاشته می‌شود. این حکم، تنها تا جایی معتبر است که گواهی یا بیانیهٔ انطباق (یا بخشی از آن) الزامات امنیت سایبری این قانون را پوشش دهد و ماهیت داوطلبانهٔ آن طرح امنیت سایبری همچنان محفوظ می‌ماند.

۱۲۳. برای تضمین سطح بالایی از قابلیت اعتماد سامانه‌های هوش مصنوعی پرخطر، لازم است این سامانه‌ها پیش از عرضه به بازار یا بهره‌برداری، تحت *ارزیابی انطباق* قرار گیرند.

۱۲۴. به منظور کاهش بار بر فعالان اقتصادی و جلوگیری از هر گونه تکرار در خصوص سامانه‌های هوش مصنوعی پرخطر مرتبط با محصولاتی که مشمول قوانین هماهنگ‌سازی اتحادیه در چارچوب *چارچوب قانونگذاری جدید* هستند، انطباق این سامانه‌ها با الزامات این قانون باید بخشی از ارزیابی انطباقی باشد که پیش‌تر در آن قوانین پیش‌بینی شده است. الزامات این قانون نباید منطق، روش‌شناسی یا ساختار کلی ارزیابی انطباق مقرر در آن قوانین را تحت تأثیر قرار دهد.

۱۲۵. با توجه به پیچیدگی سامانه‌های هوش مصنوعی پرخطر و خطرات آن‌ها، لازم است فرآیند ارزیابی انطباق مناسبی شامل نهادهای ارزیابی اعلام‌شده (که اصطلاحاً *ارزیابی انطباق شخص ثالث* خوانده می‌شوند) تدوین شود. با این حال، به دلیل تجربهٔ محدود گواهی‌دهندگان حرفه‌ای در حوزهٔ ایمنی محصولات و ماهیت متفاوت خطرات، بهتر است در مرحلهٔ نخست اجرای این قانون، دامنهٔ ارزیابی شخص ثالث برای سامانه‌های هوش مصنوعی پرخطر به‌غیر از موارد مرتبط با محصولات، محدود شود. بنابراین ارزیابی انطباق چنین سامانه‌هایی باید به‌طور کلی بر عهدهٔ خود ارائه‌دهنده و تحت مسئولیت او انجام شود، مگر در مورد سامانه‌های هوش مصنوعی با کاربری زیست‌سنجی که استثنا محسوب می‌شوند.

۱۲۶. در مواردی که ارزیابی انطباق شخص ثالث الزامی است، نهادهای اعلام‌شده باید از سوی مقامات صلاحیت‌دار ملی معرفی شوند. این معرفی منوط به رعایت معیارهایی ازجمله استقلال، صلاحیت فنی، نبود تعارض منافع و شرایط مناسب امنیت سایبری است. مقامات ملی باید اطلاعات مربوط به معرفی نهادها را از طریق سامانهٔ الکترونیکی اطلاع‌رسانی که کمیسیون طبق ماده R23 پیوست اول تصمیم شمارهٔ EC/۲۰۰۸/۷۶۸ ایجاد و مدیریت کرده، به کمیسیون و سایر دولت‌های عضو ارسال کنند.

۱۲۷. در راستای تعهدات اتحادیهٔ اروپا ذیل موافقت‌نامهٔ موانع فنی تجارت سازمان تجارت جهانی، باید امکان شناسایی متقابل نتایج ارزیابی انطباق صادرشده توسط نهادهای واجد صلاحیت

فراهم شود، حتی اگر این نهادها در قلمروی خارج از اتحادیه مستقر باشند. البته این امر مشروط به آن است که نهادهای کشورهای ثالث، الزامات این قانون را رعایت کرده و اتحادیه توافق لازم را منعقد کرده باشد. کمیسیون باید فعالانه ابزارهای بین‌المللی ممکن را بررسی کند و به‌طور خاص در پی انعقاد توافق‌های شناسایی متقابل با کشورهای ثالث باشد.

۱۲۸. مطابق مفهوم رایج *تغییر اساسی* برای محصولات مشمول قوانین هماهنگ‌سازی اتحادیه، هر گاه تغییری رخ دهد که ممکن است انطباق یک سامانهٔ هوش مصنوعی پرخطر با این قانون را تحت تأثیر قرار دهد (مانند تغییر سیستم عامل یا معماری نرم‌افزار) یا هدف موردنظر سامانه تغییر کند، آن سامانه باید به‌عنوان سامانه‌ای جدید تلقی شده و مجدداً ارزیابی انطباق صورت گیرد. با این حال، تغییرات الگوریتم و عملکرد سامانه‌های هوش مصنوعی که پس از عرضه به بازار یا بهره‌برداری همچنان *یاد می‌گیرند* و به‌طور خودکار، نحوهٔ اجرای کارکردها را تطبیق می‌دهند، *تغییر اساسی* محسوب نمی‌شود، مشروط بر آنکه این تغییرات قبلاً توسط ارائه‌دهنده تعیین شده و در زمان ارزیابی انطباق بررسی شده باشند.

۱۲۹. سامانه‌های هوش مصنوعی پرخطر باید *نشان CE* را داشته باشند تا انطباق آن‌ها با این قانون مشخص و امکان گردش آزاد آن‌ها در بازار داخلی فراهم شود. برای سامانه‌های پرخطری که در یک محصول تعبیه شده‌اند، نشان CE فیزیکی الزامی است و می‌توانند با نشان CE دیجیتال تکمیل شوند؛ اما در مورد سامانه‌هایی که صرفاً به‌صورت دیجیتال ارائه می‌شوند، تنها نشان CE دیجیتال باید استفاده شود. دولت‌های عضو مجاز نیستند برای عرضه یا بهره‌برداری از سامانه‌های پرخطری که با این قانون منطبق بوده و نشان CE دارند، موانع غیرموجهی ایجاد کنند.

۱۳۰. در شرایط خاص، دسترسی سریع به فناوری‌های نوآورانه می‌تواند برای سلامت و ایمنی افراد، حفاظت از محیط‌زیست و مقابله با تغییرات اقلیمی و منافع عمومی جامعه حیاتی باشد. از این رو در موارد استثنایی و به دلایل امنیت عمومی یا حفاظت از جان و سلامت اشخاص، حفاظت محیط‌زیست، صیانت از دارایی‌های صنعتی و زیرساختی حیاتی، مقامات نظارت بر بازار می‌توانند اجازهٔ عرضه یا بهره‌برداری از سامانه‌های هوش مصنوعی فاقد ارزیابی انطباق را صادر کنند. همچنین در شرایط کاملاً موجه و مطابق این قانون، مقامات انتظامی یا مقامات حفاظت مدنی می‌توانند یک سامانهٔ هوش مصنوعی پرخطر مشخص را بدون اخذ پیشینی مجوز از مرجع نظارت بر بازار به کار گیرند، مشروط بر آنکه چنین مجوزی در حین یا بلافاصله پس از استفاده و بدون تأخیر غیرموجه درخواست شود.

۱۳۱. به منظور تسهیل کار کمیسیون و دولت‌های عضو در حوزهٔ هوش مصنوعی و نیز افزایش شفافیت عمومی، ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر (به‌غیر از آن‌هایی که مربوط

به محصولاتی هستند که در محدودهٔ قوانین هماهنگ‌سازی موجود اتحادیه قرار می‌گیرند) و همچنین ارائه‌دهندگانی که بر اساس استثنا معتقدند یک سامانهٔ مندرج در موارد استفادهٔ پرخطر پیوست این قانون پرخطر نیست، باید خود و اطلاعات مربوط به سامانهٔ هوش مصنوعی‌شان را در *پایگاه دادهٔ اتحادیهٔ اروپا* ثبت کنند. این پایگاه باید توسط کمیسیون ایجاد و مدیریت شود. پیش از استفاده از یک سامانهٔ مندرج در موارد استفادهٔ پرخطر، بهره‌برداران عمومی (مراجع دولتی، نهادها و سازمان‌ها) باید در این پایگاه ثبت‌نام کرده و سامانهٔ موردنظر خود را انتخاب کنند. این در حالی است که سایر بهره‌برداران می‌توانند این کار را داوطلبانه انجام دهند. این بخش از پایگاه دادهٔ اتحادیه باید به‌صورت عمومی و رایگان قابل دسترس باشد و با قابلیت جستجوی آسان، قابل فهم و خواندن توسط ماشین باشد. پایگاه داده باید با رابط کاربری آسان طراحی شود، مانند امکان جستجو از طریق کلیدواژه‌ها تا عموم بتوانند اطلاعات مربوط به ثبت سامانه‌های پرخطر و موارد استفادهٔ مندرج در پیوست این قانون را بیابند. هر تغییر اساسی در سامانه‌های پرخطر نیز باید در این پایگاه ثبت شود. برای سامانه‌های پرخطر در حوزهٔ اجرای قانون، مهاجرت، پناهندگی و مدیریت کنترل مرزها، ثبت باید در بخشی امن و غیرعمومی از پایگاه انجام شود. دسترسی به این بخش، صرفاً برای کمیسیون و مقامات نظارت بر بازار (صرفاً برای بخش ملی مربوطه) مجاز است. در مورد سامانه‌های پرخطر در حوزهٔ زیرساخت‌های حیاتی، ثبت فقط در سطح ملی الزامی است. کمیسیون، مطابق قانون (اتحادیهٔ اروپا) ۱۷۲۵/۲۰۱۸ کنترل‌کنندهٔ دادهٔ این پایگاه خواهد بود. برای اطمینان از عملکرد کامل پایگاه، فرآیند راه‌اندازی آن باید شامل تدوین مشخصات عملکردی توسط کمیسیون و ارائهٔ یک گزارش حسابرسی مستقل باشد. همچنین کمیسیون باید در ایفای نقش خود به‌عنوان کنترل‌کنندهٔ داده، خطرات امنیت سایبری را نیز مدنظر قرار دهد. برای به‌حداکثررساندن دسترسی و استفادهٔ عمومی، پایگاه داده و اطلاعات آن باید با الزامات دستورالعمل (اتحادیهٔ اروپا) ۸۸۲/۲۰۱۹ مطابقت داشته باشد.

۱۳۲. برخی سامانه‌های هوش مصنوعی که برای تعامل با اشخاص یا تولید محتوا طراحی شده‌اند، حتی اگر پرخطر نباشند، ممکن است خطرات خاصی از قبیل جعل هویت یا فریب ایجاد کنند. بنابراین استفاده از آن‌ها در برخی شرایط باید مشمول الزامات شفافیت خاص شود و خدشه‌ای به الزامات سامانه‌های پرخطر وارد نکند و همچنین باید استثناهای ضروری برای اجرای قانون را در نظر گرفت. به‌طور ویژه باید به اشخاص اعلام شود که در حال تعامل با یک سامانهٔ هوش مصنوعی هستند، مگر آنکه این موضوع برای شخص آگاه، هوشیار و متعارف در شرایط استفاده بدیهی باشد. برای اجرای این تعهد، چنانچه سامانه‌ای برای تعامل با گروه‌های آسیب‌پذیر طراحی شده باشد، باید ویژگی‌های اشخاص آسیب‌پذیر به دلیل سن یا ناتوانی نیز در نظر گرفته شود. همچنین زمانی که اشخاص در

معرض سامانه‌هایی قرار می‌گیرند که از طریق پردازش داده‌های زیست‌سنجی قادر به شناسایی یا استنتاج احساسات یا مقاصد آن‌ها هستند، یا می‌توانند آن‌ها را در دسته‌بندی‌های خاص قرار دهند، باید مطلع شوند. این دسته‌ها می‌تواند شامل جنسیت، سن، رنگ مو، رنگ چشم، خال‌کوبی، ویژگی‌های شخصیتی، منشأ قومی، علایق و سلایق شخصی باشد. چنین اطلاعات و اطلاع‌رسانی‌هایی باید در قالب‌های قابل‌دسترس برای افراد دارای معلولیت ارائه شود.

۱۳۳. انواع مختلفی از سامانه‌های هوش مصنوعی می‌توانند حجم زیادی محتوای مصنوعی تولید کنند که تشخیص آن از محتوای اصیل انسانی برای افراد دشوارتر می‌شود. دسترسی گسترده و توانایی‌های فزایندهٔ این سامانه‌ها تأثیر قابل‌توجهی بر یکپارچگی و اعتماد در اکوسیستم اطلاعات دارد و خطرهای جدیدی ازجمله انتشار گستردهٔ اطلاعات گمراه‌کننده، دستکاری، کلاهبرداری، جعل هویت و فریب مصرف‌کننده ایجاد می‌کند. با توجه به این خطرات، سرعت بالای تحولات فناوری و نیاز به روش‌های جدید برای ردیابی منشأ اطلاعات، لازم است ارائه‌دهندگان این سامانه‌ها راه‌حل‌های فنی جهت علامت‌گذاری محتوای تولیدشده یا دستکاری‌شده توسط هوش مصنوعی را با قابلیت خوانش ماشینی و قابلیت شناسایی تعبیه کنند. این روش‌ها باید تا حد امکان، قابل اعتماد، سازگار، مؤثر و مقاوم باشند و می‌توانند شامل واترمارک (علامت کم‌رنگ)، فراداده، روش‌های رمزنگاری برای اثبات اصالت و منشأ محتوا، ثبت رویدادها، اثر انگشت دیجیتال یا دیگر روش‌های مناسب باشند.

این راهکارها می‌توانند در سطح خود سامانه یا مدل هوش مصنوعی (ازجمله مدل‌های چندمنظوره مولد محتوا) انجام شوند تا ارائه‌کنندگان بعدی سامانه بتوانند به‌آسانی این الزامات را رعایت کنند. برای حفظ تناسب، این الزام شامل سامانه‌هایی نمی‌شود که صرفاً نقش کمکی در ویرایش استاندارد دارند یا ورودی را به‌طور اساسی و از نظر معنا تغییر نمی‌دهند.

۱۳۴. علاوه بر راهکارهای فنی به‌کارگرفته‌شده توسط ارائه‌دهندگان سامانهٔ هوش مصنوعی، بهره‌بردارانی که با استفاده از سامانهٔ هوش مصنوعی، محتواهای تصویری، صوتی یا ویدئویی تولید یا دستکاری می‌کنند که به‌طور قابل‌توجهی شبیه افراد، اشیاء، مکان‌ها، نهادها یا رویدادهای واقعی است و می‌تواند به‌نادرست، واقعی جلوه کند (دیپ‌فیک)، باید به‌طور واضح و قابل تشخیص، اعلام کنند که این محتوا مصنوعی است و منشأ آن را افشا کنند. رعایت این تعهد شفافیت نباید به گونه‌ای تفسیر شود که استفاده از سامانه یا خروجی آن را مغایر با آزادی بیان و آزادی هنر و علوم تضمین‌شده در منشور اروپایی بداند. به‌ویژه وقتی که آن محتوا بخشی از یک اثر یا برنامهٔ خلاقانه، طنزآمیز، هنری، داستانی یا مشابه باشد، منوط به رعایت مناسب حقوق و آزادی‌های اشخاص ثالث است. در چنین مواردی، الزام شفافیت به افشای وجود محتوای تولید یا دستکاری‌شده محدود

می‌شود، به گونه‌ای که نمایش یا استفادهٔ عادی از اثر را مختل نکند. همچنین می‌بایست تعهدی مشابه در خصوص افشای متن‌های تولیدشده یا دستکاری‌شده توسط هوش مصنوعی پیش‌بینی شود. این پیش‌بینی تا جایی است که این متون با هدف اطلاع‌رسانی عمومی دربارهٔ مسائل دارای منافع عمومی منتشر می‌شوند، مگر آنکه پیش از انتشار توسط انسان بازبینی یا ویرایش شده و مسئولیت ویراستاری آن بر عهدهٔ یک شخص حقیقی یا حقوقی باشد.

۱۳۵. بدون خدشه به الزام‌آوربودن و قابلیت اجرای کامل تعهدات شفافیت، کمیسیون می‌تواند تدوین کدهای رفتاری در سطح اتحادیه را تشویق و تسهیل کند تا اجرای مؤثر الزامات مربوط به شناسایی و برچسب‌گذاری محتوای مصنوعی را پشتیبانی کند. این کدها می‌توانند شامل ترتیبات عملی برای دسترس‌پذیرکردن سازوکارهای شناسایی و در صورت اقتضا، تسهیل همکاری با سایر کنشگران در زنجیرهٔ ارزش، ازجمله در زمینهٔ انتشار محتوا یا بررسی اصالت و منشأ آن باشند، به گونه‌ای که عموم مردم بتوانند به‌طور مؤثر میان محتوای تولیدشده توسط هوش مصنوعی و محتوای اصیل، تمایز قائل شوند.

۱۳۶. الزامات مندرج در این قانون برای ارائه‌دهندگان و بهره‌برداران برخی سامانه‌های هوش مصنوعی، در راستای امکان شناسایی و افشای تولید یا دستکاری مصنوعی خروجی این سامانه‌ها، نقش ویژه‌ای در اجرای مؤثر قانون (اتحادیهٔ اروپا) ۲۰۶۵/۲۰۲۲ ایفا می‌کند. این امر به‌ویژه در خصوص تعهدات ارائه‌دهندگان سکوهای برخط بسیار بزرگ یا موتورهای جستجوی بسیار بزرگ برای شناسایی و کاهش خطرات نظام‌مند ناشی از انتشار محتوای مصنوعی حائز اهمیت است؛ مخصوصاً خطر پیامدهای منفی بالفعل یا قابل پیش‌بینی که بر فرآیندهای دموکراتیک، گفتمان عمومی و فرآیندهای انتخاباتی که مثلاً از طریق انتشار اطلاعات نادرست ناشی می‌شود، صدق می‌کند. الزام به برچسب‌گذاری محتوا طبق این قانون، بدون خدشه به تعهد مقرر در ماده ۱۶(۶) قانون ۲۰۶۵/۲۰۲۲ برای ارائه‌دهندگان خدمات میزبانی در پردازش اخطارهای مربوط به محتوای غیرقانونی به موجب ماده ۱۶(۱) آن قانون است و نباید بر ارزیابی یا تصمیم‌گیری در خصوص غیرقانونی‌بودن محتوای خاص تأثیر بگذارد. این ارزیابی باید صرفاً بر اساس قواعد ناظر بر مشروعیت محتوا انجام پذیرد.

۱۳۷. رعایت تعهدات شفافیت در مورد سامانه‌های تحت پوشش این قانون، نباید به گونه‌ای تفسیر شود که استفاده از سامانه یا خروجی آن را خودبه‌خود قانونی بداند. این امر بدون خدشه به سایر تعهدات شفافیت مندرج در قوانین اتحادیه یا قوانین ملی برای بهره‌برداران سامانه‌های هوش مصنوعی خواهد بود.

۱۳۸. هوش مصنوعی یک خانواده از فناوری‌های در حال رشد سریع است که نیازمند نظارت مقرراتی و همچنین فضایی ایمن و کنترل‌شده برای آزمایش است؛ این در حالی است که باید نوآوری مسئولانه و ادغام سازوکارهای مناسب حفاظتی و کاهش خطر تضمین شود. به منظور ایجاد چارچوب حقوقی‌ای که نوآوری را ترویج کند، در برابر تحولات آتی مقاوم باشد و تاب‌آوری نهادی داشته باشد، دولت‌های عضو باید اطمینان دهند که مقامات صلاحیت‌دار ملی دست‌کم یک *سندباکس نظارتی هوش مصنوعی* در سطح ملی ایجاد کنند تا توسعه و آزمون سامانه‌های نوآورانهٔ هوش مصنوعی پیش از عرضه به بازار یا بهره‌برداری، تحت نظارت دقیق قانونی انجام گیرد. دولت‌های عضو می‌توانند این تعهد را از طریق مشارکت در سندباکس‌های موجود یا با ایجاد مشترک یک سندباکس با سایر دولت‌های عضو ایفا کنند. چنین امری مشروط بر آن است تا مشارکت در سطح ملی و معادل آن برای اعضای ذی‌نفع فراهم شود. سندباکس‌های نظارتی می‌توانند فیزیکی، دیجیتالی یا ترکیبی ایجاد شوند و محصولات فیزیکی یا دیجیتال را پوشش دهند. مقامات مسئول ایجاد این سندباکس‌ها باید منابع کافی، ازجمله منابع مالی و انسانی را برای کارکرد مؤثر آن‌ها تضمین کنند.

۱۳۹. اهداف سندباکس‌های نظارتی هوش مصنوعی باید تقویت نوآوری از طریق ایجاد محیط کنترل‌شده برای آزمون و خطا در مراحل توسعه و پیش از عرضهٔ آن باشد؛ این خود نیز باید با هدف تضمین انطباق سامانه‌های نوآورانه با این قانون و سایر قوانین اتحادیه و قوانین ملی مرتبط با آن باشد. افزون بر این، سندباکس‌ها باید با افزایش قطعیت حقوقی برای نوآوران، بهبود نظارت مقامات صلاحیت‌دار، ارتقاء شناخت نسبت به فرصت‌ها، خطرات نوظهور و آثار استفاده از هوش مصنوعی، به یادگیری قوانین برای مراجع و فعالان اقتصادی یاری رسانند و به‌ویژه با هدف انطباق چارچوب‌های حقوقی آینده، به همکاری و تبادل بهترین رویه‌ها میان مراجع ذی‌ربط کمک کنند. این سندباکس‌ها باید مسیر دسترسی به بازار را تسهیل نمایند و به‌طور گسترده در سراسر اتحادیه قابل دسترس باشند؛ همچنین می‌بایست رفع موانع پیش روی بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا در اولویت قرار گیرد. مشارکت در سندباکس‌ها باید بر موضوعاتی متمرکز باشد که برای ارائه‌دهندگان، ابهام حقوقی ایجاد می‌کند و مانع نوآوری می‌شود. از این رو نظارت در چارچوب سندباکس باید شامل کل چرخهٔ توسعه، آموزش، آزمون و اعتبارسنجی سامانه پیش از عرضه یا بهره‌برداری، و نیز تغییرات اساسی‌ای باشد که ممکن است مستلزم فرآیند ارزیابی انطباق جدید شود. هر گاه در جریان توسعه یا آزمون، خطرات جدی شناسایی شود، باید تدابیر کاهشی مناسب اعمال و در صورت ناکامی، فرآیند توسعه یا آزمون متوقف شود. مقامات ملی صلاحیت‌دار ایجادکنندهٔ سندباکس باید در صورت اقتضا با دیگر مراجع ذی‌ربط، ازجمله مراجع ناظر بر حمایت از حقوق بنیادین، همکاری کنند و می‌توانند مشارکت دیگر بازیگران زیست‌بوم هوش مصنوعی نظیر سازمان‌های ملی یا اروپایی استانداردسازی، نهادهای

اعلام‌شده، مراکز آزمایش، آزمایشگاه‌های تحقیق و نوآوری، پایگاه‌های اروپایی نوآوری دیجیتال و سازمان‌های ذی‌نفع و جامعهٔ مدنی را نیز امکان‌پذیر کنند. برای تضمین اجرای یکنواخت در سراسر اتحادیه و صرفه‌جویی در مقیاس، باید قواعد مشترکی برای پیاده‌سازی سندباکس‌های نظارتی و چارچوبی برای همکاری میان مراجع ناظر بر آن‌ها ایجاد شود. سندباکس‌های ایجادشده ذیل این قانون نباید به گونه‌ای تفسیر شوند که مانع ایجاد سندباکس‌های دیگری به موجب سایر قوانین اتحادیه یا ملی با اهداف متفاوت شوند. در صورت اقتضا، مراجع صلاحیت‌دار مربوط به آن سندباکس‌ها باید مزایای استفاده از آن‌ها را برای تضمین انطباق سامانه‌های هوش مصنوعی با این قانون نیز در نظر گیرند. همچنین با توافق میان مقامات ملی صلاحیت‌دار و مشارکت‌کنندگان در سندباکس، امکان اجرای آزمون در شرایط واقعی نیز در چارچوب سندباکس نظارتی وجود خواهد داشت.

۱۴۰. این قانون باید مبنای حقوقی لازم را برای ارائه‌دهندگان و ارائه‌دهندگان بالقوه در سندباکس نظارتی هوش مصنوعی فراهم کند تا از داده‌های شخصی گردآوری‌شده برای اهداف دیگر، صرفاً تحت شرایط معین و برای توسعهٔ برخی سامانه‌های هوش مصنوعی در جهت منافع عمومی استفاده کنند. این استفاده باید مطابق ماده ۶(۴) و ماده ۹(۲)(ز) قانون ۲۰۱۶/۶۷۹ (اتحادیهٔ اروپا) و مواد ۵، ۶ و ۱۰ قانون ۲۰۱۸/۱۷۲۵ (اتحادیهٔ اروپا)، و بدون خدشه به ماده ۴(۲) و ماده ۱۰ دستورالعمل ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) باشد. سایر تعهدات کنترل‌کنندگان داده و حقوق اشخاص موضوع داده در قانون‌های ۲۰۱۶/۶۷۹ و ۲۰۱۸/۱۷۲۵ و دستورالعمل ۲۰۱۶/۶۸۰ به‌طور کامل لازم‌الاجرا باقی می‌مانند. به‌ویژه این قانون مبنای حقوقی به معنای ماده ۲۲(۲)(ب) قانون ۲۰۱۶/۶۷۹ و ماده ۲۴(۲)(ب) قانون ۲۰۱۸/۱۷۲۵ محسوب نمی‌شود. ارائه‌دهندگان باید تدابیر حفاظتی مناسب اتخاذ کرده و با مقامات صلاحیت‌دار همکاری کنند. این تدابیر با پیروی از راهنمایی‌های آن‌ها و اقدام فوری و با حسن‌نیت برای کاهش خطرات جدی شناسایی‌شده علیه ایمنی، سلامت و حقوق بنیادین که ممکن است در طول توسعه، آزمون و آزمایش در سندباکس ایجاد شود، اتخاذ می‌شود.

۱۴۱. به منظور تسریع روند توسعه و عرضهٔ سامانه‌های هوش مصنوعی با خطر بالا که در پیوست این قانون فهرست شده‌اند، ضروری است که ارائه‌دهندگان و ارائه‌دهندگان بالقوهٔ این سامانه‌ها بتوانند از یک نظام ویژه برای آزمون این سامانه‌ها در شرایط واقعی، بدون لزوم مشارکت در سندباکس‌های نظارتی هوش مصنوعی بهره‌مند شوند. با این حال، در چنین مواردی و با توجه به پیامدهای احتمالی این نوع آزمون‌ها بر افراد، ضروری است این قانون تضمین‌ها و شرایط مناسب و کافی را پیش‌بینی کند. این تضمین‌ها باید شامل مواردی ازجمله اخذ رضایت آگاهانهٔ اشخاص حقیقی برای مشارکت در آزمون در شرایط واقعی باشد، مگر در مواردی که در زمینهٔ اجرای قانون، اخذ چنین رضایتی مانع از انجام آزمون سامانهٔ هوش مصنوعی شود. رضایت اشخاص

برای مشارکت در آزمون بر اساس این قانون، متمایز از رضایت موضوع داده برای پردازش داده‌های شخصی ایشان تحت قوانین مربوط به حفاظت از داده بوده و به آن خدشه‌ای وارد نمی‌کند. افزون بر این، باید تمهیداتی برای کاهش خطرات و تضمین نظارت مؤثر توسط مقامات صلاحیت‌دار در نظر گرفته شود. بدین منظور، ارائه‌دهندگان بالقوه مکلف‌اند یک آزمون شرایط واقعی را به مرجع صالح نظارت بر بازار طرح کرده و آن را ارائه کنند؛ آزمون را (جز در موارد محدود) در بخش‌های ویژهٔ پایگاه داده اتحادیه ثبت، محدودیت زمانی برای انجام آزمون را رعایت، تدابیر حفاظتی تکمیلی برای گروه‌های آسیب‌پذیر پیش‌بینی و توافقنامه‌ای کتبی در خصوص تعیین نقش‌ها و مسئولیت‌های ارائه‌دهندگان بالقوه و بهره‌برداران همراه با نظارت مؤثر کارکنان ذی‌صلاح منعقد کنند. علاوه بر این، باید تضمین‌های مضاعفی پیش‌بینی شود تا اطمینان حاصل شود که پیش‌بینی‌ها، توصیه‌ها یا تصمیمات سامانهٔ هوش مصنوعی قابلیت بازگشت و بی‌اعتبارشدن را داشته باشد، داده‌های شخصی محفوظ بمانند و در صورتی که اشخاص، رضایت خود را برای مشارکت در آزمون پس بگیرند، حذف شوند، بدون اینکه به حقوق آنان به‌عنوان اشخاص موضوع داده تحت حقوق اتحادیه در حوزهٔ حفاظت از داده، لطمه‌ای وارد آید. در خصوص انتقال داده نیز باید مقرر شود که داده‌های گردآوری و پردازش‌شده برای اهداف آزمون در شرایط واقعی تنها زمانی به کشورهای ثالث منتقل شوند که تدابیر حفاظتی لازم و مناسب طبق حقوق اتحادیه اعمال شده باشد، به‌ویژه بر اساس مبانی انتقال داده‌های شخصی مقرر در حقوق اتحادیه در زمینهٔ حفاظت از داده. در مورد داده‌های غیرشخصی نیز باید تدابیر حفاظتی مناسب طبق حقوق اتحادیه (ازجمله مقررات (اتحادیهٔ اروپا) ۸۶۸/۲۰۲۲[۷۸] و ۲۸۵۴/۲۰۲۳[۷۹] پارلمان و شورای اروپا) برقرار شود.

۱۴۲. برای تضمین آنکه هوش مصنوعی به نتایج اجتماعی و زیست‌محیطی سودمند منجر شود، از دولت‌های عضو خواسته شده است که پژوهش و توسعهٔ راه‌حل‌های مبتنی بر هوش مصنوعی را در این حوزه‌ها حمایت و ترویج کنند. این راه‌حل‌ها می‌تواند شامل افزایش دسترسی افراد دارای معلولیت، کاهش نابرابری‌های اجتماعی ـ اقتصادی یا تحقق اهداف زیست‌محیطی باشد. برای این منظور باید منابع کافی، ازجمله بودجهٔ عمومی و بودجهٔ اتحادیه اختصاص یابد. در صورت احراز شرایط لازم، پروژه‌هایی که چنین اهدافی را دنبال می‌کنند باید در اولویت قرار گیرند. این

۷۸. قانون ۸۶۸/۲۰۲۲ پارلمان اروپا و شورای اروپا در ۳۰ مه ۲۰۲۲ در مورد حاکمیت داده‌های اروپایی و اصلاحیهٔ آیین‌نامهٔ ۱۷۲۴/۲۰۱۸ قانون حاکمیت داده‌ها (روزنامهٔ رسمی ۱۵۲، ۳/۶/۲۰۲۲، ص ۱).

۷۹. آیین‌نامهٔ ۲۸۵۴/۲۰۲۳ پارلمان اروپا و شورای ۱۳ دسامبر ۲۰۲۳ در مورد قوانین هماهنگ در مورد دسترسی منصفانه به داده‌ها و استفاده از آن‌ها و اصلاحیهٔ آیین‌نامهٔ ۲۳۹۴/۲۰۱۷ (اتحادیهٔ اروپا) و دستورالعمل ۱۸۲۸/۲۰۲۰ (اتحادیهٔ اروپا) (قانون داده‌ها) (روزنامهٔ رسمی ۲۸۵۴/۲۰۲۳، ۲۲/۱۲/۲۰۲۳، ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

پروژه‌ها باید بر پایهٔ همکاری میان‌رشته‌ای میان توسعه‌دهندگان هوش مصنوعی، متخصصان نابرابری و عدم تبعیض، دسترس‌پذیری، حقوق مصرف‌کننده، حقوق زیست‌محیطی و دیجیتال و همچنین دانشگاهیان استوار باشند.

۱۴۳. به منظور ترویج و حمایت از نوآوری، ضروری است که منافع شرکت‌های کوچک و متوسط،[80] ازجمله شرکت‌های نوپا که ارائه‌دهنده یا بهره‌بردار سامانه‌های هوش مصنوعی هستند، به‌طور ویژه مورد توجه قرار گیرد. در این راستا، دولت‌های عضو باید ابتکاراتی ویژه برای این دسته از فعالان، به‌ویژه در حوزهٔ ارتقاء آگاهی و اطلاع‌رسانی تدوین کنند. دولت‌های عضو باید به شرکت‌های کوچک و متوسط مخصوصاً شرکت‌های نوپایی که دفتر مرکزی یا شعبه‌ای در اتحادیه دارند، در صورت احراز شرایط و معیارهای انتخاب، دسترسی اولویت‌دار به سندباکس‌های نظارتی هوش مصنوعی بدهند. این باید در حالی باشد که دسترسی سایر ارائه‌دهندگان و متقاضیان واجد شرایط مسدود نشود. دولت‌های عضو باید از کانال‌های موجود برای ارتباط با شرکت‌های کوچک و متوسط، شرکت‌های نوپا، بهره‌برداران، نوآوران دیگر و در صورت لزوم، مقامات محلی استفاده و در صورت نیاز، کانال‌های اختصاصی تازه ایجاد کنند. این کانال‌ها باید راهنمایی ارائه، به پرسش‌ها دربارهٔ اجرای این قانون پاسخ دهند و در صورت امکان با همکاری یکدیگر هم‌افزایی ایجاد کنند تا راهنمایی‌ها هماهنگ و یکسان باشد. همچنین دولت‌های عضو باید مشارکت شرکت‌های کوچک و متوسط و سایر ذی‌نفعان مرتبط را در فرآیند تدوین استانداردها تسهیل کنند. علاوه بر این، نیازها و منافع خاص ارائه‌دهندگانی که شرکت کوچک و متوسط هستند، ازجمله شرکت‌های نوپا، باید هنگام تعیین هزینه‌های ارزیابی انطباق توسط نهادهای ابلاغ‌شده مورد توجه قرار گیرد. کمیسیون باید به‌طور منظم و از طریق مشاوره‌های شفاف، هزینه‌های صدور گواهی و انطباق را برای شرکت‌های کوچک و متوسط بخصوص شرکت‌های نوپا ارزیابی کند و با همکاری دولت‌های عضو این هزینه‌ها را کاهش دهد. برای مثال، ممکن است هزینه‌های ترجمهٔ اسناد الزامی و مکاتبه با مقامات برای فعالان کوچک بسیار سنگین باشد. دولت‌های عضو باید تا حد امکان، اطمینان حاصل کنند که یکی از زبان‌های تعیین‌شده و پذیرفته‌شده برای اسناد مربوط به ارائه‌دهندگان و ارتباط با فعالان، زبانی باشد که بیشترین تعداد از بهره‌برداران فرامرزی بتوانند آن را بفهمند. برای رفع نیازهای خاص شرکت‌های کوچک و متوسط، کمیسیون باید به درخواست هیئت، الگوهای استانداردسازی‌شده برای حوزه‌های تحت پوشش این قانون ارائه دهد. کمیسیون باید اقدامات دولت‌های عضو را تکمیل کند. این امر از طریق ایجاد سکوی اطلاعاتی واحد با رابط کاربری آسان در خصوص این قانون برای همهٔ ارائه‌دهندگان و بهره‌برداران محقق می‌شود. کمیسیون همچنین باید کارزارهای ارتباطی مناسبی را برای افزایش آگاهی از الزامات

80. Small and Medium-sized Enterprises - SMEs

این قانون سازمان‌دهی کند. افزون بر این، ارزیابی و ترویج همگرایی بهترین رویه‌ها در فرآیندهای تدارکات عمومی مرتبط با سامانه‌های هوش مصنوعی نیز از وظایف تکمیلی کمیسیون است. شرکت‌های متوسطی که تا همین اواخر طبق پیوست توصیه‌نامهٔ EC/۲۰۰۳/۳۶۱[۸۱] کمیسیون به‌عنوان شرکت کوچک طبقه‌بندی می‌شدند، باید به این تدابیر حمایتی دسترسی داشته باشند زیرا ممکن است این شرکت‌های متوسط جدید، گاهی فاقد منابع حقوقی و آموزشی لازم برای درک صحیح و انطباق با این قانون باشند.

۱۴۴. به منظور ترویج و حمایت از نوآوری، *سکوی هوش مصنوعی بر حسب تقاضا*[۸۲] و کلیهٔ برنامه‌ها و پروژه‌های تأمین مالی اتحادیه، مانند *برنامهٔ اروپای دیجیتال* و *افق اروپا*[۸۳] که توسط کمیسیون و دولت‌های عضو در سطح اتحادیه یا ملی اجرا می‌شوند، باید حسب مورد در تحقق اهداف این قانون مشارکت کنند.

۱۴۵. به منظور کاهش خطرات ناشی از کمبود دانش و تخصص در بازار و نیز تسهیل پایبندی ارائه‌دهندگان، به‌ویژه بنگاه‌های کوچک و متوسط (ازجمله شرکت‌های نوپا) و همچنین نهادهای ارزیابی انطباق با تعهدات خود ذیل این قانون، *سکوی هوش مصنوعی بر حسب تقاضا*، *مراکز نوآوری دیجیتال اروپا*[۸۴] و *مراکز آزمون و آزمایش*[۸۵] که توسط کمیسیون و دولت‌های عضو در سطح اتحادیه یا ملی ایجاد شده‌اند، باید در اجرای این قانون مشارکت کنند. این نهادها در چارچوب مأموریت و حوزهٔ صلاحیت خود، به‌ویژه می‌توانند پشتیبانی فنی و علمی لازم را برای ارائه‌دهندگان و نهادهای ارزیابی انطباق فراهم کنند.

۱۴۶. با توجه به اینکه برخی فعالان اقتصادی بسیار کوچک هستند و به منظور رعایت تناسب

---

۸۱. توصیه‌نامهٔ کمیسیون در ۶ مه ۲۰۰۳ در مورد تعریف بنگاه‌های خرد، کوچک و متوسط (روزنامهٔ رسمی ۱۲۴، ۲۰۳/۵/۲۰، ص ۳۶).

۸۲. سکوی AI-on-demand یک زیرساخت دیجیتال اروپایی برای هوش مصنوعی است که قابلیت دسترسی به مدل‌ها، مجموعهٔ داده‌ها و ابزارهای هوش مصنوعی را برای محققان و کسب‌وکارها، جهت تقویت نوآوری و همکاری فراهم می‌کند.

83. Horizon Europe

84. the European Digital Innovation Hubs – EDIHs

مراکز نوآوری دیجیتال اروپا، مراکزی جامع هستند که از شرکت‌های کوچک و متوسط، شرکت‌های کوچک با سرمایهٔ متوسط و سازمان‌های بخش دولتی برای تحول دیجیتالی، رقابتی‌ترشدن و پذیرش فناوری‌های پیشرفته مانند هوش مصنوعی و امنیت سایبری پشتیبانی می‌کنند.

85. the Testing and Experimentation Facilities – TEFs

مراکز آزمایش و تست، مراکز تخصصی و بزرگی هستند که ترکیبی از زیرساخت‌های فیزیکی و مجازی را برای ارائه‌دهندگان فناوری فراهم می‌کنند که تا قبل از استقرار در بازار، ابزارهای هوش مصنوعی و رباتیک را در محیط‌های واقعی آزمایش و اعتبارسنجی کنند.

در هزینه‌های نوآوری، بهتر است به *خُردبنگاه‌ها*[۸۶] اجازه داده شود که یکی از پرهزینه‌ترین الزامات یعنی ایجاد نظام مدیریت کیفیت را به شیوه‌ای ساده‌شده اجرا کنند. این رویکرد، بی‌آنکه سطح حفاظت یا ضرورت پایبندی به الزامات مربوط به سامانه‌های هوش مصنوعی پرخطر را کاهش دهد، بار اداری و هزینه‌ها را برای این بنگاه‌ها سبک‌تر می‌کند. کمیسیون باید دستورالعمل‌هایی برای تعیین اجزای نظام مدیریت کیفیت که خُردبنگاه‌ها می‌توانند به این شیوهٔ ساده‌شده اجرا کنند، تدوین کند.

۱۴۷. شایسته است که کمیسیون تا حد امکان، دسترسی به مراکز آزمون و آزمایش را برای نهادها، گروه‌ها یا آزمایشگاه‌هایی که طبق قوانین هماهنگ‌سازی اتحادیه تأسیس یا تأیید صلاحیت شده‌اند و وظایفی در زمینهٔ ارزیابی انطباق محصولات یا تجهیزات مشمول آن قوانین بر عهده دارند، تسهیل کند. این موضوع در مورد *هیئت‌های کارشناسی*، *آزمایشگاه‌های تخصصی* و *آزمایشگاه‌های مرجع* در حوزهٔ تجهیزات پزشکی طبق مقررات ۲۰۱۸/۷۴۵ و ۲۰۱۷/۷۴۶ (اتحادیهٔ اروپا) صدق می‌کند.

۱۴۸. این قانون باید چارچوب حکمرانی ایجاد کند که هم هماهنگی و پشتیبانی از اجرای آن را در سطح ملی ممکن کند و هم ظرفیت‌سازی را در سطح اتحادیه تقویت کرده و ذی‌نفعان حوزهٔ هوش مصنوعی را در این روند مشارکت دهد. اجرای مؤثر و اجرای صحیح این قانون مستلزم وجود سازوکار حکمرانی است که بتواند هماهنگی را تضمین و تخصص متمرکز در سطح اتحادیه را تقویت کند. *دفتر هوش مصنوعی* که بر اساس تصمیم کمیسیون[۸۷] تأسیس شده، مأموریت دارد دانش و ظرفیت‌های اتحادیه در حوزهٔ هوش مصنوعی را توسعه دهد و به اجرای حقوق اتحادیه در زمینهٔ هوش مصنوعی کمک کند. دولت‌های عضو باید برای تسهیل وظایف این دفتر همکاری کنند تا از توسعهٔ تخصص و ظرفیت‌ها در سطح اتحادیه و تقویت کارکرد بازار واحد دیجیتال حمایت شود. علاوه بر این، باید هیئتی متشکل از نمایندگان دولت‌های عضو، تحت عنوان *هیئت علمی* برای ادغام جامعهٔ علمی، و *مجمع مشورتی* برای جلب مشارکت ذی‌نفعان در اجرای این قانون در سطح اتحادیه و ملی تشکیل شود. توسعهٔ تخصص و ظرفیت‌های اتحادیه باید همچنین شامل بهره‌گیری از منابع و تخصص‌های موجود، به‌ویژه از طریق همکاری با ساختارهای شکل‌گرفته در بستر اجرای سایر قوانین اتحادیه و ابتکارات مرتبط در سطح اتحادیه، مانند *سازوکار مشترک محاسبات پیشرفتهٔ اروپا*[۸۸] و *مراکز آزمون و آزمایش هوش مصنوعی* ذیل برنامهٔ *اروپای دیجیتال* باشد.

---

86. Microenterprises

۸۷. تصمیم کمیسیون در ۲۰۲۴/۰۱/۲۴ مبنی بر تأسیس دفتر هوش مصنوعی اروپا 390 (2024)C.

88. European High-Performance Computing Joint Undertaking - EuroHPC

۱۴۹. برای تضمین اجرای روان، مؤثر و هماهنگ این قانون، باید هیئتی تشکیل شود. این هیئت باید بازتاب‌دهندهٔ منافع متنوع زیست‌بوم هوش مصنوعی بوده و متشکل از نمایندگان کشورهای عضو باشد. این هیئت مسئول انجام مجموعه‌ای از وظایف مشورتی است، مانند ارائهٔ نظرات، توصیه‌ها و مشورت یا مشارکت در تدوین رهنمودها دربارهٔ موضوعات مربوط به اجرای این قانون، در خصوص مسائل اجرایی، مشخصات فنی یا استانداردهای موجود در خصوص الزامات مندرج در این قانون، ارائهٔ مشورت به کمیسیون، دولت‌های عضو و مراجع ذی‌صلاح ملی در موضوعات خاص مرتبط با هوش مصنوعی. برای اعطای انعطاف به کشورهای عضو در تعیین نمایندگان خود در این هیئت، چنین نمایندگانی می‌توانند هر فردی از نهادهای عمومی باشند که صلاحیت و اختیارات لازم را برای تسهیل هماهنگی در سطح ملی و مشارکت در انجام وظایف هیئت دارا باشند. هیئت باید دو زیرگروه دائمی ایجاد کند که بستری برای همکاری و تبادل میان مقامات نظارت بر بازار و مقامات ارزیابی انطباق در موضوعات مرتبط، به‌ترتیب با نظارت بر بازار و نهادهای ارزیابی انطباق فراهم آورد. زیرگروه دائمی نظارت بر بازار باید نقش *گروه همکاری اداری*[۸۹] برای این قانون را در معنای مندرج در ماده ۳۰ قانون (اتحادیهٔ اروپا) ۱۰۲۰/۲۰۱۹ ایفا کند. مطابق ماده ۳۳، کمیسیون باید با انجام ارزیابی‌ها یا مطالعات بازار، به‌ویژه با هدف شناسایی جنبه‌هایی از این قانون که نیازمند هماهنگی خاص و فوری میان مقامات نظارت بر بازار است، از فعالیت‌های این زیرگروه پشتیبانی کند. هیئت می‌تواند سایر زیرگروه‌های دائمی یا موقت را برای بررسی موضوعات خاص، در صورت لزوم ایجاد کند. همچنین هیئت باید حسب مورد با نهادهای مرتبط اتحادیه، گروه‌های کارشناسی و شبکه‌های فعال در چارچوب قوانین مرتبط اتحادیه به‌ویژه آن‌هایی که در حوزهٔ داده، محصولات و خدمات دیجیتال فعالیت دارند، همکاری کند.

۱۵۰. به منظور تضمین مشارکت ذی‌نفعان در اجرای این قانون، باید *انجمن مشورتی* تشکیل شود تا به هیئت و کمیسیون، مشاورهٔ تخصصی و فنی ارائه کند. برای اطمینان از نمایندگی متنوع و متوازن میان منافع تجاری و غیرتجاری، و در حوزهٔ منافع تجاری با توجه به شرکت‌های کوچک و متوسط، شرکت‌های نوپا و دیگر بنگاه‌ها، این انجمن مشورتی باید شامل نمایندگان بخش صنعت، شرکت‌های نوپا، بنگاه‌های کوچک و متوسط، دانشگاه‌ها، جامعهٔ مدنی (ازجمله شرکای اجتماعی) و همچنین نهادهایی چون *آژانس حقوق بنیادین*،[۹۰] *آژانس امنیت سایبری اتحادیهٔ اروپا*،[۹۱] *کمیتهٔ اروپایی استانداردسازی*،[۹۲] *کمیتهٔ اروپایی استانداردسازی الکتروتکنیک*[۹۳] و *مؤسسهٔ استانداردهای*

89. The Administrative Cooperation Group - ADCO
90. European Union Agency for Fundamental Rights - FRA
91. European Union Agency for Cybersecurity - ENISA
92. European Committee for Standardization - CEN
93. European Committee for Electrotechnical Standardization - CENELEC

مخابراتی اروپا[۹۴] باشد.

۱۵۱. به منظور پشتیبانی از اجرای این قانون و به‌ویژه فعالیت‌های نظارتی دفتر هوش مصنوعی در خصوص مدل‌های هوش مصنوعی عمومی، باید *هیئت علمی* متشکل از کارشناسان مستقل تشکیل شود. این کارشناسان مستقل باید بر اساس تخصص علمی یا فنی به‌روز در حوزهٔ هوش مصنوعی انتخاب شوند و وظایف خود را با بی‌طرفی و عینیت انجام دهند. آن‌ها باید محرمانگی اطلاعات و داده‌های به‌دست‌آمده در جریان انجام وظایف و فعالیت‌های خود را حفظ و رعایت کنند. برای تقویت ظرفیت‌های ملی لازم جهت اجرای مؤثر این قانون، دولت‌های عضو باید بتوانند در چارچوب فعالیت‌های اجرایی خود، از مجموعهٔ کارشناسان این هیئت علمی درخواست پشتیبانی کنند.

۱۵۲. به منظور پشتیبانی از اجرای مؤثر قانون در خصوص سامانه‌های هوش مصنوعی و تقویت ظرفیت‌های دولت‌های عضو، باید ساختارهای پشتیبانی آزمون هوش مصنوعی در سطح اتحادیه ایجاد شده و در اختیار دولت‌های عضو قرار گیرد.

۱۵۳. دولت‌های عضو، نقش کلیدی در اعمال و اجرای این قانون دارند. از این رو هر کشور عضو باید حداقل یک مرجع اعلام‌کننده و یک مرجع نظارت بر بازار را به‌عنوان مراجع ذی‌صلاح ملی برای نظارت بر اجرای این قانون تعیین کند. دولت‌های عضو می‌توانند با توجه به ویژگی‌ها و نیازهای سازمانی ملی خود، هر نهاد عمومی را برای انجام وظایف مراجع ذی‌صلاح ملی منصوب کنند. به منظور ارتقاء کارآیی سازمانی و ایجاد نقطهٔ تماس واحد با عموم و دیگر طرفین ذی‌ربط در سطوح ملی و اتحادیه، هر کشور عضو باید یک مرجع نظارت بر بازار را به‌عنوان *نقطهٔ تماس واحد* تعیین کند.

۱۵۴. مراجع ذی‌صلاح ملی باید اختیارات خود را به‌طور مستقل، بی‌طرف و بدون هر گونه جانبداری اعمال کنند تا اصول عینیت در فعالیت‌ها و وظایفشان تضمین شود و اجرای قانون به‌درستی صورت گیرد. اعضای این مراجع باید از هر گونه اقدام مغایر با وظایف خود خودداری کنند و مشمول قواعد محرمانگی مقرر در این قانون باشند.

۱۵۵. به منظور آنکه ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر بتوانند از تجربه‌های حاصل از استفاده از این سامانه‌ها برای بهبود سامانه‌های خود و نیز فرآیند طراحی و توسعه بهره‌مند شوند، یا بتوانند اقدامات اصلاحی لازم را به‌موقع انجام دهند، تمامی ارائه‌دهندگان باید *سامانه پایش پس از عرضه* برقرار کنند. در صورت اقتضا، این پایش باید شامل تحلیل تعامل با دیگر سامانه‌های هوش مصنوعی، ازجمله سایر دستگاه‌ها و نرم‌افزارها باشد. پایش پس از عرضه نباید داده‌های عملیاتی حساس بهره‌برداران را که مراجع اجرای قانون هستند، پوشش دهد. این سامانه همچنین برای

94. European Telecommunications Standards Institute - ETSI

مقابلهٔ مؤثرتر و سریع‌تر با خطرات احتمالی ناشی از سامانه‌های هوش مصنوعی که پس از عرضه به بازار یا بهره‌برداری، همچنان به *یادگیری* ادامه می‌دهند، اهمیت کلیدی دارد. در این چارچوب، ارائه‌دهندگان می‌بایست سامانه‌ای برای گزارش هر حادثهٔ جدی ناشی از استفاده از سامانه‌های خود به مراجع ذی‌صلاح داشته باشند. حادثهٔ جدی به معنای رویداد یا نقص عملکردی است که مِنجر به مرگ یا آسیب جدی به سلامت، اختلال جدی و غیرقابل بازگشت در مدیریت و بهره‌برداری از زیرساخت‌های حیاتی، نقض تعهدات مقرر در حقوق اتحادیه برای حمایت از حقوق بنیادین یا واردآمدن خسارت جدی به اموال یا محیط‌زیست شود.

۱۵۶. برای تضمین اجرای مناسب و مؤثر الزامات و تعهدات مقرر در این قانون (که یک قانون هماهنگ‌سازی اتحادیه محسوب می‌شود)، نظام نظارت بر بازار و انطباق محصولات که در قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) ایجاد شده است، باید به‌طور کامل اعمال شود. مراجع نظارت بر بازار که مطابق این قانون تعیین می‌شوند، باید از تمامی اختیارات اجرایی پیش‌بینی‌شده در این قانون و قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) برخوردار باشند و این اختیارات را به‌طور مستقل، بی‌طرف و بدون جانبداری اعمال کنند. هرچند اکثریت سامانه‌های هوش مصنوعی مشمول الزامات و تعهدات خاص این قانون نیستند، مراجع نظارت بر بازار می‌توانند در مورد هر سامانه‌ای که مطابق این قانون ایجاد خطر می‌کند، اقدامات لازم را در قبال آن اتخاذ کنند. با توجه به ماهیت خاص نهادها، آژانس‌ها و ارگان‌های اتحادیه که در حوزهٔ شمول این قانون قرار دارند، شایسته است *ناظر اروپایی حفاظت از داده‌ها* به‌عنوان مرجع ذی‌صلاح نظارت بر بازار برای آن‌ها تعیین شود. این امر نباید به اختیارات دولت‌های عضو در تعیین مراجع ذی‌صلاح ملی خدشه‌ای وارد کند. فعالیت‌های نظارت بر بازار نباید توانایی نهادهای تحت نظارت را برای انجام مستقل وظایفشان، در مواردی که این استقلال به موجب حقوق اتحادیه الزامی است مختل کند.

۱۵۷. این قانون به صلاحیت‌ها، وظایف، اختیارات و استقلال مراجع یا نهادهای عمومی ملی ذی‌ربط که بر اجرای حقوق اتحادیه در زمینهٔ حمایت از حقوق بنیادین نظارت می‌کنند (ازجمله نهادهای برابری و مراجع حفاظت از داده)، خدشه‌ای وارد نمی‌کند. این مراجع یا نهادها باید در صورت نیاز برای انجام مأموریت خود، به کلیهٔ اسناد ایجادشده بر اساس این قانون دسترسی داشته باشند. برای مقابلهٔ به‌موقع و مؤثر با سامانه‌های هوش مصنوعی که تهدیدی برای سلامت، ایمنی یا حقوق بنیادین هستند، باید رویهٔ حفاظتی ویژه ایجاد شود. این رویه شامل سامانه‌های هوش مصنوعی پرخطر، سامانه‌های ممنوعی که برخلاف قانون در بازار عرضه یا به خدمت گرفته شده‌اند، و همچنین سامانه‌هایی است که در نقض الزامات شفافیت عرضه شده و ایجاد خطر می‌کنند.

۱۵۸. قانون خدمات مالی اتحادیه، شامل قواعد حاکمیت داخلی و الزامات مدیریت ریسک است. این قواعد بر مؤسسات مالی تحت نظارت، هنگام ارائهٔ خدمات، ازجمله هنگام استفاده از سامانه‌های هوش مصنوعی اعمال می‌شود. برای تضمین اجرای منسجم این قانون و دیگر قواعد خدمات مالی اتحادیه، مقام‌های صلاحیت‌دار باید مسئولیت نظارت و اجرای این مقررات را بر عهده گیرند. این مقام‌ها همان نهادهای نظارتی هستند که در این مقام‌ها همان نهادهای نظارتی هستند که در قانون شمارهٔ ۲۰۱۳/۵۷۵ پارلمان و شورای اروپا[۹۵] و دستورالعمل‌های EC/۴۸/۲۰۰۸،[۹۶] EC/۱۳۸/۲۰۰۹،[۹۷] EU/۳۶/۲۰۱۳،[۹۸] EU/۱۷/۲۰۱۴ [۹۹]و ۲۰۱۶/۹۷ پارلمان و شورای اروپا[۱۰۰] نیز تعریف شده‌اند. آن‌ها باید در حدود صلاحیت خود، به‌عنوان مقام‌های ناظر برای اجرای این قانون و نیز انجام فعالیت‌های پایش بازار در زمینهٔ سامانه‌های هوش مصنوعی که توسط مؤسسات مالی تحت نظارت عرضه یا به کار گرفته می‌شوند، عمل کنند. با این حال، کشورهای عضو می‌توانند نهاد دیگری را برای انجام وظایف پایش بازار تعیین کنند. این مراجع ناظر باید از کلیهٔ اختیارات پیش‌بینی‌شده در این قانون و قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) برای اجرای الزامات و تعهدات مندرج در آن برخوردار باشند؛ ازجمله اختیارات انجام فعالیت‌های نظارت پسابازاری که می‌تواند در صورت لزوم، در سازوکارها و رویه‌های نظارتی موجود آن‌ها در چارچوب حقوق خدمات مالی اتحادیه ادغام شود. همچنین زمانی که این نهادها در مقام مقام‌های پایش بازار فعالیت می‌کنند، باید بی‌درنگ اطلاعاتی را که طی فعالیت‌های پایشی به دست می‌آورند و ممکن است برای وظایف نظارتی بانک مرکزی اروپا اهمیت داشته باشد، به بانک مرکزی اروپا گزارش دهند. این موضوع، به‌ویژه در مورد نهادهای ملی ناظر بر مؤسسات

۹۵. آیین‌نامهٔ (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۳/۵۷۵ پارلمان اروپا و شورای اروپا در ۲۶ ژوئن ۲۰۱۳ در مورد الزامات احتیاطی برای مؤسسات اعتباری و شرکت‌های سرمایه‌گذاری و اصلاحیهٔ آیین‌نامهٔ (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۲/۶۴۸ (روزنامهٔ رسمی ۱۷۶، ۲۷.۶.۲۰۱۳، ص ۱).

۹۶. دستورالعمل EC/۴۸/۲۰۰۸ پارلمان اروپا و شورا در ۲۳ آوریل ۲۰۰۸ در مورد قراردادهای اعتباری برای مصرف‌کنندگان و لغو دستورالعمل شورا EEC/۱۰۲/۸۷ (روزنامهٔ رسمی ۱۳۳، ۲۰۰۸/۵/۲۲، ص ۶۶).

۹۷. دستورالعمل EC/۱۳۸/۲۰۰۹ پارلمان اروپا و شورا در ۲۵ نوامبر ۲۰۰۹ در مورد پذیرش و پیگیری کسب و کار بیمه و بیمهٔ اتکایی (توانگری مالی دوم) (روزنامهٔ رسمی ۳۳۵، ۲۰۰۹/۱۲/۱۷، ص ۱).

۹۸. دستورالعمل EU/۳۶/۲۰۱۳ پارلمان اروپا و شورا در ۲۶ ژوئن ۲۰۱۳ در مورد دسترسی به فعالیت مؤسسات اعتباری و نظارت احتیاطی بر مؤسسات اعتباری و شرکت‌های سرمایه‌گذاری، اصلاح دستورالعمل EC/۸۷/۲۰۰۲ و لغو دستورالعمل‌های EC/۴۸/۲۰۰۶ و EC/۴۹/۲۰۰۶ (روزنامهٔ رسمی ۱۷۶، ۲۰۱۳/۶/۲۷، ص ۳۳۸).

۹۹. دستورالعمل EU/۱۷/۲۰۱۴ پارلمان اروپا و شورای ۴ فوریهٔ ۲۰۱۴ در مورد قراردادهای اعتباری برای مصرف‌کنندگان مربوط به اموال غیرمنقول مسکونی و اصلاحیهٔ دستورالعمل‌های EC/۴۸/۲۰۰۸ و EU/۳۶/۲۰۱۳ و آیین‌نامهٔ (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۰/۱۰۹۳ (روزنامهٔ رسمی ۶۰، ۲۰۱۴/۲/۲۸، ص ۳۴).

۱۰۰. دستورالعمل ۲۰۱۶/۹۷ پارلمان اروپا و شورا در ۲۰ ژانویهٔ ۲۰۱۶ در مورد توزیع بیمه (روزنامهٔ رسمی ۲۶، ۲۰۱۶/۲/۲، ص ۱۹).

اعتباری تحت شمول دستورالعمل EU/۳۶/۲۰۱۳ که در سازوکار نظارتی واحد مشارکت دارند (مطابق قانون[۱۰۱] شمارهٔ ۱۰۲۴/۲۰۱۳ اتحادیهٔ اروپا) مصداق دارد. برای تقویت انسجام میان این قانون و قواعد حاکم بر مؤسسات اعتباری، لازم است برخی تعهدات شکلی ارائه‌دهندگان در زمینهٔ مدیریت ریسک، پایش پس از عرضه و مستندسازی، در تعهدات و رویه‌های موجود تحت دستورالعمل EU/۳۶/۲۰۱۳ ادغام شود. به منظور جلوگیری از تداخل، باید معافیت‌های محدودی در رابطه با نظام مدیریت کیفیت ارائه‌دهندگان و تعهد پایش استفاده‌کنندگان از سامانه‌های پرخطر هوش مصنوعی برای مؤسسات اعتباری تحت شمول این دستورالعمل در نظر گرفته شود. همین رژیم باید در مورد شرکت‌های بیمه و بیمهٔ اتکایی و شرکت‌های هلدینگ بیمه‌ای تحت دستورالعمل EC/۱۳۸/۲۰۰۹ و کارگزاران بیمه تحت دستورالعمل ۲۰۱۶/۹۷ (اتحادیهٔ اروپا) و سایر مؤسسات مالی که مشمول الزامات مربوط به حاکمیت داخلی و فرآیندهای مقرر بر اساس قوانین خدمات مالی اتحادیه هستند نیز اعمال شود، تا انسجام و رفتار برابر در بخش مالی تضمین شود.

۱۵۹. هر مرجع نظارت بر بازار برای سامانه‌های هوش مصنوعی پرخطر در حوزهٔ زیست‌سنجی، طبق فهرست پیوست این قانون و تا آنجا که این سامانه‌ها برای مقاصد اجرای قانون، مهاجرت، پناهندگی و مدیریت کنترل مرز یا ادارهٔ عدالت و فرآیندهای دموکراتیک استفاده می‌شوند، باید از اختیارات مؤثر تحقیقاتی و اصلاحی برخوردار باشد. این اختیارات باید شامل حق دسترسی به تمام داده‌های شخصی در حال پردازش و اطلاعات لازم برای انجام وظایف مرجع باشد. مراجع نظارت بر بازار باید بتوانند اختیارات خود را با استقلال کامل اعمال کنند. هر گونه محدودیت بر دسترسی آن‌ها به داده‌های عملیاتی حساس تحت این قانون، نباید به اختیارات اعطاشده به آن‌ها به موجب دستورالعمل ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) خدشه‌ای وارد کند. همچنین هیچ محدودیتی بر افشای داده‌ها به مراجع حفاظت از داده‌های ملی تحت این قانون، نباید بر اختیارات فعلی یا آتی این مراجع فراتر از حوزهٔ شمول این قانون، تأثیری بگذارد.

۱۶۰. مراجع نظارت بر بازار و کمیسیون باید بتوانند پیشنهاد فعالیت‌های مشترک، ازجمله تحقیقات مشترک را ارائه دهند. این فعالیت‌ها می‌تواند توسط مراجع نظارت بر بازار یا به‌صورت مشترک با کمیسیون انجام شود و هدف آن‌ها ارتقاء رعایت مقررات، شناسایی موارد عدم انطباق، افزایش آگاهی و ارائهٔ راهنمایی در ارتباط با این قانون نسبت به دسته‌های خاصی از سامانه‌های هوش مصنوعی پرخطر باشد که در دو یا چند کشور عضو، خطر جدی ایجاد می‌کنند. فعالیت‌های مشترک برای ترویج انطباق باید مطابق ماده ۹ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) اجرا شود. دفتر هوش مصنوعی

۱۰۱. آیین‌نامهٔ شورای اتحادیهٔ اروپا شمارهٔ ۲۰۱۳/۱۰۲۴ در ۱۵ اکتبر ۲۰۱۳ که وظایف خاصی را در رابطه با سیاست‌های مربوط به نظارت احتیاطی بر مؤسسات اعتباری به بانک مرکزی اروپا محول می‌کند (روزنامهٔ رسمی ۲۸۷، ۲۰۱۳/۱۰/۲۹، ص ۶۳).

باید از تحقیقات مشترک حمایت و هماهنگی لازم را فراهم آورد.

۱۶۱. ضروری است که مسئولیت‌ها و صلاحیت‌ها در سطح اتحادیه و ملی در خصوص سامانه‌های هوش مصنوعی مبتنی بر مدل‌های هوش مصنوعی عمومی روشن شود. برای جلوگیری از تداخل صلاحیت‌ها، در صورتی که یک سامانهٔ هوش مصنوعی مبتنی بر مدل با کاربرد عمومی باشد و مدل و سامانه، هر دو توسط یک ارائه‌دهنده عرضه شوند، نظارت باید در سطح اتحادیه و از طریق *دفتر هوش مصنوعی* صورت گیرد. این دفتر می‌بایست برای این منظور، اختیارات یک مرجع نظارت بر بازار را طبق قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) دارا باشد. در سایر موارد، مسئولیت نظارت بر سامانه‌های هوش مصنوعی بر عهدهٔ مراجع ملی نظارت بر بازار می‌ماند. با این حال، در مورد سامانه‌های هوش مصنوعی عمومی که می‌توانند مستقیماً توسط بهره‌برداران برای حداقل یک کارکرد طبقه‌بندی‌شده به‌عنوان پرخطر استفاده شوند، مراجع نظارت بر بازار باید با دفتر هوش مصنوعی همکاری کنند. آن‌ها باید برای ارزیابی انطباق اقدام و هیئت و سایر مراجع نظارت بر بازار را مطلع کنند. علاوه بر این، مراجع نظارت بر بازار باید بتوانند در صورتی که به دلیل عدم دسترسی به برخی اطلاعات مربوط به مدل با کاربرد عمومی که سامانهٔ هوش مصنوعی پرخطر بر پایهٔ آن ساخته شده، قادر به تکمیل تحقیقات نباشند، از دفتر هوش مصنوعی درخواست کمک کنند. در چنین مواردی، رویهٔ مربوط به مساعدت متقابل در موارد فرامرزی مندرج در فصل ششم قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) با رعایت تغییرات لازم اعمال می‌شود.

۱۶۲. برای استفادهٔ بهینه از تخصص متمرکز اتحادیه و هم‌افزایی در سطح اتحادیه، صلاحیت نظارت و اجرای تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی باید در اختیار کمیسیون باشد. دفتر هوش مصنوعی باید بتواند تمامی اقدامات لازم را برای پایش اجرای مؤثر این قانون، در خصوص مدل‌های هوش مصنوعی عمومی انجام دهد. این دفتر باید قادر باشد هم به ابتکار خود (بر اساس نتایج فعالیت‌های پایشی) و هم به درخواست مراجع نظارت بر بازار، تحقیقات لازم را دربارهٔ تخلفات احتمالی ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی انجام دهد. برای حمایت و پشتیبانی از پایش مؤثر، دفتر باید این امکان را فراهم آورد که ارائه‌دهندگان پایین‌دستی بتوانند شکایاتی دربارهٔ تخلفات احتمالی ارائه‌دهندگان مدل‌ها و سامانه‌های هوش مصنوعی عمومی ثبت کنند.

۱۶۳. به منظور تکمیل نظام حکمرانی در خصوص مدل‌های هوش مصنوعی عمومی، هیئت علمی باید از فعالیت‌های پایشی دفتر هوش مصنوعی پشتیبانی کند و در موارد خاص، هشدارهای تخصصی ارائه دهد که پیگیری‌هایی مانند تحقیقات را به دنبال داشته باشد. این وضعیت، زمانی پیش می‌آید که هیئت علمی، دلایلی برای ظن وجود خطر واقعی و قابل شناسایی در سطح اتحادیه، ناشی

از یک مدل هوش مصنوعی عمومی داشته باشد. همچنین این امر، زمانی باید انجام شود که هیئت علمی، دلیلی برای ظن قوی مبنی بر اینکه یک مدل هوش مصنوعی عمومی معیارهای طبقه‌بندی به‌عنوان *مدل با خطر سیستماتیک* را داراست، پیدا کند. برای تجهیز هیئت علمی به اطلاعات لازم جهت انجام این وظایف باید سازوکاری پیش‌بینی شود که به موجب آن، هیئت بتواند از کمیسیون درخواست کند تا اسناد یا اطلاعاتی را از یک ارائه‌دهنده مطالبه کند.

۱۶۴. دفتر هوش مصنوعی باید بتواند اقدامات لازم را برای پایش اجرای مؤثر و انطباق با تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی طبق این قانون انجام دهد. این دفتر باید بتواند در چارچوب اختیارات پیش‌بینی‌شده در این قانون، تخلفات احتمالی را بررسی کند. این اقدامات شامل درخواست اسناد و اطلاعات، انجام ارزیابی‌ها و مطالبهٔ اقدامات از ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی است. در زمان انجام ارزیابی‌ها به منظور بهره‌گیری از تخصص، دفتر باید بتواند کارشناسان مستقل را برای انجام ارزیابی‌ها به نمایندگی از خود به کار گیرد. اجرای تعهدات باید از طریق ابزارهایی مانند درخواست اقدامات مناسب، ازجمله اقدامات کاهش ریسک در موارد شناسایی خطرات نظام‌مند و همچنین محدودکردن عرضه در بازار یا خارج‌کردن و بازخواندن مدل، تحقق یابد. به‌عنوان تضمین، هر گاه در مواردی که فراتر از آیین دادرسیِ پیش‌بینی‌شده در این قانون ضرورت داشته باشد، ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی باید از حقوق آیین دادرسی مندرج در ماده ۱۸ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) برخوردار باشند. این حقوق باید با رعایت تغییرات لازم و بدون خدشه به رویهٔ خاص‌تر پیش‌بینی شده اعمال شود.

۱۶۵. توسعهٔ سامانه‌های هوش مصنوعی غیرپرخطر، در صورت انطباق با الزامات این قانون می‌تواند منجر به گسترش بیشتر هوش مصنوعی اخلاق‌مدار و قابل اعتماد در اتحادیه شود. ارائه‌دهندگان سامانه‌های هوش مصنوعی که پرخطر محسوب نمی‌شوند، باید تشویق شوند که *آیین‌نامه‌های رفتاری* شامل سازوکارهای حکمرانی مرتبط ایجاد کنند. این آیین‌نامه‌ها باید با هدف ترویج اجرای داوطلبانهٔ برخی یا همهٔ الزامات اجباری سامانه‌های هوش مصنوعی پرخطر تدوین و متناسب با هدف سامانه، سطح پایین‌تر خطر، با توجه به راهکارهای فنی موجود و بهترین رویه‌های صنعتی مانند *کارت‌های مدل* و *کارت‌های داده* تنظیم شوند. ارائه‌دهندگان و در صورت اقتضا، بهره‌برداران همهٔ سامانه‌ها و مدل‌های هوش مصنوعی (اعم از پرخطر یا غیرپرخطر) باید به اجرای داوطلبانهٔ الزامات اضافی تشویق شوند. این الزامات می‌تواند شامل عناصر *رهنمودهای اخلاقی اتحادیه برای هوش مصنوعی قابل اعتماد*، پایداری زیست‌محیطی، اقدامات ارتقاء سواد هوش مصنوعی، طراحی و توسعهٔ فراگیر و متنوع سامانه‌ها (با توجه به افراد آسیب‌پذیر و دسترسی‌پذیری برای افراد دارای معلولیت)، و مشارکت ذی‌نفعان از طریق دخالت نهادهایی مانند کسب‌وکارها (بخش

خصوصی)، سازمان‌های جامعهٔ مدنی، دانشگاه‌ها، مراکز پژوهشی، اتحادیه‌های کارگری و سازمان‌های حمایت از مصرف‌کنندگان در فرآیند طراحی و توسعهٔ سامانه‌ها باشد. تنوع تیم‌های توسعه‌دهنده، ازجمله تعادل جنسیتی نیز باید مورد توجه قرار گیرد. برای مؤثربودن آیین‌نامه‌های رفتاری داوطلبانه، آن‌ها باید بر اهداف روشن و شاخص‌های کلیدی عملکرد مبتنی باشند تا تحقق اهداف، قابل سنجش باشد. همچنین باید به‌طور فراگیر و با مشارکت ذی‌نفعان ذی‌ربط، مانند کسب‌وکارها، سازمان‌های جامعهٔ مدنی، دانشگاه‌ها، مراکز پژوهشی، اتحادیه‌های کارگری و سازمان‌های حمایت از مصرف‌کنندگان توسعه یابند. کمیسیون می‌تواند ابتکاراتی ازجمله در سطح بخشی، برای تسهیل کاهش موانع فنی که مانع تبادل فرامرزی داده برای توسعهٔ هوش مصنوعی می‌شود ارائه دهد. این امر می‌تواند شامل زیرساخت‌های دسترسی به داده و تضمین قابلیت تعامل معنایی و فنی میان انواع مختلف داده‌ها باشد.

۱۶۶. مهم است که سامانه‌های هوش مصنوعی مرتبط با محصولاتی که بر اساس این قانون، پرخطر محسوب نمی‌شوند و بنابراین ملزم به رعایت الزامات مقرر برای سامانه‌های هوش مصنوعی پرخطر نیستند، هنگام عرضه در بازار یا بهره‌برداری نیز ایمن باشند. برای تحقق این هدف، قانون ۲۰۲۳/۹۸۸ پارلمان و شورای اروپا[۱۰۲] به‌عنوان ابزار ایمنی اعمال خواهد شد.

۱۶۷. برای تضمین همکاری قابل اعتماد و سازنده میان مراجع صلاحیت‌دار در سطح اتحادیه و ملی، کلیهٔ طرفین ذی‌ربط در اجرای این قانون باید محرمانگی اطلاعات و داده‌هایی را که در انجام وظایف خود به دست می‌آورند، مطابق حقوق اتحادیه یا ملی رعایت کنند. آن‌ها باید وظایف و فعالیت‌های خود را به گونه‌ای انجام دهند که به‌ویژه از حقوق مالکیت فکری، اطلاعات محرمانهٔ تجاری و اسرار تجاری، اجرای مؤثر این قانون، منافع امنیت عمومی و ملی، یکپارچگی دادرسی‌های کیفری و اداری و تمامیت اطلاعات طبقه‌بندی‌شده حفاظت شود.

۱۶۸. اجرای این قانون باید از طریق اعمال مجازات‌ها و سایر تدابیر اجرایی تضمین شود. دولت‌های عضو باید تمامی اقدامات لازم را برای اجرای مقررات این قانون اتخاذ کنند. این اقدامات شامل تعیین مجازات‌های مؤثر، متناسب و بازدارنده برای نقض آن و رعایت اصل عدم مجازات مضاعف است. به منظور تقویت و هماهنگ‌سازی مجازات‌های اداری مربوط به نقض این قانون، باید سقف‌های بالایی برای جریمه‌های اداری برخی تخلفات مشخص تعیین شود. هنگام ارزیابی میزان جریمه، دولت‌های عضو باید در هر مورد خاص، تمامی شرایط مرتبط با موقعیت ویژه را مدنظر قرار دهند. در این خصوص باید به ماهیت، شدت، مدت نقض و پیامدهای آن و همچنین

۱۰۲. آیین‌نامهٔ ۲۰۲۳/۹۸۸ پارلمان اروپا و شورا در ۱۰ مه ۲۰۲۳ در مورد ایمنی عمومی محصولات، اصلاحیهٔ آیین‌نامهٔ (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۲/۱۰۲۵ پارلمان اروپا و شورا و دستورالعمل ۲۰۲۰/۱۸۲۸ پارلمان اروپا و شورا، و لغو دستورالعمل EC/۹۵/۲۰۰۱ پارلمان اروپا و شورا و دستورالعمل شورا EEC/۳۵۷/۸۷ (روزنامهٔ رسمی ۱۳۵، ۲۰۲۳/۵/۲۳، ص ۱).

اندازهٔ ارائه‌دهنده توجه ویژه شود. این امر به‌ویژه در مواردی که ارائه‌دهنده، شرکت کوچک یا متوسط یا شرکت نوپا است، اهمیت دارد. *ناظر اروپایی حفاظت از داده‌ها* باید اختیار اعمال جریمه علیه نهادها، آژانس‌ها و ارگان‌های اتحادیه را که مشمول این قانون می‌شوند، داشته باشد.

۱۶۹. رعایت تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی که به موجب این قانون وضع شده است، باید ازجمله از طریق جریمه‌ها قابل اجرا باشد. برای این منظور، سطوح مناسب جریمه‌ها باید برای نقض این تعهدات تعیین شود. این امر شامل عدم رعایت اقداماتی است که کمیسیون طبق این قانون مطالبه کرده است. تعیین جریمه‌ها باید مشمول دوره‌های محدودیت مناسب و مطابق اصل تناسب باشد. تمامی تصمیم‌هایی که کمیسیون بر اساس این قانون اتخاذ می‌کند، باید قابل رسیدگی و بازبینی در *دیوان دادگستری اتحادیهٔ اروپا* و مطابق معاهدهٔ عملکرد اتحادیهٔ اروپا باشد. این بازبینی شامل صلاحیت قضایی نامحدود دیوان در خصوص مجازات‌ها طبق ماده ۲۶۱ معاهدهٔ عملکرد اتحادیهٔ اروپا نیز هست.

۱۷۰. حقوق اتحادیه و حقوق ملی، هم‌اکنون نیز راهکارهای مؤثری برای اشخاص حقیقی و حقوقی که حقوق و آزادی‌هایشان بر اثر استفاده از سامانه‌های هوش مصنوعی به‌طور منفی تحت تأثیر قرار گرفته است، فراهم می‌کند. بدون لطمه به این راهکارها، هر شخص حقیقی یا حقوقی که دلایل کافی برای اعتقاد به وقوع نقض این قانون داشته باشد، باید حق داشته باشد شکایتی را نزد مرجع نظارت بر بازار مربوط مطرح کند.

۱۷۱. هنگامی که تصمیم بهره‌بردار، عمدتاً بر خروجی سامانه‌های خاص هوش مصنوعی پرخطری استوار است که مشمول این قانون می‌شوند، اشخاص متأثر باید حق داشته باشند توضیحی دریافت کنند. این حق، زمانی ایجاد می‌شود که تصمیم یادشده، آثار حقوقی به جا بگذارد یا به‌طور مشابه تأثیرات قابل‌توجهی بر آن اشخاص داشته باشد، به گونه‌ای که آن‌ها آن را به زیان سلامت، ایمنی یا حقوق بنیادین خود بدانند. توضیح باید روشن و معنادار باشد و مبنایی فراهم کند تا اشخاص متأثر بتوانند حقوق خود را اعمال کنند. حق دریافت توضیح نباید شامل استفاده از سامانه‌های هوش مصنوعی‌ای شود که طبق حقوق اتحادیه یا ملی استثنا یا محدودیت برای آن‌ها پیش‌بینی شده است. همچنین این حق صرفاً تا حدی اعمال می‌شود که پیش‌تر تحت حقوق اتحادیه مقرر نشده باشد.

۱۷۲. اشخاصی که به‌عنوان افشاگر، موارد نقض این قانون را گزارش می‌دهند، باید تحت حمایت حقوق اتحادیه باشند. از این رو دستورالعمل ۲۰۱۹/۱۹۳۷ پارلمان و شورای اروپا[۱۰۳] باید در خصوص گزارش موارد نقض این قانون و حمایت از اشخاص گزارش‌دهنده اعمال شود.

---

۱۰۳. دستورالعمل ۲۰۱۹/۱۹۳۷ پارلمان اروپا و شورا در ۲۳ اکتبر ۲۰۱۹ در مورد حمایت از افرادی که نقض قانون اتحادیه را گزارش می‌دهند (روزنامهٔ رسمی ۳۰۵، ۲۰۱۹/۱۱/۲۶، ص ۱۷).

۱۷۳. برای اطمینان از اینکه این چارچوب مقرراتی در موارد ضروری سازگاری داشته باشد، اختیار تصویب اقدامات تفویضی مطابق ماده ۲۹۰ معاهدهٔ عملکرد اتحادیهٔ اروپا باید به کمیسیون واگذار شود. این اختیار باید شامل اصلاح شرایطی باشد که تحت آن، سامانهٔ هوش مصنوعی پرخطر محسوب نمی‌شود. فهرست سامانه‌های پرخطر، مقررات مربوط به مستندات فنی، محتوای *اعلامیهٔ انطباق اتحادیهٔ اروپا*، مقررات مربوط به رویه‌های ارزیابی انطباق، مقررات مربوط به تعیین سامانه‌های پرخطری که ارزیابی انطباق آن‌ها مبتنی بر ارزیابی نظام مدیریت کیفیت و مستندات فنی است، آستانه‌ها، معیارها و شاخص‌ها (ازجمله تکمیل آن‌ها) در قواعد مربوط به طبقه‌بندی مدل‌های هوش مصنوعی عمومی دارای خطر نظام‌مند، معیارهای تعیین این مدل‌ها، مستندات فنی ارائه‌دهندگان این مدل‌ها و اطلاعات شفافیت مربوط به آن‌ها است. اهمیت ویژه دارد که کمیسیون در جریان کارهای مقدماتی خود، مشاوره‌های مقتضی، ازجمله در سطح کارشناسی انجام دهد. این مشاوره‌ها باید مطابق اصول مندرج در *توافقنامهٔ بین‌نهادی ۱۳ آوریل ۲۰۱۶ دربارهٔ قانونگذاری بهتر*[۱۰۴] صورت گیرد. به‌ویژه برای تضمین مشارکت برابر در تهیهٔ اعمال تفویضی، پارلمان و شورای اروپا، اتحادیه باید هم‌زمان با کارشناسان کشورهای عضو، تمامی اسناد را دریافت کنند. کارشناسان آن‌ها باید به‌طور نظام‌مند به جلسات گروه‌های کارشناسی کمیسیون که به تهیهٔ اعمال تفویضی می‌پردازند، دسترسی داشته باشند.

۱۷۴. با توجه به تحولات سریع فناوری و تخصص فنی مورد نیاز برای اجرای مؤثر این قانون، کمیسیون باید این قانون را تا ۲ اوت ۲۰۲۹ و سپس هر چهار سال یک بار، ارزیابی و بازنگری کرده و گزارش آن را به پارلمان و شورای اروپا ارائه دهد. علاوه بر این، با لحاظ آثار احتمالی بر دامنهٔ شمول این قانون، کمیسیون باید هر سال یک بار، نیاز به اصلاح فهرست سامانه‌های پرخطر و فهرست رویه‌های ممنوعه را ارزیابی کند. همچنین تا ۲ اوت ۲۰۲۸ و سپس هر چهار سال یک بار، کمیسیون باید ضرورت اصلاح فهرست عناوین حوزه‌های پرخطر مندرج در پیوست این قانون، فهرست سامانه‌های هوش مصنوعی مشمول الزامات شفافیت، اثربخشی نظام نظارت و حکمرانی و پیشرفت در توسعهٔ استانداردهای مرتبط با توسعهٔ بهینهٔ انرژی در مدل‌های هوش مصنوعی عمومی را ارزیابی کند. این ارزیابی باید شامل نیاز به اقدامات یا تدابیر تکمیلی نیز باشد و به پارلمان و شورای اروپا گزارش دهد. در آخر، کمیسیون باید تا ۲ اوت ۲۰۲۸ و سپس هر سه سال یک بار، تأثیر و کارآمدی آیین‌نامه‌های رفتاری داوطلبانه را در ترویج اجرای الزامات مقرر برای سامانه‌های پرخطر در مورد سامانه‌های غیرپرخطر و احتمالاً الزامات اضافی دیگر برای این سامانه‌ها ارزیابی کند.

۱۷۵. برای تضمین شرایط یکنواخت در اجرای این قانون، باید اختیارات اجرایی به کمیسیون

---

۱۰۴. (روزنامهٔ رسمی ۱۲۳، ۲۰۱۶/۵/۱۲، ص ۱).

اعطا شود. این اختیارات باید مطابق قانون شمارهٔ ۱۸۲/۲۰۱۱ پارلمان و شورای اروپا اتحادیه[۱۰۵] اعمال شود.

۱۷۶. هدف این قانون یعنی بهبود کارکرد بازار داخلی و ترویج استفاده از هوش مصنوعی انسان‌محور و قابل اعتماد، همراه با تضمین سطح بالایی از حمایت از سلامت، ایمنی، حقوق بنیادین مندرج در منشور ازجمله دموکراسی، حاکمیت قانون و حفاظت محیط‌زیست در برابر آثار زیان‌بار سامانه‌های هوش مصنوعی در اتحادیه و در عین حال، حمایت از نوآوری است و نمی‌تواند به اندازهٔ کافی توسط کشورهای عضو محقق شود؛ لذا با توجه به مقیاس گستردهٔ آثار اقدامات، بهتر است این هدف در سطح اتحادیه به انجام رسد. بنابراین اتحادیه می‌تواند بر اساس اصل *واگذاری صلاحیت* مندرج در ماده ۵ معاهدهٔ اتحادیهٔ اروپا، تدابیری را اتخاذ کند. همچنین مطابق *اصل تناسب* مندرج در همان ماده، این قانون از آنچه برای دستیابی به هدف یادشده ضروری است، فراتر نمی‌رود.

۱۷۷. به منظور تضمین قطعیت حقوقی، فراهم‌کردن دورهٔ تطبیق مناسب برای فعالان اقتصادی و جلوگیری از اختلال در بازار، ازجمله با تضمین استمرار استفاده از سامانه‌های هوش مصنوعی، شایسته است که این قانون تنها در مورد سامانه‌های هوش مصنوعی پرخطری که پیش از تاریخ اجرای کلی آن در بازار عرضه یا به بهره‌برداری رسیده‌اند، قابل اعمال باشد؛ آن هم فقط در صورتی که از آن تاریخ به بعد، تغییرات اساسی در طراحی یا هدف موردنظر آن‌ها ایجاد شود. در این خصوص، لازم است روشن شود که مفهوم *تغییر اساسی* باید از نظر ماهوی معادل اصطلاح *اصلاح اساسی یا عمده* در نظر گرفته شود که صرفاً در ارتباط با سامانه‌های هوش مصنوعی پرخطر طبق این قانون به کار می‌رود. به‌طور استثنایی و با توجه به ضرورت پاسخگویی عمومی، بهره‌برداران سامانه‌های هوش مصنوعی که بخشی از سامانه‌های فناوری اطلاعات در مقیاس بزرگ هستند (که این سامانه‌ها بر اساس اسناد حقوقی مندرج در پیوست این قانون ایجاد شده‌اند) و نیز بهره‌برداران سامانه‌های هوش مصنوعی پرخطری که برای استفاده توسط مقامات عمومی در نظر گرفته شده‌اند، باید به‌ترتیب، اقدامات لازم را برای انطباق با الزامات این قانون تا پایان سال ۲۰۳۰ و تا ۲ اوت ۲۰۳۰ اتخاذ کنند.

۱۷۸. از ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر خواسته می‌شود که حتی در دورهٔ گذار، داوطلبانه اجرای الزامات مربوط به این قانون را آغاز کنند.

۱۷۹. این قانون باید از ۲ اوت ۲۰۲۶ لازم‌الاجرا شود. با این حال، با توجه به خطر غیرقابل قبول ناشی از برخی کاربردهای هوش مصنوعی، ممنوعیت‌ها و نیز مقررات عمومی این قانون باید از ۲ فوریهٔ ۲۰۲۵ به اجرا گذاشته شود. اگرچه آثار کامل این ممنوعیت‌ها پس از استقرار سازوکارهای

۱۰۵. قانون شمارهٔ ۲۰۱۱/۱۸۲ پارلمان اروپا و شورای اروپا در ۱۶ فوریهٔ ۲۰۱۱ که قواعد و اصول کلی مربوط به سازوکارهای کنترل اعمال اختیارات اجرایی کمیسیون توسط کشورهای عضو را تعیین می‌کند (روزنامهٔ رسمی ۵۵، ۲۰۱۱/۲/۲۸، ص ۱۳).

حکمرانی و اجرای این قانون محقق می‌شود، اجرای زودهنگام این ممنوعیت‌ها، برای مقابله با خطرات غیرقابل قبول و اثرگذاری بر سایر رویه‌ها همچون حقوق مدنی اهمیت دارد. افزون بر این، زیرساخت‌های مرتبط با نظام حکمرانی و سامانهٔ ارزیابی انطباق باید پیش از ۲ اوت ۲۰۲۶ عملیاتی شوند؛ از این رو مقررات مربوط به نهادهای اعلام‌شده و ساختار حاکمیتی باید از ۲ اوت ۲۰۲۵ لازم‌الاجرا شوند. با توجه به سرعت بالای پیشرفت‌های فناوری و گسترش استفاده از مدل‌های هوش مصنوعی عمومی، تعهدات مربوط به ارائه‌دهندگان این مدل‌ها باید از ۲ اوت ۲۰۲۵ اعمال شود. همچنین آیین‌نامه‌های رویه‌ای باید تا ۲ مه ۲۰۲۵ آماده باشند تا امکان انطباق به‌موقع برای تأمین‌کنندگان فراهم شود. دفتر هوش مصنوعی باید اطمینان حاصل کند که قواعد و رویه‌های طبقه‌بندی در پرتو تحولات فناوری به‌روز می‌ماند. افزون بر این، دولت‌های عضو باید مقررات مربوط به مجازات‌ها، ازجمله جریمه‌های اداری را تدوین کرده و به کمیسیون اعلام کنند و تضمین دهند که این مقررات تا تاریخ اجرای این قانون به‌درستی و به‌طور مؤثر اعمال می‌شود. بنابراین مقررات جزایی باید از ۲ اوت ۲۰۲۵ لازم‌الاجرا شود.

۱۸۰. ناظر اروپایی حفاظت از داده‌ها و هیئت اروپایی حفاظت از داده‌ها که بر اساس بندهای ۱ و ۲ ماده ۴۲ قانون ۲۰۱۸/۱۷۲۵ (اتحادیهٔ اروپا) مشاوره داده شدند و در ۱۸ ژوئن ۲۰۲۱ نظر مشترک خود را ارائه کردند،

قانون حاضر را تصویب کردند:

فصل اول. احکام کلی

ماده ۱. موضوع قانون

۱. هدف از این قانون، بهبود کارکرد بازار داخلی و ترویج به‌کارگیری هوش مصنوعی انسان‌محور و قابل اعتماد است. در عین حال، این قانون تضمین سطح بالای حمایت از سلامت، ایمنی، حقوق بنیادین مندرج در منشور، ازجمله دموکراسی، حاکمیت قانون و حفاظت از محیط‌زیست در برابر آثار زیان‌بار سامانه‌های هوش مصنوعی در اتحادیه و نیز حمایت از نوآوری را دنبال می‌کند.

۲. این قانون شامل موارد زیر است:

الف) قواعد هماهنگ‌شده در خصوص عرضه در بازار، بهره‌برداری و استفاده از سامانه‌های هوش مصنوعی در اتحادیه؛

ب) ممنوعیت برخی از رویه‌های خاص هوش مصنوعی؛

پ) الزامات ویژه برای سامانه‌های هوش مصنوعی پرخطر و تعهدات بهره‌برداران این سامانه‌ها؛

ت) قواعد هماهنگ‌شده در زمینهٔ شفافیت برای برخی از سامانه‌های هوش مصنوعی؛

ث) قواعد هماهنگ‌شده دربارهٔ مدل‌های هوش مصنوعی برای عرضه در بازار با مقاصد عام؛
ج) قواعد مربوط به پایش بازار، نظارت بر بازار، حکمرانی و اجرای مقررات؛
چ) تدابیری در حمایت از نوآوری، با تمرکز ویژه بر شرکت‌های کوچک و متوسط، ازجمله شرکت‌های نوپا.

ماده ۲. دامنهٔ شمول

۱. این قانون در موارد زیر اعمال می‌شود:
الف) ارائه‌دهندگانی که سامانه‌ها یا مدل‌های هوش مصنوعی با مقاصد عام را در اتحادیه عرضه یا به کار می‌گیرند، صرف‌نظر از آنکه این ارائه‌دهندگان در قلمرو اتحادیه یا در کشور ثالث مستقر یا فعالیت داشته باشند؛
ب) بهره‌برداران سامانه‌های هوش مصنوعی که محل استقرار یا فعالیت آن‌ها در قلمرو اتحادیه قرار دارد؛
پ) ارائه‌دهندگان و بهره‌برداران سامانه‌های هوش مصنوعی که محل استقرار یا فعالیت آن‌ها در کشور ثالث است، در صورتی که خروجی تولیدشده توسط سامانهٔ هوش مصنوعی در اتحادیه استفاده شود؛
ت) واردکنندگان و توزیع‌کنندگان سامانه‌های هوش مصنوعی؛
ث) تولیدکنندگان کالا که سامانهٔ هوش مصنوعی را همراه با محصول خود و تحت نام یا علامت تجاری خویش در بازار عرضه می‌کنند یا به کار می‌گیرند؛
ج) نمایندگان مجاز ارائه‌دهندگانی که در اتحادیه مستقر نیستند؛
چ) اشخاص ذی‌نفعی که در قلمرو اتحادیه مستقر هستند.

۲. در خصوص سامانه‌های هوش مصنوعی که بر اساس بند (۱) ماده ۶ به‌عنوان سامانه‌های پرخطر طبقه‌بندی شده و به کالاهایی مربوط می‌شوند که در بخش (ب) پیوست شمارهٔ (۱) تحت پوشش قوانین هماهنگ اتحادیه قرار دارند، تنها بند (۱) ماده ۶، مواد ۱۰۲ تا ۱۰۹ و ماده ۱۱۲ اعمال می‌شود. ماده ۵۷ صرفاً تا جایی اعمال می‌شود که الزامات مربوط به سامانه‌های پرخطر هوش مصنوعی در چارچوب همان قوانین هماهنگ اتحادیه ادغام شده باشد.

۳. این قانون در حوزه‌هایی که خارج از دامنهٔ حقوق اتحادیه است اعمال نمی‌شود و در هیچ حال به صلاحیت‌های کشورهای عضو در خصوص امنیت ملی خدشه‌ای وارد نمی‌کند، صرف‌نظر از نوع نهادهایی که از سوی کشورهای عضو برای انجام وظایف مرتبط با این صلاحیت‌ها مأمور شده‌اند. همچنین این قانون در مورد سامانه‌های هوش مصنوعی مرتبط با مقاصد صرفاً نظامی، دفاعی یا

امنیت ملی که با یا بدون تغییر در بازار عرضه و به کار گرفته یا مورد استفاده قرار می‌گیرند، صرف‌نظر از نوع نهاد انجام‌دهندهٔ این فعالیت‌ها اعمال نمی‌شود. افزون بر این، قانون حاضر شامل آن دسته از سامانه‌های هوش مصنوعی که در اتحادیه عرضه یا به کار گرفته نمی‌شوند ولی خروجی آن‌ها منحصراً برای مقاصد نظامی، دفاعی یا امنیت ملی در اتحادیه مورد استفاده قرار می‌گیرند نیز نمی‌شود.

۴. این قانون شامل مقامات عمومی کشورهای ثالث و نیز سازمان‌های بین‌المللی‌ای که بر اساس پاراگراف (۱) در دامنهٔ شمول آن قرار می‌گیرند، نمی‌شود، در صورتی که این مقامات یا سازمان‌ها از سامانه‌های هوش مصنوعی در چارچوب همکاری‌های بین‌المللی یا توافقات مربوط به همکاری قضایی و اجرای قانون با اتحادیه یا یک یا چند کشور عضو استفاده کنند، مشروط بر اینکه کشور ثالث یا سازمان بین‌المللی مزبور، تضمین‌های کافی در زمینهٔ حمایت از حقوق و آزادی‌های بنیادین اشخاص ارائه دهد.

۵. قانون حاضر بر اجرای مقررات مربوط به مسئولیت ارائه‌دهندگان خدمات واسطه‌ای که در فصل دوم قانون شمارهٔ ۲۰۲۲/۲۰۶۵ (اتحادیهٔ اروپا) آمده است، تأثیری ندارد.

۶. این قانون شامل سامانه‌ها یا مدل‌های هوش مصنوعی ازجمله خروجی‌های آن‌ها که به‌طور خاص برای اهداف پژوهش و توسعهٔ علمی طراحی و به کار گرفته شده‌اند، نمی‌شود.

۷. حقوق اتحادیه در زمینهٔ حمایت از داده‌های شخصی، حریم خصوصی و محرمانگی ارتباطات در مورد داده‌های شخصیِ پردازش‌شده در ارتباط با حقوق و تعهدات مقرر در این قانون اعمال می‌شود. قانون حاضر به هیچ وجه، تأثیری بر مقررات (اتحادیهٔ اروپا) به شمارهٔ ۲۰۱۶/۶۷۹ و ۲۰۱۸/۱۷۲۵، یا دستورالعمل ۲۰۰۲/۵۸ و ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) ندارد، بدون آن که به مواد ۱۰(۵) و ۵۹ این قانون، لطمه‌ای وارد آید.

۸. این قانون شامل هیچ فعالیت تحقیقاتی، آزمایشی یا توسعه‌ای مربوط به سامانه‌ها یا مدل‌های هوش مصنوعی پیش از عرضه در بازار یا بهره‌برداری نمی‌شود. این گونه فعالیت‌ها باید مطابق حقوق قابل اعمال اتحادیه انجام گیرند. با این حال، ارزیابی عملکرد سامانه در شرایط واقعی بهره‌برداری از شمول این استثنا خارج است.

۹. این قانون بدون خدشه به قواعد مقرر در سایر اسناد حقوقی اتحادیه در زمینهٔ حمایت از مصرف‌کننده و ایمنی محصول است.

۱۰. این قانون شامل تعهدات بهره‌بردارانی که اشخاص حقیقی بوده و از سامانه‌های هوش مصنوعی در چارچوب فعالیت‌های صرفاً شخصی و غیرحرفه‌ای استفاده می‌کنند، نمی‌شود.

۱۱. این قانون مانع از آن نیست که اتحادیه یا کشورهای عضو، قوانین، مقررات یا اقدامات اداری

مطلوب‌تری در راستای حمایت از حقوق کارگران در قبال استفادهٔ کارفرمایان از سامانه‌های هوش مصنوعی وضع یا حفظ کنند یا اجرای موافقت‌نامه‌های جمعی را که برای کارگران شرایط مساعدتری ایجاد می‌کند، تشویق یا مجاز کنند.

۱۲. این قانون شامل سامانه‌های هوش مصنوعی‌ای که تحت مجوزهای آزاد و متن‌باز منتشر می‌شوند، نمی‌شود، مگر آنکه چنین سامانه‌هایی به‌عنوان سامانه‌های هوش مصنوعی پرخطر یا مشمول مواد ۵ یا ۵۰ طبقه‌بندی شده باشند.

ماده ۳. تعاریف

۱. برای اهداف این قانون، تعاریف زیر اعمال می‌شود:

(۱) *سامانهٔ هوش مصنوعی*[۱۰۶] به معنای سامانه‌ای مبتنی بر ماشین است که برای فعالیت با درجات متفاوتی از خودکاربودن طراحی شده و ممکن است پس از به‌کارگیری، قابلیت سازگاری یا تطبیق‌پذیری از خود نشان دهد. این سامانه به منظور دستیابی به اهداف صریح یا ضمنی، از داده‌های ورودی که دریافت می‌کند نتیجه‌گیری می‌کند تا خروجی‌هایی همچون پیش‌بینی‌ها، محتوا، توصیه‌ها یا تصمیم‌هایی تولید کند که می‌توانند بر محیط‌های فیزیکی یا مجازی تأثیر بگذارند.

(۲) *خطر*[۱۰۷] به معنای ترکیب احتمال وقوع زیان و شدت آن زیان است.

(۳) *ارائه‌دهنده*[۱۰۸] به شخص حقیقی یا حقوقی، مقام عمومی، نهاد یا هر مرجع دیگری گفته می‌شود که سامانه یا مدل هوش مصنوعی با کاربرد عام را توسعه یا توسعهٔ آن را از طریق شخص دیگری انجام می‌دهد و سپس آن را با نام یا علامت تجاری خود، خواه در برابر پرداخت یا رایگان در بازار عرضه کرده یا مورد بهره‌برداری قرار می‌دهد.

(۴) *به‌کارگیرنده*[۱۰۹] به شخص حقیقی یا حقوقی، مقام عمومی، نهاد یا مرجع دیگری اطلاق می‌شود که سامانهٔ هوش مصنوعی را تحت اختیار خود به کار می‌گیرد، مگر آنکه این سامانه در چارچوب فعالیت شخصی و غیرحرفه‌ای استفاده شود.

(۵) *نمایندهٔ مجاز*[۱۱۰] به شخص حقیقی یا حقوقی مستقر یا مقیم در اتحادیه اطلاق می‌شود که از سوی ارائه‌دهندهٔ سامانه یا مدل هوش مصنوعی با کاربرد عام، اختیارنامهٔ کتبی دریافت کرده و آن را پذیرفته باشد تا به نمایندگی از او تعهدات و رویه‌های مقرر در این قانون را انجام دهد.

---

106. AI system
107. Risk
108. Provider
109. Deployer
110. Authorised representative

(۶) *واردکننده*[۱۱۱] به شخص حقیقی یا حقوقی مستقر یا مقیم در اتحادیه گفته می‌شود که سامانهٔ هوش مصنوعی‌ای را که با نام یا علامت تجاری شخص حقیقی یا حقوقی مستقر در کشور ثالث عرضه می‌شود، در بازار اتحادیه عرضه می‌کند.

(۷) *توزیع‌کننده*[۱۱۲] به شخص حقیقی یا حقوقی در زنجیرهٔ تأمین اطلاق می‌شود که غیر از ارائه‌دهنده یا واردکننده است و سامانهٔ هوش مصنوعی را در بازار اتحادیه در دسترس قرار می‌دهد.

(۸) *بهره‌بردار*[۱۱۳] به ارائه‌دهنده، تولیدکنندهٔ محصول، به‌کارگیرنده، نمایندهٔ مجاز، واردکننده یا توزیع‌کننده گفته می‌شود.

(۹) *عرضه به بازار*[۱۱۴] به معنای نخستین دردسترس‌قراردادن سامانه یا مدل هوش مصنوعی با کاربرد عام در بازار اتحادیه است.

(۱۰) *دردسترس‌قراردادن در بازار*[۱۱۵] به معنای تأمین سامانه یا مدل هوش مصنوعی با کاربرد عام برای توزیع یا استفاده در بازار اتحادیه در چارچوب فعالیت تجاری است، خواه در برابر پرداخت یا رایگان باشد.

(۱۱) *به‌کارگیری*[۱۱۶] به معنای تأمین سامانهٔ هوش مصنوعی برای استفادهٔ نخستین به‌طور مستقیم توسط به‌کارگیرنده یا برای استفادهٔ شخصی در اتحادیه مطابق هدف موردنظر آن است.

(۱۲) *هدف موردنظر*[۱۱۷] به معنای نوع استفاده‌ای است که ارائه‌دهنده برای سامانهٔ هوش مصنوعی در نظر گرفته است ازجمله زمینه و شرایط خاص استفاده، همان گونه که در اطلاعات ارائه‌شده از سوی ارائه‌دهنده در دستورالعمل استفاده، موارد تبلیغاتی یا فروش، اظهارات رسمی و همچنین در مستندات فنی تصریح شده است.

(۱۳) *سوءاستفادهٔ قابل پیش‌بینی معقول*[۱۱۸] به معنای استفاده از سامانهٔ هوش مصنوعی به شیوه‌ای مغایر با هدف موردنظر آن است اما استفاده‌ای که می‌تواند ناشی از رفتار انسانیِ معقولِ قابل پیش‌بینی یا تعامل با سایر سامانه‌ها ازجمله سامانه‌های هوش مصنوعی دیگر باشد.

(۱۴) *جزء ایمنی*[۱۱۹] به مؤلفه‌ای از یک محصول یا سامانهٔ هوش مصنوعی گفته می‌شود که وظیفهٔ ایمنی برای آن محصول یا سامانه را دارد یا خرابی یا نقص عملکرد آن، سلامت و ایمنی اشخاص یا اموال را به خطر می‌اندازد.

111. Importer
112. Distributor
113. Operator
114. Placing on the market
115. Making available on the market
116. Putting into service
117. Intended purpose
118. Reasonably foreseeable misuse
119. safety component

(۱۵) *دستورالعمل استفاده*[۱۲۰] به اطلاعاتی اطلاق می‌شود که از سوی ارائه‌دهنده برای آگاهی‌رسانی به به‌کارگیرنده دربارهٔ هدف موردنظر سامانهٔ هوش مصنوعی و نحوهٔ استفادهٔ صحیح از آن ارائه می‌شود.

(۱۶) *فراخوان سامانهٔ هوش مصنوعی*[۱۲۱] به هر اقدامی گفته می‌شود که با هدف بازگرداندن سامانهٔ هوش مصنوعی به ارائه‌دهنده یا خارج‌کردن آن از خدمت یا غیرفعال‌سازی استفاده از آن توسط به‌کارگیرندگان انجام می‌گیرد.

(۱۷) *خروج سامانهٔ هوش مصنوعی از بازار*[۱۲۲] به هر اقدامی اطلاق می‌شود که با هدف جلوگیری از در دسترس‌قرارگرفتن سامانهٔ هوش مصنوعی در زنجیرهٔ تأمین برای عرضه در بازار انجام می‌شود.

(۱۸) *کارآیی سامانهٔ هوش مصنوعی*[۱۲۳] به توانایی سامانهٔ هوش مصنوعی برای تحقق هدف موردنظر خود گفته می‌شود.

(۱۹) *مرجع اعلام‌کننده*[۱۲۴] به مقام ملی مسئول ایجاد و اجرای رویه‌های لازم برای ارزیابی، تعیین و اعلام نهادهای ارزیابی انطباق و نظارت بر آن‌ها گفته می‌شود.

(۲۰) *ارزیابی انطباق*[۱۲۵] به فرآیند اثبات این امر گفته می‌شود که الزامات مقرر در بخش دوم از فصل سوم، مربوط به سامانه‌های هوش مصنوعی با ریسک بالا رعایت شده است.

(۲۱) *نهاد ارزیابی انطباق*[۱۲۶] به نهادی گفته می‌شود که فعالیت‌های ارزیابی انطباق را به‌صورت شخص ثالث انجام می‌دهد، ازجمله آزمون، صدور گواهی و بازرسی.

(۲۲) *نهاد اعلام‌شده*[۱۲۷] به نهاد ارزیابی انطباقی اطلاق می‌شود که طبق این قانون و سایر قوانین هماهنگ‌شدهٔ اتحادیه به‌طور رسمی اعلام شده باشد.

(۲۳) *تغییر اساسی*[۱۲۸] به تغییری در سامانهٔ هوش مصنوعی پس از عرضه به بازار یا به‌کارگیری آن گفته می‌شود که در ارزیابی انطباق اولیه پیش‌بینی یا برنامه‌ریزی نشده و در نتیجهٔ آن، مطابقت سامانه با الزامات مقرر در بخش دوم از فصل سوم تحت تأثیر قرار گیرد یا موجب تغییر در هدف موردنظر سامانه شود.

(۲۴) *نشان CE*[۱۲۹] به علامتی گفته می‌شود که ارائه‌دهنده از طریق آن اعلام می‌کند سامانهٔ

120. instructions for use
121. Recall of an AI system
122. withdrawal of an AI system
123. Performance of an AI system
124. Notifying authority
125. Conformity assessment
126. Conformity assessment body
127. Notified body
128. Substantial modification
129. CE marking

هوش مصنوعی با الزامات مقرر در بخش دوم از فصل سوم و سایر قوانین هماهنگ‌شدهٔ اتحادیه که نصب این نشان را پیش‌بینی کرده‌اند، مطابقت دارد.

(۲۵) *سامانهٔ پایش پس از عرضه به بازار*[۱۳۰] به تمامی اقداماتی گفته می‌شود که توسط ارائه‌دهندگان سامانه‌های هوش مصنوعی برای گردآوری و بررسی تجربیات استفاده از سامانه‌هایی که در بازار عرضه کرده یا به کار گرفته‌اند، به منظور شناسایی نیاز به انجام فوری اقدامات اصلاحی یا پیشگیرانهٔ لازم انجام می‌شود.

(۲۶) *مرجع نظارت بر بازار*[۱۳۱] به مقام ملی اطلاق می‌شود که بر اساس مقررات شمارهٔ ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) وظیفهٔ انجام فعالیت‌ها و اتخاذ اقدامات نظارتی را بر عهده دارد.

(۲۷) *استاندارد هماهنگ‌شده*[۱۳۲] به معنای استاندارد هماهنگ‌شده‌ای است که در بند (ج) از ماده ۲(۱) مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا تعریف شده است.

(۲۸) *مشخصات مشترک*[۱۳۳] به مجموعه‌ای از مشخصات فنی اطلاق می‌شود که طبق بند (۴) ماده ۲ مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ تعریف شده و ابزار لازم برای رعایت الزامات معینی را که در این قانون مقرر شده فراهم می‌آورد.

(۲۹) *داده‌های آموزشی*[۱۳۴] داده‌هایی هستند که برای آموزش سامانهٔ هوش مصنوعی از طریق تنظیم معیارهای قابل یادگیری آن به کار می‌روند.

(۳۰) *داده‌های اعتبارسنجی*[۱۳۵] داده‌هایی هستند که برای ارزیابی سامانهٔ هوش مصنوعی آموزش‌دیده و تنظیم معیارهای غیرقابل یادگیری و فرآیند یادگیری آن ازجمله به منظور جلوگیری از ناکافی‌بودن یا یادگیری افراطی به کار می‌روند.

(۳۱) *مجموعهٔ داده‌های اعتبارسنجی*[۱۳۶] به مجموعه‌ای مستقل از داده‌ها یا بخشی از مجموعهٔ داده‌های آموزشی گفته می‌شود که می‌تواند به‌صورت ثابت یا متغیر تقسیم شده باشد.

(۳۲) *داده‌های آزمون*[۱۳۷] داده‌هایی هستند که برای ارزیابی مستقل سامانهٔ هوش مصنوعی به منظور تأیید عملکرد مورد انتظار آن پیش از عرضه به بازار یا به‌کارگیری استفاده می‌شوند.

(۳۳) *داده‌های ورودی*[۱۳۸] به داده‌هایی گفته می‌شود که به سامانهٔ هوش مصنوعی ارائه می‌شوند یا مستقیماً توسط آن دریافت می‌شوند و سامانه بر مبنای آن‌ها خروجی تولید می‌کند.

130. Post-market monitoring system
131. Market surveillance authority
132. Harmonised standard
133. Common specification
134. Training data
135. Validation data
136. Validation data set
137. Testing data
138. Input data

(۳۴) *داده‌های زیست‌سنجی*[۱۳۹] به داده‌های شخصی حاصل از پردازش فنی خاصی اطلاق می‌شود که به ویژگی‌های فیزیکی، فیزیولوژیکی یا رفتاری شخص حقیقی، مانند تصاویر چهره یا داده‌های اثر انگشت مربوط می‌شود.

(۳۵) *شناسایی زیست‌سنجی*[۱۴۰] به فرآیند شناسایی خودکار ویژگی‌های فیزیکی، فیزیولوژیکی، رفتاری یا روان‌شناختی انسان برای تعیین هویت یک شخص حقیقی از طریق مقایسهٔ داده‌های زیست‌سنجی او با داده‌های زیست‌سنجی ذخیره‌شده در یک پایگاه داده گفته می‌شود.

(۳۶) *تأیید هویت زیست‌سنجی*[۱۴۱] به فرآیند خودکار تطبیق فردی راستی‌آزمایی یا احراز هویت اشخاص حقیقی از طریق مقایسهٔ داده‌های زیست‌سنجی آن‌ها با داده‌های زیست‌سنجی پیش‌تر ارائه‌شده اطلاق می‌شود.

(۳۷) *دسته‌های ویژهٔ داده‌های شخصی*[۱۴۲] به دسته‌هایی از داده‌های شخصی گفته می‌شود که در ماده ۹(۱) مقررات ۲۰۱۶/۶۷۹ (اتحادیهٔ اروپا)، ماده ۱۰ دستورالعمل ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) و ماده ۱۰(۱) مقررات ۲۰۱۸/۱۷۲۵ (اتحادیهٔ اروپا) مورد اشاره قرار گرفته‌اند.

(۳۸) *داده‌های عملیاتی حساس*[۱۴۳] به داده‌های عملیاتی مربوط به فعالیت‌های پیشگیری، کشف، تحقیق یا تعقیب جرایم گفته می‌شود که ممکن است افشای آن‌ها سلامت و تمامیت دادرسی کیفری را به خطر اندازد.

(۳۹) *سامانهٔ تشخیص احساسات*[۱۴۴] به سامانهٔ هوش مصنوعی‌ای گفته می‌شود که برای شناسایی یا استنباط احساسات یا مقاصد اشخاص حقیقی بر مبنای داده‌های زیست‌سنجی آنان طراحی شده است.

(۴۰) *سامانهٔ دسته‌بندی زیست‌سنجی*[۱۴۵] به سامانهٔ هوش مصنوعی‌ای گفته می‌شود که برای طبقه‌بندی اشخاص حقیقی در دسته‌های معین بر مبنای داده‌های زیست‌سنجی آنان طراحی شده است، مگر آنکه به‌عنوان بخشی فرعی از یک خدمت تجاری دیگر بوده و تنها به دلایل فنی عینی و ضروری مورد استفاده قرار گیرد.

(۴۱) *سامانهٔ شناسایی زیست‌سنجی از راه دور*[۱۴۶] به سامانهٔ هوش مصنوعی‌ای اطلاق می‌شود که با هدف شناسایی اشخاص حقیقی بدون مشارکت فعال آنان، معمولاً از طریق مقایسهٔ داده‌های

139. Biometric data
140. Biometric identification
141. Biometric verification
142. Special categories of personal data
143. Sensitive operational data
144. Emotion recognition system
145. Biometric categorisation system
146. Remote biometric identification system

زیست‌سنجی فرد با داده‌های زیست‌سنجی موجود در یک پایگاه دادهٔ مرجع و از راه دور عمل می‌کند.

(۴۲) *سامانهٔ شناسایی زیست‌سنجی از راه دور در زمان واقعی*[۱۴۷] نوعی سامانهٔ شناسایی زیست‌سنجی از راه دور است که در آن گردآوری داده‌های زیست‌سنجی، مقایسه و شناسایی بدون تأخیر قابل‌توجه صورت می‌گیرد. این مفهوم علاوه بر شناسایی آنی، شامل تأخیرهای کوتاه محدودی نیز می‌شود که برای جلوگیری از دورزدن سامانه ضروری است.

(۴۳) *سامانهٔ شناسایی زیست‌سنجی پس از ضبط از راه دور*[۱۴۸] به سامانهٔ شناسایی زیست‌سنجی از راه دوری گفته می‌شود که در زمان واقعی عمل نمی‌کند.

(۴۴) *فضای در دسترس عموم*[۱۴۹] به هر مکان فیزیکی عمومی یا خصوصی اطلاق می‌شود که برای تعداد نامعینی از اشخاص حقیقی قابل دسترسی است، بدون توجه به اینکه ورود به آن مشروط به شرایط خاصی باشد یا محدودیت ظرفیت برای آن اعمال شود.

(۴۵) *مرجع اجرای قانون*[۱۵۰] به معنای:

الف) هر مرجع عمومی دارای صلاحیت برای پیشگیری، تحقیق، کشف یا تعقیب جرایم کیفری یا اجرای مجازات‌های کیفری، ازجمله حفاظت در برابر تهدیدات علیه امنیت عمومی و پیشگیری از آن‌ها؛ یا

ب) هر نهاد یا مرجع دیگری که بر اساس قوانین یک دولت عضو برای اعمال اقتدار و صلاحیت عمومی به منظور پیشگیری، تحقیق، کشف یا تعقیب جرایم کیفری یا اجرای مجازات‌های کیفری، ازجمله حفاظت در برابر تهدیدات علیه امنیت عمومی و پیشگیری از آن‌ها مأمور شده باشد.

(۴۶) *اجرای قانون*[۱۵۱] به معنای فعالیت‌هایی است که از سوی مراجع اجرای قانون یا به نمایندگی از آن‌ها برای پیشگیری، تحقیق، کشف یا تعقیب جرایم کیفری یا اجرای مجازات‌های کیفری، ازجمله حفاظت در برابر تهدیدات علیه امنیت عمومی و پیشگیری از آن‌ها انجام می‌شود.

(۴۷) *دفتر هوش مصنوعی*[۱۵۲] به معنای وظیفهٔ کمیسیون در زمینهٔ مشارکت در اجرا، پایش و نظارت بر سامانه‌های و مدل‌های هوش مصنوعی با کاربرد عام و همچنین حکمرانی هوش مصنوعی است. این وظیفه بر اساس تصمیم کمیسیون مورخ ۲۴ ژانویهٔ ۲۰۲۴ ایجاد شده است. هر جا در این قانون به *دفتر هوش مصنوعی* اشاره شود، مقصود *کمیسیون* است.

(۴۸) *مرجع صلاحیت‌دار ملی*[۱۵۳] به معنای مرجع اعلام‌کننده یا مرجع نظارت بر بازار است. در

147. Real-time remote biometric identification system
148. Post-remote biometric identification system
149. Publicly accessible space
150. Law enforcement authority
151. Law enforcement
152. AI Office
153. National competent authority

خصوص سامانه‌های هوش مصنوعی که از سوی نهادها، آژانس‌ها، دفاتر و ارگان‌های اتحادیه مورد استفاده یا بهره‌برداری قرار می‌گیرند، هر گونه اشاره در این قانون به مراجع صلاحیت‌دار ملی یا مراجع نظارت بر بازار، به منزلهٔ اشاره به *ناظر اروپایی حفاظت از داده‌ها*[۱۵۴] تلقی می‌شود.

(۴۹) *حادثهٔ جدی*[۱۵۵] به معنای بروز رخداد یا نقص عملکرد در یک سامانهٔ هوش مصنوعی است که به‌صورت مستقیم یا غیرمستقیم منجر به یکی از موارد زیر شود:

الف) مرگ شخص یا آسیب جدی به سلامت او؛

ب) اختلال شدید و غیرقابل بازگشت در مدیریت یا عملکرد زیرساخت‌های حیاتی؛

پ) نقض تعهدات مقرر در حقوق اتحادیهٔ اروپا که به منظور حمایت از حقوق بنیادین وضع شده‌اند؛

ت) واردآمدن خسارت جدی به اموال یا محیط‌زیست.

(۵۰) *دادهٔ شخصی*[۱۵۶] به معنای دادهٔ شخصی است مطابق تعریف مندرج در بند (۱) ماده ۴ مقررات شمارهٔ ۲۰۱۶/۶۷۹ (اتحادیهٔ اروپا).

(۵۱) *دادهٔ غیرشخصی*[۱۵۷] به معنای داده‌ای است غیر از دادهٔ شخصی مطابق تعریف بند (۱) ماده ۴ مقررات شمارهٔ ۲۰۱۶/۶۷۹ (اتحادیهٔ اروپا).

(۵۲) *پروفایل‌سازی*[۱۵۸] به معنای پروفایل‌سازی است طبق تعریف مندرج در بند (۴) ماده ۴ مقررات شمارهٔ ۲۰۱۶/۶۷۹ (اتحادیهٔ اروپا).

(۵۳) *طرح آزمون در شرایط واقعی*[۱۵۹] به معنای سندی است که اهداف، روش‌شناسی، دامنهٔ جغرافیایی، جمعیتی و زمانی، نحوهٔ نظارت، سازمان‌دهی و اجرای آزمون در شرایط واقعی را تشریح می‌کند.

(۵۴) *طرح سندباکس*[۱۶۰] به معنای سندی است که میان ارائه‌دهنده، مشارکت‌کننده و مرجع صلاحیت‌دار مورد توافق قرار گرفته و اهداف، شرایط، بازهٔ زمانی، روش‌شناسی و الزامات فعالیت‌های انجام‌شده در چارچوب سندباکس را مشخص می‌کند.

(۵۵) *سندباکس نظارتی هوش مصنوعی*[۱۶۱] به معنای چارچوبی کنترل‌شده است که توسط مرجع صلاحیت‌دار ایجاد می‌شود و این امکان را برای ارائه‌دهندگان بالقوهٔ سامانه‌های هوش مصنوعی فراهم می‌کند تا مطابق طرح سندباکس و تحت نظارت مقرراتی برای مدت زمانی محدود، سامانهٔ هوش مصنوعی نوآورانه‌ای را توسعه، آموزش، اعتبارسنجی و در صورت اقتضا در شرایط واقعی

154. The European Data Protection Supervisor
155. Serious incident
156. personal data
157. Non-personal data
158. Profiling
159. Real-world testing plan
160. Sandbox plan
161. AI regulatory sandbox

آزمایش کنند.

(۵۶) *سواد هوش مصنوعی*[۱۶۲] به معنای مهارت‌ها، دانش و درکی است که به ارائه‌دهندگان، بهره‌برداران و اشخاص ذی‌نفع، با درنظرگرفتن حقوق و تعهدات مربوطه در چارچوب این قانون امکان می‌دهد تا آگاهانه از سامانه‌های هوش مصنوعی استفاده کنند و نسبت به فرصت‌ها، خطرات و آسیب‌های احتمالی ناشی از هوش مصنوعی شناخت پیدا کنند.

(۵۷) *آزمون در شرایط واقعی*[۱۶۳] به معنای آزمون موقتی یک سامانهٔ هوش مصنوعی برای هدف موردنظر آن در شرایط واقعی خارج از محیط آزمایشگاهی یا محیط‌های شبیه‌سازی‌شده با هدف گردآوری داده‌های قابل اعتماد و مستحکم و ارزیابی و راستی‌آزمایی انطباق سامانهٔ هوش مصنوعی با الزامات این قانون است. چنین آزمونی، در صورتی که تمامی شرایط مندرج در مواد ۵۷ یا ۶۰ رعایت شده باشد، به منزلهٔ عرضهٔ سامانهٔ هوش مصنوعی در بازار یا بهره‌برداری از آن در معنای مقرر در این قانون تلقی نمی‌شود.

(۵۸) *موضوع آزمون*[۱۶۴] برای مقاصد آزمون در شرایط واقعی، به شخص حقیقی گفته می‌شود که در فرآیند آزمون در شرایط واقعی شرکت می‌کند.

(۵۹) *رضایت آگاهانه*[۱۶۵] به معنای ابراز تمایل آزادانه، مشخص، صریح و داوطلبانه برای شرکت در آزمون معین در شرایط واقعی است، پس از آنکه تمامی جنبه‌های مرتبط با آن آزمون که برای تصمیم جهت مشارکت اهمیت دارند، به او اطلاع داده شده باشد.

(۶۰) *محتوای ساختگی هوش مصنوعی یا دیپ‌فیک*[۱۶۶] به معنای محتوای تصویری، صوتی یا ویدئویی تولیدشده یا دستکاری‌شده به‌وسیلهٔ هوش مصنوعی است که شباهت زیادی با اشخاص، اشیاء، مکان‌ها، نهادها یا رویدادهای واقعی دارد و ممکن است برای بیننده به‌نادرست، اصیل یا واقعی جلوه کند.

(۶۱) *تخلف گسترده*[۱۶۷] به معنای هر گونه فعل یا ترک فعل مغایر با حقوق اتحادیهٔ اروپا در زمینهٔ حمایت از منافع افراد است که:

الف) به منافع جمعی افراد مقیم دست‌کم دو کشور عضو دیگر، غیر از کشوری که:

(۱) منشأ فعل یا ترک فعل در آن بوده یا رخ داده است؛

(۲) ارائه‌دهندهٔ ذی‌ربط یا حسب مورد، نمایندهٔ مجاز او در آنجا مستقر است؛ یا

(۳) بهره‌بردار در آنجا مستقر است، در صورتی که تخلف از سوی بهره‌بردار ارتکاب یافته باشد، آسیب رسانده یا احتمال آسیب‌رساندن به آن‌ها را داشته باشد؛ یا

162. AI literacy
163. Testing in real-world conditions
164. subject
165. Informed consent
166. Deep fake
167. Widespread infringement

ب) موجب واردآمدن، ایجاد یا احتمال واردآمدن آسیب به منافع جمعی افراد شده و ویژگی‌های مشترکی دارد، ازجمله ارتکاب همان رویهٔ غیرقانونی یا نقض همان منافع، و به‌طور هم‌زمان توسط همان عامل اقتصادی در دست‌کم سه کشور عضو رخ می‌دهد.

(۶۲) *زیرساخت حیاتی*[۱۶۸] به معنای زیرساخت حیاتی طبق تعریف مندرج در بند (۴) ماده ۲، از دستورالعمل شمارهٔ ۲۰۲۲/۲۵۵۷ (اتحادیهٔ اروپا).

(۶۳) *مدل هوش مصنوعی با کاربرد عام*[۱۶۹] به معنای مدلی از هوش مصنوعی است ازجمله در مواردی که چنین مدلی با حجم وسیعی از داده‌ها و از طریق خودنظارتی در مقیاس کلان آموزش داده شده باشد که دارای درجهٔ بالایی از کلیت است و می‌تواند طیف گسترده‌ای از وظایف متمایز را فارغ از نحوهٔ عرضهٔ آن در بازار به‌طور شایسته انجام دهد و قابلیت ادغام در انواع سامانه‌ها یا برنامه‌های فرعی را دارد؛ به‌استثنای مدل‌های هوش مصنوعی که صرفاً برای مقاصد پژوهشی، توسعه‌ای یا نمونه‌سازی پیش از عرضه در بازار به کار می‌روند.

(۶۴) *قابلیت‌های با اثرگذاری بالا*[۱۷۰] به معنای قابلیت‌هایی است که با قابلیت‌های ثبت‌شده در پیشرفته‌ترین مدل‌های هوش مصنوعی با کاربرد عام برابری می‌کند یا از آن فراتر می‌رود.

(۶۵) *خطر نظام‌مند*[۱۷۱] به معنای خطری است که به قابلیت‌های اثرگذاری بالای مدل‌های هوش مصنوعی با کاربرد عام اختصاص دارد و به دلیل گسترهٔ تأثیرگذاری آن‌ها در بازار اتحادیه یا به علت آثار منفی بالفعل یا قابل پیش‌بینی بر سلامت عمومی، ایمنی، امنیت عمومی، حقوق بنیادین یا جامعه به‌طور کلی می‌تواند در مقیاس وسیع در سراسر زنجیرهٔ ارزش گسترش یابد.

(۶۶) *سامانهٔ هوش مصنوعی با کاربرد عام*[۱۷۲] به معنای سامانه‌ای از هوش مصنوعی است که بر پایهٔ یک مدل هوش مصنوعی با کاربرد عام ساخته شده و توانایی دارد برای مقاصد گوناگون مورد استفادهٔ مستقیم قرار گیرد یا در دیگر سامانه‌های هوش مصنوعی ادغام شود.

(۶۷) *عملیات ممیز شناور*[۱۷۳] به معنای هر گونه عملیات یا تخصیص ریاضی مرتبط با اعداد ممیز شناور است؛ اعدادی که زیرمجموعه‌ای از اعداد حقیقی بوده و معمولاً در رایانه‌ها به‌صورت عدد صحیح با دقت ثابت و مقیاس‌یافته بر اساس توان صحیح از پایه‌ای ثابت نمایش داده می‌شوند.

(۶۸) *ارائه‌دهندهٔ پایین‌دستی*[۱۷۴] به معنای ارائه‌دهندهٔ سامانهٔ هوش مصنوعی ازجمله سامانه‌های هوش مصنوعی با کاربرد عام است که در آن یک مدل هوش مصنوعی را ادغام می‌کند، صرف‌نظر

168. Critical infrastructure
169. General-purpose AI model
170. High-impact capabilities
171. Systemic risk
172. General-purpose AI system
173. Floating-point operation
174. Downstream provider

از اینکه آن مدل توسط خود او و به‌صورت عمودی توسعه یافته باشد یا از طریق روابط قراردادی از سوی نهاد دیگری فراهم شده باشد.

ماده ۴. سواد هوش مصنوعی

ارائه‌دهندگان و بهره‌برداران سامانه‌های هوش مصنوعی موظف‌اند در حد توان خود، تدابیری را اتخاذ کنند تا سطح کافی از سواد هوش مصنوعی را در میان کارکنان و سایر افرادی که از سوی آن‌ها در بهره‌برداری و استفاده از سامانه‌های هوش مصنوعی دخیل هستند، تضمین کنند. در این اقدام، باید دانش فنی، تجربه، تحصیلات و آموزش‌های آنان و همچنین زمینه و شرایطی که سامانه‌های هوش مصنوعی در آن استفاده می‌شوند و افراد یا گروه‌های هدفی که سامانه‌های هوش مصنوعی بر آن‌ها اعمال می‌شوند، مدنظر قرار گیرد.

فصل دوم. اعمال ممنوعه مرتبط با هوش مصنوعی

ماده ۵. اعمال ممنوعهٔ هوش مصنوعی

۱. اعمال زیر در زمینهٔ هوش مصنوعی ممنوع است:

الف) عرضه در بازار، به‌کارگیری یا استفاده از هر سامانهٔ هوش مصنوعی که از تکنیک‌های اثرگذاری بر افراد بدون آگاهی آن‌ها[۱۷۵] و فراتر از سطح آگاهی انسان یا از روش‌های عامدانهٔ دستکاری‌کننده یا فریبنده استفاده کند و با هدف یا نتیجهٔ انحراف اساسی در رفتار فرد یا گروهی از افراد از طریق تضعیف محسوس توانایی آنان در اتخاذ تصمیم آگاهانه به نحوی که موجب شود تصمیمی بگیرند که در شرایط عادی اتخاذ نمی‌کردند و این تصمیم موجب واردآمدن آسیب جدی یا به‌طور معقول محتمل به آن شخص، شخص دیگر یا گروهی از اشخاص شود یا احتمالاً چنین آسیبی را به‌دنبال داشته باشد، ممنوع است؛

ب) عرضه در بازار، به‌کارگیری یا استفاده از هر سامانهٔ هوش مصنوعی که از آسیب‌پذیری‌های انسانی فردی یا گروه خاصی از افراد ناشی از سن، ناتوانی (جسمی یا ذهنی) یا وضعیت اجتماعی یا اقتصادی خاص آنان سوءاستفاده کند، با هدف یا نتیجهٔ انحراف اساسی در رفتار آن فرد یا اعضای آن گروه به نحوی که موجب واردآمدن آسیب جدی یا به‌طور معقول محتمل به آن شخص یا شخص دیگر شود، ممنوع است؛

پ) عرضه در بازار، به‌کارگیری یا استفاده از سامانه‌های هوش مصنوعی با هدف ارزیابی یا طبقه‌بندی افراد یا گروه‌هایی از اشخاص در بازهٔ زمانی معین، بر اساس رفتار اجتماعی آنان یا ویژگی‌های

175. Subliminal techniques

شخصی یا شخصیتی شناخته‌شده، استنباط‌شده یا پیش‌بینی‌شده، در صورتی که امتیاز اجتماعی[۱۷۶] حاصل منجر به وقوع یکی یا هر دو مورد زیر شود، ممنوع است؛

۱) رفتار زیان‌بار یا نامطلوب با برخی افراد یا گروه‌هایی از اشخاص در بسترهای اجتماعی که ارتباطی با زمینهٔ اولیهٔ تولید یا گردآوری داده‌ها ندارند؛

۲) رفتار زیان‌بار یا نامطلوب با برخی افراد یا گروه‌هایی از اشخاص که ناموجه یا نامتناسب با رفتار اجتماعی آنان یا میزان اهمیت آن رفتار باشد؛

ت) عرضه در بازار، به‌کارگیری یا استفاده از سامانهٔ هوش مصنوعی با هدف ارزیابی ریسک افراد به منظور پیش‌بینی احتمال ارتکاب جرم توسط یک فرد که صرفاً بر اساس پروفایل‌سازی فرد یا ارزیابی ویژگی‌ها و خصایص شخصیتی او انجام می‌شود، ممنوع است. این ممنوعیت شامل سامانه‌های هوش مصنوعی نمی‌شود که برای حمایت از ارزیابی انسانی دربارهٔ دخالت فرد در فعالیت‌های مجرمانه به کار می‌روند، به شرط آنکه این ارزیابی مبتنی بر حقایق عینی و قابل‌اثبات باشد که به‌طور مستقیم با فعالیت مجرمانه مرتبط هستند.

ث) عرضه، راه‌اندازی یا استفاده از سامانه‌های هوش مصنوعی که بانک‌های اطلاعاتی تشخیص چهره را ایجاد یا گسترش می‌دهند، از طریق جمع‌آوری غیرهدفمند تصاویر چهره از اینترنت یا *دوربین‌های مداربسته*[۱۷۷] ممنوع است.

ج) عرضه، راه‌اندازی یا استفاده از سامانه‌های هوش مصنوعی برای تشخیص احساسات یک فرد در محیط‌های کاری و مؤسسات آموزشی ممنوع است، مگر اینکه استفاده از سامانهٔ هوش مصنوعی برای اهداف پزشکی یا ایمنی باشد.

چ) عرضه، راه‌اندازی یا استفاده از سامانه‌های دسته‌بندی زیست‌سنجی که افراد را بر اساس داده‌های زیست‌سنجی‌شان طبقه‌بندی کرده و نژاد، عقاید سیاسی، عضویت در اتحادیه‌های کارگری، باورهای دینی یا فلسفی، زندگی یا گرایش جنسی آنان را مورد استنباط یا نتیجه‌گیری قرار دهند، ممنوع است. این ممنوعیت شامل برچسب‌گذاری یا فیلترکردن داده‌های زیست‌سنجی به‌صورت قانونی مانند تصاویر، بر اساس داده‌های زیست‌سنجی یا دسته‌بندی داده‌های زیست‌سنجی در حوزهٔ اجرای قانون نمی‌شود.

ح) استفاده از سامانه‌های شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون ممنوع است، مگر در صورتی که استفاده از آن دقیقاً برای یکی از اهداف زیر ضروری باشد:

---

۱۷۶. *امتیاز اجتماعی* (social score) یعنی نتیجهٔ ارزیابی الگوریتمی رفتار یا ویژگی‌های شخصی افراد به منظور رتبه‌بندی یا قضاوت دربارهٔ میزان اعتماد، مطلوبیت یا صلاحیت اجتماعی آنان.

177. CCTV (Closed-Circuit Television)

۱) جستجوی هدفمند برای یافتن قربانیان مشخص آدم‌ربایی، قاچاق انسان یا بهره‌کشی جنسی از انسان‌ها و همچنین جستجو برای افراد مفقودالاثر؛

۲) پیشگیری از تهدیدی مشخص، قابل‌توجه و قریب‌الوقوع نسبت به جان یا سلامت جسمانی افراد یا تهدید واقعی و حاضر یا تهدید واقعی و قابل‌پیش‌بینی وقوع حملهٔ تروریستی؛

۳) محل‌یابی یا شناسایی شخصی که مظنون به ارتکاب جرم است، به منظور انجام تحقیقات کیفری یا تعقیب قضایی یا اجرای مجازات کیفری نسبت به جرایم مندرج در پیوست شمارهٔ ۲ که در دولت عضو مربوطه، مستوجب مجازات حبس یا قرار بازداشت دست‌کم به مدت چهار سال هستند.

بند (ح) خللی در ماده ۹ مقررات ۲۰۱۶/۶۷۹ (اتحادیهٔ اروپا) ایجاد نمی‌کند و به پردازش داده‌های زیست‌سنجی برای اهدافی غیر از اجرای قانون مرتبط نیست.

۲. استفاده از سامانه‌های شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون، برای هر یک از اهداف ذکرشده در بند ۱، پاراگراف اول، قسمت (ح)، تنها باید به منظور تأیید هویت فرد مشخص هدف‌گیری‌شده به کار گرفته شود و در این استفاده باید عناصر زیر مدنظر قرار گیرد:

الف) ماهیت وضعیتی که ممکن است استفاده از سامانه را ایجاب کند، به‌ویژه شدت، احتمال و وسعت آسیبی که در صورت عدم استفاده از سامانه رخ می‌دهد؛

ب) پیامدهای استفاده از سامانه برای حقوق و آزادی‌های تمام افراد ذی‌ربط، به‌ویژه شدت، احتمال و گسترهٔ این پیامدها.

علاوه بر این، استفاده از سامانه‌های شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون، برای هر یک از اهداف ذکرشده در بند ۱، پاراگراف اول، قسمت (ح)، باید با رعایت تضمین‌ها و شرایط لازم و متناسب با قوانین ملی مجاز به استفاده از سامانه به‌ویژه در زمینهٔ محدودیت‌های زمانی، جغرافیایی و شخصی انجام شود. استفاده از این سامانه‌ها تنها در صورتی مجاز است که مرجع اجرای قانون، ارزیابی تأثیر بر حقوق بنیادین را طبق ماده ۲۷ انجام داده و سامانه را مطابق ماده ۴۹ در پایگاه دادهٔ اتحادیهٔ اروپا ثبت کرده باشد. با این حال، در موارد اضطراری با دلایل موجه، استفاده از چنین سامانه‌هایی می‌تواند قبل از ثبت در پایگاه دادهٔ اتحادیهٔ اروپا آغاز شود، به شرط آنکه ثبت سامانه بدون تأخیر غیرموجه تکمیل شود.

۳. برای اهداف بند ۱، پاراگراف اول، قسمت (ح) و بند ۲، هر استفاده از سامانهٔ شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون، منوط به دریافت مجوز قبلی از مرجع قضایی یا مرجع اداری مستقل است که تصمیم آن برای دولت عضو مربوطه الزام‌آور باشد. این مجوز باید بر اساس درخواست موجه و مطابق جزئیات قوانین ملیِ ذکرشده در بند ۵

صادر شود. با این حال، در موارد اضطراری با دلایل موجه، استفاده از این سامانه می‌تواند قبل از دریافت مجوز آغاز شود، به شرط آنکه درخواست مجوز بدون تأخیر غیرموجه، حداکثر ظرف ۲۴ ساعت ارائه شود. در صورتی که چنین مجوزی رد شود، استفاده از سامانه فوراً متوقف شده و تمام داده‌ها، نتایج و خروجی‌های حاصل از آن استفاده باید بلافاصله دور ریخته و حذف شوند.

مرجع قضایی ذی‌صلاح یا مرجع اداری مستقل که تصمیم آن الزام‌آور است، تنها زمانی مجوز را صادر می‌کند که بر اساس شواهد عینی یا دلایل روشن ارائه‌شده، مطمئن شود که استفاده از سامانهٔ شناسایی زیست‌سنجی از راه دور در *زمان واقعی*، برای دستیابی به یکی از اهداف مشخص‌شده در بند ۱، پاراگراف اول، قسمت (ح) ضروری و متناسب است، همان گونه که در درخواست مشخص شده است و به‌ویژه محدود به حداقل نیازهای دقیق از نظر مدت زمان، محدودهٔ جغرافیایی و افراد مشمول باشد.

در تصمیم‌گیری دربارهٔ درخواست، آن مرجع باید عناصری را که در بند ۲ اشاره شده است در نظر گیرد. همچنین هیچ تصمیمی که اثر حقوقی منفی بر شخص داشته باشد، نباید تنها بر اساس خروجی سامانهٔ شناسایی زیست‌سنجی از راه دور در *زمان واقعی* اتخاذ شود.

۴. بدون خدشه به بند ۳، هر استفاده از سامانهٔ شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون، باید به مرجع نظارت بر بازار مربوطه و مرجع ملی حفاظت از داده‌ها مطابق قوانین ملی ذکرشده در بند ۵ اعلام شود. این اطلاع‌رسانی حداقل باید شامل اطلاعات مشخص‌شده در بند ۶ باشد و شامل داده‌های عملیاتی حساس نباشد.

۵. دولت عضو می‌تواند امکان صدور مجوز کامل یا جزئی برای استفاده از سامانه‌های شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون را در چارچوب محدودیت‌ها و شرایط ذکرشده در بند ۱، پاراگراف اول، قسمت (ح) و بندهای ۲ و ۳ پیش‌بینی کند. دولت‌های عضو مربوطه باید در قوانین ملی خود، قواعد جزئی و لازم برای درخواست، صدور، اعمال، نظارت و گزارش‌دهی مربوط به مجوزهای مذکور در بند ۳ را تعیین کنند. همچنین این قواعد باید مشخص کنند که برای کدام‌یک از اهداف ذکرشده در بند ۱، پاراگراف اول، قسمت (ح) ازجمله کدام‌یک از جرایم مندرج در تبصره‌های قسمت (ح) هستند. مقامات ذی‌صلاح می‌توانند از این سامانه‌ها برای اهداف اجرایی قانون استفاده کنند. دولت‌های عضو باید این قواعد را حداکثر ظرف ۳۰ روز پس از تصویب به کمیسیون اطلاع دهند. همچنین دولت‌های عضو می‌توانند مطابق قوانین اتحادیهٔ اروپا، قوانین محدودکننده‌تری برای استفاده از سامانه‌های شناسایی زیست‌سنجی از راه دور تصویب کنند.

۶. مراجع ملی نظارت بر بازار و حفاظت از داده‌ها در دولت‌های عضوی که اطلاع‌رسانی دربارهٔ استفاده از سامانه‌های شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون مطابق بند ۴ به آن‌ها ارائه شده است، باید گزارش سالانه‌ای از نحوهٔ استفاده به

کمیسیون ارائه کنند. برای این منظور، کمیسیون یک قالب گزارش‌دهی در اختیار دولت‌های عضو و مراجع ملی نظارت بر بازار و حفاظت از داده‌ها قرار می‌دهد که شامل اطلاعاتی دربارهٔ تعداد تصمیمات مراجع قضایی ذی‌صلاح یا مراجع اداری مستقل که تصمیم آن‌ها الزام‌آور است، نسبت به درخواست‌های مجوز طبق بند ۳ و نتایج آن‌ها باشد.

۷. بر اساس داده‌های تجمیعی در دولت‌های عضو که در گزارش‌های سالانهٔ مذکور در بند ۶ ارائه شده است، کمیسیون گزارش‌های سالانه دربارهٔ استفاده از سامانه‌های شناسایی زیست‌سنجی از راه دور در *زمان واقعی* در فضاهای عمومی برای اهداف اجرایی قانون منتشر خواهد کرد. این گزارش‌های سالانه شامل داده‌های عملیاتی حساس مربوط به فعالیت‌های اجرایی قانون نخواهد بود.

۸. این ماده، بر ممنوعیت‌هایی که در صورت نقض دیگر قوانین اتحادیهٔ اروپا توسط فعل یک هوش مصنوعی اعمال می‌شوند، تأثیری ندارد.

فصل سوم. سامانه‌های هوش مصنوعی پرخطر

بخش نخست. طبقه‌بندی سامانه‌های هوش مصنوعی به‌عنوان پرخطر

ماده ۶. قواعد طبقه‌بندی سامانه‌های هوش مصنوعی پرخطر

۱. صرف‌نظر از اینکه سامانهٔ هوش مصنوعی به‌طور مستقل یا همراه با محصولات مذکور در بندهای (الف) و (ب) در بازار عرضه شود یا مورد استفاده قرار گیرد، در صورتی که هر دو شرط زیر محقق باشند، آن سامانه به‌عنوان سامانهٔ هوش مصنوعی پرخطر تلقی می‌شود:

الف) سامانهٔ هوش مصنوعی برای استفاده به‌عنوان یک جزء ایمنی از یک محصول طراحی شده باشد، یا خودِ سامانهٔ هوش مصنوعی محصولی باشد که مشمول قوانین هماهنگ‌شدهٔ اتحادیه مندرج در پیوست یک در نظر گرفته شود؛

ب) محصولی که جزء ایمنی آن مطابق بند (الف) سامانهٔ هوش مصنوعی است، یا خودِ سامانهٔ هوش مصنوعی به‌عنوان محصول باید مورد ارزیابی انطباق توسط شخص ثالث قرار گیرد تا اجازهٔ عرضه در بازار یا بهره‌برداری از آن محصول مطابق قوانین هماهنگ‌شدهٔ اتحادیه مندرج در پیوست یک صادر شود.

۲. علاوه بر سامانه‌های هوش مصنوعی پرخطری که در بند (۱) به آن‌ها اشاره شد، سامانه‌های هوش مصنوعی مذکور در پیوست سه نیز پرخطر محسوب می‌شوند.

۳. به موجب استثنایی بر بند (۲)، سامانهٔ هوش مصنوعی مذکور در پیوست سه در صورتی پرخطر تلقی نمی‌شود که خطر قابل‌توجهی از حیث آسیب به سلامت، ایمنی یا حقوق بنیادین اشخاص حقیقی

ایجاد نکند، ازجمله در مواردی که تأثیر مادی و معناداری بر نتیجهٔ فرآیند تصمیم‌گیری نداشته باشد.

حکم بند نخست در صورتی اعمال می‌شود که هر یک از شرایط زیر محقق شود:

الف) سامانهٔ هوش مصنوعی برای انجام وظیفهٔ رویه‌ای محدود طراحی شده باشد؛

ب) سامانهٔ هوش مصنوعی با هدف بهبود نتیجهٔ فعالیت انسانیِ پیش‌تر انجام‌شده مورد استفاده قرار گیرد؛

پ) سامانهٔ هوش مصنوعی برای شناسایی الگوهای تصمیم‌گیری یا انحراف از الگوهای تصمیم‌گیری پیشین طراحی شده باشد و هدف از آن جایگزینی یا تأثیرگذاری بر ارزیابی انسانی پیش‌تر انجام‌شده نباشد، مگر با انجام بازبینی انسانی مناسب؛

ت) سامانهٔ هوش مصنوعی برای انجام وظیفه‌ای مقدماتی در راستای ارزیابی مرتبط با موارد کاربرد مندرج در پیوست سه طراحی شده باشد.

با وجود حکم بند نخست، هر سامانهٔ هوش مصنوعی مذکور در پیوست سه که اقدام به تهیهٔ پروفایل (پروفایل‌سازی) از اشخاص حقیقی کند، همواره پرخطر تلقی خواهد شد.

۴. هر ارائه‌دهنده‌ای که تشخیص دهد یکی از سامانه‌های هوش مصنوعی مذکور در پیوست سه پرخطر نیست، باید پیش از عرضهٔ آن سامانه در بازار یا بهره‌برداری از آن، ارزیابی خود را مستند کند. چنین ارائه‌دهنده‌ای مشمول الزام ثبت مندرج در بند (۲) ماده ۴۹ خواهد بود و در صورت درخواست مراجع صلاحیت‌دار ملی، موظف است مستندات ارزیابی انجام‌شده را در اختیار آن مراجع قرار دهد.

۵. کمیسیون اروپا موظف است پس از مشورت با هیئت اروپایی هوش مصنوعی (هیئت) و حداکثر تا ۲ فوریهٔ ۲۰۲۶، دستورالعمل‌هایی برای تبیین اجرای عملی این ماده مطابق ماده ۹۶ صادر کند. این دستورالعمل‌ها باید شامل فهرستی جامع از نمونه‌های عملی موارد کاربرد سامانه‌های هوش مصنوعی پرخطر و غیرپرخطر نیز باشد.

۶. کمیسیون اروپا اختیار دارد مطابق ماده ۹۷، در صورت وجود دلایل مشخص و قابل اعتماد مبنی بر وجود سامانه‌های هوش مصنوعی مشمول پیوست سه که با این حال، خطر قابل‌توجهی برای سلامت، ایمنی یا حقوق بنیادین اشخاص حقیقی ایجاد نمی‌کنند، این اقدامات را اتخاذ کند تا قسمت دوم از بند (۳) این ماده را از طریق افزودن شرایط جدید به شرایط موجود یا اصلاح آن‌ها تغییر دهد.

۷. کمیسیون اروپا موظف است مطابق ماده ۹۷، در صورت وجود دلایل مشخص و قابل اعتماد، مبنی بر ضرورت اقدامات تفویضی برای حفظ سطح حفاظت از سلامت، ایمنی و حقوق بنیادینِ پیش‌بینی‌شده در این قانون، این اقدامات را اتخاذ کند تا قسمت دوم از بند (۳) این ماده را از طریق حذف هر یک از شرایط مندرج در آن اصلاح کند.

۸. هر گونه تغییر در شرایط مندرج در قسمت دوم از بند (۳) که مطابق بندهای (۶) و (۷) این ماده اتخاذ شود، نباید سطح کلی حفاظت از سلامت، ایمنی و حقوق بنیادین پیش‌بینی‌شده در این قانون را کاهش دهد و باید با اقدامات تفویضی صادرشده مطابق ماده ۷(۱) همخوانی داشته باشد و تحولات بازار و فناوری را نیز مدنظر قرار دهد.

ماده ۷. اصلاحات پیوست سه

۱. کمیسیون مجاز است بر اساس ماده ۹۷، اعمال تفویض‌شده‌ای را برای اصلاح پیوست شمارهٔ ۳ تصویب کند، به نحوی که موارد استفاده از سامانه‌های هوش مصنوعی پرخطر را اضافه یا اصلاح کند، مشروط بر آنکه هر دو شرط زیر محقق شده باشند:

الف) سامانه‌های هوش مصنوعی موردنظر، برای استفاده در یکی از حوزه‌های مندرج در پیوست شمارهٔ ۳ طراحی شده باشند؛

ب) سامانه‌های هوش مصنوعی، متضمن خطر آسیب به سلامت و ایمنی یا اثر نامطلوب بر حقوق بنیادین باشند و این خطر از حیث شدت یا ماهیت معادل یا بیشتر از خطر آسیب یا اثر نامطلوب ناشی از سامانه‌های هوش مصنوعی پرخطر باشد که پیش‌تر در پیوست شمارهٔ ۳ ذکر شده‌اند.

۲. در هنگام ارزیابی شرط مندرج در جزء (ب) بند ۱، کمیسیون باید به معیارهای زیر توجه کند:

الف) هدف موردنظر از به‌کارگیری سامانهٔ هوش مصنوعی؛

ب) میزان به‌کارگیری یا احتمال به‌کارگیری سامانهٔ هوش مصنوعی؛

پ) ماهیت و حجم داده‌هایی که توسط سامانهٔ هوش مصنوعی پردازش و استفاده می‌شوند به‌ویژه در مواردی که داده‌های شخصیِ حساس پردازش می‌شوند؛

ت) میزان خودمختاری سامانهٔ هوش مصنوعی و امکان مداخلهٔ انسان برای لغو تصمیم‌ها یا توصیه‌هایی که ممکن است منجر به آسیب احتمالی شوند؛

ث) گستره‌ای که در آن، استفاده از سامانهٔ هوش مصنوعی پیش‌تر موجب آسیب به سلامت و ایمنی شده، اثر نامطلوبی بر حقوق بنیادین داشته یا نگرانی‌های قابل‌توجهی در خصوص احتمال بروز چنین آسیب یا اثر نامطلوبی ایجاد کرده است؛ امری که می‌تواند برای نمونه از طریق گزارش‌ها یا شکایات مستند ارائه‌شده به مقامات صلاحیت‌دار ملی یا سایر گزارش‌ها حسب مورد، احراز شود؛

ج) دامنهٔ بالقوهٔ این آسیب یا اثر نامطلوب به‌ویژه از حیث شدت آن و توانایی تأثیرگذاری بر افراد متعدد یا تأثیر نامتناسب بر گروه خاصی از اشخاص؛

چ) میزان وابستگی اشخاصی که ممکن است دچار آسیب یا اثر نامطلوب شوند به نتیجه‌ای که توسط سامانهٔ هوش مصنوعی تولید می‌شود، به‌ویژه در مواردی که به دلایل عملی یا حقوقی، امکان

معقولِ خودداری از پذیرش آن نتیجه وجود ندارد؛

ح) میزان نابرابری قدرت یا موقعیت آسیب‌پذیری اشخاصی که ممکن است دچار آسیب یا اثر نامطلوب شوند در مقایسه با بهره‌بردار سامانهٔ هوش مصنوعی به‌ویژه با توجه به جایگاه، اقتدار، دانش، وضعیت اقتصادی یا اجتماعی یا سن آنان؛

خ) میزان قابلیت اصلاح یا بازگشت‌پذیری نتیجه‌ای که با دخالت سامانهٔ هوش مصنوعی حاصل شده است، با درنظرگرفتن راه‌حل‌های فنی موجود برای اصلاح یا بازگرداندن آن؛ با این توضیح که نتایجی که اثر نامطلوبی بر سلامت، ایمنی یا حقوق بنیادین دارند، نباید به‌عنوان نتایجِ به‌آسانی قابل اصلاح یا بازگشت‌پذیر تلقی شوند؛

د) اندازه و احتمال منافع ناشی از به‌کارگیری سامانهٔ هوش مصنوعی برای افراد، گروه‌ها یا جامعه به‌طور کلی، ازجمله بهبودهای احتمالی در ایمنی محصولات؛

ذ) میزان پیش‌بینی مقررات موجود در حقوق اتحادیه (اتحادیهٔ اروپا) برای موارد زیر؛

۱) تدابیر مؤثر جبرانی در ارتباط با مخاطرات ناشی از سامانهٔ هوش مصنوعی به استثنای دعاوی مربوط به خسارت؛

۲) تدابیر مؤثر برای پیشگیری یا کاهش اساسی آن مخاطرات.

۳) کمیسیون مجاز است بر اساس ماده ۹۷، اعمال تفویض‌شده‌ای را برای اصلاح پیوست شمارهٔ ۳ تصویب کند، به نحوی که موارد استفاده از سامانه‌های هوش مصنوعی پرخطر را اضافه یا اصلاح کند، مشروط بر آنکه هر دو شرط زیر محقق شده باشند:

الف) سامانهٔ هوش مصنوعی پرخطر موردنظر، دیگر هیچ خطر قابل‌توجهی برای حقوق بنیادین، سلامت یا ایمنی ایجاد نکند، با درنظرگرفتن معیارهای مندرج در بند ۲؛

ب) حذف آن، سطح کلی حفاظت از سلامت، ایمنی و حقوق بنیادین تحت قوانین اتحادیه را کاهش ندهد.

بخش دوم. الزامات سامانه‌های هوش مصنوعی پرخطر

ماده ۸. رعایت الزامات

۱. سامانه‌های هوش مصنوعی پرخطر باید با الزامات مندرج در این بخش مطابقت داشته باشند به گونه‌ای که هدف موردنظر از به‌کارگیری آن‌ها و وضعیت شناخته‌شده و متعارف فناوری‌های هوش مصنوعی و فناوری‌های مرتبط با آن در نظر گرفته شود. در اطمینان از رعایت این الزامات، سیستم مدیریت ریسک مندرج در ماده ۹ نیز باید مورد توجه قرار گیرد.

۲. هر گاه محصول حاوی سامانهٔ هوش مصنوعی باشد که مشمول الزامات این قانون و همچنین

الزامات قوانین هماهنگ‌شدهٔ اتحادیه مندرج در بخش (الف) پیوست شمارهٔ ۱ می‌شود، تأمین‌کنندگان مسئول اطمینان از این هستند که محصول آن‌ها به‌طور کامل با تمامی الزامات قابل اعمال تحت قوانین هماهنگ‌شدهٔ اتحادیه مطابقت دارد. برای اطمینان از رعایت الزامات این بخش توسط سامانه‌های هوش مصنوعی پرخطر مندرج در بند ۱ و به منظور تضمین انسجام، جلوگیری از تکرار و کاهش بار اضافی، تأمین‌کنندگان می‌توانند در صورت لزوم، فرآیندهای آزمون و گزارش‌دهی، اطلاعات و مستندات لازم مربوط به محصول خود را با مستندات و رویه‌های موجود و الزامی تحت قوانین هماهنگ‌شدهٔ اتحادیه مندرج در بخش (الف) پیوست شمارهٔ ۱ ادغام کنند.

ماده ۹. سیستم مدیریت ریسک

۱. باید سیستم مدیریت ریسک در ارتباط با سامانه‌های هوش مصنوعی پرخطر ایجاد، اجرا، مستندسازی و نگهداری شود.

۲. سیستم مدیریت ریسک باید به‌عنوان فرآیند تکراری و مستمر درک شود که در طول کل چرخهٔ عمر سامانهٔ هوش مصنوعی پرخطر برنامه‌ریزی و اجرا می‌شود و نیازمند بازبینی و به‌روزرسانی منظم و نظام‌مند است. این سیستم باید شامل مراحل زیر باشد:

الف) شناسایی و تحلیل خطرات شناخته‌شده و به‌طور معقول قابل پیش‌بینی که ممکن است سامانهٔ هوش مصنوعی پرخطر، هنگام استفاده مطابق هدف موردنظر برای سلامت، ایمنی یا حقوق بنیادین ایجاد کند؛

ب) برآورد و ارزیابی خطراتی که ممکن است هنگام استفاده از سامانهٔ هوش مصنوعی پرخطر مطابق هدف موردنظر و تحت شرایط سوءاستفادهٔ معقول قابل پیش‌بینی بروز کنند؛

پ) ارزیابی سایر خطرات احتمالی بر اساس تحلیل داده‌های جمع‌آوری‌شده از سیستم پایش پس از عرضه به بازار مندرج در ماده ۷۲؛

ت) اتخاذ تدابیر مدیریت ریسک مناسب و هدفمند، طراحی‌شده برای رسیدگی به خطراتی که مطابق بند (الف) شناسایی شده‌اند.

۳. خطرات مندرج در این ماده، تنها باید شامل آن دسته از خطراتی باشد که به‌طور معقول از طریق توسعه یا طراحی سامانهٔ هوش مصنوعی پرخطر یا ارائهٔ اطلاعات فنی کافی قابل کاهش یا رفع باشند.

۴. تدابیر مدیریت ریسک مندرج در بند ۲، جزء (ت) باید اثرات و تعاملات احتمالی ناشی از اعمال ترکیبی الزامات مندرج در این بخش را به‌طور شایسته در نظر گیرد به گونه‌ای که خطرات به‌طور مؤثرتر کاهش یابند و در عین حال، تعادل مناسب در اجرای تدابیر برای رعایت آن الزامات حفظ شود.

۵. تدابیر مدیریت ریسک مندرج در بند ۲، جزء (ت) باید به گونه‌ای باشند که خطر باقی‌ماندهٔ مرتبط با هر مخاطره و همچنین خطر باقی‌ماندهٔ کلی سامانه‌های هوش مصنوعی پرخطر، قابل قبول ارزیابی شوند.

در شناسایی مناسب‌ترین تدابیر مدیریت ریسک، باید موارد زیر تضمین شوند:

الف) حذف یا کاهش خطرات شناسایی‌شده و ارزیابی‌شده مطابق بند ۲ تا جایی که از نظر فنی امکان‌پذیر باشد از طریق طراحی و توسعهٔ مناسب سامانهٔ هوش مصنوعی پرخطر؛

ب) در صورت لزوم، اجرای تدابیر کاهش و کنترل مناسب برای خطراتی که قابل حذف نیستند؛

پ) ارائهٔ اطلاعات مورد نیاز مطابق ماده ۱۳ و در صورت لزوم، آموزش به بهره‌برداران.

به منظور حذف یا کاهش خطرات مرتبط با استفاده از سامانهٔ هوش مصنوعی پرخطر، باید توجه شایسته‌ای به دانش فنی، تجربه، تحصیلات، آموزش مورد انتظار بهره‌بردار و زمینهٔ محتمل استفاده از سامانه صورت گیرد.

۶. سامانه‌های هوش مصنوعی پرخطر باید برای شناسایی مناسب‌ترین و هدفمندترین تدابیر مدیریت ریسک مورد آزمایش قرار گیرند. آزمایش باید اطمینان دهد که سامانه‌های هوش مصنوعی پرخطر، مطابق هدف موردنظر عمل می‌کنند و با الزامات مندرج در این بخش مطابقت دارند.

۷. روش‌های آزمایش می‌تواند شامل آزمایش در شرایط واقعی مطابق ماده ۶۰ باشد.

۸. آزمایش سامانه‌های هوش مصنوعی پرخطر باید در صورت لزوم در هر مرحله از فرآیند توسعه انجام شود و در هر حال، پیش از عرضه به بازار یا بهره‌برداری از آن انجام گیرد. آزمایش باید بر اساس معیارها و آستانه‌های احتمالاتی از پیش تعریف‌شده انجام شود که با هدف موردنظر سامانهٔ هوش مصنوعی پرخطر متناسب باشند.

۹. هنگام اجرای سیستم مدیریت ریسک مندرج در بندهای ۱ تا ۷، تأمین‌کنندگان باید در نظر داشته باشند که آیا با توجه به هدف موردنظر، ممکن است سامانهٔ هوش مصنوعی پرخطر، اثر نامطلوبی بر افراد زیر ۱۸ سال و احتمالاً سایر گروه‌های آسیب‌پذیر داشته باشد.

۱۰. برای تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر که مشمول الزامات مربوط به فرآیندهای مدیریت ریسک داخلی تحت سایر مقررات مرتبط اتحادیه هستند، جنبه‌های مندرج در بندهای ۱ تا ۹ می‌تواند بخشی از رویه‌های مدیریت ریسک برقرارشده طبق آن مقررات باشد یا با آن ترکیب شود.

ماده ۱۰. داده‌ها و حاکمیت داده‌ها

۱. سامانه‌های هوش مصنوعی پرخطر که از تکنیک‌هایی استفاده می‌کنند که شامل آموزش

مدل‌های هوش مصنوعی با داده‌ها است، باید بر اساس مجموعهٔ داده‌های آموزش، اعتبارسنجی و آزمون توسعه یابند که هنگام استفاده از چنین مجموعهٔ داده‌هایی، معیارهای کیفیت مندرج در بندهای ۲ تا ۵ را رعایت کنند.

۲. مجموعهٔ داده‌های آموزش، اعتبارسنجی و آزمون باید مشمول رویه‌های حاکمیت و مدیریت داده باشند که با هدف موردنظر سامانهٔ هوش مصنوعی با ریسک بالا سازگار باشد. این رویه‌ها به‌ویژه باید شامل موارد زیر باشند:

الف) انتخاب‌های طراحی مرتبط؛

ب) فرآیندهای جمع‌آوری داده و منبع آن‌ها و در خصوص داده‌های شخصی، هدف اصلی جمع‌آوری داده‌ها؛

پ) عملیات مرتبط با آماده‌سازی داده‌ها مانند حاشیه‌نویسی، برچسب‌گذاری، پاک‌سازی، به‌روزرسانی، غنی‌سازی و تجمیع؛

ت) تدوین فرضیات به‌ویژه در ارتباط با اطلاعاتی که داده‌ها قرار است اندازه‌گیری و نمایش دهند؛

ث) ارزیابی در دسترس‌بودن، حجم و تناسب مجموعهٔ داده‌های مورد نیاز؛

ج) بررسی با توجه به احتمال سوگیری‌هایی که ممکن است بر سلامت و ایمنی افراد تأثیر بگذارند و اثر منفی بر حقوق بنیادین داشته باشند یا منجر به تبعیض ممنوعه تحت قوانین اتحادیه شوند به‌ویژه در مواردی که خروجی‌های داده بر ورودی‌های عملیات آینده تأثیرگذارند؛

چ) تدابیر مناسب برای شناسایی، پیشگیری و کاهش سوگیری‌های احتمالی که مطابق بند (ف) شناسایی شده‌اند؛

ح) شناسایی شکاف‌ها یا کاستی‌های مرتبط داده که مانع از رعایت این قانون می‌شوند و چگونگی رفع آن شکاف‌ها و کاستی‌ها.

۳. مجموعهٔ داده‌های آموزش، اعتبارسنجی و آزمون باید مرتبط و تا حد امکان، عاری از خطا و با توجه به هدف موردنظر باشند. این داده‌ها باید دارای ویژگی‌های آماری مناسب باشند، ازجمله در صورت لزوم با توجه به اشخاص یا گروه‌های افرادی که سامانهٔ هوش مصنوعی پرخطر قرار است برای آن‌ها استفاده شود. این ویژگی‌ها می‌توانند در سطح هر مجموعهٔ داده به‌طور مجزا یا در سطح ترکیب آن‌ها محقق شوند.

۴. مجموعهٔ داده‌ها باید تا حدی که با هدف موردنظر سازگار است، ویژگی‌ها یا عناصر خاص مرتبط با محیط جغرافیایی، زمینه‌ای، رفتاری یا عملکردی خاصی را که سامانهٔ هوش مصنوعی پرخطر قرار است در آن استفاده شود، در نظر بگیرند.

۵. تا حدی که به‌طور ضروری برای اطمینان از شناسایی و اصلاح سوگیری‌ها در سامانه‌های

هوش مصنوعی پرخطر مطابق بند (۲)، جزءهای (ف) و (چ) این ماده باشد، تأمین‌کنندگان چنین سامانه‌هایی می‌توانند استثنائاً داده‌های شخصی حساس را پردازش کنند، مشروط بر اتخاذ تدابیر حفاظتی مناسب برای حقوق و آزادی‌های بنیادین اشخاص حقیقی. علاوه بر قواعد مندرج در مقررات شمارهٔ ۶۷۹ /۲۰۱۶ و ۱۷۲۵ /۲۰۱۸ و دستورالعمل ۶۸۰ /۲۰۱۶، تمامی شرایط زیر باید برای انجام چنین پردازشی محقق شوند:

الف) شناسایی و اصلاح سوگیری‌ها به گونه‌ای مؤثر از طریق پردازش داده‌های دیگر ازجمله داده‌های مصنوعی یا ناشناس‌شده، ممکن نباشد؛

ب) دسته‌های خاص داده‌های شخصی مشمول محدودیت‌های فنی در خصوص استفادهٔ مجدد از داده‌های شخصی بوده و با استفاده از تدابیر امنیتی و حفظ حریم خصوصی مبتنی بر جدیدترین فناوری‌ها ازجمله *مستعارسازی*[۱۷۸] محافظت شوند؛

پ) دسته‌های خاص داده‌های شخصی تحت تدابیری قرار گیرند که امنیت و حفاظت داده‌های پردازش‌شده را تضمین کرده و متضمن سازوکارهای حفاظتی مناسب ازجمله کنترل‌های سختگیرانه و مستندسازی دسترسی‌ها باشند تا از هر گونه سوءاستفاده جلوگیری شود و صرفاً اشخاص مجاز با تعهدات محرمانگی مناسب به آن داده‌ها دسترسی داشته باشند؛

ت) دسته‌های خاص داده‌های شخصی به هیچ وجه به اشخاص ثالث منتقل، ارسال یا توسط آن‌ها مورد دسترسی قرار نگیرند؛

ث) دسته‌های خاص داده‌های شخصی پس از اصلاح سوگیری یا در پایان دورهٔ نگهداری داده‌ها، هرکدام که زودتر واقع شود، حذف شوند؛

ج) سوابق فعالیت‌های پردازشی مطابق مقررات شمارهٔ ۶۷۹ /۲۰۱۶ و ۲۰۱۸/۱۷۲۵ و دستورالعمل ۲۰۱۶/۶۸۰ باید شامل دلایلی باشد که نشان دهد پردازش دسته‌های خاص داده‌های شخصی برای شناسایی و اصلاح سوگیری‌ها به‌طور کاملاً ضروری بوده و هدف موردنظر از طریق پردازش داده‌های دیگر قابل تحقق نبوده است.

۶. در مورد توسعهٔ سامانه‌های هوش مصنوعی پرخطر که از روش‌های مبتنی بر آموزش مدل‌های هوش مصنوعی استفاده نمی‌کنند، مفاد بندهای ۲ تا ۵ صرفاً در خصوص *مجموعه‌داده‌های مورد آزمون*[۱۷۹] اعمال می‌شود.

ماده ۱۱. مستندات فنی

۱. مستندات فنی مربوط به سامانهٔ هوش مصنوعی پرخطر باید پیش از عرضهٔ آن به بازار یا

178. pseudonymisation
179. Testing data sets

به‌کارگیری تهیه و همواره به‌روز نگه داشته شود.

مستندات فنی باید به نحوی تنظیم شود که انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در این بخش را اثبات کند و اطلاعات لازم را به‌صورت روشن و جامع در اختیار مقامات صلاحیت‌دار ملی و نهادهای اعلام‌شده قرار دهد تا بتوانند میزان انطباق سامانه با الزامات مذکور را ارزیابی کنند. این مستندات باید حداقل شامل عناصر مندرج در پیوست چهارم باشد. شرکت‌های کوچک و متوسط ازجمله شرکت‌های نوپا می‌توانند عناصر مستندات فنی مقرر در پیوست چهارم را به‌صورت ساده‌شده ارائه دهند. به همین منظور، کمیسیون فرم ساده‌شده‌ای برای مستندات فنی متناسب با نیازهای بنگاه‌های کوچک و خرد تهیه خواهد کرد. در صورتی که شرکت کوچک یا نوپا انتخاب کند که اطلاعات مورد نیاز در پیوست چهارم را به‌صورت ساده‌شده ارائه دهد، باید از فرم مذکور در این بند استفاده کند و نهادهای اعلام‌شده موظف‌اند این فرم را برای مقاصد ارزیابی انطباق بپذیرند.

۲. در مواردی که سامانهٔ هوش مصنوعی پرخطر، مرتبط با محصولی باشد که مشمول قوانین هماهنگ‌شدهٔ اتحادیه مندرج در بخش (الف) پیوست یک است و آن محصول در بازار عرضه شود یا مورد بهره‌برداری قرار گیرد، باید یک مجموعهٔ واحد از مستندات فنی تهیه شود که شامل تمام اطلاعات مذکور در بند (۱) این ماده، به‌علاوه اطلاعات مورد نیاز در قوانین مذکور باشد.

۳. کمیسیون مجاز است طبق ماده ۹۷ اقدامات تفویضی اتخاذ کند تا در صورت لزوم، پیوست چهارم را اصلاح کند به گونه‌ای که با توجه به پیشرفت‌های فنی، مستندات فنی شامل تمامی اطلاعات لازم برای ارزیابی میزان انطباق سامانه با الزامات مقرر در این بخش باشد.

ماده ۱۲. نگهداری سوابق

۱. سامانه‌های هوش مصنوعی پرخطر باید از لحاظ فنی به گونه‌ای طراحی شوند که امکان ثبت خودکار رویدادها (گزارش‌ها یا لاگ‌ها) را در طول دورهٔ عمر سامانه فراهم کنند.

۲. به منظور تضمین سطحی از قابلیت رهگیری عملکرد سامانهٔ هوش مصنوعی پرخطر که متناسب با هدف موردنظر از کاربرد آن باشد، قابلیت‌های ثبت رویداد باید امکان ضبط رویدادهای مرتبط را برای موارد زیر فراهم کنند:

الف) شناسایی موقعیت‌هایی که ممکن است منجر به ایجاد خطری از نوع مندرج در بند (۱) ماده ۷۹ یا منجر به اصلاح اساسی سامانه شوند؛

ب) تسهیل نظارت پس از عرضه در بازار مطابق ماده ۷۲؛ و

پ) پایش عملکرد سامانه‌های هوش مصنوعی پرخطر موضوع بند (۵) ماده ۲۶.

۳. در خصوص سامانه‌های هوش مصنوعی پرخطری که در قسمت (الف) بند (۱) پیوست شمارهٔ

۳ ذکر شده‌اند، قابلیت‌های ثبت رویداد باید حداقل شامل موارد زیر باشند:

الف) ثبت مدت زمان هر بار استفاده از سامانه (شامل تاریخ و ساعت آغاز و پایان هر استفاده)؛

ب) پایگاه دادهٔ مبنا که داده‌های ورودی سامانه با آن مقایسه می‌شوند؛

پ) داده‌های ورودی‌ای که جستجو در سامانه منجر به تطبیق یا انطباق آن‌ها شده است؛

ت) شناسایی اشخاص حقیقی درگیر در فرآیند راستی‌آزمایی نتایج مطابق بند (۵) ماده ۱۴.

ماده ۱۳. شفافیت و ارائهٔ اطلاعات به بهره‌برداران

۱. سامانه‌های هوش مصنوعی پرخطر باید به گونه‌ای طراحی شده و توسعه یابند که عملکرد آن‌ها به‌طور کافی شفاف باشد تا بهره‌برداران بتوانند خروجی سامانه را تفسیر کرده و به‌طور مناسب از آن استفاده کنند. سطح و نوع شفافیت مناسب باید به گونه‌ای تضمین شود که انطباق با تعهدات مربوطه تأمین‌کننده و بهره‌بردار مندرج در بخش ۳ حاصل شود.

۲. سامانه‌های هوش مصنوعی پرخطر باید همراه با دستورالعمل‌های استفاده در قالب دیجیتال مناسب یا هر قالب دیگری ارائه شوند که شامل اطلاعات مختصر، کامل، صحیح و شفاف باشد و برای بهره‌برداران مرتبط، قابل دسترسی و قابل فهم باشد.

۳. دستورالعمل‌های استفاده باید حداقل شامل اطلاعات زیر باشند:

الف) هویت و اطلاعات تماس تأمین‌کننده و در صورت لزوم نمایندهٔ مجاز آن؛

ب) ویژگی‌ها، قابلیت‌ها و محدودیت‌های عملکرد سامانهٔ هوش مصنوعی پرخطر، ازجمله:

۱) هدف موردنظر از به‌کارگیری سامانه؛

۲) سطح دقت ازجمله شاخص‌های آن، مقاومت سامانه و امنیت سایبری مندرج در ماده ۱۵ که سامانهٔ هوش مصنوعی پرخطر بر اساس آن‌ها آزمایش و اعتبارسنجی شده و قابل انتظار است و هر گونه شرایط شناخته‌شده یا قابل پیش‌بینی که ممکن است بر این سطح دقت، مقاومت و امنیت سایبری مورد انتظار تأثیر بگذارد.

۳) هر گونه شرایط شناخته‌شده یا قابل پیش‌بینی مرتبط با استفاده از سامانهٔ هوش مصنوعی پرخطر مطابق هدف موردنظر یا تحت شرایط سوءاستفادهٔ معقول قابل پیش‌بینی که ممکن است منجر به خطرات برای سلامت، ایمنی یا حقوق بنیادین مندرج در بند (۲) ماده ۹ شود.

۴) در صورت لزوم، قابلیت‌ها و ویژگی‌های فنی سامانهٔ هوش مصنوعی پرخطر برای ارائهٔ اطلاعاتی که مرتبط با تبیین خروجی سامانه باشد.

۵) در صورت لزوم، عملکرد سامانه در رابطه با اشخاص یا گروه‌های خاصی که سامانه قرار است برای آن‌ها استفاده شود.

۶) در صورت لزوم، مشخصات داده‌های ورودی یا هر اطلاعات مرتبط دیگر در خصوص مجموعهٔ داده‌های آموزش، اعتبارسنجی و آزمون مورد استفاده، با درنظرگرفتن هدف موردنظر سامانهٔ هوش مصنوعی پرخطر.

۷. در صورت لزوم، اطلاعاتی که به بهره‌برداران، امکان تفسیر خروجی سامانهٔ هوش مصنوعی پرخطر و استفادهٔ مناسب از آن را می‌دهد.

پ) تغییرات سامانهٔ هوش مصنوعی پرخطر و عملکرد آن که توسط تأمین‌کننده در زمان ارزیابی انطباق اولیه و در صورت وجود پیش‌بینی شده است؛

ت) تدابیر نظارت انسانی مندرج در ماده ۱۴ ازجمله تدابیر فنی اتخاذشده برای تسهیل تفسیر خروجی‌های سامانه‌های هوش مصنوعی توسط بهره‌برداران؛

ث) منابع محاسباتی و سخت‌افزاری مورد نیاز، طول عمر پیش‌بینی‌شدهٔ سامانهٔ هوش مصنوعی پرخطر و هر گونه تدابیر لازم برای نگهداری و مراقبت ازجمله فراوانی آن‌ها به منظور تضمین عملکرد صحیح سامانه ازجمله به‌روزرسانی‌های نرم‌افزاری؛

ج) در صورت لزوم، توضیح مکانیزم‌های موجود در سامانهٔ هوش مصنوعی پرخطر که امکان جمع‌آوری، ذخیره و تفسیر صحیح لاگ‌ها توسط بهره‌برداران را مطابق ماده ۱۲ فراهم می‌کند.

ماده ۱۴. نظارت انسانی

۱. سامانه‌های هوش مصنوعی پرخطر باید به گونه‌ای طراحی شده و توسعه یابند که از طریق ابزارهای مناسب رابط انسان و ماشین، نظارت مؤثر اشخاص حقیقی در مدت زمان استفاده از آن‌ها ممکن باشد.

۲. هدف از نظارت انسانی، پیشگیری یا به‌حداقل‌رساندن خطرات احتمالی برای سلامت، ایمنی یا حقوق بنیادین افراد است که ممکن است هنگام استفاده از سامانهٔ هوش مصنوعی پرخطر در چارچوب هدف موردنظر آن یا در شرایط سوءاستفادهٔ قابل پیش‌بینی متعارف بروز کنند، به‌ویژه در مواردی که چنین خطراتی علی‌رغم اجرای سایر الزامات مندرج در این بخش همچنان وجود داشته باشند.

۳. تدابیر نظارتی باید متناسب با میزان خطر، سطح خودکاربودن و زمینهٔ استفاده از سامانهٔ هوش مصنوعی پرخطر باشند و از طریق یکی از دو روش زیر یا هر دو تضمین شوند:

الف) تدابیری که در صورت امکان فنی پیش از عرضه به بازار یا بهره‌برداری از سامانهٔ هوش مصنوعی پرخطر از سوی ارائه‌دهنده شناسایی و در ساختار سامانه گنجانده شده باشند؛

ب) تدابیری که ارائه‌دهنده پیش از عرضه به بازار یا بهره‌برداری از سامانهٔ هوش مصنوعی پرخطر شناسایی کرده و اجرای آن‌ها از سوی بهره‌بردار مناسب و مقتضی تشخیص داده شده باشد.

۴. به منظور اجرای بندهای ۱، ۲ و ۳، سامانهٔ هوش مصنوعی پرخطر باید به نحوی در اختیار بهره‌بردار قرار گیرد که اشخاص حقیقی مسئول نظارت انسانی بتوانند به‌صورت متناسب و درخور،

الف) توانایی‌ها و محدودیت‌های مرتبط با سامانهٔ هوش مصنوعی پرخطر را به‌درستی درک کرده و قادر به پایش صحیح عملکرد آن باشند، ازجمله در راستای شناسایی و رفع ناهنجاری‌ها، اختلال‌ها و عملکردهای غیرمنتظره؛

ب) نسبت به گرایش احتمالی به اعتماد بیش از اندازه به خروجی تولیدشده توسط سامانهٔ هوش مصنوعی پرخطر (سوگیری ناشی از خودکارسازی) آگاهی کافی داشته باشند، به‌ویژه در خصوص سامانه‌هایی که برای ارائهٔ اطلاعات یا توصیه‌هایی در تصمیم‌گیری‌های انسانی به کار می‌روند.

ت) خروجی سامانهٔ هوش مصنوعی پرخطر را به‌درستی تفسیر کنند، با درنظرگرفتن ابزارها و روش‌های تفسیر موجود، ازجمله آن‌هایی که برای فهم نتایج سامانه در دسترس است.

ث) بتوانند در هر وضعیت خاص تصمیم بگیرند از سامانهٔ هوش مصنوعی پرخطر استفاده نکنند یا در غیر این صورت، خروجی آن را نادیده گرفته، از آن عبور کرده یا آن را معکوس کنند؛

ج) بتوانند در روند عملکرد سامانهٔ هوش مصنوعی پرخطر مداخله کرده یا از طریق دکمهٔ *توقف* یا رویه‌ای مشابه، عملکرد سامانه را متوقف کنند به گونه‌ای که سامانه در وضعیتی ایمن از کار بایستد.

۵. در مورد سامانه‌های هوش مصنوعی پرخطر موضوع بند (الف) از پیوست شمارهٔ ۳، تدابیر مذکور در بند ۳ این ماده باید به نحوی باشند که علاوه بر موارد پیش‌گفته، هیچ اقدام یا تصمیمی از سوی بهره‌بردار بر اساس شناسایی حاصل از سامانه انجام نگیرد، مگر آنکه این شناسایی، جداگانه و مستقل، دست‌کم توسط دو شخص حقیقی واجد صلاحیت، آموزش و اختیار لازم، راستی‌آزمایی و تأیید شده باشد.

الزام مربوط به راستی‌آزمایی جداگانه توسط حداقل دو شخص حقیقی در مورد سامانه‌های هوش مصنوعی پرخطر مورد استفاده برای مقاصد اجرای قانون، مهاجرت، کنترل مرزی یا پناهندگی، در صورتی که حقوق اتحادیه یا حقوق ملی، اجرای این الزام را نامتناسب تشخیص دهد اعمال نمی‌شود.

ماده ۱۵. دقت، استحکام و امنیت سایبری

۱. سامانه‌های هوش مصنوعی پرخطر باید به گونه‌ای طراحی شده و توسعه یابند که سطحی مناسب از دقت، استحکام و امنیت سایبری را محقق کنند و این ویژگی‌ها در سراسر چرخهٔ عمر سامانه به‌صورت پایدار حفظ شوند.

۲. به منظور تبیین جنبه‌های فنی مربوط به سنجش سطح مناسب دقت و استحکام مندرج در بند ۱ و سایر شاخص‌های عملکرد مرتبط، کمیسیون باید با همکاری ذی‌نفعان و سازمان‌های ذی‌ربط

ازجمله نهادهای مسئول سنجش و مرجع‌گذاری حسب اقتضا توسعهٔ معیارهای مرجع و روش‌های سنجش را تشویق و ترغیب کند.

۳. سطوح دقت و شاخص‌های مرتبط با دقت سامانه‌های هوش مصنوعی پرخطر باید در دستورالعمل‌های همراه با سامانه اعلام شوند.

۴. سامانه‌های هوش مصنوعی پرخطر باید تا حد امکان در برابر خطاها، نقص‌ها یا ناهماهنگی‌هایی که ممکن است در درون سامانه یا در محیط عملیاتی آن به‌ویژه بر اثر تعامل با اشخاص حقیقی یا سایر سامانه‌ها رخ دهند، مقاوم و پایدار باشند. در این راستا باید تدابیر فنی و سازمانی لازم اتخاذ شود. استحکام سامانه‌های هوش مصنوعی پرخطر می‌تواند از طریق راهکارهای فنی سامانه‌های پشتیبان حاصل شود که ممکن است شامل برنامه‌ها یا طرح‌های ایمنی جایگزین باشند.

سامانه‌های هوش مصنوعی پرریسکی که پس از عرضه به بازار یا آغاز بهره‌برداری به‌صورت مستمر به یادگیری ادامه می‌دهند، باید به گونه‌ای طراحی شوند که خطر تأثیرگذاری خروجی‌های جانبدارانه بر داده‌های ورودی عملیات آتی (حلقه‌های بازخورد) تا حد امکان حذف یا کاهش یابد، و اطمینان حاصل شود که چنین حلقه‌های بازخوردی با تدابیر مناسب کاهش خطر به‌درستی مدیریت می‌شوند.

بخش سوم. تعهدات ارائه‌دهندگان و بهره‌برداران سامانه‌های هوش مصنوعی پرخطر و سایر اشخاص

ماده ۱۶. تعهدات ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر

ارائه‌دهندگان سامانه‌های هوش مصنوعی پرریسک موظف‌اند که:

الف) اطمینان حاصل کنند که سامانه‌های هوش مصنوعی پرخطر آن‌ها با الزامات مقرر در بخش ۲ این قانون مطابقت دارند؛

ب) نام، نام تجاری یا علامت تجاری ثبت‌شده خود و نشانی محل تماس را بر روی سامانهٔ هوش مصنوعی پرخطر و در صورتی که این امر ممکن نباشد، بر روی بسته‌بندی یا در مستندات همراه آن، حسب مورد درج کنند؛

ج) نظام مدیریت کیفیتی را برقرار کنند که با مفاد ماده ۱۷ این قانون منطبق باشد؛

د) مستندات موضوع ماده ۱۸ را نگهداری کنند؛

هـ) در مواردی که سامانه تحت کنترل آنان است، گزارش‌های خودکار تولیدشده توسط سامانه‌های هوش مصنوعی پرخطر را مطابق ماده ۱۹ حفظ کنند؛

و) پیش از عرضه به بازار یا بهره‌برداری از سامانه، اطمینان حاصل کنند که سامانهٔ هوش مصنوعی پرخطر مراحل ارزیابی انطباق مربوطه را طبق ماده ۴۳ گذرانده است؛

ز) اعلامیهٔ انطباق اتحادیهٔ اروپا را مطابق ماده ۴۷ تنظیم کنند؛

ح) نشان CE را به سامانهٔ هوش مصنوعی پرخطر یا در صورت عدم امکان، به بسته‌بندی یا مستندات همراه آن الصاق نمایند تا انطباق با مفاد این قانون را مطابق ماده ۴۸ نشان دهند؛

ط) الزامات ثبت مندرج در بند ۱ ماده ۴۹ را رعایت کنند؛

ی) اقدامات اصلاحی لازم را اتخاذ کرده و اطلاعات مورد نیاز را طبق ماده ۲۰ ارائه دهند؛

ک) بنا به درخواست مستدل مقام صلاحیت‌دار ملی، انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات مقرر در بخش ۲ را اثبات کنند؛

ل) اطمینان حاصل کنند که سامانهٔ هوش مصنوعی پرخطر با الزامات دسترسی‌پذیری مندرج در دستورالعمل‌های ۲۱۰۲/۲۰۱۶ و ۸۸۲/۲۰۱۹ (اتحادیهٔ اروپا) مطابقت دارد.

ماده ۱۷. نظام مدیریت کیفیت

۱. ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر باید نظامی برای مدیریت کیفیت برقرار کنند که انطباق با مفاد این قانون را تضمین کند. این نظام باید به‌صورت منظم و نظام‌مند، در قالب سیاست‌ها، رویه‌ها و دستورالعمل‌های مکتوب مستندسازی شود و حداقل شامل جنبه‌های زیر باشد:

الف) راهبرد انطباق مقرراتی ازجمله رعایت رویه‌های ارزیابی انطباق و رویه‌های مربوط به مدیریت تغییرات در سامانهٔ هوش مصنوعی پرخطر؛

ب) فنون، رویه‌ها و اقدامات نظام‌مند مورد استفاده برای طراحی، کنترل طراحی و راستی‌آزمایی طراحی سامانهٔ هوش مصنوعی پرخطر؛

پ) فنون، رویه‌ها و اقدامات نظام‌مند مورد استفاده برای توسعه، کنترل کیفیت و تضمین کیفیت سامانهٔ هوش مصنوعی پرخطر؛

ت) روش‌های آزمون، بازرسی و اعتبارسنجی که باید پیش از توسعه، در حین توسعه و پس از توسعهٔ سامانهٔ هوش مصنوعی پرخطر اجرا شوند و همچنین تناوب انجام این فرآیندها.

ث) مشخصات فنی ازجمله استانداردهایی که باید اعمال شوند و در مواردی که استانداردهای هماهنگ مربوطه به‌طور کامل اعمال نشوند یا تمام الزامات مرتبط مندرج در بخش ۲ را پوشش ندهند، روش‌های مورد استفاده برای اطمینان از انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات آن؛

ج) سامانه‌ها و رویه‌های مدیریت داده‌ها ازجمله کسب، جمع‌آوری، تحلیل، برچسب‌گذاری، ذخیره‌سازی و پالایش داده، داده‌کاوی، تجمیع و نگهداری داده و هر عملیات دیگری که بر داده‌ها پیش از عرضه به بازار یا بهره‌برداری از سامانه‌های هوش مصنوعی پرخطر انجام می‌شود؛

چ) نظام مدیریت ریسک موضوع ماده ۹؛

ح) ایجاد، اجرا و نگهداری سامانهٔ پایش پس از عرضه مطابق ماده ۷۲؛

خ) رویه‌های مربوط به گزارش دهی حوادث جدی مطابق ماده ۷۳؛

د) نحوهٔ مدیریت ارتباطات با مقامات صلاحیت‌دار ملی، سایر مقامات ذی‌ربط ازجمله آن‌هایی که دسترسی به داده‌ها را فراهم یا پشتیبانی می‌کنند، نهادهای اعلان‌شده، سایر بهره‌برداران، مشتریان یا سایر ذی‌نفعان؛

ذ) سامانه‌ها و رویه‌های نگهداری سوابق تمام مستندات و اطلاعات مرتبط؛

ر) مدیریت منابع ازجمله تدابیر مرتبط با تأمین امنیت منابع؛

ز) چارچوب پاسخگویی که مسئولیت‌های مدیریت و سایر کارکنان را در خصوص تمام جنبه‌های مندرج در این بند مشخص می‌کند.

۲. اجرای جنبه‌های مندرج در بند ۱ باید متناسب با اندازهٔ سازمان ارائه‌دهنده باشد. با این حال، ارائه‌دهندگان باید در هر صورت سطح دقت و میزان حفاظت لازم را برای تضمین انطباق سامانه‌های هوش مصنوعی پرخطر خود با این قانون رعایت کنند.

۳. ارائه‌دهندگانی از سامانه‌های هوش مصنوعی پرخطر که مشمول تعهدات مربوط به نظام‌های مدیریت کیفیت یا عملکرد معادل آن طبق قوانین بخشی اتحادیهٔ اروپا هستند، می‌توانند جنبه‌های مندرج در بند ۱ را به‌عنوان بخشی از نظام‌های مدیریت کیفیت طبق آن قوانین لحاظ کنند.

۴. برای ارائه‌دهندگانی که مؤسسات مالی بوده و مشمول الزامات مربوط به حاکمیت داخلی، ترتیبات یا فرآیندها طبق قوانین خدمات مالی اتحادیهٔ اروپا هستند، تعهد ایجاد نظام مدیریت کیفیت با استثنای بند ۱، نکات (ز)، (ح) و (ط) این ماده از طریق رعایت قواعد مربوط به ترتیبات یا فرآیندهای حاکمیت داخلی طبق قوانین خدمات مالی اتحادیه مربوطه، محقق شده تلقی می‌شود. در این راستا، هر گونه استاندارد هماهنگ مورد اشاره در ماده ۴۰ باید مدنظر قرار گیرد.

ماده ۱۸. نگهداری مستندات

۱. ارائه‌دهنده باید به مدت ۱۰ سال پس از عرضهٔ سامانهٔ هوش مصنوعی پرخطر به بازار یا آغاز بهره‌برداری از آن، مستندات مربوطه را در اختیار مقامات صلاحیت‌دار ملی قرار دهد:

الف) مستندات فنی موضوع ماده ۱۱؛

ب) مستندات مربوط به نظام مدیریت کیفیت موضوع ماده ۱۷؛

پ) مستندات مربوط به تغییرات مصوب نهادهای اعلان‌شده در صورت کاربرد؛

ت) تصمیمات و سایر مستندات صادرشده توسط نهادهای اعلان‌شده در صورت کاربرد؛

ث) اعلامیهٔ انطباق اتحادیهٔ اروپا موضوع ماده ۴۷.

۲. هر کشور عضو باید شرایطی را تعیین کند که بر اساس آن، مستندات موضوع بند ۱ برای مدت مقرر در همان بند، در اختیار مقامات صلاحیت‌دار ملی باقی بماند، در مواردی که ارائه‌دهنده یا نمایندهٔ مجاز آن که در قلمرو آن کشور مستقر است، ورشکسته شود یا فعالیت خود را پیش از پایان آن مدت متوقف کند.

۳. ارائه‌دهندگانی که مؤسسات مالی بوده و مشمول الزامات مربوط به حاکمیت داخلی، ترتیبات یا فرآیندها طبق قوانین خدمات مالی اتحادیهٔ اروپا هستند، باید مستندات فنی را به‌عنوان بخشی از مستنداتی که طبق همان قوانین خدمات مالی اتحادیه نگهداری می‌شوند، حفظ کنند.

ماده ۱۹. گزارش‌های خودکار تولیدشده

۱. ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر باید گزارش‌های موضوع بند ۱ ماده ۱۲ را که به‌صورت خودکار توسط سامانه‌های هوش مصنوعی پرخطر آن‌ها تولید می‌شود تا حدی که تحت کنترل آنان است، نگهداری کنند. بدون خدشه به قوانین قابل اجرا در اتحادیه یا ملی، این گزارش‌ها باید برای مدتی متناسب با هدف موردنظر سامانهٔ هوش مصنوعی پرخطر و حداقل شش ماه نگهداری شوند، مگر اینکه در قوانین اتحادیه یا ملی قابل اعمال، به‌ویژه در قوانین اتحادیه در زمینهٔ حفاظت از داده‌های شخصی مقرر شده باشد.

۲. ارائه‌دهندگانی که مؤسسات مالی بوده و مشمول الزامات مربوط به حاکمیت داخلی، ترتیبات یا فرآیندها طبق قوانین خدمات مالی اتحادیهٔ اروپا هستند، باید گزارش‌های خودکار تولیدشده توسط سامانه‌های هوش مصنوعی پرخطر خود را به‌عنوان بخشی از مستنداتی که طبق همان قوانین خدمات مالی نگهداری می‌شوند، حفظ کنند.

ماده ۲۰. اقدامات اصلاحی و وظیفهٔ اطلاع‌رسانی

۱. ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر که تصور می‌کنند یا دلایلی دارند که نشان می‌دهد سامانهٔ هوش مصنوعی پرخطری که آن‌ها به بازار عرضه کرده یا مورد بهره‌برداری قرار گرفته است، با این قانون مطابقت ندارد، باید فوراً اقدامات اصلاحی لازم را برای همسوسازی سامانه با مقررات، جمع‌آوری، غیرفعال‌سازی یا فراخوانی آن حسب مورد، انجام دهند. آن‌ها باید توزیع‌کنندگان سامانهٔ موردنظر و در صورت لزوم، بهره‌برداران، نمایندهٔ مجاز و واردکنندگان را در این خصوص مطلع کنند.

۲. در صورتی که سامانهٔ هوش مصنوعی پرخطر باشد و طبق بند ۱ ماده ۷۹ ارائه‌دهنده از آن خطر

مطلع شود، باید فوراً علت‌ها را بررسی کرده و در صورت لزوم، با بهره‌بردار گزارش‌دهنده همکاری کند و مقامات نظارت بر بازار مربوطه و در صورت کاربرد، نهاد اعلان‌شده‌ای را که گواهی سامانه را صادر کرده است به‌ویژه در خصوص ماهیت عدم انطباق و هر گونه اقدام اصلاحی مرتبط انجام‌شده طبق ماده ۴۴ مطلع کند.

ماده ۲۱. همکاری با مقامات صلاحیت‌دار

۱. تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر موظف‌اند بنا به درخواست مستدل مقام صلاحیت‌دار، تمامی اطلاعات و اسناد لازم را برای اثبات انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در بخش ۲ در اختیار آن مقام قرار دهند. این اطلاعات باید به زبانی ارائه شود که برای مقام مذکور قابل فهم باشد و در زمرهٔ یکی از زبان‌های رسمی نهادهای اتحادیه باشد که توسط دولت عضو مربوطه تعیین شده است.

۲. بنا به درخواست مستدل مقام صلاحیت‌دار، تأمین‌کنندگان باید در صورت اقتضا، دسترسی مقام درخواست‌کننده را به سوابق خودکار تولیدشده سامانهٔ هوش مصنوعی پرخطر موضوع بند ۱ ماده ۱۲ تا حدی که این سوابق تحت کنترل آنان است، فراهم کنند.

۳. هر گونه اطلاعاتی که مقام صلاحیت‌دار به موجب این ماده دریافت می‌کند باید مطابق تعهدات محرمانگی مقرر در ماده ۷۸ مورد رسیدگی قرار گیرد.

ماده ۲۲. نمایندگان مجاز تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر

۱. تأمین‌کنندگانی که در کشورهای ثالث مستقر هستند باید پیش از عرضهٔ سامانه‌های هوش مصنوعی پرخطر خود در بازار اتحادیه، بر اساس اختیارنامهٔ کتبی، نماینده‌ای مجاز را که در قلمرو اتحادیه مستقر است منصوب کنند.

۲. تأمین‌کننده باید امکانات لازم را برای نمایندهٔ مجاز خود فراهم آورد تا وی بتواند وظایفی را که در اختیارنامه تعیین شده است، انجام دهد.

۳. نمایندهٔ مجاز باید وظایفی را که در اختیارنامهٔ صادره از سوی تأمین‌کننده به وی محول شده است، انجام دهد. وی باید بنا به درخواست، نسخه‌ای از اختیارنامه را در یکی از زبان‌های رسمی نهادهای اتحادیه به تشخیص مقام صلاحیت‌دار، در اختیار مقامات نظارت بر بازار قرار دهد.

در چارچوب این قانون، اختیارنامه باید به نمایندهٔ مجاز اجازهٔ انجام وظایف زیر را بدهد:

الف) اطمینان از آنکه *بیانیهٔ انطباق اتحادیهٔ اروپا* موضوع ماده ۴۷ و *مستندات فنی* موضوع ماده

۱۱ تهیه شده و تأمین‌کننده، روند مناسب ارزیابی انطباق را اجرا کرده است؛

ب) نگهداری اطلاعات تماس تأمین‌کنندهٔ منصوب‌کنندهٔ نمایندهٔ مجاز، نسخه‌ای از بیانیهٔ انطباق اتحادیهٔ اروپا موضوع ماده ۴۷، مستندات فنی و در صورت وجود، گواهی صادره از سوی نهاد اعلام‌شده را برای مدت ده سال پس از عرضهٔ سامانهٔ هوش مصنوعی پرخطر در بازار یا آغاز بهره‌برداری از آن، در دسترس مقامات صلاحیت‌دار و مقامات یا نهادهای ملی موضوع بند ۱۰ ماده ۷۴ قرار دهد؛

پ) ارائهٔ کلیهٔ اطلاعات و مستندات لازم ازجمله موارد مذکور در بند (ب) به مقام صلاحیت‌دار بنا به درخواست مستدل و به منظور اثبات انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در بخش ۲، ازجمله دسترسی به سوابق خودکار تولیدشده توسط سامانهٔ هوش مصنوعی پرخطر مطابق بند ۱ ماده ۱۲ تا حدی که این سوابق تحت کنترل تأمین‌کننده باشد؛

ت) همکاری با مقامات صلاحیت‌دار بنا به درخواست مستدل آنان در هر اقدامی که در ارتباط با سامانهٔ هوش مصنوعی پرخطر انجام می‌دهند به‌ویژه برای کاهش یا رفع خطرات ناشی از آن سامانه؛

ث) در صورت اقتضا، رعایت الزامات ثبت‌نام مندرج در بند ۱ ماده ۴۹ یا در صورتی که ثبت‌نام توسط خود تأمین‌کننده انجام شده باشد، اطمینان از صحت اطلاعات مذکور در بند ۳ بخش (الف) پیوست هشتم.

اختیارنامه باید به نمایندهٔ مجاز این اختیار را بدهد که مقامات صلاحیت‌دار بتوانند در همهٔ امور مرتبط با تضمین انطباق با این قانون، علاوه بر تأمین‌کننده یا به جای وی، مستقیماً با نمایندهٔ مجاز تماس بگیرند.

۴. نمایندهٔ مجاز باید اختیارنامه را در صورتی خاتمه دهد که تشخیص دهد یا دلایل موجهی برای این باور داشته باشد که تأمین‌کننده برخلاف تعهدات خود به موجب این قانون عمل می‌کند. در چنین حالتی، نمایندهٔ مجاز باید فوراً مقام نظارت بر بازار ذی‌ربط و در صورت اقتضا، نهاد اعلام‌شدهٔ مربوط را از خاتمهٔ اختیارنامه و دلایل آن آگاه کند.

ماده ۲۳. تعهدات واردکنندگان

۱. پیش از عرضهٔ سامانهٔ هوش مصنوعی پرخطر در بازار، واردکنندگان باید اطمینان حاصل کنند که سامانهٔ مزبور با مفاد این قانون از طریق بررسی موارد زیر انطباق دارد:

الف) فرآیند ارزیابی انطباق مربوطه طبق ماده ۴۳، توسط تأمین‌کنندهٔ سامانهٔ هوش مصنوعی پرخطر انجام شده است؛

ب) تأمین‌کنندهٔ مستندات فنی لازم را مطابق ماده ۱۱ و پیوست چهارم تهیه کرده است؛

پ) سامانه دارای نشان الزامی CE بوده و همراه با *بیانیهٔ انطباق اتحادیهٔ اروپا* موضوع ماده ۴۷ و دستورالعمل‌های استفاده ارائه می‌شود؛

ت) تأمین‌کننده طبق بند ۱ ماده ۲۲، نمایندهٔ مجاز خود را منصوب کرده است.

۲. هر گاه واردکننده دلایل کافی برای این باور داشته باشد که سامانهٔ هوش مصنوعی پرخطر با مفاد این قانون منطبق نیست یا جعلی است یا اسناد همراه آن جعل شده است، نباید آن سامانه را تا زمان حصول اطمینان از انطباق کامل با این قانون، در بازار عرضه کند. در صورتی که سامانهٔ هوش مصنوعی پرخطر دارای خطری در معنای بند ۱ ماده ۷۹ باشد، واردکننده باید تأمین‌کنندهٔ سامانه، نمایندهٔ مجاز و مقامات نظارت بر بازار را از این امر آگاه کند.

۳. واردکنندگان باید نام، نام یا علامت تجاری ثبت‌شده خود و نشانی تماس را بر روی سامانهٔ هوش مصنوعی پرخطر و بسته‌بندی آن یا در صورت اقتضا، بر روی مستندات همراه آن درج کنند.

۴. واردکنندگان باید اطمینان حاصل کنند که در مدتی که سامانهٔ هوش مصنوعی پرخطر تحت مسئولیت آنان است، شرایط نگهداری یا حمل و نقل (در صورت وجود) به گونه‌ای نباشد که انطباق سامانه با الزامات مندرج در بخش ۲ را به خطر اندازد.

۵. واردکنندگان باید برای مدت ده سال پس از عرضهٔ سامانهٔ هوش مصنوعی پرخطر در بازار یا آغاز بهره‌برداری از آن، نسخه‌ای از گواهی صادرشده توسط نهاد اعلام‌شده (در صورت وجود)، دستورالعمل‌های استفاده و بیانیهٔ انطباق اتحادیهٔ اروپا موضوع ماده ۴۷ را نگهداری کنند.

۶. واردکنندگان باید بنا به درخواست مستدل مقامات صلاحیت‌دار ذی‌ربط، تمامی اطلاعات و مستندات لازم ازجمله موارد مذکور در بند ۵ را به زبانی که برای آن مقامات به‌آسانی قابل فهم باشد، جهت اثبات انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در بخش ۲ ارائه دهند. بدین منظور، آنان باید اطمینان حاصل کنند که مستندات فنی نیز در صورت درخواست، در اختیار مقامات مربوط قرار گیرد.

۷. واردکنندگان باید در تمامی اقداماتی که مقامات صلاحیت‌دار ذی‌ربط در ارتباط با سامانهٔ هوش مصنوعی پرخطری که توسط آنان در بازار عرضه شده و انجام می‌دهند، همکاری کامل داشته باشند، به‌ویژه در اقداماتی که با هدف کاهش، کنترل یا رفع خطرات ناشی از آن سامانه صورت می‌گیرد.

ماده ۲۴. تعهدات توزیع‌کنندگان

۱. پیش از عرضهٔ سامانهٔ هوش مصنوعی پرخطر در بازار، توزیع‌کنندگان باید اطمینان حاصل کنند که سامانه دارای نشان الزامی CE است. همچنین نسخه‌ای از *بیانیهٔ انطباق اتحادیهٔ اروپا*

موضوع ماده ۴۷ و دستورالعمل‌های استفاده ارائه می‌شود و نیز تأمین‌کننده و واردکنندهٔ آن سامانه حسب مورد، تعهدات مقرر در جزءهای (ب) و (پ) ماده ۱۶ و بند ۳ ماده ۲۳ را رعایت کرده‌اند.

۲. هر گاه توزیع‌کننده بر اساس اطلاعات در اختیار خود تشخیص دهد یا دلایل موجهی برای این باور داشته باشد که سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در بخش ۲ انطباق ندارد، نباید آن را در بازار عرضه کند تا زمانی که سامانه با الزامات مذکور منطبق شود. افزون بر این، اگر سامانهٔ هوش مصنوعی پرخطر دارای خطری در معنای بند ۱ ماده ۷۹ باشد، توزیع‌کننده باید تأمین‌کننده یا واردکنندهٔ مربوط را از این امر آگاه کند.

۳. توزیع‌کنندگان باید اطمینان حاصل کنند که در مدت زمانی که سامانهٔ هوش مصنوعی پرخطر تحت مسئولیت آنان قرار دارد، شرایط نگهداری یا حمل و نقل (در صورت اقتضا) به گونه‌ای نباشد که انطباق سامانه با الزامات مندرج در بخش ۲ را به خطر اندازد.

۴. هر گاه توزیع‌کننده بر اساس اطلاعات در اختیار خود تشخیص دهد یا دلایل موجهی برای این باور داشته باشد که سامانهٔ هوش مصنوعی پرخطری که توسط وی در بازار عرضه شده، با الزامات مندرج در بخش ۲ انطباق ندارد، باید اقدامات اصلاحی لازم را برای انطباق آن با الزامات مذکور انجام دهد یا نسبت به جمع‌آوری یا فراخوانی آن از بازار اقدام یا اطمینان حاصل کند که تأمین‌کننده، واردکننده یا هر عامل ذی‌ربط دیگری حسب مورد، اقدامات اصلاحی لازم را انجام داده است.

در صورتی که سامانهٔ هوش مصنوعی پرخطر دارای خطری در معنای بند ۱ ماده ۷۹ باشد، توزیع‌کننده باید بی‌درنگ تأمین‌کننده یا واردکنندهٔ سامانه و مقامات صلاحیت‌دار مربوط به آن سامانه را از موضوع آگاه کرده و جزئیات مربوطه به‌ویژه در خصوص موارد عدم انطباق و اقدامات اصلاحی انجام‌شده را ارائه کند.

۵. بنا به درخواست مستدل مقام صلاحیت‌دار ذی‌ربط، توزیع‌کنندگان سامانه‌های هوش مصنوعی پرخطر باید تمامی اطلاعات و مستندات مربوط به اقدامات انجام‌شده موضوع بندهای ۱ تا ۴ را به منظور اثبات انطباق سامانه با الزامات مندرج در بخش ۲، در اختیار آن مقام قرار دهند.

۶. توزیع‌کنندگان باید با مقامات صلاحیت‌دار ذی‌ربط در تمامی اقداماتی که در ارتباط با سامانهٔ هوش مصنوعی پرخطری که توسط آنان در بازار عرضه و انجام می‌شود، همکاری کنند، به‌ویژه در اقداماتی که هدف از آن کاهش یا رفع خطرات ناشی از آن سامانه است.

ماده ۲۵. مسئولیت‌ها در زنجیرهٔ ارزش هوش مصنوعی

۱. هر توزیع‌کننده، واردکننده، بهره‌بردار یا هر شخص ثالث دیگری در هر یک از موارد زیر به‌عنوان

تأمین‌کنندهٔ سامانهٔ هوش مصنوعی پرخطر تلقی می‌شود و مشمول تعهدات مقرر برای تأمین‌کننده در ماده ۱۶ خواهد بود:

الف) زمانی که بدون لطمه به ترتیبات قراردادی که تقسیم متفاوت تعهدات را مقرر می‌دارد، نام یا علامت تجاری خود را بر روی سامانهٔ هوش مصنوعی پرخطری که پیش‌تر در بازار عرضه یا مورد بهره‌برداری قرار گرفته است، درج کند؛

ب) زمانی که تغییری اساسی در سامانهٔ هوش مصنوعی پرخطری که قبلاً در بازار عرضه یا از آن آن بهره‌برداری شده است ایجاد کند، به گونه‌ای که آن سامانه همچنان مطابق ماده ۶ در زمرهٔ سامانه‌های هوش مصنوعی پرخطر باقی بماند؛

پ) زمانی که هدف موردنظر از سامانهٔ هوش مصنوعی ازجمله سامانهٔ هوش مصنوعی عمومی را که پیش‌تر به‌عنوان سامانهٔ پرخطر طبقه‌بندی نشده و در بازار عرضه شده یا مورد بهره‌برداری قرار گرفته است به نحوی تغییر دهد که سامانهٔ مزبور طبق ماده ۶ در زمرهٔ سامانه‌های هوش مصنوعی پرخطر قرار گیرد.

۲. در موارد مذکور در بند ۱، تأمین‌کننده‌ای که در ابتدا سامانهٔ هوش مصنوعی را در بازار عرضه کرده یا مورد بهره‌برداری قرار داده است، دیگر برای اهداف این قانون، تأمین‌کنندهٔ آن سامانهٔ خاص محسوب نمی‌شود. تأمین‌کنندهٔ اولیه باید با تأمین‌کنندهٔ جدید همکاری نزدیک داشته باشد و اطلاعات لازم، دسترسی فنی معقول و سایر مساعدت‌های ضروری را برای اجرای تعهدات مندرج در این قانون به‌ویژه در خصوص انطباق با الزامات ارزیابی انطباق سامانه‌های هوش مصنوعی پرخطر در اختیار او قرار دهد.

با این حال، این بند در مواردی اعمال نمی‌شود که تأمین‌کنندهٔ اولیه به‌طور صریح اعلام کرده باشد که سامانهٔ هوش مصنوعی وی نباید به سامانه‌ای پرخطر تبدیل شود و از این رو مشمول تعهد تحویل مستندات نیست.

۳. در خصوص سامانه‌های هوش مصنوعی پرخطری که به‌عنوان اجزای ایمنی محصولات مشمول قوانین همسوسازی اتحادیه (مندرج در بخش (الف) پیوست اول) به شمار می‌روند، تولیدکنندهٔ محصول، تأمین‌کنندهٔ سامانهٔ هوش مصنوعی پرخطر محسوب می‌شود و در هر یک از موارد زیر مشمول تعهدات مندرج در ماده ۱۶ خواهد بود:

الف) سامانهٔ هوش مصنوعی پرخطر همراه با محصول و تحت نام یا علامت تجاری تولیدکنندهٔ محصول در بازار عرضه شود؛

ب) سامانهٔ هوش مصنوعی پرخطر پس از عرضهٔ محصول در بازار، تحت نام یا علامت تجاری تولیدکنندهٔ محصول مورد بهره‌برداری قرار گیرد.

۴. تأمین‌کنندهٔ سامانهٔ هوش مصنوعی پرخطر و شخص ثالثی که سامانهٔ هوش مصنوعی، ابزارها، خدمات، اجزاء یا فرآیندهایی را که در سامانهٔ هوش مصنوعی پرخطر به کار رفته یا در آن ادغام شده‌اند تأمین می‌کند، باید از طریق توافق‌نامه کتبی، اطلاعات، قابلیت‌ها، دسترسی فنی و سایر مساعدت‌های لازم را بر اساس سطح شناخته‌شده فناوری تعیین کنند تا تأمین‌کنندهٔ سامانهٔ هوش مصنوعی پرخطر بتواند به‌طور کامل تعهدات خود را طبق این قانون انجام دهد. این بند شامل اشخاص ثالثی نمی‌شود که ابزارها، خدمات، فرآیندها یا اجزای (غیر از مدل‌های هوش مصنوعی عمومی) را تحت مجوز آزاد و متن‌باز در دسترس عموم قرار می‌دهند.

دفتر هوش مصنوعی می‌تواند شرایط نمونه برای قراردادهای میان تأمین‌کنندگان سامانه‌های هوش مصنوعی پرخطر و اشخاص ثالثی که ابزارها، خدمات، اجزاء یا فرآیندهایی را برای استفاده در آن سامانه‌ها فراهم می‌کنند، تدوین و پیشنهاد کند. در تنظیم این شرایط نمونه، دفتر هوش مصنوعی باید الزامات قراردادی خاص قابل اعمال در بخش‌ها یا موقعیت‌های تجاری ویژه را نیز مدنظر قرار دهد. این شرایط نمونه باید منتشر شده و به‌صورت الکترونیکی، رایگان و در قالبی آسان برای استفاده در دسترس عموم قرار گیرد.

۵. مفاد بندهای ۲ و ۳ بدون خدشه به الزامات مربوط به رعایت و حمایت از حقوق مالکیت فکری، اطلاعات محرمانه تجاری و اسرار بازرگانی طبق حقوق اتحادیه و قوانین ملی است.

ماده ۲۶. تعهدات بهره‌برداران سامانه‌های هوش مصنوعی پرخطر

۱. بهره‌برداران سامانه‌های هوش مصنوعی پرخطر باید تدابیر فنی و سازمانی مناسب را اتخاذ کنند تا اطمینان یابند استفاده از این سامانه‌ها مطابق دستورالعمل‌های استفادهٔ همراه آن‌ها طبق مفاد بندهای ۳ و ۶ این ماده صورت می‌گیرد.

۲. بهره‌برداران باید نظارت انسانی را به اشخاص حقیقی‌ای محول کنند که از شایستگی، آموزش و اختیارات لازم برخوردارند و همچنین از پشتیبانی کافی برای انجام این وظیفه بهره‌مند هستند.

۳. تعهدات مقرر در بندهای ۱ و ۲ این ماده بدون خدشه به سایر تعهدات بهره‌بردار تحت قوانین اتحادیه یا قوانین ملی و نیز بدون خدشه به آزادی بهره‌بردار در سازمان‌دهی منابع و فعالیت‌های خود جهت اجرای تدابیر نظارت انسانی تعیین‌شده از سوی ارائه‌دهنده است.

۴. بدون خدشه به بندهای ۱ و ۲ در مواردی که بهره‌بردار بر داده‌های ورودی کنترل دارد، وی باید اطمینان حاصل کند که داده‌های ورودی مرتبط و از لحاظ هدف موردنظر سامانهٔ هوش مصنوعی پرخطر، به میزان کافی شناخته‌شده و گویا هستند.

۵. بهره‌برداران باید عملکرد سامانهٔ هوش مصنوعی پرخطر را بر اساس دستورالعمل‌های استفاده پایش کنند و در صورت لزوم مطابق ماده ۷۲ ارائه‌دهندگان را مطلع کنند. چنانچه بهره‌بردار، دلیلی داشته باشد که تصور کند ممکن است استفاده از سامانه بر اساس دستورالعمل‌ها خطری را در معنای ماده ۷۹(۱) ایجاد کند، باید بدون تأخیر ناموجه، ارائه‌دهنده یا توزیع‌کننده و نیز مرجع نظارت بر بازار مربوطه را مطلع و استفاده از آن سامانه را تعلیق کند. در صورتی که بهره‌بردار، حادثه‌ای جدی را شناسایی کند باید بلافاصله ابتدا ارائه‌دهنده و سپس واردکننده یا توزیع‌کننده و مراجع نظارت بر بازار ذی‌ربط را از وقوع آن حادثه آگاه کند. اگر بهره‌بردار نتواند به ارائه‌دهنده دسترسی پیدا کند، ماده ۷۳ با رعایت تغییرات لازم اعمال می‌شود. این تعهد شامل داده‌های عملیاتی حساس بهره‌برداران سامانه‌های هوش مصنوعی که مراجع اجرای قانون هستند، نمی‌شود.

برای بهره‌بردارانی که مؤسسات مالی مشمول الزامات حاکمیت داخلی، ترتیبات یا فرآیندهای مندرج در حقوق خدمات مالی اتحادیهٔ اروپا هستند، تعهد نظارت مذکور در بند نخست با رعایت قواعد مربوط به ترتیبات، فرآیندها و سازوکارهای حاکمیت داخلی به موجب قوانین خدمات مالی اتحادیه، تحقق‌یافته تلقی می‌شود.

۶. بهره‌برداران سامانه‌های هوش مصنوعی پرخطر باید سوابق خودکار تولیدشده توسط آن سامانه را تا جایی که در کنترل آنان است به مدت متناسب با هدف موردنظر سامانه و حداقل شش ماه نگهداری کنند، مگر آنکه در قوانین اتحادیه یا ملی، به‌ویژه در حقوق اتحادیه مربوط به حمایت از داده‌های شخصی، ترتیب دیگری مقرر شده باشد.

بهره‌بردارانی که مؤسسات مالی مشمول الزامات حاکمیت داخلی به موجب حقوق خدمات مالی اتحادیه هستند، باید این سوابق را به‌عنوان بخشی از مستندات نگهداری‌شده طبق قوانین خدمات مالی مربوط، حفظ کنند.

۷. پیش از به‌کارگیری یا استفاده از سامانهٔ هوش مصنوعی پرخطر در محیط کار، بهره‌بردارانی که کارفرما هستند باید نمایندگان کارگران و کارگران ذی‌نفع را از اینکه در معرض استفاده از سامانهٔ هوش مصنوعی پرخطر قرار خواهند گرفت، مطلع کنند. این اطلاع‌رسانی در صورت اقتضا باید مطابق قواعد و رویه‌های مقرر در حقوق و رویهٔ ملی و اتحادیه‌ای دربارهٔ اطلاع‌رسانی به کارگران و نمایندگان آنان انجام شود.

۸. بهره‌برداران سامانه‌های هوش مصنوعی پرخطر که ازجمله مقامات عمومی یا نهادها، ارگان‌ها، دفاتر یا آژانس‌های اتحادیه هستند، باید به تعهدات ثبت‌نامی مذکور در ماده ۴۹ پایبند باشند. چنانچه این بهره‌برداران دریابند که سامانهٔ هوش مصنوعی پرخطری که قصد استفاده از آن را دارند در پایگاه دادهٔ اتحادیه موضوع ماده ۷۱ ثبت نشده است، نباید از آن سامانه استفاده کنند و باید ارائه‌دهنده یا

توزیع‌کننده را مطلع کنند.

۹. در صورت اقتضا، بهره‌برداران سامانه‌های هوش مصنوعی پرخطر باید از اطلاعات ارائه‌شده طبق ماده ۱۳ این قانون برای ایفای تعهد خود در انجام *ارزیابی تأثیر بر حمایت از داده‌ها* موضوع ماده ۳۵ مقررات شمارهٔ ۲۰۱۶/۶۷۹ یا ماده ۲۷ دستورالعمل شمارهٔ ۲۰۱۶/۶۸۰ استفاده کنند.

۱۰. بدون خدشه به دستورالعمل شمارهٔ ۲۰۱۶/۶۸۰ در چارچوب تحقیقات مربوط به جستجوی هدفمند فردی که مظنون یا محکوم به ارتکاب جرم است، بهره‌بردار سامانهٔ هوش مصنوعی پرخطر برای شناسایی زیستی پس از وقوع باید پیش از استفاده از سامانه، یا بدون تأخیر ناموجه و حداکثر ظرف ۴۸ ساعت، از مرجع قضایی یا مرجع اداری موردنظر که تصمیم آن الزام‌آور و قابل بازبینی قضایی است، مجوز دریافت کند، مگر در مواردی که سامانه برای شناسایی اولیهٔ مظنون احتمالی بر اساس داده‌های عینی و قابل راستی‌آزمایی مرتبط با جرم به کار رود. هر مورد استفاده باید صرفاً به میزانی محدود شود که برای تحقیق دربارهٔ جرم خاص ضرورت دارد. در صورتی که درخواست مجوز مطابق بند فوق رد شود، استفاده از سامانهٔ شناسایی زیستی پس از وقوع[۱۸۰] مرتبط با آن مجوز باید بلافاصله متوقف شود و داده‌های شخصی مرتبط با استفاده از سامانهٔ هوش مصنوعی پرخطر که مجوز آن رد شده، حذف شود.

در هیچ موردی، استفاده از چنین سامانهٔ هوش مصنوعی پرخطری برای شناسایی زیستی از راه دور پس از وقوع نباید برای مقاصد اجرای قانون به‌صورت غیرهدفمند و بدون وجود هر گونه ارتباط با جرم، دادرسی کیفری، تهدید واقعی و حاضر یا قابل پیش‌بینیِ ارتکاب جرم یا جستجوی شخص مفقود خاصی به کار رود.

باید اطمینان حاصل شود که هیچ تصمیمی که اثر حقوقی زیان‌بار بر شخصی داشته باشد، صرفاً بر مبنای خروجی چنین سامانه‌های شناسایی زیستی از راه دور پس از وقوع از سوی مقامات اجرای قانون اتخاذ نشود.

این بند بدون خدشه به ماده ۹ مقررات شمارهٔ ۲۰۱۶/۶۷۹ و ماده ۱۰ دستورالعمل ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) در خصوص پردازش داده‌های زیستی است. صرف‌نظر از هدف یا بهره‌بردار، هر مورد از استفاده از چنین سامانه‌های هوش مصنوعی پرخطر باید در پرونده مربوط به پلیس مستند شود و بنا به درخواست، در اختیار مقام نظارت بر بازار و مقام ملی حفاظت از داده‌ها قرار گیرد، البته بدون افشای داده‌های عملیاتی حساس مرتبط با اجرای قانون. این بند فرعی نیز بدون خدشه به اختیارات اعطاشده به مقامات ناظر طبق دستورالعمل ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) خواهد بود.

بهره‌برداران باید گزارش‌های سالانه‌ای دربارهٔ استفادهٔ خود از سامانه‌های شناسایی زیستی از راه دور پس از وقوع، بدون افشای داده‌های عملیاتی حساس مرتبط با اجرای قانون، به مقام نظارت

180. Post-remote biometric identification

بر بازار و مقام ملی حفاظت از داده‌ها ارائه دهند. این گزارش‌ها می‌توانند به‌صورت تجمیعی و شامل بیش از یک مورد بهره‌برداری باشند. دولت‌های عضو می‌توانند در چارچوب حقوق اتحادیهٔ اروپا، قوانین محدودکننده‌تری در زمینهٔ استفاده از سامانه‌های شناسایی زیستی از راه دور پس از وقوع وضع کنند.

بند ۱۱. بدون خدشه به ماده ۵۰ این قانون، بهره‌برداران سامانه‌های هوش مصنوعی پرخطری که در پیوست شمارهٔ ۳ ذکر شده‌اند و در تصمیم‌گیری یا همکاری در تصمیم‌گیری مربوط به اشخاص حقیقی نقش دارند، باید به آن اشخاص اطلاع دهند که در معرض استفاده از چنین سامانه‌ای قرار دارند.

در مورد سامانه‌های هوش مصنوعی پرخطری که برای مقاصد اجرای قانون به کار می‌روند، ماده ۱۳ دستورالعمل (اتحادیهٔ اروپا) ۶۸۰/۲۰۱۶ اعمال خواهد شد.

بند ۱۲. بهره‌برداران باید با مقامات ذی‌صلاح مربوطه در هر اقدامی که آن مقامات در ارتباط با سامانهٔ هوش مصنوعی پرخطر جهت اجرای این قانون انجام می‌دهند، همکاری کنند.

ماده ۲۷. ارزیابی تأثیر بر حقوق بنیادین در خصوص سامانه‌های هوش مصنوعی پرخطر

۱. پیش از به‌کارگیری هر سامانهٔ هوش مصنوعی پرخطری که در بند ۲ ماده ۶ ذکر شده است به استثنای سامانه‌های هوش مصنوعی پرخطری که برای استفاده در حوزهٔ مندرج در بند ۲ پیوست سوم پیش‌بینی شده‌اند. اشخاص به‌کارگیرنده (اعم از نهادهای تابع حقوق عمومی یا اشخاص خصوصی ارائه‌دهندهٔ خدمات عمومی) و نیز به‌کارگیرندگان سامانه‌های هوش مصنوعی پرخطر موضوع بندهای ۵ (ب) و (ج) پیوست سوم موظف‌اند در مورد تأثیر استفاده از این سیستم‌ها بر حقوق بنیادین ارزیابی انجام دهند.

برای این منظور، ارزیابی به‌کارگیرندگان باید شامل موارد زیر انجام دهند:

الف) توصیف فرآیندهایی که در آن‌ها سامانهٔ هوش مصنوعی پرخطر مطابق هدف موردنظر خود به کار گرفته خواهد شد؛

ب) توصیف بازهٔ زمانی و دفعات استفاده از هر سامانهٔ هوش مصنوعی پرخطر؛

پ) دسته‌های اشخاص حقیقی و گروه‌هایی که احتمالاً در بستر خاص استفاده از سیستم تحت تأثیر قرار خواهند گرفت؛

ت) خطرات مشخص زیان‌آوری که ممکن است بر دسته‌های اشخاص یا گروه‌های شناسایی‌شده در بند (پ) این بند تأثیر بگذارد، با درنظرگرفتن اطلاعاتی که ارائه‌دهنده مطابق ماده ۱۳ فراهم

کرده است؛

ث) توصیف تدابیر نظارت انسانی مطابق دستورالعمل‌های استفاده از سیستم؛

ج) تدابیر لازم در صورت تحقق خطرات مذکور، ازجمله سازوکارهای حاکمیت داخلی و نظام رسیدگی به شکایات.

۲. تعهد مقرر در بند ۱ این ماده، مربوط به اولین استفاده از سامانهٔ هوش مصنوعی پرخطر است. به‌کارگیرنده می‌تواند در موارد مشابه، به ارزیابی‌های پیش‌تر انجام‌شده از تأثیر بر حقوق بنیادین یا ارزیابی‌های موجودی که توسط ارائه‌دهنده انجام گرفته است، استناد کند. در صورتی که در جریان استفاده از سامانهٔ هوش مصنوعی پرخطر، به‌کارگیرنده تشخیص دهد که هر یک از عناصر مندرج در بند ۱ تغییر یافته یا دیگر به‌روز نیست، موظف است اقدامات لازم را برای به‌روزرسانی اطلاعات انجام دهد.

۳. پس از انجام ارزیابی مندرج در بند ۱ این ماده، به‌کارگیرنده باید نتایج آن را به مقام ناظر بازار اطلاع دهد و الگوی تکمیل‌شده‌ای را که در بند ۵ این ماده به آن اشاره شده است، به‌عنوان بخشی از فرآیند اطلاع‌رسانی ارائه کند. با این حال، در مواردی که در بند ۱ ماده ۴۶ پیش‌بینی شده است، ممکن است به‌کارگیرندگان از الزام به اطلاع‌رسانی معاف شوند.

۴. در صورتی که هر یک از تعهدات مقرر در این ماده از طریق انجام ارزیابی تأثیر بر حفاظت از داده‌ها بر اساس ماده ۳۵ مقررات شمارهٔ ۲۰۱۶/۶۷۹ یا ماده ۲۷ دستورالعمل ۲۰۱۶/۲۸۰ (اتحادیهٔ اروپا) تحقق یافته باشد، ارزیابی تأثیر بر حقوق بنیادین مذکور در بند ۱ این ماده، مکمل آن ارزیابی حفاظت از داده‌ها خواهد بود.

۵. دفتر هوش مصنوعی موظف است الگوی پرسش‌نامه‌ای (ازجمله به‌صورت ابزار خودکار) تدوین کند تا به‌کارگیرندگان را در انجام ساده‌تر تعهداتشان بر اساس این ماده یاری رساند.

بخش چهارم. مراجع اطلاع‌دهنده و نهادهای اطلاع‌یافته

ماده ۲۸. مراجع اطلاع‌دهنده

۱. هر یک از دولت‌های عضو باید دست‌کم یک مرجع اطلاع‌دهنده را تعیین یا ایجاد کند که مسئولیت ایجاد و اجرای رویه‌های لازم برای ارزیابی، تعیین صلاحیت، اطلاع‌رسانی و نظارت بر نهادهای ارزیابی انطباق را بر عهده دارد. این رویه‌ها باید با همکاری مراجع اطلاع‌دهندهٔ کلیهٔ دولت‌های عضو تدوین شوند.

۲. دولت‌های عضو می‌توانند تصمیم بگیرند که ارزیابی و نظارت مذکور در بند ۱ توسط *نهاد اعتباربخشی ملی*[۱۸۱] انجام شود مشروط بر آنکه مطابق مقررات شمارهٔ ۲۰۰۸/۷۶۵ اتحادیهٔ اروپا

181. National accreditation body

اقدام کند.

۳. مراجع اطلاع‌دهنده باید به گونه‌ای ایجاد، سازمان‌دهی و اداره شوند که هیچ تعارض منافعی با نهادهای ارزیابی انطباق ایجاد نشود و عینیت و بی‌طرفی فعالیت‌های آنان تضمین شود.

۴. ساختار مراجع اطلاع‌دهنده باید به نحوی باشد که تصمیمات مربوط به اطلاع‌رسانی نهادهای ارزیابی انطباق توسط اشخاص صلاحیت‌دارِ متفاوت، یعنی اشخاصی غیر از کسانی که ارزیابی آن نهادها را انجام داده‌اند اتخاذ شود.

۵. مراجع اطلاع‌دهنده نباید هیچ‌گونه فعالیت مشابه با نهادهای ارزیابی انطباق یا خدمات مشاوره‌ای با ماهیت تجاری یا رقابتی ارائه دهند.

۶. مراجع اطلاع‌دهنده موظف‌اند مطابق ماده ۷۸، محرمانگی اطلاعاتی را که به دست می‌آورند حفظ کنند.

۷. مراجع اطلاع‌دهنده باید از تعداد کافی از کارکنان متخصص و واجد صلاحیت برای اجرای صحیح وظایف خود برخوردار باشند. کارکنان متخصص باید در صورت لزوم، دانش و صلاحیت لازم را در حوزه‌هایی چون فناوری اطلاعات، هوش مصنوعی، حقوق و به‌ویژه نظارت بر حقوق بنیادین دارا باشند.

ماده ۲۹. درخواست نهاد ارزیابی انطباق برای اطلاع‌رسانی رسمی

۱. نهادهای ارزیابی انطباق باید درخواست اطلاع‌رسانی رسمی خود را به مرجع اطلاع‌دهندهٔ دولت عضوی که در قلمرو آن مستقر هستند، تسلیم کنند.

۲. درخواست اعلام رسمی باید همراه با موارد زیر باشد: توصیف فعالیت‌های ارزیابی انطباق، ماژول یا ماژول‌های ارزیابی انطباق و انواع سامانه‌های هوش مصنوعی که نهاد ارزیابی انطباق مدعی صلاحیت در خصوص آن‌هاست، گواهی اعتباربخشی (در صورت وجود) صادره از سوی نهاد اعتباربخشی ملی که گواهی می‌دهد نهاد ارزیابی انطباق الزامات مقرر در ماده ۳۱ را رعایت کرده است.

هر سند معتبر مربوط به صلاحیت‌های اعطاشدهٔ موجود آن نهاد طبق سایر قوانین هماهنگ‌ساز اتحادیه که باید به درخواست پیوست شود.

۳. چنانچه نهاد ارزیابی انطباق نتواند گواهی اعتباربخشی ارائه کند، موظف است کلیهٔ مدارک مستند لازم را جهت تأیید، شناسایی و نظارت منظم بر انطباق خود با الزامات ماده ۳۱ در اختیار مرجع اطلاع‌دهنده قرار دهد.

۴. در مورد نهادهای اطلاع‌یافته‌ای که قبلاً طبق سایر قوانین هماهنگ‌ساز اتحادیه تعیین شده‌اند،

کلیهٔ اسناد و گواهی‌های مرتبط با آن صلاحیت‌های اعطا شده می‌توانند حسب مورد برای پشتیبانی از فرآیند اعلام رسمی تحت این قانون به کار روند. نهاد اطلاع‌یافته باید مدارک موضوع بندهای ۲ و ۳ این ماده را هر گاه تغییرات مرتبطی رخ دهد به‌روزرسانی کند تا مرجع مسئول نهادهای اطلاع‌یافته بتواند نظارت و راستی‌آزمایی مستمر بر رعایت همهٔ الزامات مندرج در ماده ۳۱ را انجام دهد.

ماده ۳۰. فرآیند اطلاع‌رسانی

۱. مراجع اطلاع‌دهنده مجازند تنها نهادهای ارزیابی انطباق را به‌صورت رسمی مطلع کنند که الزامات مقرر در ماده ۳۱ را رعایت کرده باشند.

۲. مراجع اطلاع‌دهنده موظف‌اند هر نهاد ارزیابی انطباق موضوع بند ۱ را به کمیسیون و سایر دولت‌های عضو با استفاده از ابزار الکترونیکی اعلام رسمی که توسط کمیسیون توسعه و مدیریت می‌شود، اطلاع دهند.

۳. اطلاع‌رسانی مندرج در بند ۲ این ماده باید شامل جزئیات کامل فعالیت‌های ارزیابی انطباق، ماژول یا ماژول‌های ارزیابی انطباق، انواع سامانه‌های هوش مصنوعی مربوطه و گواهی صلاحیت مرتبط باشد. در مواردی که اعلام رسمی بر اساس گواهی اعتباربخشی موضوع ماده ۲۹(۲) نباشد، مرجع اطلاع‌دهنده باید مدارک مستندی را به کمیسیون و سایر دولت‌های عضو ارائه دهد که صلاحیت نهاد ارزیابی انطباق و سازوکارهای نظارتی مستمر آن را تأیید و تضمین کند که نهاد مذکور به‌طور مستمر الزامات ماده ۳۱ را رعایت خواهد کرد.

۴. نهاد ارزیابی انطباق تنها زمانی مجاز است فعالیت‌های یک نهاد اطلاع‌یافته را انجام دهد که طی مدت دو هفته (در صورت ارائهٔ گواهی اعتباربخشی موضوع ماده ۲۹(۲)) یا دو ماه (در صورت ارائهٔ مدارک مستند موضوع ماده ۲۹(۳)) هیچ اعتراضی از سوی کمیسیون یا سایر دولت‌های عضو مطرح نشده باشد.

۵. در صورتی که اعتراضاتی مطرح شود، کمیسیون باید بدون تأخیر وارد مشورت با دولت‌های عضو ذی‌ربط و نهاد ارزیابی انطباق شود. براساس این مشورت، کمیسیون تصمیم خواهد گرفت که آیا صدور مجوز موجه است یا خیر و تصمیم خود را به دولت عضو مربوطه و نهاد ارزیابی انطباق ذی‌ربط ابلاغ می‌کند.

ماده ۳۱. الزامات مربوط به نهادهای اطلاع‌یافته

۱. هر نهاد اطلاع‌یافته باید بر اساس قوانین ملی یک دولت عضو تأسیس شود و دارای شخصیت

حقوقی مستقل باشد.

۲. نهادهای اطلاع‌یافته باید الزامات مربوط به ساختار سازمانی، مدیریت کیفیت، منابع و فرآیندها را که برای انجام وظایفشان ضروری است، رعایت کنند و همچنین الزامات مناسب امنیت سایبری را تأمین کنند.

۳. ساختار سازمانی، تخصیص وظایف، خطوط گزارش‌دهی و عملکرد نهادهای اطلاع‌یافته باید به گونه‌ای باشد که اعتماد به عملکرد آن‌ها و نتایج فعالیت‌های ارزیابی انطباق که انجام می‌دهند، تضمین شود.

۴. نهادهای اطلاع‌یافته باید در رابطه با نهاد ارزیابی انطباق خود مستقل از ارائه‌دهندهٔ سامانهٔ هوش مصنوعی پرخطر باشند. همچنین نهادهای اطلاع‌یافته باید مستقل از هر اپراتور دیگری که منافع اقتصادی در سامانه‌های هوش مصنوعی پرخطر ارزیابی‌شده و نیز رقبای ارائه‌دهنده باشند. این الزامی‌بودن استقلال، مانع استفاده از سامانه‌های هوش مصنوعی پرخطر ارزیابی‌شده نمی‌شود، اگر استفاده از آن‌ها برای عملیات نهاد ارزیابی انطباق ضروری باشد یا برای مصارف شخصی باشد.

۵. هیچ یک از نهادهای ارزیابی انطباق، مدیران ارشد آن یا پرسنل مسئول انجام وظایف ارزیابی انطباق نباید به‌صورت مستقیم در طراحی، توسعه، بازاریابی یا استفاده از سامانه‌های هوش مصنوعی پرخطر مشارکت داشته باشند و نباید نمایندهٔ طرف‌هایی باشند که در این فعالیت‌ها دخیل‌اند. آن‌ها نباید در هیچ فعالیتی شرکت کنند که ممکن است استقلال رأی یا یکپارچگی آن‌ها در فعالیت‌های ارزیابی انطباق را به خطر اندازد. این الزام، به‌ویژه در خصوص خدمات مشاوره‌ای صادق است.

۶. نهادهای اطلاع‌یافته باید به گونه‌ای سازمان‌دهی و اداره شوند که استقلال، عینیت و بی‌طرفی فعالیت‌های آن‌ها حفظ شود. همچنین باید ساختار و رویه‌هایی مستند داشته باشند و بی‌طرفی را تضمین کرده و اصول بی‌طرفی را در سراسر سازمان، پرسنل و فعالیت‌های ارزیابی اعمال و ترویج کنند.

۷. نهادهای اطلاع‌یافته باید رویه‌های مستند داشته باشند که اطمینان دهد پرسنل، کمیته‌ها، شرکت‌های تابعه، پیمانکاران فرعی و هر نهاد یا پرسنل مرتبط با نهادهای خارجی مطابق ماده ۷۸، محرمانگی اطلاعاتی که در جریان انجام فعالیت‌های ارزیابی انطباق به دست می‌آورند، رعایت شود، مگر آنکه افشای آن طبق قانون الزامی باشد. پرسنل نهادهای اطلاع‌یافته موظف به رعایت اسرار حرفه‌ای در مورد تمام اطلاعات به‌دست‌آمده در انجام وظایف خود طبق این قانون هستند، مگر در ارتباط با مراجع اطلاع‌دهندهٔ دولت عضو که فعالیت‌هایشان در آنجا انجام می‌شود.

۸. نهادهای اطلاع‌یافته باید رویه‌هایی برای انجام فعالیت‌ها داشته باشند که به‌طور شایسته حجم فعالیت ارائه‌دهنده، بخش فعالیت، ساختار آن و درجهٔ پیچیدگی سامانهٔ هوش مصنوعی مربوطه را در نظر بگیرند.

۹. نهادهای اطلاع‌یافته باید بیمهٔ مسئولیت مناسب برای فعالیت‌های ارزیابی انطباق خود داشته باشند، مگر آنکه مسئولیت طبق قانون ملی توسط دولت عضو تأسیس‌کننده به عهده گرفته شده باشد یا آن دولت مستقیماً مسئول انجام ارزیابی انطباق باشد.

۱۰. نهادهای اطلاع‌یافته باید قادر باشند تمام وظایف خود را طبق این قانون با بالاترین سطح یکپارچگی حرفه‌ای و صلاحیت لازم در حوزهٔ مربوطه انجام دهند، چه این وظایف توسط خود نهاد انجام شود یا به نمایندگی از آن و تحت مسئولیت آن واگذار شده باشد.

۱۱. نهادهای اطلاع‌یافته باید صلاحیت‌های داخلی کافی داشته باشند تا بتوانند وظایف انجام‌شده توسط اشخاص خارجی به نمایندگی از خود را به‌طور مؤثر ارزیابی کنند. همچنین نهاد اطلاع‌یافته باید به‌طور دائم از پرسنل اداری، فنی، حقوقی و علمی کافی برخوردار باشد که دارای تجربه و دانش مربوط به انواع سامانه‌های هوش مصنوعی، داده‌ها و پردازش داده‌ها و الزامات مندرج در بخش ۲ باشند.

۱۲. نهادهای اطلاع‌یافته باید در فعالیت‌های هماهنگی مندرج در ماده ۳۸ مشارکت داشته باشند. آن‌ها همچنین باید به‌طور مستقیم یا از طریق نمایندگی در سازمان‌های استانداردسازی اروپایی شرکت یا اطمینان حاصل کنند که از استانداردهای مرتبط آگاه و به‌روز هستند.

ماده ۳۲. فرض انطباق با الزامات مربوط به نهادهای اطلاع‌یافته

چنانچه نهاد ارزیابی انطباق بتواند انطباق خود را با معیارهای مندرج در استانداردهای هماهنگ‌شدهٔ مربوطه یا بخش‌هایی از آن‌ها نشان دهد، به شرط آنکه ارجاعات این استانداردها در روزنامهٔ رسمی اتحادیهٔ اروپا منتشر شده باشد، فرض بر این خواهد بود که نهاد مذکور، الزامات مندرج در ماده ۳۱ را رعایت کرده است تا جایی که استانداردهای هماهنگ‌شدهٔ قابل اعمال، آن الزامات را پوشش دهند.

ماده ۳۳. شرکت‌های تابع نهادهای اطلاع‌یافته و پیمانکار فرعی

۱. هر گاه نهاد اطلاع‌یافته برخی وظایف مرتبط با ارزیابی انطباق را به پیمانکار فرعی واگذار یا از یک شرکت تابعه استفاده کند، باید اطمینان حاصل کند که پیمانکار فرعی یا شرکت تابعه، الزامات مندرج در ماده ۳۱ را رعایت می‌کنند و مرجع اطلاع‌دهنده را در این خصوص مطلع کند.

۲. نهادهای اطلاع‌یافته تمام مسئولیت وظایف انجام‌شده توسط هر پیمانکار فرعی یا شرکت تابعه را بر عهده دارند.

۳. انجام فعالیت‌ها توسط پیمانکار فرعی یا شرکت تابعه تنها با توافق ارائه‌دهنده مجاز است. همچنین نهادهای اطلاع‌یافته باید فهرستی از شرکت‌های تابعهٔ خود را به‌صورت عمومی منتشر کنند.

۴. مدارک مربوط به ارزیابی صلاحیت پیمانکار فرعی یا شرکت تابعه و کارهای انجام‌شده توسط آنان طبق این قانون باید برای مدت پنج سال از تاریخ پایان پیمانکاری در اختیار مرجع اطلاع‌دهنده نگهداری شود.

ماده ۳۴. تعهدات عملیاتی نهادهای اطلاع‌یافته

۱. نهادهای اطلاع‌یافته موظف‌اند انطباق سامانه‌های هوش مصنوعی پرخطر را مطابق فرآیندهای ارزیابی انطباق مندرج در ماده ۴۳ بررسی و تأیید کنند.

۲. نهادهای اطلاع‌یافته باید هنگام انجام فعالیت‌های خود، از ایجاد تعهدات غیرضروری برای ارائه‌دهندگان خودداری کرده و حجم فعالیت ارائه‌دهنده، بخش فعالیت، ساختار آن و درجهٔ پیچیدگی سامانهٔ هوش مصنوعی پرخطر را به‌ویژه به منظور کاهش تعهدات اداری و هزینه‌های انطباق برای شرکت‌های کوچک و خرد مطابق تعریف دستورالعمل ۳۶۱ /۲۰۰۳به‌طور مناسب مدنظر قرار دهند. با این حال، نهاد اطلاع‌یافته باید سطح دقت و حفاظت لازم را برای تضمین انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات این قانون رعایت کند.

۳. نهادهای اطلاع‌یافته موظف‌اند تمام مستندات مرتبط ازجمله مستندات ارائه‌دهندگان را در دسترس قرار داده و در صورت درخواست، به مرجع اطلاع‌دهندهٔ موضوع ماده ۲۸ ارائه کنند تا آن مرجع بتواند فعالیت‌های ارزیابی، تعیین صلاحیت، اعلام رسمی و نظارت خود را انجام دهد و فرآیند ارزیابی مندرج در این بخش را تسهیل کند.

ماده ۳۵. شماره‌های شناسایی و فهرست نهادهای اطلاع‌یافته

۱. کمیسیون موظف است به هر نهاد اطلاع‌یافته یک شمارهٔ شناسایی واحد اختصاص دهد حتی اگر آن نهاد بر اساس بیش از یک قانون اتحادیه اطلاع یافته باشد.

۲. کمیسیون باید فهرست نهادهای اطلاع‌یافته طبق این قانون را شامل شماره‌های شناسایی و فعالیت‌هایی که برای آن‌ها اطلاع‌یافته شده‌اند به‌صورت عمومی در دسترس قرار دهد. کمیسیون موظف است اطمینان حاصل کند که این فهرست به‌روز نگه داشته شود.

ماده ۳۶. تغییرات در اطلاع‌رسانی

۱. مرجع اطلاع‌دهنده موظف است کمیسیون و سایر دولت‌های عضو را در مورد هر گونه تغییر مرتبط در اطلاع‌رسانی یک نهاد اطلاع‌یافته از طریق ابزار الکترونیکی اطلاع‌رسانی موضوع ماده ۳۰(۲) مطلع کند.

۲. رویه‌های مقرر در مواد ۲۹ و ۳۰ برای گسترش دامنهٔ اطلاع‌رسانی اعمال می‌شود. برای تغییرات در اطلاع‌رسانی به‌غیر از گسترش دامنهٔ آن، رویه‌های مندرج در بندهای (۳) تا (۹) اعمال خواهد شد.

۳. هر گاه نهاد تأییدشده تصمیم بگیرد فعالیت‌های ارزیابی انطباق خود را متوقف کند، باید در اسرع وقت و در صورت توقف برنامه‌ریزی‌شده، حداقل یک سال پیش از پایان فعالیت‌های خود، مرجع اعلام‌کننده و ارائه‌دهندگان ذی‌ربط را مطلع کند. گواهی‌نامه‌های صادره از سوی آن نهاد تأییدشده می‌توانند تا مدت نه ماه پس از توقف فعالیت‌های آن نهاد معتبر باقی بمانند، مشروط بر آنکه نهاد تأییدشدهٔ دیگری به‌صورت کتبی تأیید کند که مسئولیت سامانه‌های هوش مصنوعی پرخطرِ مشمول آن گواهی‌نامه‌ها را بر عهده خواهد گرفت. نهاد تأییدشدهٔ اخیر باید ارزیابی کامل سامانه‌های هوش مصنوعی پرخطر مربوطه را تا پایان دورهٔ نه‌ماهه تکمیل و سپس گواهی‌نامه‌های جدید را برای آن سامانه‌ها صادر کند. در صورتی که نهاد تأییدشده فعالیت خود را متوقف کرده باشد، مرجع اعلام‌کننده باید انتصاب آن را لغو کند.

۴. هر گاه مرجع اعلام‌کننده، دلایل کافی برای این نتیجه‌گیری داشته باشد که یک نهاد تأییدشدهٔ دیگر با الزامات مندرج در ماده ۳۱ انطباق ندارد یا از انجام تعهدات خود قصور ورزیده است، باید بدون تأخیر و با نهایت دقت و جدیت، موضوع را بررسی کند. در این چارچوب، مرجع اعلام‌کننده باید نهاد تأییدشدهٔ ذی‌ربط را از ایرادات مطرح‌شده مطلع کرده و به آن فرصت دهد تا دیدگاه‌های خود را ارائه کند. اگر مرجع اعلام‌کننده به این نتیجه برسد که نهاد تأییدشدهٔ دیگر با الزامات مندرج در ماده ۳۱ مطابقت ندارد یا تعهدات خود را انجام نمی‌دهد، باید بر اساس شدت تخلف، در خصوص محدودسازی، تعلیق یا لغو انتصاب آن نهاد، تصمیم مقتضی اتخاذ کند. در این صورت، کمیسیون و سایر کشورهای عضو باید فوراً از تصمیم مذکور مطلع شوند.

۵. در صورتی که انتصاب نهاد تأییدشده به حالت تعلیق درآید، محدود شود یا به‌طور کامل یا جزئی لغو شود، آن نهاد موظف است حداکثر ظرف ده روز، ارائه‌دهندگان ذی‌ربط را از این موضوع آگاه کند.

۶. در صورت محدودسازی، تعلیق یا لغو انتصاب، مرجع اعلام‌کننده باید اقدامات مقتضی را برای حفظ پرونده‌های نهاد تأییدشدهٔ مربوطه اتخاذ کند و این پرونده‌ها را بنا به درخواست، در اختیار

مراجع اعلام‌کنندهٔ سایر کشورهای عضو و مراجع نظارت بر بازار قرار دهد.

۷. در صورت محدودسازی، تعلیق یا لغو انتصاب، مرجع اعلام‌کننده مکلف است:

الف) تأثیر این اقدام بر گواهی‌نامه‌های صادره از سوی نهاد تأییدشده را ارزیابی کند؛

ب) گزارشی از یافته‌های خود را ظرف سه ماه از تاریخ اطلاع‌رسانی تغییرات در انتصاب، به کمیسیون و سایر کشورهای عضو ارسال کند؛

پ) از نهاد تأییدشده بخواهد تا در مهلتی معقول که از سوی مرجع تعیین می‌شود، هر گونه گواهی‌نامه‌ای را که به‌صورت غیرمجاز صادر شده است تعلیق یا لغو کند تا بدین وسیله انطباق مستمر سامانه‌های هوش مصنوعی پرخطر موجود در بازار تضمین شود؛

ت) کمیسیون و کشورهای عضو را از گواهی‌نامه‌هایی که تعلیق یا لغو آن‌ها را الزامی دانسته است، مطلع کند؛

ث) کلیهٔ اطلاعات مرتبط با گواهی‌نامه‌هایی را که تعلیق یا لغو آن‌ها درخواست شده است، در اختیار مرجع صلاحیت‌دار ملی کشور عضوی که ارائه‌دهنده در آن ثبت شده است قرار دهد. آن مرجع، در صورت لزوم، باید اقدامات مقتضی را برای جلوگیری از خطر احتمالی برای سلامت، ایمنی یا حقوق بنیادین اتخاذ کند.

۸. به استثنای گواهی‌نامه‌هایی که به‌صورت غیرمجاز صادر شده‌اند، در مواردی که انتصاب یک نهاد تأییدشده، معلق یا محدود شده باشد، گواهی‌نامه‌های آن نهاد در یکی از شرایط زیر همچنان معتبر باقی می‌مانند:

الف) مرجع اعلام‌کننده ظرف مدت یک ماه از تاریخ تعلیق یا محدودسازی تأیید کرده باشد که هیچ‌گونه خطری برای سلامت، ایمنی یا حقوق بنیادین در ارتباط با گواهی‌نامه‌های مشمول تعلیق یا محدودسازی وجود ندارد و نیز برنامهٔ زمانی مشخصی برای رفع دلایل تعلیق یا محدودسازی ارائه کرده باشد؛

ب) مرجع اعلام‌کننده تأیید کرده باشد که در طول مدت تعلیق یا محدودسازی، هیچ گواهی‌نامهٔ جدیدی مرتبط با موضوع تعلیق صادر، اصلاح یا تمدید نخواهد شد و همچنین اعلام کرده باشد که آیا نهاد تأییدشده توانایی لازم را برای ادامه نظارت و حفظ مسئولیت نسبت به گواهی‌نامه‌های موجود در دورهٔ تعلیق یا محدودسازی دارد یا خیر. در صورتی که مرجع اعلام‌کننده تشخیص دهد نهاد تأییدشده توانایی پشتیبانی از گواهی‌نامه‌های موجود را ندارد، ارائه‌دهندهٔ سامانهٔ مشمول گواهی‌نامه باید ظرف سه ماه از تاریخ تعلیق یا محدودسازی، به‌صورت کتبی به مرجع صلاحیت‌دار ملی کشور عضوی که محل ثبت وی در آن قرار دارد اعلام کند که یک نهاد تأییدشدهٔ واجد صلاحیت دیگر، به‌طور موقت وظایف نظارتی و مسئولیت‌های نهاد تأییدشدهٔ پیشین را در طول مدت تعلیق

یا محدودسازی بر عهده گرفته است.

۹. به استثنای گواهی‌نامه‌هایی که به‌صورت غیرمجاز صادر شده‌اند، در صورتی که انتصاب یک نهاد تأییدشده لغو شود، گواهی‌نامه‌های صادره از سوی آن نهاد می‌توانند به‌مدت نه ماه دیگر معتبر باقی بمانند، مشروط بر تحقق شرایط زیر:

الف) مرجع صلاحیت‌دار ملی کشور عضوی که ارائه‌دهندهٔ سامانهٔ هوش مصنوعی پرخطر و گواهی‌نامه در آن ثبت شده است، تأیید کرده باشد که هیچ‌گونه خطری برای سلامت، ایمنی یا حقوق بنیادین در ارتباط با سامانه‌های هوش مصنوعی مذکور وجود ندارد؛ و

ب) نهاد تأییدشدهٔ دیگری به‌صورت کتبی تأیید کرده باشد که بی‌درنگ مسئولیت آن سامانه‌های هوش مصنوعی را بر عهده می‌گیرد و ارزیابی مربوط را حداکثر ظرف دوازده ماه از تاریخ لغو انتصاب نهاد قبلی تکمیل می‌کند. در شرایط مذکور در بند نخست، مرجع صلاحیت‌دار ملی کشور عضوی که ارائه‌دهندهٔ سامانه در آن به ثبت رسیده است، می‌تواند اعتبار موقت گواهی‌نامه‌ها را برای دوره‌های سه‌ماهه تمدید کند، مشروط بر آنکه مجموع مدت این تمدید از دوازده ماه تجاوز نکند. مرجع صلاحیت‌دار ملی یا نهاد تأییدشده‌ای که وظایف نهاد قبلیِ مشمول لغو انتصاب را بر عهده گرفته است، باید فوراً کمیسیون، سایر کشورهای عضو و دیگر نهادهای تأییدشده را از این موضوع مطلع کند.

ماده ۳۷. تغییرات در اطلاع‌رسانی

۱. کمیسیون در صورت لزوم، در تمامی مواردی که دلایلی برای تردید در صلاحیت یک نهاد تأییدشده یا در تداوم رعایت الزامات مندرج در ماده ۳۱ و مسئولیت‌های مرتبط با آن وجود داشته باشد، تحقیق خواهد کرد.

۲. مرجع اعلام‌کننده موظف است در صورت درخواست کمیسیون، تمامی اطلاعات مرتبط با اعلام یا حفظ صلاحیت نهاد تأییدشدهٔ مربوطه را در اختیار کمیسیون قرار دهد.

۳. کمیسیون باید اطمینان حاصل کند که تمامی اطلاعات حساس به‌دست‌آمده در جریان تحقیقات موضوع این ماده، مطابق ماده ۷۸ به‌صورت محرمانه رسیدگی شود.

۴. چنانچه کمیسیون احراز کند که یک نهاد تأییدشده با الزامات لازم برای اعلام انطباق ندارد یا دیگر آن الزامات را رعایت نمی‌کند، باید کشور عضو اعلام‌کننده را مطلع کرده و از آن بخواهد اقدامات اصلاحی لازم را اتخاذ کند، ازجمله در صورت اقتضا، تعلیق یا لغو اعلامیه. در صورتی که کشور عضو مربوطه اقدامات اصلاحی لازم را انجام ندهد، کمیسیون می‌تواند از طریق *اقدام اجرایی*، انتصاب نهاد مزبور را معلق، محدود یا لغو کند. این اقدام اجرایی باید طبق رویهٔ بررسی مقرر در بند (۲) ماده ۹۸ تصویب شود.

ماده ۳۸. هماهنگی میان نهادهای تأییدشده

۱. کمیسیون باید اطمینان حاصل کند که در خصوص سامانه‌های هوش مصنوعی پرخطر، هماهنگی و همکاری مناسب میان نهادهای تأییدشدهٔ فعال در فرآیندهای ارزیابی انطباقِ موضوع این قانون، برقرار و به‌درستی اجرا شود؛ این همکاری باید در قالب یک گروه و به‌عنوان بخشی از نهادهای تأییدشده، سازمان‌دهی شود.

۲. هر مرجع اعلام‌کننده موظف است اطمینان یابد که نهادهای تأییدشدهٔ تحت صلاحیت آن، مستقیماً یا از طریق نمایندگان تعیین‌شده، در فعالیت‌های گروه مذکور در بند (۱) مشارکت دارند.

۳. کمیسیون باید تبادل دانش و تجربیات برتر میان مراجع اعلام‌کننده را تسهیل و پشتیبانی کند.

ماده ۳۹. نهادهای ارزیابی انطباق کشورهای ثالث

نهادهای ارزیابی انطباق که بر اساس قوانین یک کشور ثالث و با کشوری که اتحادیه با آن توافقنامه‌ای منعقد کرده است تأسیس شده‌اند، می‌توانند مجاز به انجام فعالیت‌های نهادهای تأییدشده طبق این قانون باشند، مشروط بر آنکه الزامات مندرج در ماده ۳۱ را رعایت کنند یا سطح انطباق با الزمات قانونی را تضمین کنند.

بخش پنجم. استانداردها، ارزیابی انطباق، گواهی‌نامه‌ها، ثبت

ماده ۴۰. استانداردهای هماهنگ و نتایج فرآیند استانداردسازی

۱. فرض بر این است که سامانه‌های هوش مصنوعی پرخطر یا مدل‌های هوش مصنوعی عمومی که با استانداردهای هماهنگ یا بخش‌هایی از آن مطابقت دارند و مراجع آن‌ها طبق مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ در روزنامهٔ رسمی اتحادیهٔ اروپا منتشر شده‌اند، با الزامات مندرج در بخش ۲ این فصل مطابقت دارند یا در صورت لزوم با تعهدات مندرج در فصل پنجم، بخش‌های ۲ و ۳ این قانون، تا حدی که آن استانداردها شامل این الزامات یا تعهدات باشد، منطبق هستند.

۲. مطابق ماده ۱۰ مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا، کمیسیون باید بدون تأخیر غیرضروری، درخواست‌های استانداردسازی را صادر کند که شامل تمامی الزامات مندرج در بخش ۲ این فصل یا در صورت لزوم، درخواست‌های استانداردسازی شامل تعهدات مندرج در فصل پنجم بخش‌های ۲ و ۳ این قانون باشد. همچنین خروجی‌های استانداردسازی باید مرتبط با فرآیندهای گزارش‌دهی و مستندسازی برای بهبود عملکرد منابع سامانه‌های هوش مصنوعی ازجمله کاهش مصرف انرژی و سایر منابع توسط سامانه‌های هوش مصنوعی پرخطر در طول چرخهٔ عمر آن‌ها و توسعه

و بهره‌وری انرژی مدل‌های هوش مصنوعی عمومی باشد. در هنگام تهیهٔ درخواست استانداردسازی، کمیسیون باید با هیئت و ذی‌نفعان مرتبط ازجمله مجمع مشورتی مشورت کند.

۳. شرکت‌کنندگان در فرآیند استانداردسازی باید سرمایه‌گذاری و نوآوری در حوزهٔ هوش مصنوعی را ترویج دهند، ازجمله افزایش اطمینان حقوقی و همچنین ارتقاء رقابت‌پذیری و رشد بازار اتحادیه به منظور تقویت همکاری‌های جهانی در زمینهٔ استانداردسازی با درنظرگرفتن استانداردهای بین‌المللی موجود در حوزهٔ هوش مصنوعی که با ارزش‌ها، حقوق بنیادین و منافع اتحادیه همخوانی دارند و همچنین تقویت حاکمیت چندطرفه به گونه‌ای که نمایندگی متوازن منافع و مشارکت مؤثر تمامی ذی‌نفعان مرتبط مطابق مواد ۵، ۶ و ۷ مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا تضمین شود.

ماده ۴۱. مشخصات مشترک

۱. کمیسیون می‌تواند از طریق اقدامات اجرایی، مشخصات مشترک برای الزامات مندرج در بخش ۲ این فصل یا در صورت لزوم، برای تعهدات مندرج در بخش‌های ۲ و ۳ فصل پنجم تدوین و تصویب کند، مشروط بر آنکه شرایط زیر محقق شده باشد:

الف) کمیسیون مطابق بند (۱) ماده ۱۰ مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا، از یک یا چند سازمان استانداردسازی اروپایی درخواست کرده باشد تا استاندارد هماهنگ برای الزامات مندرج در بخش ۲ این فصل یا در صورت لزوم برای تعهدات مندرج در بخش‌های ۲ و ۳ فصل پنجم تهیه کنند و:

۱) درخواست مذکور توسط هیچ‌یک از سازمان‌های استانداردسازی اروپایی پذیرفته نشده باشد؛

۲) استانداردهای هماهنگی که به آن درخواست پاسخ می‌دهند در مهلت مقرر مطابق بند (۱) ماده ۱۰ مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا ارائه نشده‌اند؛

۳) استانداردهای هماهنگ مربوط به‌طور ناکافی به مسائل مرتبط با حقوق بنیادین پرداخته‌اند؛

۴) استانداردهای هماهنگ با محتوای درخواست مطابقت ندارند؛

ب) هیچ ارجاعی به استانداردهای هماهنگ که الزامات مندرج در بخش ۲ این فصل یا در صورت لزوم، تعهدات مندرج در بخش‌های ۲ و ۳ فصل پنجم را پوشش دهند طبق مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا منتشر نشده است و انتظار نمی‌رود که چنین ارجاعی ظرف مدت معقول منتشر شود. هنگام تهیهٔ مشخصات مشترک، کمیسیون باید با مجمع مشورتیِ ذکرشده در ماده ۶۷ مشورت کند. اقدامات اجرایی مذکور در بند نخست این ماده باید مطابق رویهٔ بررسی مقرر در بند (۲) ماده ۹۸ اعمال شوند.

۲. پیش از تهیهٔ پیش‌نویس اقدام اجرایی، کمیسیون باید کمیتهٔ مذکور در ماده ۲۲ مقررات

شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا را مطلع کند که شرایط مندرج در بند ۱ این ماده را مدنظر قرار دهد.

۳. فرض بر این است که سامانه‌های هوش مصنوعی پرخطر یا مدل‌های هوش مصنوعی عمومی که با مشخصات مشترک مندرج در بند ۱ یا بخشی‌هایی از آن مطابقت دارند، با الزامات مندرج در بخش ۲ این فصل یا در صورت لزوم با تعهدات مندرج در بخش‌های ۲ و ۳ فصل پنجم مطابقت دارند، تا حدی که آن مشخصات مشترک شامل این الزامات یا تعهدات باشند.

۴. هر گاه استاندارد هماهنگ توسط سازمان استانداردسازی اروپایی تصویب شده و برای انتشار مرجع آن در روزنامهٔ رسمی اتحادیهٔ اروپا به کمیسیون پیشنهاد شود، کمیسیون باید استاندارد هماهنگ را مطابق مقررات شمارهٔ ۲۰۱۲/۱۰۲۵ اتحادیهٔ اروپا ارزیابی کند. هنگامی که ارجاع به استاندارد هماهنگ در روزنامهٔ رسمی اتحادیهٔ اروپا منتشر شود، کمیسیون باید اقدامات اجرایی مذکور در بند ۱ یا بخش‌هایی از آن را که همان الزامات مندرج در بخش ۲ این فصل یا در صورت لزوم، همان تعهدات مندرج در بخش‌های ۲ و ۳ فصل پنجم را پوشش می‌دهند، لغو کند.

۵. هر گاه ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر یا مدل‌های هوش مصنوعی عمومی با مشخصات مشترک مندرج در بند ۱ مطابقت نداشته باشند، آن‌ها باید به‌طور موجه توضیح دهند که راهکارهای فنی آن‌ها الزامات مندرج در بخش ۲ این فصل یا در صورت لزوم، تعهدات مندرج در بخش‌های ۲ و ۳ فصل پنجم را مطابق الزمات مزبور رعایت می‌کنند.

۶. هر گاه کشور عضو تشخیص دهد که مشخصات مشترک به‌طور کامل الزامات مندرج در بخش ۲ یا در صورت لزوم، تعهدات مندرج در بخش‌های ۲ و ۳ فصل پنجم را برآورده نمی‌کند، باید کمیسیون را با توضیحی دقیق، از این موضوع مطلع کند. کمیسیون موظف است آن اطلاعات را ارزیابی و در صورت مقتضی، اقدام اجرایی مربوط به مشخصات مشترک مذکور را اصلاح کند.

ماده ۴۲. فرض انطباق با برخی الزامات

۱. فرض بر این است که سامانه‌های هوش مصنوعی پرخطر که بر اساس داده‌ها آزمایش شده‌اند و نشان‌دهندهٔ شرایط جغرافیایی، رفتاری، زمینه‌ای یا عملکردی مشخصی هستند که قرار است در آن استفاده شوند، با الزامات مربوط مندرج در ماده ۱۰ بند ۴ مطابقت دارند.

۲. فرض بر این است که سامانه‌های هوش مصنوعی پرخطر که تأیید شده‌اند یا برای آن‌ها گواهی انطباق بر اساس طرح امنیت سایبری مندرج در مقررات شمارهٔ ۲۰۱۹/۸۸۱ اتحادیهٔ اروپا صادر و مراجع آن‌ها در روزنامهٔ رسمی اتحادیهٔ اروپا منتشر شده‌اند، با الزامات امنیت سایبری مندرج در

ماده ۱۵ این قانون مطابقت دارند تا حدی که گواهی امنیت سایبری یا گواهی انطباق یا بخش‌هایی از آن‌ها، آن الزامات را پوشش دهند.

ماده ۴۳. ارزیابی انطباق

۱. برای سامانه‌های هوش مصنوعی پرخطر مندرج در پیوست سه، در صورتی که ارائه‌دهنده برای اثبات انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در بخش ۲، از استانداردهای هماهنگ مندرج در ماده ۴۰ یا در صورت لزوم، مشخصات مشترک مندرج در ماده ۴۱ استفاده کرده باشد، ارائه‌دهنده باید یکی از روش‌های ارزیابی انطباق زیر را انتخاب کند و بر اساس این روش‌ها باشد:

الف) کنترل داخلی مندرج در پیوست ۴؛ یا

ب) ارزیابی سیستم مدیریت کیفیت و ارزیابی مستندات فنی با مشارکت نهاد تأییدشدهٔ مندرج در پیوست ۷.

در اثبات انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در بخش ۲، ارائه‌دهنده باید روش ارزیابی انطباق مندرج در پیوست ۷ را بر اساس شرایط زیر دنبال کند:

۱) استانداردهای هماهنگ مندرج در ماده ۴۰ وجود ندارد و مشخصات مشترک مندرج در ماده ۴۱ نیز در دسترس نیست؛

۲) ارائه‌دهنده، استانداردهای هماهنگ‌شده را اعمال نکرده یا تنها بخشی از آن را اعمال کرده است؛

۳) مشخصات مشترک مندرج در بند (الف) وجود دارد، اما ارائه‌دهنده آن‌ها را اعمال نکرده است؛

۴) یک یا چند استاندارد هماهنگ مندرج در بند (الف) با محدودیت منتشر شده‌اند و محدودیت تنها بر بخشی از استاندارد اعمال شده است. برای اهداف روش ارزیابی انطباق مندرج در پیوست ۷، ارائه‌دهنده می‌تواند هر یک از نهادهای تأییدشده را انتخاب کند. با این حال، در صورتی که قرار است سامانهٔ هوش مصنوعی پرخطر توسط مقامات اجرای قانون، مهاجرت یا پناهندگی یا توسط مؤسسات، نهادها، دفاتر یا آژانس‌های اتحادیه به کار گرفته شود، مرجع نظارت بر بازار مندرج در بندهای (۸) یا (۹) ماده ۷۴ به‌عنوان نهاد تأییدشده عمل خواهد کرد.

۲. برای سامانه‌های هوش مصنوعی پرخطر مندرج در بندهای ۲ تا ۸ پیوست ۳، ارائه‌دهندگان باید روش ارزیابی انطباق مبتنی بر کنترل داخلی مندرج در پیوست ۴ را دنبال کنند که مشارکت نهاد تأییدشده در آن پیش‌بینی نشده است.

۳. در مورد سامانه‌های هوش مصنوعی پرخطر که مشمول قوانین هماهنگ‌شدهٔ اتحادیه (مندرج در بخش (الف) از پیوست شمارهٔ یک) هستند، ارائه‌دهنده باید رویهٔ ارزیابی انطباق مربوط

را مطابق الزامات مقرر در آن اسناد حقوقی دنبال کند. الزامات مندرج در بخش دوم این فصل نیز در خصوص آن دسته از سامانه‌های هوش مصنوعی پرخطر اعمال می‌شود و بخشی از فرآیند ارزیابی مذکور به شمار می‌آید. همچنین بندهای ۴.۳، ۴.۴، ۴.۵ و بند پنجم از بند ۴.۶ پیوست هفتم نیز در این زمینه قابل اجرا هستند.

برای مقاصد این ارزیابی، *نهادهای اطلاع‌رسانی‌شده*[۱۸۲] که بر اساس اسناد حقوقی مذکور اطلاع‌رسانی شده‌اند، حق خواهند داشت انطباق سامانه‌های هوش مصنوعی پرخطر با الزامات مندرج در بخش دوم را کنترل کنند، مشروط بر آنکه رعایت الزامات مندرج در بندهای ۴، ۵، ۱۰ و ۱۱ ماده ۳۱ از سوی آن نهادها، در چارچوب فرآیند اطلاع‌رسانی طبق همان اسناد حقوقی ارزیابی شده باشد.

در صورتی که یکی از اسناد حقوقی مندرج در بخش (الف) پیوست شمارهٔ یک، به تولیدکنندهٔ محصول اجازه دهد تا در صورت به‌کارگیری تمامی استانداردهای هماهنگ با کلیهٔ الزامات مربوطه، از انجام ارزیابی انطباق توسط شخص ثالث صرف‌نظر کند، تولیدکننده صرفاً زمانی می‌تواند از این گزینه استفاده کند که علاوه بر آن، استانداردهای هماهنگ یا در صورت اقتضا، مشخصات مشترک موضوع ماده ۴۱ را که تمام الزامات مندرج در بخش دوم این فصل را پوشش می‌دهد نیز به کار گرفته باشد.

۴. سامانه‌های هوش مصنوعی پرخطری که پیش‌تر تحت رویهٔ ارزیابی انطباق قرار گرفته‌اند، در صورت اعمال تغییرات اساسی باید مجدداً تحت فرآیند جدید ارزیابی انطباق قرار گیرند؛ فارغ از اینکه سامانهٔ اصلاح‌شده برای توزیع مجدد در نظر گرفته شده باشد یا همچنان توسط کاربر فعلی مورد استفاده قرار گیرد. در مورد سامانه‌های هوش مصنوعی پرخطری که پس از عرضه به بازار یا به‌کارگیری، همچنان قابلیت یادگیری دارند، تغییراتی که در عملکرد سامانه ایجاد می‌شود و از پیش توسط ارائه‌دهنده در زمان انجام نخستین ارزیابی انطباق تعیین شده و در اسناد فنی موضوع بند ۲(و) پیوست چهارم درج شده است، تغییر اساسی محسوب نمی‌شود.

۵. کمیسیون اختیار دارد اعمال تفویضی را مطابق ماده ۹۷ تصویب کند تا پیوست‌های ششم و هفتم را با توجه به پیشرفت‌های فنی مورد بازنگری و به‌روزرسانی قرار دهد.

۶. کمیسیون اختیار دارد اعمال تفویضی را طبق ماده ۹۷ تصویب کند تا بندهای ۱ و ۲ این ماده را اصلاح کند، به نحوی که سامانه‌های هوش مصنوعی پرخطری که در بندهای ۲ تا ۸ پیوست سوم ذکر شده‌اند، مشمول رویهٔ ارزیابی انطباق مندرج در پیوست هفتم یا بخش‌هایی از آن شوند. کمیسیون باید این اعمال تفویضی را با درنظرگرفتن کارآمدی رویهٔ ارزیابی انطباق مبتنی بر کنترل داخلی (موضوع پیوست ششم) در پیشگیری یا کاهش خطرات علیه سلامت و ایمنی و حمایت از

182. Notified bodies

حقوق بنیادین ناشی از چنین سامانه‌هایی، و نیز با توجه به در دسترس‌بودن ظرفیت‌ها و منابع کافی در میان نهادهای اطلاع‌رسانی‌شده تصویب کند.

ماده ۴۴. گواهی‌ها

۱. گواهی‌هایی که توسط نهادهای اطلاع‌رسانی‌شده مطابق پیوست هفتم صادر می‌شوند، باید به زبانی تنظیم شوند که برای مقامات ذی‌ربط در کشور عضو محل استقرار نهاد اطلاع‌رسانی‌شده، به‌راحتی قابل درک باشد.

۲. گواهی‌ها برای مدتی معتبر خواهند بود که در خود گواهی قید شده است. با این حال، این مدت برای سامانه‌های هوش مصنوعی مشمول پیوست اول، نباید از پنج سال و برای سامانه‌های مشمول پیوست سوم، از چهار سال تجاوز کند. بنا به درخواست ارائه‌دهنده، ممکن است اعتبار گواهی برای دوره‌های بعدی نیز تمدید شود، مشروط بر آنکه هر دورهٔ تمدید از پنج سال برای سامانه‌های مندرج در پیوست اول و چهار سال برای سامانه‌های مندرج در پیوست سوم فراتر نرود و تمدید یادشده بر اساس ارزیابی مجدد مطابق رویه‌های ارزیابی انطباق قابل اعمال انجام گیرد. هر گونه پیوست یا مکمل گواهی تا زمانی معتبر است که گواهی اصلی که به آن پیوست شده اعتبار داشته باشد.

۳. هر گاه نهاد اطلاع‌رسانی‌شده تشخیص دهد که سامانهٔ هوش مصنوعی دیگر با الزامات مندرج در بخش دوم مطابقت ندارد، باید با رعایت اصل تناسب، گواهی صادرشده را معلق یا ابطال یا محدودیت‌هایی بر آن اعمال کند، مگر آنکه ارائه‌دهندهٔ سامانه با اقدامات اصلاحی مناسب در مهلت مقتضی تعیین‌شده از سوی نهاد اطلاع‌رسانی‌شده، انطباق با الزامات را تضمین کرده باشد. نهاد اطلاع‌رسانی‌شده باید دلایل تصمیم خود را اعلام کند. فرآیند تجدیدنظر (اعتراض) نسبت به تصمیمات نهادهای اطلاع‌رسانی‌شده، ازجمله در مورد گواهی‌های انطباق صادرشده باید در دسترس باشد.

ماده ۴۵. تعهدات اطلاع‌رسانی نهادهای اطلاع‌رسانی‌شده

۱. نهادهای اطلاع‌رسانی‌شده باید مرجع اطلاع‌دهنده[۱۸۳] را از موارد زیر آگاه کنند:

الف) هر گونه گواهی ارزیابی مستندات فنی اتحادیهٔ اروپا، پیوست یا مکمل مربوط به آن گواهی‌ها و نیز هر گونه تأییدیهٔ نظام مدیریت کیفیت که مطابق الزامات مندرج در پیوست هفتم صادر شده باشد؛

183. Notifying Authority

ب) هر گونه رد، محدودسازی، تعلیق یا ابطال گواهی ارزیابی مستندات فنی اتحادیه یا تأییدیهٔ نظام مدیریت کیفیت صادرشده طبق الزامات پیوست هفتم؛

پ) هر گونه وضعیت یا شرایطی که بر دامنه یا شرایط اطلاع‌رسانی اثر بگذارد؛

ت) هر درخواست اطلاعاتی که از سوی مقامات نظارت بر بازار در خصوص فعالیت‌های ارزیابی انطباق دریافت کرده باشند؛

ث) بنا به درخواست، فعالیت‌های ارزیابی انطباق انجام‌شده در محدودهٔ اطلاع‌رسانی آن‌ها و نیز هر گونه فعالیت دیگر ازجمله فعالیت‌های برون‌مرزی یا واگذارشده به پیمانکاران فرعی.

۲. هر نهاد اطلاع‌رسانی‌شده باید سایر نهادهای اطلاع‌رسانی‌شده را از موارد زیر مطلع کند:

الف) تأییدیه‌های نظام مدیریت کیفیت که رد، معلق یا ابطال کرده است و در صورت درخواست، تأییدیه‌های صادرشده را نیز اطلاع دهد؛

ب) گواهی‌های ارزیابی مستندات فنی اتحادیه یا هر گونه پیوست آن‌ها که رد، ابطال، تعلیق یا به هر نحو محدود کرده است و در صورت درخواست، گواهی‌ها و/یا ضمایم صادرشده را نیز اطلاع دهد.

۳. هر نهاد اطلاع‌رسانی‌شده باید اطلاعات مرتبط دربارهٔ نتایج منفی و در صورت درخواست، نتایج مثبت ارزیابی انطباق را در اختیار سایر نهادهای اطلاع‌رسانی‌شده‌ای قرار دهد که فعالیت‌های مشابه ارزیابی انطباق را در خصوص انواع سامانه‌های هوش مصنوعی انجام می‌دهند.

۴. نهادهای اطلاع‌رسانی‌شده باید محرمانگی اطلاعاتی را که به دست می‌آورند مطابق ماده ۷۸ حفظ کنند.

ماده ۴۶. استثنا از رویهٔ ارزیابی انطباق

۱. به‌عنوان استثنا از ماده ۴۳ و بنا به درخواست موجه و مستند، هر مقام نظارت بر بازار می‌تواند اجازه دهد که سامانه‌های هوش مصنوعی پرخطر خاصی در قلمرو کشور عضو مربوط، به دلایل استثنایی مربوط به امنیت عمومی، حفاظت از جان و سلامت اشخاص، حفاظت از محیط‌زیست یا صیانت از دارایی‌های کلیدی صنعتی و زیربنایی، وارد بازار شده یا به کار گرفته شوند. این مجوز باید برای مدت محدودی صادر شود تا در طول آن، رویه‌های لازم ارزیابی انطباق در حال انجام باشند. با لحاظ دلایل استثنایی که صدور استثنا را توجیه می‌کنند، تکمیل این رویه‌ها باید بدون تأخیر غیرموجه صورت گیرد.

۲. در شرایط فوریت موجه به دلایل استثنایی مرتبط با امنیت عمومی یا در صورت وجود تهدیدی خاص، جدی و قریب‌الوقوع علیه جان یا امنیت جسمانی اشخاص، مقامات اجرای قانون یا مقامات

حفاظت مدنی می‌توانند سامانهٔ هوش مصنوعی پرخطر خاص را بدون دریافت مجوز موضوع بند ۱ به کار گیرند، مشروط بر آنکه درخواست مجوز مذکور در حین استفاده یا بلافاصله پس از آن بدون تأخیر غیرموجه ارائه شود.

اگر مجوز موضوع بند ۱ رد شود، استفاده از سامانهٔ هوش مصنوعی پرخطر باید فوراً متوقف و تمامی نتایج و خروجی‌های حاصل از آن استفاده نیز بلافاصله حذف شود.

۳. مجوز موضوع بند ۱ تنها در صورتی صادر می‌شود که مقام نظارت بر بازار به این نتیجه برسد که سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در بخش دوم مطابقت دارد. مقام نظارت بر بازار باید کمیسیون و سایر کشورهای عضو را از هر گونه مجوز صادرشده طبق بندهای ۱ و ۲ مطلع کند. این تعهد اطلاع‌رسانی شامل داده‌های عملیاتی حساس مربوط به فعالیت‌های مقامات اجرای قانون نخواهد شد.

۴. اگر ظرف ۱۵ روز تقویمی از تاریخ دریافت اطلاعات موضوع بند ۳، هیچ اعتراضی از سوی هیچ کشور عضو یا کمیسیون نسبت به مجوز صادرشده از سوی مقام نظارت بر بازار کشور عضو (مطابق بند ۱) مطرح نشود، آن مجوز معتبر و موجه تلقی خواهد شد.

۵. در صورتی که ظرف همان مهلت ۱۵ روز تقویمی، کشوری عضو به مجوز صادرشده از سوی مقام نظارت بر بازار کشور دیگر اعتراض کند یا کمیسیون تشخیص دهد که مجوز با حقوق اتحادیه مغایرت دارد یا نتیجه‌گیری کشور عضو دربارهٔ انطباق سامانه (موضوع بند ۳) بی‌اساس است، کمیسیون باید بی‌درنگ با کشور عضو ذی‌ربط وارد مشورت شود. اپراتورهای مربوط نیز باید مورد مشورت قرار گیرند و فرصت ارائهٔ دیدگاه‌های خود را داشته باشند. با توجه به نتایج این مشورت‌ها، کمیسیون تصمیم می‌گیرد که آیا مجوز صادرشده موجه است یا خیر. تصمیم کمیسیون به کشور عضو ذی‌ربط و اپراتورهای مربوطه ابلاغ می‌شود.

۶. اگر کمیسیون مجوز را ناموجه تشخیص دهد، مقام نظارت بر بازار کشور عضو مربوطه باید آن را ابطال کند.

۷. در مورد سامانه‌های هوش مصنوعی پرخطری که مرتبط با محصولات مشمول قوانین هماهنگ‌شدهٔ اتحادیه مندرج در بخش (الف) پیوست شمارهٔ یک هستند، صرفاً استثناهای پیش‌بینی‌شده از رویهٔ ارزیابی انطباق در همان قوانین هماهنگ‌شدهٔ اتحادیه قابل اعمال خواهد بود.

ماده ۴۷. اعلامیهٔ انطباق اتحادیهٔ اروپا[۱۸۴]

۱. ارائه‌دهنده باید برای هر سامانهٔ هوش مصنوعی پرخطر، اعلامیهٔ انطباق اتحادیهٔ اروپا

184. EU Declaration of Conformity

به‌صورت مکتوب، قابل خوانش توسط ماشین، فیزیکی یا دارای امضای الکترونیکی تنظیم کند و آن را به‌مدت ۱۰ سال پس از عرضهٔ سامانه به بازار یا آغاز بهره‌برداری از آن در دسترس مقامات صلاحیت‌دار ملی نگه دارد. اعلامیهٔ انطباق اتحادیهٔ اروپا باید سامانهٔ هوش مصنوعی پرخطری را که برای آن صادر شده، شناسایی کند. یک نسخه از این اعلامیه باید بنا به درخواست، به مقامات صلاحیت‌دار ملی مربوطه ارائه شود.

۲. اعلامیهٔ انطباق اتحادیهٔ اروپا باید تصریح کند که سامانهٔ هوش مصنوعی پرخطر مربوطه با الزامات مندرج در بخش دوم مطابقت دارد. این اعلامیه باید اطلاعات مندرج در پیوست پنجم را دربرداشته و به زبانی ترجمه شود که برای مقامات صلاحیت‌دار ملی کشورهای عضو محل عرضه یا دسترسی سامانه به‌راحتی قابل درک باشد.

۳. در صورتی که سامانه‌های هوش مصنوعی پرخطر مشمول سایر قوانین هماهنگ‌سازی اتحادیهٔ اروپا نیز باشند که صدور اعلامیهٔ انطباق اتحادیه را الزام می‌کنند، باید یک اعلامیهٔ واحد در خصوص تمامی قوانین اتحادیه قابل اعمال بر آن سامانه تنظیم شود. این اعلامیه باید شامل تمام اطلاعات لازم برای شناسایی قوانین هماهنگ‌شدهٔ اتحادیه مربوطه باشد.

۴. با تنظیم اعلامیهٔ انطباق اتحادیهٔ اروپا، ارائه‌دهنده مسئولیت انطباق با الزامات مندرج در بخش دوم را بر عهده می‌گیرد. ارائه‌دهنده باید اعلامیهٔ انطباق را حسب مورد به‌روز نگه دارد.

۵. کمیسیون اختیار دارد طبق ماده ۹۷، اعمال تفویضی را به منظور اصلاح پیوست پنجم تصویب کند تا محتوای اعلامیهٔ انطباق اتحادیهٔ اروپا را با توجه به پیشرفت‌های فنی به‌روزرسانی کرده و عناصر جدید لازم را در آن بگنجاند.

ماده ۴۸. علامت CE

۱. علامت CE تابع اصول کلی مندرج در ماده ۳۰ مقررات شمارهٔ ۲۰۰۸/۷۶۵ اتحادیهٔ اروپا خواهد بود.

۲. برای سامانه‌های هوش مصنوعی پرخطر که به‌صورت دیجیتال ارائه می‌شوند، علامت CE دیجیتال باید استفاده شود، مشروط بر اینکه به‌راحتی از طریق رابط کاربری که سامانه از آن دسترسی دارد یا از طریق کد قابل خوانش توسط ماشین یا سایر روش‌های الکترونیکی قابل دسترسی باشد.

۳. علامت CE باید برای سامانه‌های هوش مصنوعی پرخطر به‌صورت قابل مشاهده، خوانا و غیرقابل پاک‌شدن نصب شود. در صورتی که این امر ممکن نباشد یا به دلیل ماهیت سامانه ضروری

نباشد، علامت باید روی بسته‌بندی یا اسناد همراه آن بسته به مورد نصب شود.

۴. در صورت لزوم، پس از علامت CE، شمارهٔ شناسایی نهاد اطلاع‌رسانی‌شدهٔ مسئول رویه‌های ارزیابی انطباق مندرج در ماده ۴۳ نیز باید درج شود. شمارهٔ شناسایی نهاد اطلاع‌رسانی‌شده باید توسط خود نهاد یا طبق دستور آن، توسط ارائه‌دهنده یا نمایندهٔ مجاز ارائه‌دهنده نصب شود. همچنین این شماره باید در هر گونه مواد تبلیغاتی که به انطباق سامانهٔ هوش مصنوعی پرخطر با الزامات علامت CE اشاره دارد ذکر شود.

۵. در صورتی که سامانه‌های هوش مصنوعی پرخطر مشمول سایر قوانین اتحادیهٔ اروپا باشند که نصب علامت CE را پیش‌بینی می‌کنند، علامت CE باید نشان دهد که سامانهٔ هوش مصنوعی پرخطر، الزامات آن قوانین دیگر را نیز رعایت می‌کند.

ماده ۴۹. ثبت سامانه‌ها

۱. پیش از عرضه به بازار یا به‌کارگیری سامانهٔ هوش مصنوعی پرخطر مندرج در پیوست سوم به استثنای سامانه‌های پرخطر موضوع بند دوم از پیوست سوم، ارائه‌دهنده یا در صورت لزوم، نمایندهٔ مجاز او باید خود و سامانهٔ مربوطه را در پایگاه دادهٔ اتحادیهٔ اروپا موضوع ماده ۷۱ ثبت کنند.

۲. پیش از عرضه به بازار یا به‌کارگیری سامانه‌ای که ارائه‌دهنده آن را مطابق ماده ۶ (۳)پرخطر تشخیص نداده است، ارائه‌دهنده یا نمایندهٔ مجاز او باید خود و سامانه را در پایگاه دادهٔ اتحادیهٔ اروپا موضوع ماده ۷۱ ثبت کنند.

۳. پیش از به‌کارگیری یا استفاده از سامانهٔ هوش مصنوعی پرخطر مندرج در پیوست سوم، به استثنای سامانه‌های موضوع بند ۲ پیوست سوم، استفاده‌کنندگان که شامل مقامات عمومی، نهادها، مؤسسات، دفاتر یا آژانس‌های اتحادیهٔ اروپا یا اشخاص عمل‌کننده به نمایندگی از آن‌ها هستند، باید خود را ثبت کرده، سامانه را انتخاب و استفادهٔ آن را در پایگاه دادهٔ اتحادیهٔ اروپا موضوع ماده ۷۱ ثبت کنند.

۴. برای سامانه‌های هوش مصنوعی پرخطر مندرج در بندهای ۱، ۶ و ۷ پیوست سوم، در حوزه‌های اجرای قانون، مهاجرت، پناهندگی و مدیریت کنترل مرزی، ثبت موضوع بندهای ۱، ۲ و ۳ این ماده باید در بخش غیرعمومی و امن پایگاه دادهٔ اتحادیهٔ اروپا موضوع ماده ۷۱ انجام شود و تنها شامل اطلاعات زیر باشد (حسب مورد):

الف) بخش (الف)، بندهای ۱ تا ۱۰ پیوست هشتم، با استثنای بندهای ۶، ۸ و ۹؛

ب) بخش (ب)، بندهای ۱ تا ۵ و بندهای ۸ و ۹ پیوست هشتم؛

پ) بخش (ج)، بندهای ۱ تا ۳ پیوست هشتم؛

ت) بندهای ۱، ۲، ۳ و ۵ پیوست نهم.

تنها کمیسیون و مقامات ملی موضوع ماده ۷۴(۸) مجاز به دسترسی به بخش‌های محدود پایگاه دادهٔ اتحادیهٔ اروپا هستند که در پاراگراف قبل اشاره شد.

۵. سامانه‌های هوش مصنوعی پرخطر موضوع بند ۲ پیوست سوم باید در سطح ملی ثبت شوند.

فصل چهارم. تعهدات شفافیت برای ارائه‌دهندگان و استفاده‌کنندگان برخی سامانه‌های هوش مصنوعی

ماده ۵۰. تعهدات شفافیت برای ارائه‌دهندگان و استفاده‌کنندگان برخی سامانه‌های هوش مصنوعی

۱. ارائه‌دهندگان باید اطمینان حاصل کنند که سامانه‌های هوش مصنوعی که به‌طور مستقیم با اشخاص طبیعی تعامل دارند به گونه‌ای طراحی شده و توسعه یافته باشند که اشخاص طبیعی مطلع شوند که با سامانهٔ هوش مصنوعی تعامل دارند، مگر اینکه این موضوع از دیدگاه یک شخص طبیعی نسبتاً آگاه، دقیق و محتاط، با توجه به شرایط و زمینهٔ استفاده آشکار باشد. این تعهد شامل سامانه‌های هوش مصنوعی مجاز توسط قانون برای تشخیص، پیشگیری، تحقیق یا پیگرد جرایم نمی‌شود، مشروط بر آنکه ضمانت‌های مناسب برای حقوق و آزادی‌های اشخاص ثالث رعایت شود، مگر آنکه سامانه‌ها برای گزارش‌دهی عمومی جرایم در دسترس عموم باشند.

۲. ارائه‌دهندگان سامانه‌های هوش مصنوعی، ازجمله سامانه‌های هوش مصنوعی با هدف عمومی که محتوای صوتی، تصویری، ویدیویی یا متنی تولید یا دستکاری می‌کنند، باید اطمینان حاصل کنند که خروجی‌های سامانه به‌صورت قابل خوانش توسط ماشین علامت‌گذاری شده و قابل تشخیص به‌عنوان تولید یا دستکاری مصنوعی باشند. ارائه‌دهندگان باید اطمینان دهند که راه‌حل‌های فنی آن‌ها مؤثر، قابل تعامل، مقاوم و قابل اعتماد و تا حد امکان از نظر فنی، با درنظرگرفتن ویژگی‌ها و محدودیت‌های انواع مختلف محتوا، هزینه‌های پیاده‌سازی و وضعیت فناوری مورد تأیید باشند، همان طور که در استانداردهای فنی مربوطه منعکس شده است. این تعهد شامل سامانه‌هایی نمی‌شود که صرفاً عملکرد کمکی برای ویرایش استاندارد انجام می‌دهند یا داده‌های ورودی ارائه‌شده توسط استفاده‌کننده یا معنای آن‌ها را به‌طور قابل‌توجهی تغییر نمی‌دهند، یا زمانی که توسط قانون برای تشخیص، پیشگیری، تحقیق یا پیگرد جرایم مجاز باشند.

۳. استفاده‌کنندگان سامانه‌های تشخیص احساسات یا دسته‌بندی زیست‌سنجی باید اشخاص طبیعی تحت تأثیر را از عملکرد سامانه مطلع کنند و داده‌های شخصی را در صورت اعمال، مطابق مقررات ۶۷۹ /۲۰۱۶ و ۲۰۱۸/۱۷۲۵ و دستورالعمل ۶۸۰ /۲۰۱۶ اتحادیهٔ اروپا پردازش کنند. این تعهد شامل سامانه‌های هوش مصنوعی مورد استفاده برای دسته‌بندی زیست‌سنجی و تشخیص احساسات که طبق قانون مجاز به تشخیص، پیشگیری یا تحقیق در جرایم هستند، نمی‌شود، مشروط بر آنکه ضمانت‌های مناسب برای حقوق و آزادی‌های اشخاص ثالث رعایت شود و مطابق قوانین اتحادیه باشد.

۴. استفاده‌کنندگان سامانه‌ای که محتوای تصویری، صوتی یا ویدئویی را تولید یا دستکاری می‌کنند و به شکل دیپ‌فیک[۱۸۵] (محتوای دستکاری‌شده و ساختگی) است، باید افشا کنند که محتوا به‌صورت مصنوعی تولید یا دستکاری شده است. این تعهد، مواردی را که طبق قانون برای تشخیص، پیشگیری، تحقیق یا پیگرد جرایم مجاز است دربرنمی‌گیرد. در صورتی که محتوای بخشی از اثر یا برنامه‌ای هنری، خلاقانه، طنز، داستانی یا مشابه آن باشد، تعهدات شفافیت، محدود به افشای وجود چنین محتوای تولید یا دستکاری‌شده به نحوی است که مانع نمایش یا لذت‌بردن از اثر نشود. استفاده‌کنندگان سامانه‌ای که متن تولید یا دستکاری‌شده را منتشر می‌کند، با هدف اطلاع‌رسانی عمومی در امور مرتبط با منافع عمومی، باید افشا کنند که متن به‌صورت مصنوعی تولید یا دستکاری شده است. این تعهد، مواردی را که طبق قانون برای تشخیص، پیشگیری، تحقیق یا پیگرد جرایم مجاز است یا محتوای تولیدشده توسط انسان بازبینی یا کنترل و ویراستاری شده باشد و یک شخص حقیقی یا حقوقی مسئولیت ویراستاری انتشار محتوا را بر عهده داشته باشد دربرنمی‌گیرد.

۵. اطلاعات موضوع بندهای ۱ تا ۴ باید حداقل در زمان اولین تعامل یا مواجهه به‌صورت واضح و متمایز به اشخاص طبیعی مربوطه ارائه شود. اطلاعات باید با الزامات دسترس‌پذیری قابل اعمال مطابقت داشته باشد.

۶. بندهای ۱ تا ۴ تأثیری بر الزامات و تعهدات مندرج در فصل سوم ندارد و حقایق دیگر تعهدات شفافیت مندرج در قوانین اتحادیه یا ملی برای استفاده‌کنندگان سامانه‌های هوش مصنوعی را تحت تأثیر قرار نمی‌دهد.

۷. *دفتر هوش مصنوعی*[۱۸۶] باید تشویق و تسهیل تدوین کدهای عملیاتی را در سطح اتحادیهٔ اروپا برای اجرای مؤثر تعهدات مربوط به تشخیص و برچسب‌گذاری محتوای تولید یا دستکاری‌شده

۱۸۵. عبارت Deep Fake (دیپ‌فیک) به هر محتوای رسانه‌ای اطلاق می‌شود که با استفاده از روش‌های یادگیری عمیق یا سایر فناوری‌های هوش مصنوعی به‌صورت مصنوعی ایجاد، ترکیب یا تغییر یافته باشد، به گونه‌ای که ظاهراً واقعی به نظر برسد، اما در واقع بازنمایی دروغین یا تحریف‌شده‌ای از واقعیت است.

186. AI Office

انجام دهد. کمیسیون می‌تواند اعمال اجرایی را برای تصویب این کدهای عملیاتی مطابق رویهٔ مندرج در ماده ۵۶(۶) اتخاذ کند. در صورتی که کمیسیون کد را نامناسب تشخیص دهد، می‌تواند اعمال اجرایی صادر کند که قواعد مشترک برای اجرای این تعهدات را مطابق رویهٔ بررسی ماده ۹۸(۲) مشخص کند.

فصل پنجم. مدل‌های هوش مصنوعی عمومی

قسمت نخست. قواعد طبقه‌بندی

ماده ۵۱. تعهدات شفافیت برای ارائه‌دهندگان و استفاده‌کنندگان برخی سامانه‌های هوش مصنوعی

۱. یک مدل هوش مصنوعی عمومی در صورتی به‌عنوان مدل دارای خطر نظام‌مند طبقه‌بندی می‌شود که یکی از شرایط زیر را دارا باشد:

الف) دارای قابلیت‌های اثرگذاری گسترده باشد که بر اساس ابزارها و روش‌شناسی‌های فنی مناسب ازجمله شاخص‌ها و معیارهای سنجش ارزیابی می‌شود؛

ب) بر اساس تصمیم کمیسیون، اعم از به ابتکار خود یا در پی هشدار تخصصی هیئت علمی، دارای قابلیت‌ها یا آثار معادل با موارد مندرج در بند (الف) باشد، با توجه به معیارهای مقرر در پیوست سیزدهم.

۲. مدل هوش مصنوعی عمومی به موجب بند ۱، جزء (الف)، هر گاه میزان کل محاسبات به‌کاررفته در فرآیند آموزش آن، که بر حسب تعداد عملیات ممیز شناور اندازه‌گیری می‌شود، بیش از ۱۰ باشد، دارای قابلیت‌های اثرگذاری گسترده محسوب می‌شود.

۳. کمیسیون مجاز است طبق ماده ۹۷ از طریق اعمال تفویضی، آستانه‌های مندرج در بندهای ۱ و ۲ این ماده را اصلاح کرده و همچنین شاخص‌ها و معیارهای سنجش را در پرتو تحولات فنی ازجمله بهبودهای الگوریتمی یا افزایش کارآیی سخت‌افزار تکمیل کند تا این آستانه‌ها بازتاب‌دهندهٔ آخرین سطح فناوری باشند.

ماده ۵۲. رویه

۱. هر گاه یک مدل هوش مصنوعی عمومی واجد شرط مندرج در بند (الف) از بند ۱ ماده ۵۱ باشد، ارائه‌دهندهٔ مربوطه باید بدون تأخیر و در هر حال، حداکثر ظرف دو هفته پس از تحقق آن شرط، یا پس از آگاهی از تحقق قریب‌الوقوع آن، موضوع را به کمیسیون اطلاع دهد. این اطلاعیه باید

شامل اطلاعات لازم برای اثبات تحقق آن شرط باشد. چنانچه کمیسیون از وجود یک مدل هوش مصنوعی عمومی که دارای خطرات نظام‌مند است ولی هنوز گزارش نشده، آگاه شود، می‌تواند تصمیم بگیرد آن مدل را به‌عنوان مدل دارای خطر نظام‌مند تعیین کند.

۲. ارائه‌دهندهٔ مدلی از هوش مصنوعی عمومی که واجد شرط مذکور در بند (الف) از بند ۱ ماده ۵۱ است، می‌تواند همراه با اطلاعیهٔ خود، دلایل مستند و موجهی ارائه کند تا نشان دهد که به‌طور استثنایی، با وجود تحقق آن شرط، مدل یادشده به سبب ویژگی‌های خاص خود، خطر نظام‌مند ایجاد نمی‌کند و بنابراین نباید به‌عنوان مدل هوش مصنوعی عمومی دارای خطر نظام‌مند طبقه‌بندی شود.

۳. هر گاه کمیسیون به این نتیجه برسد که استدلال‌های ارائه‌شده طبق بند (۲) به نحو کافی مستدل نیستند و ارائه‌دهندهٔ مربوط نتوانسته است اثبات کند که مدل هوش مصنوعی با هدف عمومی به سبب ویژگی‌های خاص خود، خطرات نظام‌مند ایجاد نمی‌کند، کمیسیون آن استدلال‌ها را رد می‌کند و مدل هوش مصنوعی مزبور، به‌عنوان مدل هوش مصنوعی با هدف عمومی دارای خطر نظام‌مند تلقی خواهد شد.

۴. کمیسیون می‌تواند رأساً یا بر اساس هشدار واجد صلاحیت صادره از سوی هیئت علمی موضوع بند (۱)، جزء (الف) ماده ۹۰، مدلی از هوش مصنوعی با هدف عمومی را بر مبنای معیارهای مندرج در پیوست سیزدهم دارای خطر نظام‌مند اعلام کند. کمیسیون اختیار دارد با صدور اعمال تفویضی مطابق ماده ۹۷، پیوست سیزدهم را اصلاح کرده و معیارهای مذکور در آن پیوست را مشخص‌تر و به‌روزرسانی کند.

۵. بنا به درخواست مستدل ارائه‌دهنده‌ای که مدل وی بر اساس بند (۴) به‌عنوان مدل هوش مصنوعی با هدف عمومی دارای خطر نظام‌مند تعیین شده است، کمیسیون باید به آن درخواست توجه کند و می‌تواند تصمیم بگیرد که مجدداً بررسی کند آیا همچنان ممکن است مدل مزبور بر مبنای معیارهای مندرج در پیوست سیزدهم دارای خطر نظام‌مند محسوب شود یا خیر. چنین درخواستی باید حاوی دلایل عینی، دقیق و جدیدی باشد که پس از تصمیم اولیهٔ تعیین خطر نظام‌مند پدید آمده‌اند. ارائه‌دهندگان می‌توانند زودتر از شش ماه پس از تصمیم تعیین خطر نظام‌مند، درخواست بازنگری ارائه نکنند. در صورتی که کمیسیون پس از بازنگری تصمیم بگیرد که تعیین خطر نظام‌مند را حفظ کند، ارائه‌دهندگان می‌توانند زودتر از شش ماه پس از آن تصمیم، درخواست بازنگری مجدد ارائه ندهند.

۶. کمیسیون باید فهرستی از مدل‌های هوش مصنوعی با هدف عمومی دارای خطر نظام‌مند منتشر کرده و آن فهرست را به‌روز نگاه دارد، بی‌آنکه به لزوم رعایت و حمایت از حقوق مالکیت فکری، اطلاعات محرمانهٔ تجاری یا اسرار تجاری مطابق حقوق اتحادیه و قوانین ملی لطمه‌ای وارد شود.

قسمت دوم. تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی

ماده ۵۳. تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی

۱. ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی مکلف‌اند که:

الف) مستندات فنی مربوط به مدل، ازجمله فرآیند آموزش و آزمون آن و نتایج ارزیابی‌های انجام‌شده را تهیه و به‌روز نگه دارند. این مستندات باید حداقل شامل اطلاعات مندرج در پیوست یازدهم بوده و به منظور ارائه در صورت درخواست، در اختیار دفتر هوش مصنوعی اتحادیهٔ اروپا و مراجع صلاحیت‌دار ملی قرار گیرد.

ب) اطلاعات و مستندات لازم را برای ارائه‌دهندگان سامانه‌های هوش مصنوعی که قصد دارند مدل هوش مصنوعی با هدف عمومی را در سامانه‌های خود ادغام کنند، تهیه، به‌روز و در دسترس آنان قرار دهند. با رعایت الزامات مربوط به حقوق مالکیت فکری، اسرار تجاری و اطلاعات محرمانهٔ تجاری طبق حقوق اتحادیه و قوانین ملی، این اطلاعات و مستندات باید:

۱) به ارائه‌دهندگان سامانه‌های هوش مصنوعی امکان دهند تا درک دقیقی از قابلیت‌ها و محدودیت‌های مدل هوش مصنوعی با هدف عمومی داشته باشند و بتوانند تعهدات خود را طبق این قانون انجام دهند؛ و

۲) حداقل شامل عناصر مندرج در پیوست دوازدهم باشند.

پ) سیاستی را برای رعایت مقررات حقوق اتحادیهٔ اروپا در زمینهٔ حق مؤلف و حقوق مرتبط اتخاذ کنند و به‌ویژه با استفاده از پیشرفته‌ترین فناوری‌ها، هر گونه اعلام حق رزرو را که مطابق ماده ۴(۳) از دستورالعمل ۷۹۰ /۲۰۱۹ اتحادیهٔ اروپا بیان شده است، شناسایی و رعایت کنند.

ت) خلاصه‌ای به‌قدر کافی دقیق و مشروح از محتوایی که برای آموزش مدل هوش مصنوعی با هدف عمومی استفاده شده است، مطابق الگوی ارائه‌شده از سوی دفتر هوش مصنوعی اتحادیهٔ اروپا تهیه کرده و به‌صورت عمومی منتشر کنند.

۲. تعهدات مقرر در بند ۱، جزءهای (الف) و (ب)، در مورد ارائه‌دهندگانی که مدل‌های هوش مصنوعی خود را تحت مجوز *آزاد یا متن‌باز*[۱۸۷] منتشر می‌کنند اعمال نمی‌شود. این مجوز اجازهٔ دسترسی، استفاده، تغییر و توزیع مدل را می‌دهد و همچنین معیارهای مدل ازجمله وزن‌ها، اطلاعات مربوط به معماری مدل و اطلاعات مربوط به نحوهٔ استفاده از مدل را به‌طور عمومی در دسترس قرار می‌دهد. با این حال، این استثنا شامل مدل‌های هوش مصنوعی با هدف عمومیِ دارای ریسک نظام‌مند نخواهد شد.

187. Free and Open-Source Licence

۳. ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی موظف‌اند در حدود ضرورت، برای اجرای اختیارات و صلاحیت‌های کمیسیون و مراجع صلاحیت‌دار ملی طبق مقررات این آیین‌نامه با آنان همکاری کنند.

۴. ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی می‌توانند تا زمان انتشار استانداردهای هماهنگ‌شدهٔ اروپایی، از آیین‌نامه‌های رفتاری موضوع ماده ۵۶ برای اثبات انطباق با تعهدات مندرج در بند ۱ این ماده استفاده کنند. رعایت استانداردهای هماهنگ اروپایی، برای ارائه‌دهندگان، دلیل بر مطابقت با الزامات مربوط محسوب می‌شود، تا حدی که این استانداردها آن الزامات را پوشش دهند. ارائه‌دهندگانی که به آیین‌نامهٔ رفتاری تأییدشده نپیوسته‌اند یا با استاندارد هماهنگ اروپایی مطابقت ندارند، باید راهکارهای جایگزین و مناسبی برای رعایت الزامات ارائه دهند تا کمیسیون آن را ارزیابی کند.

۵. به منظور تسهیل رعایت الزامات مندرج در پیوست یازدهم، به‌ویژه بندهای (د) و (هـ) آن، کمیسیون اختیار دارد از طریق تصویب اقدامات تفویضی طبق ماده ۹۷، روش‌های سنجش و محاسبهٔ جزئی را تعیین کند تا امکان مستندسازی قابل مقایسه و راستی‌آزمایی فراهم شود.

۶. کمیسیون اختیار دارد با استناد به ماده ۹۷(۲)، ضمائم یازدهم و دوازدهم را با توجه به تحولات فناورانهٔ در حال تغییر اصلاح کند.

۷. هر گونه اطلاعات یا مستنداتی که بر اساس این ماده به دست می‌آید ازجمله اسرار تجاری باید مطابق تعهدات محرمانگی مندرج در ماده ۷۸ مورد رسیدگی و حفاظت قرار گیرد.

ماده ۵۴. نمایندگان مجاز ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی

۱. پیش از عرضهٔ یک مدل هوش مصنوعی با هدف عمومی در بازار اتحادیه، ارائه‌دهندگان مستقر در کشورهای ثالث باید از طریق تفویض اختیار کتبی، نماینده‌ای مجاز را که در قلمرو اتحادیه مستقر است منصوب کنند.

۲. ارائه‌دهنده باید نمایندهٔ مجاز خود را قادر کند تا وظایفی را که در تفویض اختیار از سوی ارائه‌دهنده مشخص شده است، انجام دهد.

۳. نمایندهٔ مجاز باید وظایف تعیین‌شده در تفویض اختیار را انجام دهد و در صورت درخواست دفتر هوش مصنوعی، نسخه‌ای از تفویض اختیار را به یکی از زبان‌های رسمی نهادهای اتحادیه در اختیار آن قرار دهد.

براساس این قانون، تفویض اختیار باید نمایندهٔ مجاز را برای انجام وظایف زیر توانمند کند:

الف) اطمینان از اینکه مستندات فنی مندرج در پیوست یازدهم تهیه شده و کلیهٔ تعهدات مندرج در ماده ۵۳ و در صورت اقتضا، ماده ۵۵ از سوی ارائه‌دهنده انجام شده است؛

ب) نگهداری نسخه‌ای از مستندات فنی موضوع پیوست یازدهم برای مدت ده سال پس از عرضهٔ مدل هوش مصنوعی در بازار و نیز نگهداری اطلاعات تماس ارائه‌دهنده‌ای که وی را منصوب کرده است، به منظور ارائه به دفتر هوش مصنوعی و مقامات صلاحیت‌دار ملی در صورت درخواست؛

پ) ارائهٔ تمامی اطلاعات و مستندات لازم، ازجمله موارد مذکور در بند (ب)، به دفتر هوش مصنوعی بنا بر درخواست مستدل، به منظور اثبات رعایت تعهدات مقرر در این فصل؛

ت) همکاری با دفتر هوش مصنوعی و مقامات صلاحیت‌دار بنا بر درخواست مستدل آنان در هر اقدامی مرتبط با مدل هوش مصنوعی، ازجمله در مواردی که آن مدل در سامانه‌های هوش مصنوعی ادغام شده و در بازار اتحادیه عرضه یا مورد بهره‌برداری قرار گرفته است.

۴. تفویض اختیار باید به گونه‌ای باشد که دفتر هوش مصنوعی یا مقامات صلاحیت‌دار بتوانند در خصوص تمامی موضوعات مربوط به رعایت این قانون، علاوه بر ارائه‌دهنده یا به جای او، با نمایندهٔ مجاز مکاتبه یا تعامل کنند.

۵. نمایندهٔ مجاز باید در صورتی که تشخیص دهد یا دلایلی داشته باشد که ارائه‌دهنده برخلاف تعهدات خود بر اساس این قانون عمل می‌کند، تفویض اختیار را خاتمه دهد. در این صورت، وی باید فوراً دفتر هوش مصنوعی را از خاتمهٔ تفویض اختیار و دلایل آن آگاه کند.

۶. الزام مقرر در این ماده در مورد ارائه‌دهندگانی که مدل‌های هوش مصنوعی با هدف عمومی خود را تحت مجوز آزاد و متن‌باز منتشر می‌کنند به نحوی که دسترسی، استفاده، اصلاح و توزیع آن آزاد بوده و معیارها ازجمله وزن‌ها، اطلاعات معماری مدل و شیوهٔ استفاده از آن به‌صورت عمومی در دسترس باشد، اعمال نمی‌شود، مگر آنکه مدل‌های مذکور دارای خطرات نظام‌مند باشند.

قسمت سوم. تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی دارای خطرات نظام‌مند

ماده ۵۵. تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی دارای خطرات نظام‌مند

۱. افزون بر تعهدات مندرج در مواد ۵۳ و ۵۴، ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی که دارای خطرات نظام‌مند هستند، موظف‌اند:

الف) ارزیابی مدل را مطابق رویه‌ها و ابزارهای استانداردشده و منطبق با آخرین پیشرفت‌های

فنی، ازجمله اجرای آزمایش‌های تقابلی[۱۸۸] و مستندسازی آن به منظور شناسایی و کاهش خطرات نظام‌مند انجام دهند؛

ب) ارزیابی و کاهش خطرات احتمالی نظام‌مند در سطح اتحادیه، ازجمله منشأ آن که ممکن است ناشی از توسعه، عرضه در بازار یا استفاده از مدل‌های هوش مصنوعی با هدف عمومیِ دارای خطرات نظام‌مند باشد؛

ج) ثبت، مستندسازی و گزارش بدون تأخیر غیرموجه اطلاعات مرتبط با حوادث جدی و تدابیر اصلاحی احتمالی برای رفع آن‌ها، به دفتر هوش مصنوعی و در صورت اقتضا به مراجع صلاحیت‌دار ملی؛

د) تضمین سطحی مناسب از حفاظت امنیت سایبری برای مدل هوش مصنوعی با خطر نظام‌مند و زیرساخت فیزیکی مربوط به آن.

۲. ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومیِ دارای خطر نظام‌مند می‌توانند تا زمان انتشار یک استاندارد هماهنگ‌شدهٔ اتحادیهٔ اروپا، برای اثبات رعایت تعهدات مقرر در بند ۱ این ماده، به کدهای رفتاری[۱۸۹] موضوع ماده ۵۶ استناد کنند. رعایت استانداردهای هماهنگ‌شدهٔ اروپایی برای ارائه‌دهندگان، مادامی که آن استانداردها شامل این تعهدات باشند، قرینه‌ای بر انطباق با الزامات مربوطه محسوب می‌شود. ارائه‌دهندگانی که به کد رفتاری تأییدشده پایبند نیستند یا با استاندارد هماهنگ‌شدهٔ اروپایی مطابقت ندارند، باید روش‌های جایگزین و مناسب دیگری برای اثبات انطباق خود جهت ارزیابی توسط کمیسیون ارائه دهند.

۳. هر گونه اطلاعات یا اسناد به‌دست‌آمده بر اساس این ماده، ازجمله اسرار تجاری، مطابق تعهدات محرمانگی مندرج در ماده ۷۸ مورد حفاظت قرار خواهد گرفت.

قسمت چهارم. کدهای رفتاری

ماده ۵۶. کدهای رفتاری

۱. دفتر هوش مصنوعی باید تدوین آیین‌نامه‌های رفتاری در سطح اتحادیه را تشویق و تسهیل کند تا به اجرای صحیح این قانون با درنظرگرفتن رویکردهای بین‌المللی در این زمینه کمک کند.

۲. دفتر هوش مصنوعی و هیئت باید اطمینان حاصل کنند که آیین‌نامه‌های رفتاری حداقل شامل تعهدات مقرر در مواد ۵۳ و ۵۵ باشند، ازجمله در خصوص موضوعات زیر:

الف) روش‌هایی برای اطمینان از اینکه اطلاعات اشاره‌شده در بندهای (الف) و (ب) از بند (۱)

188. Adversarial testing
189. Code of practice

ماده ۵۳ با توجه به تحولات بازار و فناوری به‌روز نگه داشته می‌شود؛

ب) تعیین سطح مناسب جزئیات برای خلاصه‌ای از محتوایی که در آموزش مدل‌ها مورد استفاده قرار گرفته است؛

پ) شناسایی نوع و ماهیت خطرات نظام‌مند در سطح اتحادیه، ازجمله منابع احتمالی آن‌ها، در صورت اقتضا؛

ت) تدابیر، رویه‌ها و شیوه‌های ارزیابی و مدیریت خطرات نظام‌مند در سطح اتحادیه ازجمله مستندسازی آن‌ها، به گونه‌ای که متناسب با میزان خطرات باشد، شدت و احتمال وقوع آن‌ها را در نظر گیرد و چالش‌های خاص مربوط به مقابله با این خطرات را با توجه به راه‌های ممکن بروز و تحقق آن‌ها در زنجیرهٔ ارزش هوش مصنوعی لحاظ کند.

۳. دفتر هوش مصنوعی می‌تواند همهٔ ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عام و همچنین مراجع صلاحیت‌دار ملی ذی‌ربط را برای مشارکت در تدوین آیین‌نامه‌های رفتاری دعوت کند. سازمان‌های جامعهٔ مدنی، بخش صنعت، دانشگاهیان و سایر ذی‌نفعان مرتبط ازجمله *ارائه‌دهندگان پایین‌دست*[۱۹۰] و کارشناسان مستقل نیز می‌توانند در این فرآیند، نقش حمایتی داشته باشند.

۴. دفتر هوش مصنوعی و هیئت موظف‌اند اطمینان حاصل کنند که آیین‌نامه‌های رفتاری به‌روشنی اهداف خاص خود را بیان کرده و شامل تعهدات یا تدابیری ازجمله شاخص‌های کلیدی عملکرد در صورت اقتضا باشند تا تحقق آن اهداف تضمین شود. همچنین باید در تنظیم این آیین‌نامه‌ها، نیازها و منافع تمامی طرف‌های ذی‌نفع، ازجمله اشخاص متأثر، در سطح اتحادیه به‌طور مقتضی مورد توجه قرار گیرد.

۵. دفتر هوش مصنوعی باید اطمینان حاصل کند که مشارکت‌کنندگان در آیین‌نامه‌های رفتاری به‌صورت منظم در خصوص اجرای تعهدات، تدابیر اتخاذشده و نتایج حاصل ازجمله نتایج سنجیده‌شده بر پایهٔ شاخص‌های کلیدی عملکرد را در صورت اقتضا به این دفتر گزارش‌دهی کنند. شاخص‌های کلیدی عملکرد و الزامات گزارش‌دهی باید متناسب با تفاوت در اندازه و ظرفیت میان شرکت‌کنندگان مختلف تعیین شوند.

۶. دفتر هوش مصنوعی و هیئت باید به‌طور منظم بر میزان تحقق اهداف آیین‌نامه‌های رفتاری و نقش آن‌ها در اجرای صحیح این قانون، نظارت و ارزیابی کنند. آنان باید بررسی نمایند که آیا این آیین‌نامه‌ها الزامات مقرر در مواد ۵۳ و ۵۵ را پوشش می‌دهند یا خیر و ارزیابی خود از کفایت آیین‌نامه‌های رفتاری را منتشر کنند. کمیسیون می‌تواند از طریق آیین‌نامهٔ اجرایی، آیین‌نامهٔ‌رفتاری

190. Downstream providers

را تصویب کرده و به آن اعتبار عام در سطح اتحادیه اعطا کند. این آیین‌نامهٔ اجرایی باید طبق روند بررسی مندرج در بند (۲) ماده ۹۸ تصویب شود.

۷. دفتر هوش مصنوعی می‌تواند تمام ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عام را جهت پیوستن به آیین‌نامه‌های رفتاری دعوت کند. ممکن است این عضویت برای ارائه‌دهندگان مدل‌های فاقد خطرات نظام‌مند، صرفاً محدود به الزامات مقرر در ماده ۵۳ باشد، مگر آنکه خود به‌طور صریح تمایل به پیوستن کامل به آیین‌نامه را اعلام کنند.

۸. دفتر هوش مصنوعی همچنین باید در صورت اقتضا، بازنگری و تطبیق آیین‌نامه‌های رفتاری را به‌ویژه با توجه به استانداردهای نوظهور، تسهیل و تشویق کند. این دفتر باید در ارزیابی استانداردهای موجود نیز نقش پشتیبانی ایفا کند.

۹. آیین‌نامه‌های رفتاری باید حداکثر تا ۲ مه ۲۰۲۵ آماده باشند. دفتر هوش مصنوعی باید اقدامات لازم را، ازجمله دعوت از ارائه‌دهندگان طبق بند ۷ انجام دهد.

چنانچه تا ۲ اوت ۲۰۲۵ نتوان آیین‌نامه‌ای را نهایی کرد یا دفتر هوش مصنوعی پس از ارزیابی خود طبق بند ۶، آن را نامناسب تشخیص دهد، کمیسیون می‌تواند از طریق آیین‌نامه‌های اجرایی، قواعد مشترکی برای اجرای الزامات مندرج در مواد ۵۳ و ۵۵ ازجمله موضوعات مندرج در بند ۲ این ماده مقرر کند. این آیین‌نامه‌های اجرایی نیز باید طبق روند بررسی مندرج در بند (۲) ماده ۹۸ به تصویب برسند.

فصل ششم. تدابیر در حمایت از نوآوری

ماده ۵۷. سندباکس‌های نظارتی هوش مصنوعی

۱. کشورهای عضو تضمین می‌کنند که مقامات صلاحیت‌دار آنان دست‌کم یک سندباکس نظارتی هوش مصنوعی را در سطح ملی ایجاد کنند که حداکثر تا ۲ اوت ۲۰۲۶ عملیاتی باشد. این سندباکس می‌تواند به‌طور مشترک با مقامات صلاحیت‌دار سایر کشورهای عضو نیز ایجاد شود. کمیسیون می‌تواند برای ایجاد و بهره‌برداری از سندباکس‌های نظارتی هوش مصنوعی، پشتیبانی فنی، مشاوره و ابزارهایی ارائه دهد.

تعهد مقرر در بند نخست این پاراگراف همچنین می‌تواند از طریق مشارکت در یک سندباکس موجود ایفا شود، مشروط بر آنکه این مشارکت، سطح معادل پوشش ملی برای کشورهای عضو مشارکت‌کننده فراهم کند.

۲. سندباکس‌های نظارتی هوش مصنوعی اضافی می‌توانند در سطح منطقه‌ای یا محلی، یا به‌طور مشترک با مقامات صلاحیت‌دار سایر کشورهای عضو نیز ایجاد شوند.

۳. ناظر اروپایی حفاظت از داده‌ها می‌تواند یک سندباکس نظارتی هوش مصنوعی برای نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه ایجاد و مطابق این فصل، نقش‌ها و وظایف مقامات صلاحیت‌دار ملی را ایفا کند.

۴. کشورهای عضو تضمین می‌کنند که مقامات صلاحیت‌دار مذکور در بندهای ۱ و ۲ منابع کافی را به گونه‌ای تخصیص دهند که اجرای مؤثر و به‌موقع این ماده تضمین شود. در صورت اقتضا، مقامات صلاحیت‌دار ملی با سایر مقامات ذی‌ربط همکاری می‌کنند و می‌توانند اجازه دهند سایر بازیگران در اکوسامانهٔ هوش مصنوعی درگیر شوند. این ماده به سایر سندباکس‌های نظارتی ایجادشده بر اساس حقوق اتحادیه یا قوانین ملی خدشه‌ای وارد نمی‌کند. کشورهای عضو تضمین می‌کنند که سطح مناسبی از همکاری میان مقامات ناظر بر آن سندباکس‌ها و مقامات صلاحیت‌دار ملی برقرار شود.

۵. سندباکس‌های نظارتی هوش مصنوعی ایجادشده طبق بند ۱ محیطی کنترل‌شده را فراهم می‌کنند که نوآوری را تقویت و توسعه، آموزش، آزمایش و اعتبارسنجی سامانه‌های نوآورانهٔ هوش مصنوعی را برای مدتی محدود، پیش از عرضه در بازار یا بهره‌برداری، بر اساس طرح سندباکس مشخص و مورد توافق میان ارائه‌دهندگان یا ارائه‌دهندگان بالقوه و مقام صلاحیت‌دار، تسهیل کند. این سندباکس‌ها می‌توانند شامل آزمایش در شرایط واقعی تحت نظارت نیز باشند.

۶. مقامات صلاحیت‌دار در چارچوب سندباکس نظارتی هوش مصنوعی حسب مورد راهنمایی، نظارت و پشتیبانی فراهم می‌کنند تا ریسک‌ها، به‌ویژه نسبت به حقوق بنیادین، سلامت و ایمنی شناسایی، آزمایش و تدابیر کاهش و اثربخشی آن‌ها در ارتباط با تعهدات و الزامات این قانون و عنداللزوم سایر قوانین اتحادیه و ملی که درون سندباکس تحت نظارت قرار دارند، بررسی شود.

۷. مقامات صلاحیت‌دار به ارائه‌دهندگان و ارائه‌دهندگان بالقوهٔ مشارکت‌کننده در سندباکس نظارتی هوش مصنوعی، راهنمایی لازم را در خصوص انتظارات نظارتی و نحوهٔ ایفای الزامات و تعهدات مقرر در این قانون ارائه می‌دهند.

به درخواست ارائه‌دهنده یا ارائه‌دهندهٔ بالقوهٔ سامانهٔ هوش مصنوعی، مقام صلاحیت‌دار، گواهی کتبی در خصوص فعالیت‌های موفقیت‌آمیز انجام‌شده در سندباکس صادر می‌کند. مقام صلاحیت‌دار همچنین گزارشی پایانی شامل جزئیات فعالیت‌های انجام‌شده در سندباکس و نتایج و یافته‌های مربوط صادر خواهد کرد. ارائه‌دهندگان می‌توانند از این مستندات برای اثبات انطباق خود با این قانون از طریق فرآیند ارزیابی انطباق یا فعالیت‌های مربوط به پایش بازار استفاده کنند. در این زمینه، گزارش‌های پایانی و گواهی‌های کتبی مقام صلاحیت‌دار ملی توسط مقامات پایش بازار و مراجع ابلاغ‌شده، مثبت ارزیابی می‌شود تا به میزان معقولی روند ارزیابی انطباق تسریع شود.

۸. با رعایت مقررات محرمانگی مندرج در ماده ۷۸ و با موافقت ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه، کمیسیون و هیئت مجاز خواهند بود به گزارش‌های پایانی دسترسی داشته باشند و آن‌ها را حسب مورد در انجام وظایف خود بر اساس این قانون مدنظر قرار دهند. در صورتی که هر دو، یعنی ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه و مقام صلاحیت‌دار ملی صراحتاً موافقت کنند، گزارش پایانی می‌تواند از طریق سکوی اطلاعاتی واحد مذکور در این ماده به‌طور عمومی در دسترس قرار گیرد.

۹. ایجاد سندباکس‌های نظارتی هوش مصنوعی باید در راستای تحقق اهداف زیر باشد:

الف) بهبود قطعیت حقوقی به منظور دستیابی به انطباق نظارتی با این قانون یا عنداللزوم با سایر قوانین قابل اعمال اتحادیه و ملی؛

ب) پشتیبانی از تبادل بهترین رویه‌ها از طریق همکاری با مقامات دخیل در سندباکس نظارتی هوش مصنوعی؛

پ) تقویت نوآوری و رقابت‌پذیری و تسهیل توسعهٔ اکوسامانهٔ هوش مصنوعی؛

ت) کمک به یادگیری نظارتی مبتنی بر شواهد؛

ث) تسهیل و تسریع دسترسی سامانه‌های هوش مصنوعی به بازار اتحادیه، به‌ویژه در مورد ارائه‌شده توسط بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا.

۱۰. مقامات صلاحیت‌دار ملی تضمین می‌کنند که در صورتی که سامانه‌های نوآورانهٔ هوش مصنوعی مستلزم پردازش داده‌های شخصی باشند یا به نحوی در حوزهٔ نظارتی سایر مقامات ملی یا مقامات صلاحیت‌دار، مسئول ارائه یا پشتیبانی دسترسی به داده‌ها قرار گیرند، مقامات ملی حفاظت از داده‌ها و سایر مقامات ملی یا صلاحیت‌دار مربوط در بهره‌برداری از سندباکس نظارتی هوش مصنوعی و در نظارت بر جنبه‌های مربوط، به میزان وظایف و اختیارات خود دخیل شوند.

۱۱. سندباکس‌های نظارتی هوش مصنوعی، خدشه‌ای به اختیارات نظارتی یا اصلاحی مقامات ناظر بر آن‌ها، ازجمله در سطح منطقه‌ای یا محلی وارد نمی‌کنند. هر گونه ریسک مهم نسبت به سلامت و ایمنی و حقوق بنیادین که در جریان توسعه و آزمایش این سامانه‌های هوش مصنوعی شناسایی شود، باید به‌طور کافی کاهش یابد. مقامات صلاحیت‌دار ملی اختیار دارند در صورت عدم امکان کاهش مؤثر ریسک، فرآیند آزمایش یا مشارکت در سندباکس را به‌طور موقت یا دائم تعلیق و دفتر هوش مصنوعی را از این تصمیم مطلع کنند. مقامات صلاحیت‌دار ملی با هدف حمایت از نوآوری در هوش مصنوعی در اتحادیه، اختیارات نظارتی خود را در حدود قوانین مربوط و با استفاده از اختیارات اختیاری در اجرای مقررات قانونی نسبت به پروژه‌های مشخص سندباکس نظارتی هوش مصنوعی اعمال می‌کنند.

۱۲. ارائه‌دهندگان و ارائه‌دهندگان بالقوهٔ مشارکت‌کننده در سندباکس نظارتی هوش مصنوعی

همچنان مطابق حقوق اتحادیه و قوانین ملی مربوط به مسئولیت، در قبال هر گونه خسارت واردشده به اشخاص ثالث ناشی از آزمایش‌های انجام‌شده در سندباکس، مسئول باقی می‌مانند. معذلک، مشروط بر آنکه ارائه‌دهندگان بالقوه، طرح مشخص و شرایط و ضوابط مشارکت خود را رعایت کرده و با حسن‌نیت راهنمایی‌های ارائه‌شده از سوی مقام صلاحیت‌دار ملی را دنبال کنند، هیچ جریمهٔ اداری به دلیل نقض این قانون از سوی مقامات بر آنان تحمیل نخواهد شد. هر گاه سایر مقامات صلاحیت‌دارِ مسئول اجرای قوانین دیگر اتحادیه و قوانین ملی نیز به‌طور فعال در نظارت بر سامانهٔ هوش مصنوعی در سندباکس دخیل باشند و برای انطباق، راهنمایی ارائه دهند، هیچ جریمهٔ اداری در ارتباط با آن قوانین اعمال نخواهد شد.

۱۳. سندباکس‌های نظارتی هوش مصنوعی باید به گونه‌ای طراحی و اجرا شوند که عنداللزوم، همکاری فرامرزی میان مقامات صلاحیت‌دار ملی را تسهیل کنند.

۱۴. مقامات صلاحیت‌دار ملی فعالیت‌های خود را هماهنگ کرده و در چارچوب هیئت همکاری می‌کنند.

۱۵. مقامات صلاحیت‌دار ملی، دفتر هوش مصنوعی و هیئت را از ایجاد سندباکس مطلع می‌کنند و می‌توانند از آن‌ها درخواست پشتیبانی و راهنمایی کنند. دفتر هوش مصنوعی، فهرستی عمومی از سندباکس‌های برنامه‌ریزی‌شده و موجود منتشر و آن را به‌روز نگه می‌دارد تا تعامل بیشتر در سندباکس‌های نظارتی هوش مصنوعی و همکاری فرامرزی تشویق شود.

۱۶. مقامات صلاحیت‌دار ملی از یک سال پس از ایجاد سندباکس نظارتی هوش مصنوعی و سپس هر سال تا پایان آن، و همچنین در پایان، گزارش‌های سالانه به دفتر هوش مصنوعی و هیئت ارائه می‌کنند. این گزارش‌ها شامل اطلاعاتی دربارهٔ پیشرفت و نتایج اجرای آن سندباکس‌ها، ازجمله بهترین رویه‌ها، حوادث، درس‌های آموخته‌شده و توصیه‌ها در خصوص ایجاد آن‌ها و عنداللزوم دربارهٔ اجرای و بازنگری احتمالی این قانون (شامل اقدامات تفویضی و اجرایی آن) و دربارهٔ اجرای سایر قوانین اتحادیه که توسط مقامات صلاحیت‌دار درون سندباکس نظارت می‌شوند، خواهد بود. مقامات صلاحیت‌دار ملی این گزارش‌های سالانه یا چکیده‌ای از آن‌ها را به‌صورت عمومی و برخط منتشر می‌کنند. کمیسیون، در صورت اقتضا، گزارش‌های سالانه را در انجام وظایف خود طبق این قانون مدنظر قرار خواهد داد.

۱۷. کمیسیون یک رابط واحد و اختصاصی ایجاد می‌کند که حاوی تمام اطلاعات مرتبط با سندباکس‌های نظارتی هوش مصنوعی باشد تا ذی‌نفعان بتوانند با این سندباکس‌ها تعامل داشته و پرسش‌های خود را با مقامات صلاحیت‌دار مطرح کنند و راهنمایی غیرالزام‌آوری دربارهٔ انطباق محصولات، خدمات یا مدل‌های تجاری نوآورانهٔ متکی بر فناوری‌های هوش مصنوعی، مطابق ماده

۶۲(۱)، بند (ج) دریافت کنند. کمیسیون، عنداللزوم به‌طور فعال با مقامات صلاحیت‌دار ملی هماهنگی خواهد کرد.

ماده ۵۸. ترتیبات تفصیلی و کارکرد سندباکس‌های نظارتی هوش مصنوعی

۱. به منظور جلوگیری از تکه‌تکه‌شدن مقررات در سراسر اتحادیه، کمیسیون اقدامات اجرایی لازم را به منظور تعیین ترتیبات تفصیلی برای ایجاد، توسعه، اجرا، بهره‌برداری و نظارت بر سندباکس‌های نظارتی هوش مصنوعی تصویب خواهد کرد. اقدامات اجرایی مذکور باید اصول مشترکی را در موضوعات زیر شامل شود:

الف) معیارهای احراز شرایط و انتخاب برای مشارکت در سندباکس نظارتی هوش مصنوعی؛

ب) رویه‌های مربوط به درخواست، مشارکت، پایش، خروج و خاتمهٔ سندباکس نظارتی هوش مصنوعی، ازجمله طرح سندباکس و گزارش پایانی؛

ج) شرایط و ضوابط حاکم بر مشارکت‌کنندگان.

این اقدامات اجرایی مطابق رویهٔ بررسی مقرر در ماده ۹۸(۲) تصویب خواهند شد.

۲. اقدامات اجرایی مذکور در بند ۱ باید تضمین کنند که:

الف) سندباکس‌های نظارتی هوش مصنوعی برای هر ارائه‌دهنده یا ارائه‌دهندهٔ بالقوهٔ سامانهٔ هوش مصنوعی که معیارهای احراز شرایط و انتخاب را برآورده کند، که باید شفاف و منصفانه باشند، باز باشند و مقامات صلاحیت‌دار ملی ظرف سه ماه از تاریخ درخواست، متقاضیان را از تصمیم خود مطلع کنند؛

ب) سندباکس‌های نظارتی هوش مصنوعی، دسترسی گسترده و برابر فراهم کنند و با تقاضای مشارکت همگام شوند؛ ارائه‌دهندگان و ارائه‌دهندگان بالقوه می‌توانند درخواست‌های خود را به‌طور مشترک با بهره‌برداران و سایر اشخاص ثالث ذی‌ربط نیز ارائه دهند؛

ج) ترتیبات تفصیلی و شرایط مرتبط با سندباکس‌های نظارتی هوش مصنوعی، در بیشترین حد ممکن، انعطاف‌پذیری لازم را برای مقامات صلاحیت‌دار ملی در ایجاد و بهره‌برداری از سندباکس‌های نظارتی هوش مصنوعی آن‌ها فراهم کند؛

د) دسترسی به سندباکس‌های نظارتی هوش مصنوعی برای بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا، رایگان باشد، بدون لطمه به هزینه‌های استثنایی که مقامات صلاحیت‌دار ملی می‌توانند به شیوه‌ای منصفانه و متناسب بازیابی کنند؛

هـ) از طریق نتایج یادگیری سندباکس‌های نظارتی هوش مصنوعی، ارائه‌دهندگان و ارائه‌دهندگان بالقوه در اجرای تعهدات ارزیابی انطباق مقرر در این قانون و در کاربرد داوطلبانهٔ کدهای رفتاری

مذکور در ماده ۹۵ یاری شوند؛

و) سندباکس‌های نظارتی هوش مصنوعی، مشارکت سایر بازیگران ذی‌ربط در اکوسامانهٔ هوش مصنوعی، مانند مراجع ابلاغ‌شده، سازمان‌های استانداردسازی، بنگاه‌های کوچک و متوسط ازجمله شرکت‌های نوپا، شرکت‌ها، نوآوران، تسهیلات آزمایش و آزمون، آزمایشگاه‌های تحقیق و آزمایش، قطب‌های نوآوری دیجیتال اروپایی، مراکز برتری و پژوهشگران فردی را تسهیل کنند تا امکان و تسهیل همکاری میان بخش‌های عمومی و خصوصی فراهم شود؛

ز) رویه‌ها، فرآیندها و الزامات اداری برای درخواست، انتخاب، مشارکت و خروج از سندباکس نظارتی هوش مصنوعی ساده، به‌آسانی قابل درک و به‌طور شفاف ابلاغ شوند تا مشارکت بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا با ظرفیت‌های محدود حقوقی و اداری تسهیل شود و در سراسر اتحادیه همسو باشند تا از تکه‌تکه‌شدن جلوگیری شود، و مشارکت در یک سندباکس نظارتی هوش مصنوعی ایجادشده توسط یک کشور عضو یا توسط ناظر اروپایی حفاظت از داده‌ها به‌طور متقابل و یکنواخت شناسایی شده و همان آثار حقوقی را در سراسر اتحادیه داشته باشد؛

ح) مشارکت در سندباکس نظارتی هوش مصنوعی محدود به مدتی متناسب با پیچیدگی و مقیاس پروژه باشد و این مدت بتواند توسط مقام صلاحیت‌دار ملی تمدید شود؛

ط) سندباکس‌های نظارتی هوش مصنوعی توسعهٔ ابزارها و زیرساخت‌هایی برای آزمون، بنچمارک‌گذاری، ارزیابی و تبیین ابعاد سامانه‌های هوش مصنوعی مرتبط با یادگیری نظارتی، مانند دقت، استحکام و امنیت سایبری، و همچنین تدابیر کاهش ریسک نسبت به حقوق بنیادین و جامعه به‌طور کلی را تسهیل کنند.

۳. ارائه‌دهندگان بالقوه در سندباکس‌های نظارتی هوش مصنوعی، به‌ویژه بنگاه‌های کوچک و متوسط و شرکت‌های نوپا، عنداللزوم به خدمات پیش از بهره‌برداری مانند راهنمایی در خصوص اجرای این قانون، و سایر خدمات ارزش‌افزا مانند کمک در اسناد استانداردسازی و گواهی‌نامه، تسهیلات آزمایش و آزمون، قطب‌های نوآوری دیجیتال اروپایی و مراکز برتری هدایت خواهند شد.

۴. هر گاه مقامات صلاحیت‌دار ملی مجازدانستن آزمایش در شرایط واقعی تحت نظارت در چارچوب یک سندباکس نظارتی هوش مصنوعی ایجادشده بر اساس این ماده را مدنظر قرار دهند، باید با هدف حمایت از حقوق بنیادین، سلامت و ایمنی، شرایط و ضوابط خاص چنین آزمایشی و به‌ویژه تضمین‌های مناسب را با مشارکت‌کنندگان مورد توافق قرار دهند. در صورت اقتضا، آنان با سایر مقامات صلاحیت‌دار ملی همکاری خواهند کرد تا شیوه‌های یکسان در سراسر اتحادیه تضمین شود.

ماده ۵۹. پردازش بیشتر داده‌های شخصی به منظور توسعهٔ برخی سامانه‌های هوش مصنوعی در جهت منافع عمومی در سندباکس نظارتی هوش مصنوعی

۱. در سندباکس نظارتی هوش مصنوعی، داده‌های شخصی که به‌طور قانونی برای مقاصد دیگر جمع‌آوری شده‌اند، صرفاً برای توسعه، آموزش و آزمون برخی سامانه‌های هوش مصنوعی در سندباکس قابل پردازش خواهند بود، مشروط بر آنکه کلیهٔ شرایط زیر محقق شوند:

الف) سامانه‌های هوش مصنوعی باید توسط یک مقام عمومی یا شخص حقیقی یا حقوقی دیگر برای تضمین منافع عمومی اساسی و در یک یا چند حوزهٔ زیر توسعه یابند:

۱) ایمنی عمومی و بهداشت عمومی، ازجمله شناسایی، تشخیص، پیشگیری، کنترل و درمان بیماری و بهبود نظام‌های مراقبت‌های بهداشتی؛

۲) سطح بالای حمایت و بهبود کیفیت محیط‌زیست، حفاظت از تنوع زیستی، حفاظت در برابر آلودگی، اقدامات گذار سبز، اقدامات کاهش و سازگاری با تغییرات اقلیمی؛

۳) پایداری انرژی؛

۴) ایمنی و تاب‌آوری سامانه‌های حمل و نقل و جابجایی، زیرساخت‌ها و شبکه‌های حیاتی؛

۵) کارآمدی و کیفیت ادارهٔ عمومی و خدمات عمومی.

ب) در مواردی که این الزامات با پردازش داده‌های ناشناس، مصنوعی یا سایر داده‌های غیرشخصی به‌طور مؤثر برآورده نمی‌شوند، داده‌های پردازش‌شده برای رعایت یک یا چند الزام مذکور در بخش ۲ از فصل سوم ضروری باشند؛

ج) سازوکارهای پایش مؤثری وجود داشته باشد تا مشخص شود آیا در طول آزمایش‌های سندباکس، ریسک‌های بالایی نسبت به حقوق و آزادی‌های موضوع داده، مطابق ماده ۳۵ قانون (اتحادیهٔ اروپا) ۶۷۹/۲۰۱۶ و ماده ۳۹ قانون (اتحادیهٔ اروپا) ۱۷۲۵/۲۰۱۸ ایجاد می‌شود یا خیر؛ همچنین سازوکارهای واکنش برای کاهش سریع آن ریسک‌ها و در صورت لزوم، توقف پردازش وجود داشته باشد؛

د) هر دادهٔ شخصی که در چارچوب سندباکس پردازش می‌شود، در محیطی جداگانه، ایمن و حفاظت‌شده تحت کنترل ارائه‌دهندهٔ بالقوه پردازش شود و تنها اشخاص مجاز به آن داده‌ها دسترسی داشته باشند؛

هـ) ارائه‌دهندگان بتوانند داده‌های اولیهٔ جمع‌آوری‌شده را صرفاً طبق حقوق اتحادیه در زمینهٔ حفاظت از داده‌ها به اشتراک گذارند؛ هیچ دادهٔ شخصی ایجادشده در سندباکس، خارج از سندباکس قابل اشتراک‌گذاری نخواهد بود؛

و) هیچ پردازش دادهٔ شخصی در چارچوب سندباکس منجر به اتخاذ تدابیر یا تصمیماتی که بر موضوع دادهٔ اثر بگذارد، نشود و همچنین بر اعمال حقوق آنان، مقرر در حقوق اتحادیه در زمینهٔ حمایت از داده‌های شخصی تأثیری نگذارد؛

ز) هر دادهٔ شخصی پردازش‌شده در چارچوب سندباکس با استفاده از تدابیر فنی و سازمانی مناسب حمایت شود و پس از خاتمهٔ مشارکت در سندباکس یا پایان دورهٔ نگهداری دادهٔ شخصی، حذف شود؛

ح) گزارش‌های پردازش دادهٔ شخصی در چارچوب سندباکس برای مدت مشارکت در سندباکس نگهداری شود، مگر آنکه حقوق اتحادیه یا قوانین ملی خلاف آن مقرر کند؛

ط) شرح کامل و دقیق فرآیند و منطق پشت آموزش، آزمون و اعتبارسنجی سامانهٔ هوش مصنوعی همراه با نتایج آزمون به‌عنوان بخشی از مستندات فنی مذکور در پیوست چهارم نگهداری شود؛

ی) خلاصه‌ای کوتاه از پروژهٔ هوش مصنوعی توسعه‌افته در سندباکس، اهداف و نتایج مورد انتظار آن در وب‌سایت مقامات صلاحیت‌دار منتشر شود؛ این تکلیف شامل داده‌های عملیاتی حساس مربوط به فعالیت‌های مقامات اجرای قانون، کنترل مرزها، مهاجرت یا پناهندگی نخواهد بود.

۲. به منظور پیشگیری، تحقیق، شناسایی یا تعقیب جرایم کیفری یا اجرای مجازات‌های کیفری، ازجمله حفاظت در برابر تهدیدات علیه امنیت عمومی و جلوگیری از آن‌ها، تحت نظارت و مسئولیت مقامات اجرای قانون، پردازش داده‌های شخصی در سندباکس‌های نظارتی هوش مصنوعی باید مبتنی بر یک قانون مشخص اتحادیه یا ملی باشد و مشمول همان شرایط انباشته‌ای باشد که در بند ۱ ذکر شد.

۳. بند ۱ خدشه‌ای به حقوق اتحادیه یا قوانین ملی را که پردازش داده‌های شخصی برای مقاصدی غیر از آنچه صراحتاً در آن قوانین ذکر شده ممنوع می‌کند، وارد نمی‌سازد؛ همچنین خدشه‌ای به حقوق اتحادیه یا قوانین ملی که مبنای پردازش داده‌های شخصی ضروری برای توسعه، آزمون یا آموزش سامانه‌های نوآورانه هوش مصنوعی یا هر مبنای قانونی دیگر در انطباق با حقوق اتحادیه در زمینهٔ حمایت از داده‌های شخصی را مقرر می‌دارند، وارد نمی‌کند.

ماده ۶۰. آزمون سامانه‌های هوش مصنوعی پرخطر در شرایط واقعی خارج از سندباکس‌های نظارتی هوش مصنوعی

۱. آزمون سامانه‌های هوش مصنوعی پرخطر در شرایط واقعی خارج از سندباکس‌های نظارتی هوش مصنوعی می‌تواند توسط ارائه‌دهندگان یا ارائه‌دهندگان بالقوهٔ سامانه‌های هوش مصنوعی پرخطر مندرج در پیوست سوم و مطابق این ماده و طرح آزمون در شرایط واقعی مذکور در این ماده

انجام گیرد، بدون آنکه به ممنوعیت‌های مقرر در ماده ۵ خدشه‌ای وارد آید.

کمیسیون از طریق اقدامات اجرایی، عناصر تفصیلی طرح آزمون در شرایط واقعی را مشخص خواهد کرد. این اقدامات اجرایی طبق رویهٔ بررسی مذکور در ماده ۹۸(۲) تصویب خواهند شد.

این بند، خدشه‌ای به حقوق اتحادیه یا قوانین ملی مربوط به آزمون در شرایط واقعی سامانه‌های هوش مصنوعی پرخطر مرتبط با محصولات مشمول قانونگذاری هماهنگ‌سازی اتحادیه، مندرج در پیوست یک وارد نمی‌کند.

۲. ارائه‌دهندگان یا ارائه‌دهندگان بالقوه می‌توانند آزمون سامانه‌های هوش مصنوعی پرخطر مندرج در پیوست سوم را در شرایط واقعی، هر زمان پیش از عرضه به بازار یا بهره‌برداری از سامانهٔ هوش مصنوعی، به‌تنهایی یا در مشارکت با یک یا چند بهره‌بردار یا بهره‌برداران بالقوه انجام دهند.

۳. آزمون سامانه‌های هوش مصنوعی پرخطر در شرایط واقعی تحت این ماده، خدشه‌ای به هر گونه بررسی اخلاقی که بر اساس حقوق اتحادیه یا قوانین ملی لازم باشد، وارد نمی‌کند.

۴. ارائه‌دهندگان یا ارائه‌دهندگان بالقوه صرفاً در صورتی می‌توانند آزمون در شرایط واقعی انجام دهند که کلیهٔ شرایط زیر محقق شود:

الف) ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه، طرح آزمون در شرایط واقعی را تدوین کرده و آن را به مقام نظارت بر بازار در کشور عضو محل انجام آزمون ارائه کرده باشد؛

ب) مقام نظارت بر بازار در کشور عضو محل انجام آزمون، آزمون در شرایط واقعی و طرح آزمون در شرایط واقعی را تأیید کرده باشد؛ در صورتی که مقام نظارت بر بازار، ظرف ۳۰ روز پاسخی ارائه ندهد، آزمون در شرایط واقعی و طرح آزمون در شرایط واقعی تأییدشده تلقی خواهد شد، مگر آنکه قانون ملی تأیید ضمنی را پیش‌بینی نکرده باشد که در آن صورت، آزمون در شرایط واقعی همچنان مستلزم اخذ مجوز خواهد بود؛

ج) ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه، به‌استثنای ارائه‌دهندگان یا ارائه‌دهندگان بالقوهٔ سامانه‌های هوش مصنوعی پرخطر مندرج در بندهای ۱، ۶ و ۷ پیوست سوم در حوزه‌های اجرای قانون، مهاجرت، پناهندگی و مدیریت کنترل مرزها و همچنین سامانه‌های هوش مصنوعی پرخطر مندرج در بند ۲ پیوست سوم، آزمون در شرایط واقعی را طبق ماده ۷۱(۴) با یک شمارهٔ شناسایی یکتا در سطح اتحادیه و همراه با اطلاعات مقرر در پیوست نهم ثبت کرده باشد؛ ارائه‌دهندگان یا ارائه‌دهندگان بالقوهٔ سامانه‌های هوش مصنوعی پرخطر مندرج در بندهای ۱، ۶ و ۷ پیوست سوم در حوزه‌های اجرای قانون، مهاجرت، پناهندگی و مدیریت کنترل مرزها باید آزمون در شرایط واقعی را در بخش امن و غیرعلنی پایگاه دادهٔ اتحادیه طبق ماده ۴۹(۴)(د) ثبت کنند؛ ارائه‌دهندگان یا ارائه‌دهندگان بالقوهٔ سامانه‌های هوش مصنوعی پرخطر مندرج در بند ۲ پیوست سوم باید آزمون در

شرایط واقعی را طبق ماده ۴۹(۵) ثبت کنند؛

د) ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه‌ای که آزمون در شرایط واقعی را انجام می‌دهد در اتحادیه مستقر باشد یا نمایندهٔ حقوقی‌ای منصوب کرده باشد که در اتحادیه مستقر است؛

هـ) داده‌های گردآوری و پردازش‌شده برای مقاصد آزمون در شرایط واقعی صرفاً در صورتی به کشورهای ثالث منتقل شوند که تضمین‌های مناسب و قابل اجرا طبق حقوق اتحادیه اعمال شده باشد؛

و) آزمون در شرایط واقعی بیش از مدت لازم برای دستیابی به اهداف خود ادامه نیابد و در هر صورت بیش از شش ماه به طول نینجامد؛ این مدت می‌تواند برای دورهٔ اضافی شش‌ماهه، با اطلاع‌رسانی قبلی از سوی ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه به مقام نظارت بر بازار و همراه با توضیح ضرورت چنین تمدیدی تمدید شود؛

ز) اشخاص موضوع آزمون در شرایط واقعی که به دلیل سن یا ناتوانی جزو گروه‌های آسیب‌پذیر محسوب می‌شوند، به‌طور مقتضی حمایت شوند؛

ح) چنانچه ارائه‌دهنده یا ارائه‌دهندهٔ بالقوهٔ آزمون، شرایط واقعی را با همکاری یک یا چند بهره‌بردار یا بهره‌برداران بالقوه سازماندهی کند، طرف اخیر باید از تمامی جنبه‌های آزمون که به تصمیم آنان برای مشارکت مربوط است مطلع شده و دستورالعمل‌های مرتبط با استفاده از سامانهٔ هوش مصنوعی مذکور در ماده ۱۳ را دریافت کرده باشد؛ ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه و بهره‌بردار یا بهره‌برداران بالقوه باید توافقی منعقد کنند که نقش‌ها و مسئولیت‌های آنان را با هدف تضمین رعایت مفاد مربوط به آزمون در شرایط واقعی طبق این قانون و سایر قوانین ملی و اتحادیه مشخص کند؛

ط) اشخاص موضوع آزمون در شرایط واقعی رضایت آگاهانهٔ خود را مطابق ماده ۶۱ اعلام کرده باشند؛ یا در مورد اجرای قانون، هنگامی که اخذ رضایت آگاهانه، مانع از آزمون سامانهٔ هوش مصنوعی می‌شود، خود آزمون و نتیجهٔ آن در شرایط واقعی نباید هیچ اثر منفی بر اشخاص داشته باشد و داده‌های شخصی آنان پس از انجام آزمون حذف شود؛

ی) در شرایط واقعی به‌طور مؤثر توسط ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه، همچنین توسط بهره‌برداران یا بهره‌برداران بالقوه از طریق اشخاصی که صلاحیت کافی در حوزهٔ مربوطه دارند و از ظرفیت، آموزش و اختیار لازم برای انجام وظایف خود برخوردارند، بر آزمون نظارت شود؛

ک) پیش‌بینی‌ها، توصیه‌ها یا تصمیمات سامانهٔ هوش مصنوعی بتواند به‌طور مؤثر معکوس شده و نادیده گرفته شود.

۵. هر یک از اشخاص موضوع آزمون در شرایط واقعی، یا حسب مورد نمایندهٔ قانونی منصوب آنان می‌توانند در هر زمان و بدون تحمل هیچ زیان و بدون نیاز به ارائهٔ دلیل، با لغو رضایت آگاهانهٔ

خود از آزمون خارج شوند و حذف فوری و دائمی داده‌های شخصی خود را درخواست کنند. خروج از رضایت آگاهانه بر فعالیت‌هایی که پیش‌تر انجام شده است تأثیری نخواهد داشت.

۶. بر اساس ماده ۷۵، کشورهای عضو باید به مقامات نظارت بر بازار خود اختیاراتی برای الزام ارائه‌دهندگان و ارائه‌دهندگان بالقوه به ارائهٔ اطلاعات، انجام بازرسی‌های غیرمترقبه از راه دور یا در محل، و انجام بررسی‌ها در خصوص نحوهٔ اجرای آزمون در شرایط واقعی و سامانه‌های هوش مصنوعی پرخطر مرتبط اعطا کنند. مقامات نظارت بر بازار باید از این اختیارات برای تضمین توسعهٔ ایمن آزمون در شرایط واقعی استفاده کنند.

۷. هر گونه حادثهٔ جدی که در جریان آزمون در شرایط واقعی شناسایی شود باید مطابق ماده ۷۳ به مقام نظارت بر بازار ملی گزارش شود. ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه باید تدابیر فوری کاهش پیامدها را اتخاذ کند یا در غیر این صورت، آزمون در شرایط واقعی را تا زمان انجام کاهش پیامدها معلق کند یا خاتمه دهد. ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه باید رویه‌ای برای فراخوان سریع سامانهٔ هوش مصنوعی در صورت خاتمهٔ آزمون در شرایط واقعی برقرار کند.

۸. ارائه‌دهندگان یا ارائه‌دهندگان بالقوه باید مقام نظارت بر بازار ملی در کشور عضو محل انجام آزمون در شرایط واقعی را از تعلیق یا خاتمهٔ آزمون در شرایط واقعی و از نتایج نهایی مطلع کنند.

۹. ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه، مطابق حقوق مسئولیت مدنی اتحادیه و قوانین ملی مربوط، در قبال هر گونه خسارت وارده در جریان آزمون در شرایط واقعی مسئول خواهد بود.

ماده ۶۱. رضایت آگاهانه برای مشارکت در آزمون در شرایط واقعی خارج از سندباکس‌های نظارتی هوش مصنوعی

۱. برای مقاصد آزمون در شرایط واقعی موضوع ماده ۶۰، رضایت آگاهانهٔ آزادانهٔ ابرازشده باید پیش از مشارکت اشخاص موضوع آزمون در آن و پس از اطلاع‌رسانی مقتضی به آنان با اطلاعاتی موجز، روشن، مرتبط و قابل فهم در خصوص موارد زیر اخذ شود:

الف) ماهیت و اهداف آزمون در شرایط واقعی و مزاحمت‌های احتمالی مرتبط با مشارکت آنان؛

ب) شرایطی که آزمون در شرایط واقعی تحت آن انجام خواهد شد، ازجمله مدت‌زمان مورد انتظار مشارکت شخص یا اشخاص موضوع آزمون؛

ج) حقوق آنان و تضمین‌های مربوط به مشارکت، به‌ویژه حق امتناع از مشارکت و حق خروج از آزمون در شرایط واقعی در هر زمان، بدون آنکه هیچ زیانی بر آنان تحمیل شود و بدون نیاز به ارائهٔ هر گونه توجیه؛

د) ترتیبات مربوط به درخواست معکوس‌سازی یا نادیده‌گرفتن پیش‌بینی‌ها، توصیه‌ها یا تصمیمات سامانهٔ هوش مصنوعی؛

هـ) شمارهٔ شناسایی یکتای واحد در سطح اتحادیه برای آزمون در شرایط واقعی مطابق ماده ۶۰(۴)(ج)، و اطلاعات تماس ارائه‌دهنده یا نمایندهٔ قانونی وی که اطلاعات بیشتر از او قابل دریافت است.

۲. رضایت آگاهانه باید تاریخ‌گذاری و مستندسازی شود و یک نسخه از آن به اشخاص موضوع آزمون یا نمایندهٔ قانونی آنان تحویل شود.

ماده ۶۲. تدابیر مربوط به ارائه‌دهندگان و بهره‌برداران، به‌ویژه بنگاه‌های کوچک و متوسط ازجمله شرکت‌های نوپا

۱. کشورهای عضو، اقدامات زیر را به عمل خواهند آورد:

الف) اعطای دسترسی اولویتی به سندباکس‌های نظارتی هوش مصنوعی برای بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا که دفتر ثبت‌شده یا شعبه‌ای در اتحادیه دارند، تا حدی که شرایط احراز صلاحیت و معیارهای گزینش را دارا باشند؛ دسترسی اولویتی مانع از دسترسی سایر بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپایی غیر از آن دستهٔ مذکور در این بند، به سندباکس نظارتی هوش مصنوعی نخواهد بود، مشروط بر آنکه آنان نیز شرایط احراز صلاحیت و معیارهای گزینش را دارا باشند؛

ب) برگزاری فعالیت‌های ویژهٔ آگاهی‌بخشی و آموزشی در خصوص اجرای این قانون، متناسب با نیازهای بنگاه‌های کوچک و متوسط ازجمله شرکت‌های نوپا، بهره‌برداران و در صورت اقتضا، مقامات عمومی محلی؛

ج) استفاده از مجاری اختصاصی موجود و در صورت اقتضا، ایجاد مجاری جدید برای ارتباط با بنگاه‌های کوچک و متوسط ازجمله شرکت‌های نوپا، بهره‌برداران، سایر نوآوران و در صورت اقتضا، مقامات عمومی محلی به منظور ارائهٔ مشاوره و پاسخ به پرسش‌ها دربارهٔ اجرای این قانون، ازجمله در خصوص مشارکت در سندباکس‌های نظارتی هوش مصنوعی؛

د) تسهیل مشارکت بنگاه‌های کوچک و متوسط و سایر ذی‌نفعان مربوط در فرآیند تدوین استاندارد.

۲. منافع و نیازهای خاص ارائه‌دهندگان بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا، در تعیین هزینه‌های ارزیابی انطباق موضوع ماده ۴۳ مدنظر قرار خواهد گرفت و این هزینه‌ها متناسب با اندازه، اندازهٔ بازار و سایر شاخص‌های مربوط آنان کاهش خواهد یافت.

۳. دفتر هوش مصنوعی اقدامات زیر را به عمل خواهد آورد:

الف) ارائهٔ الگوهای استاندارد برای حوزه‌های مشمول این قانون، مطابق درخواست هیئت؛

ب) توسعه و نگهداری یک بستر اطلاعاتی واحد که اطلاعات مرتبط با این قانون را به شکلی ساده و قابل استفاده برای همهٔ فعالان در سراسر اتحادیه فراهم کند؛

ج) سازمان‌دهی پویش‌های ارتباطی مقتضی برای آگاهی‌بخشی دربارهٔ تعهدات ناشی از این قانون؛

د) ارزیابی و ترویج همگرایی بهترین رویه‌ها در رویه‌های تدارکات عمومی مرتبط با سامانه‌های هوش مصنوعی.

ماده ۶۳. معافیت‌ها برای برخی فعالان

۱. خردبنگاه‌ها به معنای توصیه2003/361/EC می‌توانند برخی عناصر نظام مدیریت کیفیت مقرر در ماده ۱۷ این قانون را به شیوه‌ای ساده‌شده رعایت کنند، مشروط بر آنکه هیچ بنگاه شریک یا بنگاه وابسته‌ای به معنای آن توصیه نداشته باشند. بدین منظور، کمیسیون دستورالعمل‌هایی در خصوص عناصری از نظام مدیریت کیفیت که می‌توان آن‌ها را به شیوه‌ای ساده‌شده رعایت کرد، با درنظرگرفتن نیازهای خردبنگاه‌ها تدوین خواهد کرد، بدون آنکه سطح حفاظت یا ضرورت انطباق با الزامات مربوط به سامانه‌های پرخطر هوش مصنوعی مخدوش شود.

۲. بند ۱ این ماده به منزلهٔ معافیت این فعالان از انجام سایر الزامات یا تعهدات مقرر در این قانون، ازجمله آنچه در مواد ۹، ۱۰، ۱۱، ۱۲، ۱۳، ۱۴، ۱۵، ۷۲ و ۷۳ مقرر شده است، تلقی نخواهد شد.

فصل هفتم. حکمرانی

بخش ۱. حکمرانی در سطح اتحادیه

ماده ۶۴. دفتر هوش مصنوعی

۱. کمیسیون از طریق دفتر هوش مصنوعی، تخصص و ظرفیت‌های اتحادیه را در حوزهٔ هوش مصنوعی توسعه خواهد داد.

۲. کشورهای عضو، وظایفی را که مطابق این قانون به دفتر هوش مصنوعی محول شده است، تسهیل خواهند کرد.

ماده ۶۵. تأسیس و ساختار هیئت هوش مصنوعی اروپا

۱. هیئت هوش مصنوعی اروپا (از این پس *هیئت*) بدین وسیله تأسیس می‌شود.

۲. هیئت متشکل از یک نماینده از هر کشور عضو خواهد بود. ناظر حفاظت از داده‌های اروپا به‌عنوان ناظر مشارکت خواهد داشت. دفتر هوش مصنوعی نیز در جلسات هیئت حضور خواهد یافت، بدون آنکه در رأی‌گیری‌ها شرکت کند. سایر مقامات، نهادها یا کارشناسان ملی و اتحادیه، حسب مورد و بر اساس تصمیم هیئت، در صورتی که موضوعات مورد بحث به آنان مرتبط باشد، می‌توانند به جلسات دعوت شوند.

۳. هر نماینده توسط کشور عضو مربوطه برای مدت سه سال منصوب می‌شود؛ این مأموریت یک بار قابل تمدید است.

۴. کشورهای عضو اطمینان حاصل خواهند کرد که نمایندگان آنان در هیئت:

الف) دارای صلاحیت‌ها و اختیارات لازم در کشور خود باشند تا بتوانند به‌طور فعال در تحقق وظایف هیئت موضوع ماده ۶۶ مشارکت کنند؛

ب) به‌عنوان تنها نقطهٔ تماس در برابر هیئت منصوب شوند و در صورت اقتضا و با توجه به نیازهای کشورهای عضو، به‌عنوان تنها نقطهٔ تماس برای ذی‌نفعان عمل کنند؛

ج) اختیار تسهیل هماهنگی و انسجام میان مقامات صلاحیت‌دار ملی کشور خود در خصوص اجرای این قانون را داشته باشند، ازجمله از طریق گردآوری داده‌ها و اطلاعات مرتبط به منظور انجام وظایف خود در هیئت.

۵. نمایندگان منصوب کشورهای عضو، آیین‌نامهٔ داخلی هیئت را با اکثریت دو سوم تصویب خواهند کرد. آیین‌نامهٔ داخلی، به‌ویژه روش‌های مربوط به فرآیند انتخاب، مدت مأموریت و مشخصات وظایف رئیس، ترتیبات تفصیلی رأی‌گیری و سازمان‌دهی فعالیت‌های هیئت و گروه‌های فرعی آن را تعیین خواهد کرد.

۶. هیئت دو گروه فرعی دائمی تشکیل خواهد داد تا بستری برای همکاری و تبادل میان مقامات نظارت بر بازار و مقامات اعلان‌کننده در خصوص موضوعات مرتبط با نظارت بر بازار و نهادهای اعلام‌شده فراهم کند.

گروه فرعی دائمی مربوط به نظارت بر بازار باید به‌عنوان گروه همکاری اداری برای این قانون در معنای مندرج در ماده ۳۰ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) عمل کند.

هیئت می‌تواند حسب مورد، گروه‌های فرعی دائمی یا موقت دیگری برای بررسی موضوعات خاص تشکیل دهد. در صورت اقتضا، نمایندگان مجمع مشورتی موضوع ماده ۶۷ می‌توانند به‌عنوان

ناظر به چنین گروه‌های فرعی یا به جلسات خاص آن‌ها دعوت شوند.

۷. هیئت به نحوی سازمان‌دهی و اداره خواهد شد که عینیت و بی‌طرفی فعالیت‌های آن تضمین شود.

۸. هیئت توسط یکی از نمایندگان کشورهای عضو ریاست خواهد شد. دفتر هوش مصنوعی، دبیرخانه هیئت را بر عهده خواهد داشت، بنا به درخواست رئیس جلسات را تشکیل خواهد داد و دستور جلسات را مطابق وظایف هیئت بر اساس این قانون و آیین‌نامهٔ داخلی آن تهیه خواهد کرد.

ماده ۶۶. وظایف هیئت

هیئت به منظور تسهیل اجرای یکنواخت و مؤثر این قانون، کمیسیون و کشورهای عضو را مشاوره و مساعدت خواهد کرد. بدین منظور، هیئت می‌تواند به‌ویژه اقدامات زیر را انجام دهد:

الف) مشارکت در هماهنگی میان مقامات صلاحیت‌دار ملی مسئول اجرای این قانون و با همکاری و مشروط به موافقت مقامات نظارت بر بازار ذی‌ربط، حمایت از فعالیت‌های مشترک مقامات نظارت بر بازار موضوع بند ۱۱ ماده ۷۴؛

ب) گردآوری و به‌اشتراک‌گذاری تخصص فنی و مقرراتی و بهترین رویه‌ها میان کشورهای عضو؛

پ) ارائهٔ مشاوره دربارهٔ اجرای این قانون، به‌ویژه در خصوص اجرای قواعد مربوط به مدل‌های هوش مصنوعی با مقاصد عام؛

ت) مشارکت در هماهنگ‌سازی رویه‌های اداری در کشورهای عضو، ازجمله در ارتباط با معافیت از رویه‌های ارزیابی انطباق موضوع ماده ۴۶، کارکرد سندباکس‌های نظارتی هوش مصنوعی و آزمون در شرایط واقعی موضوع مواد ۵۷، ۵۹ و ۶۰؛

ث) بنا به درخواست کمیسیون یا به ابتکار خود، صدور توصیه‌ها و نظرات کتبی در خصوص هر موضوع مرتبط با اجرای این قانون و اجرای یکنواخت و مؤثر آن، ازجمله:

۱) توسعه و اجرای آیین‌های رفتاری و آیین‌های عملی موضوع این قانون، همچنین رهنمودهای کمیسیون؛

۲) ارزیابی و بازنگری این قانون مطابق ماده ۱۱۲، ازجمله در خصوص گزارش‌های مربوط به حوادث جدی موضوع ماده ۷۳، کارکرد پایگاه دادهٔ اتحادیهٔ موضوع ماده ۷۱، تهیهٔ اعمال تفویضی یا اجرایی و نیز دربارهٔ همسویی احتمالی این قانون با قوانین هماهنگی اتحادیه مندرج در پیوست یک؛

۳) مشخصات فنی یا استانداردهای موجود دربارهٔ الزامات مندرج در بخش ۲ فصل سوم؛

۴) استفاده از استانداردهای هماهنگ یا مشخصات مشترک موضوع مواد ۴۰ و ۴۱؛

۵) روندها، ازجمله رقابت‌پذیری جهانی اروپا در حوزهٔ هوش مصنوعی، به‌کارگیری هوش مصنوعی در اتحادیه و توسعهٔ مهارت‌های دیجیتال؛

۶) روندهای مرتبط با تحول زنجیره‌های ارزش هوش مصنوعی، به‌ویژه پیامدهای ناشی از آن از حیث مسئولیت‌پذیری؛

۷) نیاز احتمالی به اصلاح پیوست سوم مطابق ماده ۷ و نیاز احتمالی به بازنگری ماده ۵ بر اساس ماده ۱۱۲، با لحاظ شواهد موجود مرتبط و آخرین تحولات فناوری؛

ج) حمایت از کمیسیون در ارتقاء سواد هوش مصنوعی، آگاهی عمومی و درک از منافع، مخاطرات، تضمین‌ها و حقوق و تعهدات مربوط به استفاده از سامانه‌های هوش مصنوعی؛

چ) تسهیل توسعهٔ معیارهای مشترک و فهم مشترک در میان فعالان بازار و مقامات صلاحیت‌دار از مفاهیم مندرج در این قانون، ازجمله از طریق مشارکت در توسعهٔ شاخص‌ها؛

ح) همکاری، حسب مورد، با سایر نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه، همچنین گروه‌های کارشناسی و شبکه‌های اتحادیه، به‌ویژه در حوزه‌های ایمنی محصولات، امنیت سایبری، رقابت، خدمات دیجیتال و رسانه‌ای، خدمات مالی، حمایت از مصرف‌کننده، داده و حمایت از حقوق بنیادین؛

خ) مشارکت در همکاری مؤثر با مقامات صلاحیت‌دار کشورهای ثالث و سازمان‌های بین‌المللی؛

د) یاری به مقامات صلاحیت‌دار ملی و کمیسیون در توسعهٔ تخصص سازمانی و فنی لازم برای اجرای این قانون، ازجمله از طریق مشارکت در ارزیابی نیازهای آموزشی کارکنان کشورهای عضو که در اجرای این قانون دخیل‌اند؛

ذ) یاری به دفتر هوش مصنوعی در حمایت از مقامات صلاحیت‌دار ملی در ایجاد و توسعهٔ سندباکس‌های نظارتی هوش مصنوعی و تسهیل همکاری و تبادل اطلاعات میان این سندباکس‌ها؛

ر) مشارکت در توسعهٔ اسناد راهنمایی و ارائهٔ مشاوره‌های مرتبط در این زمینه؛

ز) ارائهٔ مشاوره به کمیسیون در موضوعات بین‌المللی مرتبط با هوش مصنوعی؛

ژ) ارائهٔ نظرات به کمیسیون دربارهٔ هشدارهای واجد شرایط مرتبط با مدل‌های هوش مصنوعی با مقاصد عام؛

س) دریافت نظرات کشورهای عضو در خصوص هشدارهای واجد شرایط دربارهٔ مدل‌های هوش مصنوعی با مقاصد عام و دربارهٔ تجارب و رویه‌های ملی در زمینهٔ نظارت و اجرای مربوط به سامانه‌های هوش مصنوعی، به‌ویژه سامانه‌هایی که مدل‌های هوش مصنوعی با مقاصد عام را در خود ادغام می‌کنند.

ماده ۶۷. مجمع مشورتی

۱. مجمعی مشورتی به منظور ارائهٔ تخصص فنی و مشاوره به هیئت و کمیسیون و مشارکت در انجام وظایف آنان طبق این قانون تأسیس می‌شود.

۲. عضویت در مجمع مشورتی باید نمایانگر گزینشی متوازن از ذی‌نفعان، ازجمله صنعت، شرکت‌های نوپا، بنگاه‌های کوچک و متوسط، جامعهٔ مدنی و دانشگاه‌ها باشد. ترکیب اعضا باید با ملاحظهٔ توازن میان منافع تجاری و غیرتجاری و در میان منافع تجاری، با ملاحظهٔ توازن میان بنگاه‌های کوچک و متوسط و سایر شرکت‌ها تعیین شود.

۳. کمیسیون، اعضای مجمع مشورتی را از میان ذی‌نفعانی که دارای تخصص شناخته‌شده در حوزهٔ هوش مصنوعی هستند و مطابق معیارهای مندرج در بند ۲ منصوب خواهد کرد.

۴. مدت مأموریت اعضای مجمع مشورتی دو سال خواهد بود که حداکثر تا چهار سال دیگر قابل تمدید است.

۵. آژانس حقوق بنیادین، آژانس امنیت سایبری اتحادیه، کمیتهٔ اروپایی استانداردسازی، کمیتهٔ اروپایی استانداردسازی برق و مؤسسهٔ استانداردهای مخابراتی اروپا، اعضای دائمی مجمع مشورتی خواهند بود.

۶. مجمع مشورتی آیین‌نامهٔ داخلی خود را تنظیم خواهد کرد. این مجمع از میان اعضای خود، دو رئیس مشترک را مطابق معیارهای مندرج در بند دو انتخاب خواهد کرد. مدت مأموریت رؤسای مشترک دو سال خواهد بود که یک بار دیگر قابل تمدید است.

۷. مجمع مشورتی دست‌کم دو بار در سال تشکیل جلسه خواهد داد. مجمع می‌تواند کارشناسان و سایر ذی‌نفعان را به جلسات خود دعوت کند.

۸. مجمع مشورتی می‌تواند به درخواست هیئت یا کمیسیون، نظرات، توصیه‌ها و مشارکت‌های کتبی تهیه کند.

۹. مجمع مشورتی می‌تواند حسب مورد، گروه‌های فرعی دائمی یا موقت برای بررسی مسائل خاص مرتبط با اهداف این قانون تشکیل دهد.

۱۰. مجمع مشورتی گزارشی سالانه از فعالیت‌های خود تهیه خواهد کرد. این گزارش باید به‌طور عمومی در دسترس قرار گیرد.

ماده ۶۸. هیئت علمی متشکل از کارشناسان مستقل

۱. کمیسیون از طریق *اقدام اجرایی* مقررات مربوط به تأسیس هیئت علمی متشکل از کارشناسان

مستقل (از این پس *هیئت علمی*) را به منظور پشتیبانی از فعالیت‌های اجرایی تحت این قانون مقرر خواهد داشت. این اقدام اجرایی مطابق رویهٔ بررسی مندرج در ماده ۹۸(۲) تصویب خواهد شد.

۲. هیئت علمی از کارشناسانی تشکیل می‌شود که توسط کمیسیون بر اساس تخصص علمی یا فنی به‌روز در حوزهٔ هوش مصنوعی، مورد نیاز برای انجام وظایف مذکور در بند ۳ انتخاب می‌شوند و باید تمامی شرایط زیر را احراز کنند:

الف) برخورداری از صلاحیت و مهارت ویژه و تخصص علمی یا فنی در حوزهٔ هوش مصنوعی؛

ب) استقلال از هر ارائه‌دهندهٔ سامانه‌های هوش مصنوعی یا مدل‌های هوش مصنوعی با مقاصد عمومی؛

ج) توانایی انجام وظایف با دقت، صحت و بی‌طرفی.

کمیسیون پس از مشورت با هیئت، تعداد کارشناسان هیئت علمی را بر اساس نیازهای موجود تعیین خواهد کرد و توازن منصفانهٔ جنسیتی و جغرافیایی را تضمین خواهد کرد.

۳. هیئت علمی مشاوره و پشتیبانی لازم را برای دفتر هوش مصنوعی، به‌ویژه در خصوص وظایف زیر ارائه خواهد داد:

الف) پشتیبانی از اجرای این قانون و تضمین اعمال آن در خصوص مدل‌ها و سامانه‌های هوش مصنوعی با مقاصد عمومی، به‌ویژه از طریق:

۱) هشدار به دفتر هوش مصنوعی در خصوص خطرات سیستمی احتمالی در سطح اتحادیه ناشی از مدل‌های هوش مصنوعی با مقاصد عمومی، طبق ماده ۹۰؛

۲) مشارکت در توسعهٔ ابزارها و روش‌شناسی‌های ارزیابی قابلیت‌های مدل‌ها و سامانه‌های هوش مصنوعی با مقاصد عمومی، ازجمله از طریق بنچمارک‌ها؛

۳) ارائهٔ مشاوره دربارهٔ طبقه‌بندی مدل‌های هوش مصنوعی با مقاصد عمومی دارای ریسک سیستمی؛

۴) ارائهٔ مشاوره دربارهٔ طبقه‌بندی انواع مدل‌ها و سامانه‌های هوش مصنوعی با مقاصد عمومی؛

۵) مشارکت در توسعهٔ ابزارها و الگوها؛

ب) پشتیبانی از فعالیت‌های مراجع نظارت بازار، بنا به درخواست آن‌ها؛

ج) پشتیبانی از فعالیت‌های نظارت بازار فرامرزی موضوع ماده ۷۴(۱۱)، بدون خدشه به اختیارات مراجع نظارت بازار؛

د) پشتیبانی از دفتر هوش مصنوعی در انجام وظایف آن در چارچوب رویهٔ حفاظتی اتحادیه طبق ماده ۸۱.

۴. کارشناسان عضو هیئت علمی وظایف خود را با بی‌طرفی و عینیت انجام داده و محرمانگی

اطلاعات و داده‌های به‌دست‌آمده در جریان انجام وظایف و فعالیت‌های خود را تضمین خواهند کرد. آنان در اجرای وظایف موضوع بند ۳ نه دستور خواهند گرفت و نه به دستور کسی عمل خواهند کرد. هر کارشناس باید بیانیه‌ای در خصوص منافع خود تنظیم کند که به‌طور عمومی در دسترس قرار خواهد گرفت. دفتر هوش مصنوعی نظام‌ها و رویه‌هایی را برای مدیریت فعال و پیشگیری از تضاد منافع احتمالی برقرار خواهد ساخت.

۵. اقدام اجرایی مندرج در بند ۱ باید شامل مقرراتی دربارهٔ شرایط، رویه‌ها و ترتیبات دقیق برای هیئت علمی و اعضای آن در زمینهٔ صدور هشدار و درخواست کمک از دفتر هوش مصنوعی برای انجام وظایف هیئت علمی باشد.

ماده ۶۹. دسترسی کشورهای عضو به مجموعهٔ کارشناسان

۱. کشورهای عضو می‌توانند از کارشناسان هیئت علمی برای پشتیبانی از فعالیت‌های اجرایی خود طبق این قانون استفاده کنند.

۲. ممکن است از کشورهای عضو بابت مشاوره و پشتیبانی ارائه‌شده توسط کارشناسان، هزینه‌هایی دریافت شود. ساختار و میزان این هزینه‌ها، همچنین مقیاس و ساختار هزینه‌های قابل بازپرداخت، در اقدام اجرایی موضوع ماده ۶۸(۱) تعیین خواهد شد، با درنظرگرفتن اهداف اجرای مناسب این قانون، مقرون‌به‌صرفه‌بودن و ضرورت تضمین دسترسی مؤثر همهٔ کشورهای عضو به کارشناسان.

۳. کمیسیون دسترسی به‌موقع کشورهای عضو به کارشناسان را در صورت نیاز تسهیل خواهد کرد و اطمینان خواهد داد که ترکیب فعالیت‌های پشتیبانی انجام‌شده از سوی پشتیبانی اتحادیه در زمینهٔ آزمون‌های هوش مصنوعی طبق ماده ۸۴ و کارشناسان موضوع این ماده به‌طور کارآمد سازمان‌دهی شده و بیشترین ارزش افزوده ممکن را فراهم می‌کند.

بخش ۲. مقامات صلاحیت‌دار ملی

ماده ۷۰. تعیین مقامات صلاحیت‌دار ملی و نقاط تماس واحد

۱. هر کشور عضو باید دست‌کم یک مرجع اطلاع‌رسانی و دست‌کم یک مرجع نظارت بر بازار را برای مقاصد این قانون ایجاد یا به‌عنوان مقام صلاحیت‌دار ملی تعیین کند. این مقامات صلاحیت‌دار ملی باید اختیارات خود را به‌طور مستقل، بی‌طرفانه و بدون جانب‌داری اعمال کنند تا عینیت فعالیت‌ها و وظایف‌شان حفظ و اجرای این قانون تضمین شود. اعضای این مقامات باید از هر اقدامی که با وظایف آنان ناسازگار است خودداری کنند. مشروط بر رعایت این اصول، چنین فعالیت‌ها و وظایفی

می‌تواند توسط یک یا چند مرجع تعیین‌شده، مطابق نیازهای سازمانی کشور عضو انجام پذیرد.

۲. کشورهای عضو باید هویت مراجع اطلاع‌رسانی و مراجع نظارت بر بازار و وظایف آن‌ها و همچنین هر گونه تغییرات بعدی را به کمیسیون اطلاع دهند. کشورهای عضو باید تا ۲ اوت ۲۰۲۵ اطلاعات مربوط به نحوهٔ تماس با مقامات صلاحیت‌دار و نقاط تماس واحد را از طریق ابزارهای ارتباط الکترونیکی به‌صورت عمومی در دسترس قرار دهند. کشورهای عضو باید یک مرجع نظارت بر بازار را به‌عنوان نقطهٔ تماس واحد برای این قانون تعیین کنند و هویت نقطهٔ تماس واحد را به کمیسیون اطلاع دهند. کمیسیون، فهرست نقاط تماس واحد را به‌صورت عمومی منتشر خواهد کرد.

۳. کشورهای عضو باید اطمینان حاصل کنند که مقامات صلاحیت‌دار ملی آن‌ها از منابع فنی، مالی و انسانی کافی و همچنین زیرساخت لازم برای انجام مؤثر وظایف خود طبق این قانون برخوردار باشند. به‌ویژه مقامات صلاحیت‌دار ملی باید تعداد کافی پرسنل دائمی در اختیار داشته باشند که صلاحیت‌ها و تخصص آن‌ها شامل درک عمیق از فناوری‌های هوش مصنوعی، داده و پردازش داده، حفاظت از داده‌های شخصی، امنیت سایبری، حقوق بنیادین، خطرات بهداشت و ایمنی و آگاهی از استانداردها و الزامات حقوقی موجود باشد. کشورهای عضو باید الزامات مربوط به صلاحیت و منابع موضوع این بند را سالانه ارزیابی و در صورت لزوم به‌روزرسانی کنند.

۴. مقامات صلاحیت‌دار ملی باید تدابیر مقتضی را برای تضمین سطح کافی از امنیت سایبری اتخاذ کنند.

۵. مقامات صلاحیت‌دار ملی هنگام انجام وظایف خود باید مطابق تعهدات محرمانگی مندرج در ماده ۷۸ عمل کنند.

۶. تا ۲ اوت ۲۰۲۵ و سپس هر دو سال یک بار، کشورهای عضو باید گزارشی به کمیسیون دربارهٔ وضعیت منابع مالی و انسانی مقامات صلاحیت‌دار ملی همراه با ارزیابی کفایت آن‌ها ارائه دهند. کمیسیون این اطلاعات را برای بحث و بررسی و صدور توصیه‌های احتمالی به هیئت منتقل خواهد کرد.

۷. کمیسیون، تبادل تجربه میان مقامات صلاحیت‌دار ملی را تسهیل خواهد کرد.

۸. مقامات صلاحیت‌دار ملی می‌توانند با درنظرگرفتن راهنمایی‌ها و توصیه‌های هیئت و کمیسیون، حسب مورد، راهنمایی و مشاوره در خصوص اجرای این قانون، به‌ویژه برای بنگاه‌های کوچک و متوسط ازجمله شرکت‌های نوپا ارائه کنند. هر گاه مقامات صلاحیت‌دار ملی قصد داشته باشند در خصوص یک سامانهٔ هوش مصنوعی در حوزه‌های مشمول سایر قوانین اتحادیه راهنمایی یا مشاوره ارائه دهند، مقامات صلاحیت‌دار ذی‌ربط تحت آن قوانین اتحادیه باید حسب مورد مورد مشورت قرار گیرند.

۹. در مواردی که نهادها، ارگان‌ها، دفاتر یا آژانس‌های اتحادیه در شمول این قانون قرار گیرند، ناظر اروپایی حفاظت از داده‌ها به‌عنوان مقام صلاحیت‌دار برای نظارت بر آن‌ها عمل خواهد کرد.

فصل هشتم. پایگاه دادهٔ اتحادیه برای سامانه‌های هوش مصنوعی پرخطر

ماده ۷۱. پایگاه دادهٔ اتحادیه برای سامانه‌های هوش مصنوعی پرخطر فهرست‌شده در پیوست سوم

۱. کمیسیون باید با همکاری کشورهای عضو، یک پایگاه دادهٔ اتحادیه ایجاد و نگهداری کند که شامل اطلاعات مذکور در بندهای ۲ و ۳ این ماده دربارهٔ سامانه‌های هوش مصنوعی پرخطر موضوع ماده ۶(۲) باشد که مطابق مواد ۴۹ و ۶۰ ثبت شده‌اند، و همچنین سامانه‌های هوش مصنوعی‌ای که طبق ماده ۶(۳) پرخطر تلقی نمی‌شوند و مطابق ماده ۶(۴) و ماده ۴۹ به ثبت رسیده‌اند. هنگام تعیین مشخصات عملکردی چنین پایگاه داده‌ای، کمیسیون باید با کارشناسان ذی‌ربط مشورت کند و هنگام به‌روزرسانی مشخصات عملکردی این پایگاه داده باید با هیئت مشورت کند.

۲. داده‌های مندرج در بخش‌های (الف) و (ب) از پیوست هشتم باید توسط ارائه‌دهنده یا در صورت اقتضا، نمایندهٔ مجاز وی در پایگاه دادهٔ اتحادیه وارد شوند.

۳. داده‌های مندرج در بخش (پ) از پیوست هشتم باید توسط بهره‌برداری‌کننده‌ای که خود یک مرجع، نهاد یا سازمان عمومی است یا از طرف آن‌ها اقدام می‌کند، مطابق ماده ۴۹(۳) و (۴) در پایگاه دادهٔ اتحادیه وارد شوند.

۴. به استثنای بخشی که در ماده ۴۹(۴) و ماده ۶۰(۴)، بند (ج) به آن اشاره شده است، اطلاعات مندرج در پایگاه دادهٔ اتحادیه که مطابق ماده ۴۹ ثبت شده‌اند باید به نحوی قابل دسترس و عمومی در اختیار همگان قرار گیرد. این اطلاعات باید به‌صورت کاربرپسند، به‌راحتی قابل جستجو و به‌صورت خوانا برای ماشین ارائه شوند. اطلاعاتی که مطابق ماده ۶۰ ثبت شده‌اند صرفاً برای مقامات نظارت بر بازار و کمیسیون قابل دسترس خواهد بود، مگر آنکه ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه رضایت دهد که اطلاعات برای عموم نیز قابل دسترس باشد.

۵. پایگاه دادهٔ اتحادیه فقط تا حدی شامل داده‌های شخصی خواهد بود که برای گردآوری و پردازش اطلاعات طبق این قانون ضروری است. این اطلاعات شامل نام و جزئیات تماس اشخاص حقیقی خواهد بود که مسئول ثبت سامانه بوده و اختیار قانونی نمایندگی ارائه‌دهنده یا بهره‌برداری‌کننده (بنا بر مورد) را دارند.

۶. کمیسیون مسئولیت *کنترل‌کنندهٔ* پایگاه دادهٔ اتحادیه را بر عهده خواهد داشت. کمیسیون

باید پشتیبانی فنی و اداری مناسب را برای ارائه‌دهندگان، ارائه‌دهندگان بالقوه و بهره‌برداری‌کنندگان فراهم کند. پایگاه دادهٔ اتحادیه باید با الزامات قابلیت دسترسی قابل اعمال مطابقت داشته باشد.

فصل نهم. پایش پس از عرضه، تبادل اطلاعات و نظارت بر بازار

بخش نخست. پایش پس از عرضه

ماده ۷۲. پایش پس از عرضه توسط ارائه‌دهندگان و طرح پایش پس از عرضه برای سامانه‌های هوش مصنوعی پرخطر

۱. ارائه‌دهندگان باید نظامی برای پایش پس از عرضه ایجاد و مستندسازی کنند، به گونه‌ای که متناسب با ماهیت فناوری‌های هوش مصنوعی و میزان ریسک سامانهٔ هوش مصنوعی پرخطر باشد.

۲. نظام پایش پس از عرضه باید به‌طور فعال و نظام‌مند داده‌های مربوط را که ممکن است توسط بهره‌برداری‌کنندگان ارائه شود یا از منابع دیگر دربارهٔ عملکرد سامانه‌های هوش مصنوعی پرخطر در طول چرخهٔ عمر آن‌ها گردآوری، مستندسازی و تحلیل کند؛ این داده‌ها باید به ارائه‌دهنده امکان دهد تا انطباق مستمر سامانه‌های هوش مصنوعی را با الزامات مقرر در فصل سوم، بخش دوم ارزیابی کند. در صورت اقتضا، پایش پس از عرضه باید شامل تحلیل تعامل با سایر سامانه‌های هوش مصنوعی نیز باشد. این تعهد شامل داده‌های عملیاتی حساسِ بهره‌برداری‌کنندگان که مقامات مجری قانون هستند نمی‌شود.

۳. نظام پایش پس از عرضه باید مبتنی بر یک طرح پایش پس از عرضه باشد. طرح پایش پس از عرضهٔ بخشی از مستندات فنی مذکور در پیوست چهارم خواهد بود. کمیسیون باید تا ۲ فوریهٔ ۲۰۲۶ یک *اقدام اجرایی* تصویب کند که در آن مقررات تفصیلی شامل الگوی طرح پایش پس از عرضه و فهرست عناصر لازم برای درج در طرح تعیین می‌شود. این اقدام اجرایی باید طبق رویهٔ بررسی مندرج در ماده ۹۸(۲) تصویب شود.

۴. در خصوص سامانه‌های هوش مصنوعی پرخطری که تحت قوانین هماهنگ‌سازی اتحادیه مندرج در بخش A از پیوست اول قرار می‌گیرند و در آن قوانین نظام و طرح پایش پس از عرضه از پیش برقرار شده است، به منظور تضمین سازگاری، اجتناب از تکرار و کاهش بار اضافی، ارائه‌دهندگان می‌توانند عناصر لازم مذکور در بندهای ۱، ۲ و ۳ را در صورت اقتضا، با استفاده از الگوی مذکور در بند ۳ در چارچوب نظام‌ها و طرح‌های موجود ادغام کنند، مشروط بر اینکه همان سطح معادل از حمایت حاصل شود.

قانون مندرج در بند نخست این بند همچنین نسبت به سامانه‌های هوش مصنوعی پرخطر موضوع بند ۵ پیوست سوم که توسط مؤسسات مالی عرضه یا به خدمت گرفته می‌شوند و مشمول الزامات حقوق خدمات مالی اتحادیه در خصوص حاکمیت داخلی، ترتیبات یا فرآیندهایشان هستند نیز اعمال خواهد شد.

بخش دوم. تبادل اطلاعات در خصوص حوادث جدی

ماده ۷۳. گزارش‌دهی حوادث جدی

۱. ارائه‌دهندگان سامانه‌های هوش مصنوعی پرخطر که در بازار اتحادیه عرضه شده‌اند، باید هر حادثهٔ جدی را به مقامات نظارت بر بازار کشورهای عضو که حادثه در آن‌ها رخ داده است گزارش دهند.

۲. گزارش مذکور در بند ۱ باید فوراً پس از آنکه ارائه‌دهنده، رابطهٔ علّی میان سامانهٔ هوش مصنوعی و حادثهٔ جدی یا احتمال معقول وجود چنین رابطه‌ای را احراز کرد، و در هر حال، حداکثر ظرف ۱۵ روز پس از آنکه ارائه‌دهنده یا در صورت اقتضا بهره‌بردار از حادثهٔ جدی مطلع شد، ارائه شود.

مهلت گزارش‌دهی مذکور در بند نخست باید متناسب با شدت حادثهٔ جدی در نظر گرفته شود.

۳. برخلاف بند ۲، در صورت نقض گسترده یا حادثهٔ جدی موضوع بند (ب) از جزء (۴۹) ماده ۳، گزارش مذکور در بند ۱ باید فوراً و حداکثر ظرف دو روز پس از آگاهی ارائه‌دهنده یا در صورت اقتضا بهره‌بردار از وقوع حادثه ارائه شود.

۴. برخلاف بند ۲، در صورت فوت شخص، گزارش باید بلافاصله پس از آنکه ارائه‌دهنده یا بهره‌بردار رابطهٔ علّی میان سامانهٔ هوش مصنوعی پرخطر و حادثهٔ جدی را احراز یا به آن مظنون شد، و در هر حال، حداکثر ظرف ۱۰ روز از تاریخ اطلاع ارائه‌دهنده یا در صورت اقتضا بهره‌بردار از وقوع حادثهٔ جدی ارائه شود.

۵. ارائه‌دهنده یا در صورت اقتضا بهره‌بردار، در صورت لزوم برای تضمین گزارش‌دهی به‌موقع، می‌تواند ابتدا گزارش ناقص ارائه کرده و متعاقباً گزارش کامل را تسلیم کند.

۶. پس از گزارش‌دهی حادثهٔ جدی طبق بند ۱، ارائه‌دهنده باید بی‌درنگ تحقیقات لازم را در خصوص حادثهٔ جدی و سامانهٔ هوش مصنوعی مربوط انجام دهد. این امر باید شامل ارزیابی ریسک حادثه و اقدامات اصلاحی باشد.

ارائه‌دهنده باید در جریان تحقیقات مذکور در بند نخست با مقامات صلاحیت‌دار و در صورت اقتضا با نهاد ارزیابی انطباق مربوط همکاری کند و پیش از اطلاع به مقامات صلاحیت‌دار، هیچ‌گونه تحقیقی که مستلزم تغییر سامانهٔ هوش مصنوعی مربوط باشد به گونه‌ای که بتواند ارزیابی‌های

بعدی از علل حادثه را تحت تأثیر قرار دهد، انجام ندهد.

۷. به‌محض دریافت اخطاریه مربوط به حادثهٔ جدی موضوع بند (ج) از جزء (۴۹) ماده ۳، مرجع نظارت بر بازار ذی‌ربط باید مقامات یا نهادهای ملی عمومی مذکور در ماده ۷۷(۱) را مطلع کند. کمیسیون باید دستورالعمل‌های ویژه‌ای برای تسهیل رعایت تعهدات مقرر در بند ۱ این ماده تدوین کند. این دستورالعمل‌ها باید تا ۲ اوت ۲۰۲۵ صادر و به‌طور منظم ارزیابی شوند.

۸. مرجع نظارت بر بازار باید ظرف هفت روز از تاریخ دریافت اخطاریهٔ موضوع بند ۱ این ماده، اقدامات مقتضی را طبق ماده ۱۹ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) اتخاذ کند و رویه‌های اطلاع‌رسانی مقرر در آن قانون را دنبال کند.

۹. در خصوص سامانه‌های هوش مصنوعی پرخطر مندرج در پیوست سوم که توسط ارائه‌دهندگانی عرضه یا به خدمت گرفته می‌شوند که مشمول اسناد قانونگذاری اتحادیه مشتمل بر تعهدات گزارش‌دهی معادل با آنچه در این قانون مقرر شده‌اند، گزارش‌دهی حوادث جدی محدود به موارد موضوع بند (ج) از جزء (۴۹) ماده ۳ خواهد بود.

۱۰. در خصوص سامانه‌های هوش مصنوعی پرخطری که اجزای ایمنی دستگاه‌ها هستند یا خود دستگاه محسوب می‌شوند و مشمول مقررات ۲۰۱۷/۷۴۵ (اتحادیهٔ اروپا) و ۲۰۱۷/۷۴۶ (اتحادیهٔ اروپا) هستند، گزارش‌دهی حوادث جدی محدود به موارد موضوع بند (ج) از جزء (۴۹) ماده ۳ این قانون خواهد بود و باید به مرجع صلاحیت‌دار ملی که برای این منظور توسط کشورهای عضو تعیین شده است، ارائه شود.

۱۱. مقامات صلاحیت‌دار ملی باید بی‌درنگ کمیسیون را از هر حادثهٔ جدی، صرف‌نظر از اینکه اقدامی نسبت به آن انجام داده باشند یا خیر، مطابق ماده ۲۰ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) مطلع کنند.

بخش سوم. اعمال و اجرا

ماده ۷۴. نظارت بر بازار و کنترل سامانه‌های هوش مصنوعی در بازار اتحادیه

۱. قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) در خصوص سامانه‌های هوش مصنوعی مشمول این قانون اعمال خواهد شد. به منظور تضمین اجرای مؤثر این قانون:

الف) هر گونه اشاره به یک *عامل اقتصادی* در قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) باید به‌عنوان شمول تمامی عاملان مذکور در ماده ۲(۱) این قانون تلقی شود؛

ب) هر گونه اشاره به یک *محصول* در قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) باید به‌عنوان شمول تمامی سامانه‌های هوش مصنوعی داخل در دامنهٔ شمول این قانون تلقی شود.

۲. در چارچوب الزامات گزارش‌دهی طبق ماده ۳۴(۴) قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا)، مقامات ناظر بر بازار باید هر سال به کمیسیون و مراجع ملی رقابت مربوطه، هر گونه اطلاعاتی را که در جریان فعالیت‌های نظارت بر بازار به دست آورده‌اند و ممکن است برای اجرای حقوق رقابت اتحادیه سودمند باشد، گزارش کنند. آنان همچنین باید هر سال به کمیسیون در خصوص استفاده از رویه‌های ممنوع در طول آن سال و اقدامات اتخاذشده گزارش دهند.

۳. برای سامانه‌های هوش مصنوعی پرخطر مرتبط با محصولاتی که تحت قوانین هماهنگ‌سازی اتحادیه مندرج در بخش (الف) پیوست اول پوشش داده شده‌اند، مقام ناظر بر بازار برای مقاصد این قانون همان مرجعی خواهد بود که تحت آن اسناد حقوقی تعیین شده است.

با وجود قاعدهٔ مذکور در بند نخست و در شرایط مقتضی، دولت‌های عضو می‌توانند مرجع ذی‌صلاح دیگری را به‌عنوان مقام ناظر بر بازار تعیین کنند، مشروط بر آنکه هماهنگی با مراجع ناظر بخشی مربوط به اجرای قوانین هماهنگ‌سازی اتحادیه مندرج در پیوست اول تضمین شود.

۴. رویه‌های مذکور در مواد ۷۹ تا ۸۳ این قانون در خصوص سامانه‌های هوش مصنوعی مرتبط با محصولاتی که تحت قوانین هماهنگ‌سازی اتحادیه مندرج در بخش (الف) پیوست اول پوشش داده شده‌اند اعمال نخواهد شد، چنانچه آن اسناد حقوقی از پیش دارای رویه‌هایی باشند که سطح معادل حفاظت را تضمین کرده و همان هدف را دنبال می‌کنند. در این موارد، رویه‌های بخشی مربوطه اعمال خواهد شد.

۵. بدون لطمه به اختیارات مقامات ناظر بر بازار طبق ماده ۱۴ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا)، و به منظور تضمین اجرای مؤثر این قانون، مقامات ناظر بر بازار می‌توانند اختیارات مذکور در ماده ۱۴(۴)، بندهای (د) و (ی) آن قانون را در صورت اقتضا به‌طور دورکار اعمال کنند.

۶. برای سامانه‌های هوش مصنوعی پرخطرِ عرضه‌شده در بازار، بهره‌برداری‌شده یا مورد استفاده توسط مؤسسات مالی مشمول حقوق خدمات مالی اتحادیه، مقام ناظر بر بازار برای مقاصد این قانون، مرجع ملی ذی‌صلاح در خصوص نظارت مالی بر آن مؤسسات طبق آن اسناد حقوقی خواهد بود، تا جایی که عرضه در بازار، بهره‌برداری یا استفاده از سامانهٔ هوش مصنوعی مستقیماً با ارائهٔ آن خدمات مالی مرتبط باشد.

۷. به طریق استثنا از بند ۶، در شرایط مقتضی و مشروط بر تضمین هماهنگی، دولت عضو می‌تواند مرجع ذی‌صلاح دیگری را به‌عنوان مقام ناظر بر بازار برای مقاصد این قانون تعیین کند.

مقامات ملی ناظر بر بازار که بر مؤسسات اعتباری تحت نظارت دستورالعمل۲۰۱۳/۳۶/EU نظارت دارند و در مکانیزم نظارتی واحد تأسیس‌شده تحت قانون شمارهٔ ۱۰۲۴/۲۰۱۳ (اتحادیهٔ اروپا) مشارکت دارند، باید بدون تأخیر، هر گونه اطلاعاتی را که در جریان فعالیت‌های نظارت بر بازارشان

ممکن است برای وظایف نظارت احتیاطی بانک مرکزی اروپا (مطابق آن قانون) سودمند باشد، به بانک مرکزی اروپا گزارش کنند.

۸. برای سامانه‌های هوش مصنوعی پرخطر مندرج در بند ۱ پیوست سوم این قانون، تا آنجا که این سامانه‌ها برای مقاصد اجرای قانون، مدیریت مرزها و عدالت و دموکراسی استفاده می‌شوند و برای سامانه‌های هوش مصنوعی پرخطر مندرج در بندهای ۶، ۷ و ۸ پیوست سوم این قانون، دولت‌های عضو باید برای مقاصد این قانون یا مراجع ناظر بر حفاظت از داده طبق قانون ۲۰۱۶/۶۷۹ (اتحادیهٔ اروپا) یا دستورالعمل ۲۰۱۶/۶۸۰، یا هر مرجع دیگری که تحت همان شرایط مندرج در مواد ۴۱ تا ۴۴ دستورالعمل ۲۰۱۶/۶۸۰ تعیین شده باشد، مقامات ناظر بر بازار منصوب کنند. فعالیت‌های نظارت بر بازار به هیچ وجه نباید استقلال مقامات قضایی را تحت تأثیر قرار داده یا به گونه‌ای دیگر در فعالیت‌های آنان، زمانی که در ظرفیت قضایی خود عمل می‌کنند مداخله کند.

۹. هنگامی که نهادها، ارگان‌ها، دفاتر یا آژانس‌های اتحادیه در دامنهٔ شمول این قانون قرار گیرند، ناظر حفاظت از داده‌های اروپا به‌عنوان مقام ناظر بر بازار آنان عمل خواهد کرد، مگر در ارتباط با دیوان دادگستری اتحادیهٔ اروپا، زمانی که در ظرفیت قضایی خود عمل می‌کند.

۱۰. دولت‌های عضو باید هماهنگی میان مقامات ناظر بر بازار تعیین‌شده تحت این قانون و سایر مراجع یا نهادهای ملی مربوطه را که اجرای قوانین هماهنگ‌سازی اتحادیه مندرج در پیوست اول یا سایر قوانین اتحادیه که ممکن است برای سامانه‌های هوش مصنوعی پرخطر مندرج در پیوست سوم مرتبط باشند نظارت می‌کنند، تسهیل کنند.

۱۱. مقامات ناظر بر بازار و کمیسیون باید قادر باشند فعالیت‌های مشترک، ازجمله تحقیقات مشترک را پیشنهاد دهند که یا توسط مقامات ناظر بر بازار یا به‌طور مشترک با کمیسیون انجام شوند، با هدف ترویج انطباق، شناسایی عدم انطباق، افزایش آگاهی یا ارائهٔ راهنمایی در ارتباط با این قانون در خصوص دسته‌های خاصی از سامانه‌های هوش مصنوعی پرخطری که بر اساس ماده ۹ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) مشخص شده‌اند و در دو یا چند دولت عضو خطر جدی ایجاد می‌کنند. دفتر هوش مصنوعی پشتیبانی هماهنگی برای تحقیقات مشترک را فراهم خواهد کرد.

۱۲. بدون لطمه به اختیارات مقرر در قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) و در صورت اقتضا و محدود به آنچه برای ایفای وظایفشان ضروری است، مقامات ناظر بر بازار باید از سوی ارائه‌دهندگان دسترسی کامل به مستندات و همچنین داده‌های آموزش، اعتبارسنجی و آزمایش مورد استفاده در توسعهٔ سامانه‌های هوش مصنوعی پرخطر داشته باشند؛ این امر شامل دسترسی، در صورت مناسب‌بودن و با رعایت تدابیر امنیتی، از طریق رابط‌های برنامه‌نویسی کاربردی یا سایر ابزارها و روش‌های فنی مرتبط که امکان دسترسی دورکار را فراهم می‌کنند نیز می‌شود.

۱۳. مقامات ناظر بر بازار باید بر اساس درخواست مستدل و تنها در صورتی که هر دو شرط زیر فراهم باشد به کد منبع سامانهٔ هوش مصنوعی پرخطر دسترسی یابند:

الف) دسترسی به کد منبع برای ارزیابی انطباق یک سامانهٔ هوش مصنوعی پرخطر با الزامات مندرج در فصل سوم، بخش ۲ ضروری باشد؛ و

ب) رویه‌ها یا ممیزی‌های مبتنی بر داده‌ها و مستندات ارائه‌شده توسط ارائه‌دهنده، یا به پایان رسیده باشند یا ناکافی تشخیص داده شوند.

۱۴. هر گونه اطلاعات یا مستنداتی که توسط مقامات ناظر بر بازار به دست آمده باشد باید مطابق تعهدات محرمانگی مندرج در ماده ۷۸ مورد رسیدگی قرار گیرد.

ماده ۷۵. معاضدت متقابل، نظارت بر بازار و کنترل سامانه‌های هوش مصنوعی با مقاصد عام

۱. هر گاه یک سامانهٔ هوش مصنوعی بر مبنای یک مدل هوش مصنوعی با مقاصد عام توسعه یافته باشد و مدل و سامانه هر دو توسط ارائه‌دهندهٔ واحد ایجاد شده باشند، *دفتر هوش مصنوعی* اختیار نظارت و پایش بر رعایت الزامات این قانون توسط آن سامانه را خواهد داشت. برای اجرای وظایف نظارت و پایش خود، دفتر هوش مصنوعی واجد تمامی اختیارات یک مقام ناظر بر بازار، مندرج در این بخش و در قانون (اتحادیهٔ اروپا) ۱۰۲۰/۲۰۱۹ خواهد بود.

۲. هر گاه مقامات ناظر بر بازار مربوطه دلایل کافی در اختیار داشته باشند که سامانه‌های هوش مصنوعی با مقاصد عام که می‌توانند مستقیماً توسط بهره‌برداران برای حداقل یک کاربری طبقه‌بندی‌شده به‌عنوان پرخطر طبق این قانون به کار روند با الزامات مقرر در این قانون منطبق نیستند، باید برای انجام ارزیابی‌های انطباق با دفتر هوش مصنوعی همکاری کرده و هیئت و سایر مقامات ناظر بر بازار را نیز متعاقباً مطلع کنند.

۳. هر گاه یک مقام ناظر بر بازار نتواند به دلیل ناتوانی در دسترسی به اطلاعات خاصی مرتبط با مدل هوش مصنوعی با مقاصد عام، علی‌رغم انجام تمامی تلاش‌های مقتضی برای کسب آن اطلاعات، تحقیقات خود را دربارهٔ سامانهٔ هوش مصنوعی پرخطر خاتمه دهد، می‌تواند درخواست مستدل خود را به دفتر هوش مصنوعی ارائه کند. در این صورت، دفتر هوش مصنوعی باید بدون تأخیر و در هر حال، ظرف ۳۰ روز، هر گونه اطلاعاتی را که مرتبط با احراز عدم انطباق سامانهٔ هوش مصنوعی پرخطر تشخیص می‌دهد، در اختیار مرجع متقاضی قرار دهد. مقامات ناظر بر بازار موظف‌اند محرمانگی اطلاعاتی را که مطابق ماده ۷۸ این قانون به دست می‌آورند، رعایت کنند. رویهٔ مقرر

در فصل ششم قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) با رعایت تغییرات مقتضی اعمال خواهد شد.

ماده ۷۶. نظارت بر آزمایش در شرایط واقعی توسط مقامات ناظر بر بازار

۱. مقامات ناظر بر بازار دارای صلاحیت‌ها و اختیارات لازم خواهند بود تا اطمینان حاصل کنند که آزمایش در شرایط واقعی مطابق این قانون انجام می‌شود.

۲. در مواردی که آزمایش در شرایط واقعی برای سامانه‌های هوش مصنوعی انجام شود که در چارچوب یک سندباکس نظارتی هوش مصنوعی طبق ماده ۵۸ تحت نظارت قرار دارند، مقامات ناظر بر بازار باید به‌عنوان بخشی از نقش نظارتی خود در سندباکس نظارتی هوش مصنوعی، رعایت ماده ۶۰ را بررسی کنند. این مقامات می‌توانند حسب مورد، اجازه دهند آزمایش در شرایط واقعی توسط ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه انجام شود، به‌عنوان استثنا از شرایط مقرر در بند (و) و (ز) ماده ۶۰(۴).

۳. در صورتی که یک مقام ناظر بر بازار توسط ارائه‌دهندهٔ بالقوه، ارائه‌دهنده یا هر شخص ثالثی از وقوع یک حادثهٔ جدی مطلع شود یا دلایل دیگری برای این نتیجه‌گیری داشته باشد که شرایط مقرر در مواد ۶۰ و ۶۱ رعایت نشده است، می‌تواند حسب مورد، در قلمرو خود، یکی از تصمیمات زیر را اتخاذ کند:

الف) تعلیق یا خاتمه آزمایش در شرایط واقعی؛

ب) الزام ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه و بهره‌بردار یا بهره‌بردار بالقوه به اصلاح هر جنبه‌ای از آزمایش در شرایط واقعی.

۴. هنگامی که یک مقام ناظر بر بازار، تصمیمی از نوع مذکور در بند ۳ این ماده اتخاذ یا اعتراضی در معنای بند (ب) ماده ۶۰(۴) مطرح کند، تصمیم یا اعتراض باید متضمن دلایل آن و نیز چگونگی امکان اعتراض ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه به آن تصمیم یا اعتراض باشد.

۵. حسب مورد، هنگامی که یک مقام ناظر بر بازار، تصمیمی از نوع مذکور در بند ۳ اتخاذ کرده باشد، باید دلایل آن را به مقامات ناظر بر بازار دیگر کشورهای عضو که سامانهٔ هوش مصنوعی بر اساس برنامهٔ آزمایش در آن‌ها آزمایش شده است، اطلاع دهد.

ماده ۷۷. اختیارات مقامات حافظ حقوق بنیادین

۱. مقامات یا نهادهای عمومی ملی که نظارت یا اجرای تعهدات مقرر در حقوق اتحادیه در زمینهٔ حمایت از حقوق بنیادین، ازجمله حق برابری و عدم تبعیض را در ارتباط با استفاده از سامانه‌های

هوش مصنوعی پرخطر مذکور در پیوست سوم بر عهده دارند، اختیار خواهند داشت هر گونه مستنداتی را که بر اساس این قانون ایجاد یا نگهداری شده است، در زبانی و قالبی قابل دسترس، در صورتی که دسترسی به آن مستندات برای انجام مؤثر مأموریت‌هایشان در حدود صلاحیت‌شان ضروری باشد، درخواست و دریافت کنند. مقام یا نهاد عمومی ذی‌ربط باید مقام ناظر بر بازار کشور عضو مربوطه را از هر گونه چنین درخواستی مطلع کند.

۲. هر کشور عضو باید حداکثر تا ۲ نوامبر ۲۰۲۴، مقامات یا نهادهای عمومی موضوع بند ۱ را شناسایی و فهرستی از آن‌ها را به‌طور عمومی منتشر کند. کشورهای عضو باید این فهرست را به کمیسیون و سایر کشورهای عضو اطلاع دهند و آن را به‌روزرسانی کنند.

۳. در مواردی که مستندات مذکور در بند ۱ برای احراز اینکه آیا نقضی از تعهدات مقرر در حقوق اتحادیه در زمینهٔ حمایت از حقوق بنیادین رخ داده است کافی نباشد، مقام یا نهاد عمومی مذکور در بند ۱ می‌تواند درخواستی مستدل به مقام ناظر بر بازار ارائه کند تا آزمایش سامانهٔ هوش مصنوعی پرخطر از طریق ابزارهای فنی سازمان‌دهی شود. مقام ناظر بر بازار باید این آزمایش را با مشارکت نزدیک مقام یا نهاد عمومی درخواست‌کننده و ظرف مهلتی معقول پس از دریافت درخواست سازمان‌دهی کند.

۴. هر گونه اطلاعات یا مستنداتی که توسط مقامات یا نهادهای عمومی ملی مذکور در بند ۱ این ماده به موجب این ماده به دست آمده باشد، باید مطابق تعهدات محرمانگی مقرر در ماده ۷۸ پردازش شود.

ماده ۷۸. محرمانگی

۱. کمیسیون، مقامات ناظر بر بازار، نهادهای ارزیابی انطباق و هر شخص حقیقی یا حقوقی دیگری که در اجرای این قانون مشارکت دارد، باید مطابق حقوق اتحادیه یا حقوق ملی، محرمانگی اطلاعات و داده‌های به‌دست‌آمده در جریان انجام وظایف و فعالیت‌های خود را رعایت کنند، به نحوی که به‌ویژه از موارد زیر حمایت شود:

الف) حقوق مالکیت فکری و اطلاعات تجاری محرمانه یا اسرار تجاری اشخاص حقیقی یا حقوقی، ازجمله کُد مبدأ، مگر در موارد مذکور در ماده ۵ دستورالعمل ۲۰۱۶/۹۴۳ پارلمان و شورای اروپا اتحادیهٔ اروپا؛[۱۹۱]

ب) اجرای مؤثر این قانون، به‌ویژه برای مقاصد بازرسی‌ها، تحقیقات یا حسابرسی‌ها؛

۱۹۱. دستورالعمل ۲۰۱۶/۹۴۳ پارلمان اروپا و شورا در ۸ ژوئن ۲۰۱۶ در مورد حفاظت از دانش فنی و اطلاعات تجاری افشانشده (اسرار تجاری) در برابر کسب، استفاده و افشای غیرقانونی آن‌ها (روزنامهٔ رسمی ۱۵۷، ۲۰۱۶/۶/۱۵، ص ۱).

ج) منافع امنیت عمومی و ملی؛
د) جریان دادرسی‌های کیفری یا اداری؛
هـ) اطلاعاتی که طبق حقوق اتحادیه یا حقوق ملی طبقه‌بندی شده است.

۲. مقامات مشارکت‌کننده در اجرای این قانون، موضوع بند ۱ صرفاً باید داده‌هایی را درخواست کنند که برای ارزیابی خطر ناشی از سامانه‌های هوش مصنوعی و برای اعمال اختیاراتشان مطابق این قانون و قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) به‌طور دقیق ضروری است. آن‌ها باید تدابیر کافی و مؤثر امنیت سایبری برای حفاظت از امنیت و محرمانگی اطلاعات و داده‌های به‌دست‌آمده اتخاذ کنند و داده‌های جمع‌آوری‌شده را به‌محض اینکه دیگر برای هدفی که برای آن به دست آمده‌اند مورد نیاز نباشد، طبق حقوق اتحادیه یا حقوق ملی مربوطه حذف کنند.

۳. بدون خدشه به بندهای ۱ و ۲، اطلاعاتی که محرمانه میان مقامات صلاحیت‌دار ملی یا میان مقامات صلاحیت‌دار ملی و کمیسیون مبادله می‌شود، بدون مشورت قبلی با مقام صلاحیت‌دار ملی مبدأ و بهره‌بردار، هنگامی که سامانه‌های هوش مصنوعی پرخطر مذکور در بندهای ۱، ۶ یا ۷ پیوست سوم توسط مقامات اجرای قانون، کنترل مرزی، مهاجرت یا پناهندگی به کار می‌روند و چنین افشایی منافع امنیت عمومی و ملی را به خطر می‌اندازد، نباید افشا شود. این مبادلهٔ اطلاعات شامل داده‌های عملیاتی حساس مربوط به فعالیت‌های مقامات اجرای قانون، کنترل مرزی، مهاجرت یا پناهندگی نمی‌شود.

هنگامی که مقامات اجرای قانون، مهاجرت یا پناهندگی، خود ارائه‌دهندهٔ سامانه‌های هوش مصنوعی پرخطر مذکور در بندهای ۱، ۶ یا ۷ پیوست سوم باشند، مستندات فنی مذکور در پیوست چهارم باید در محل این مقامات باقی بماند. این مقامات باید تضمین کنند که مقامات ناظر بر بازار مذکور در ماده ۷۴ (بندهای ۸ و ۹)، حسب مورد بتوانند بنا به درخواست، بلافاصله به مستندات دسترسی پیدا کنند یا نسخه‌ای از آن را دریافت کنند. تنها کارکنان مقام ناظر بر بازار که دارای سطح صلاحیت امنیتی مناسب باشند مجاز به دسترسی به آن مستندات یا هر نسخه‌ای از آن خواهند بود.

۴. بندهای ۱، ۲ و ۳ به حقوق یا تعهدات کمیسیون، کشورهای عضو و مقامات ذی‌ربط آن‌ها و نیز به حقوق یا تعهدات نهادهای ارزیابی انطباق در خصوص تبادل اطلاعات و انتشار هشدارها، ازجمله در چارچوب همکاری فرامرزی، خدشه‌ای وارد نمی‌کند؛ همچنین تعهدات طرف‌های ذی‌ربط به ارائهٔ اطلاعات تحت حقوق کیفری کشورهای عضو را نیز تحت تأثیر قرار نمی‌دهد.

۵. کمیسیون و کشورهای عضو می‌توانند در صورت لزوم و مطابق مقررات مندرج در موافقت‌نامه‌های بین‌المللی و تجاری، اطلاعات محرمانه را با مقامات نظارتی کشورهای ثالثی که با آن‌ها ترتیبات

محرمانگی دوجانبه یا چندجانبه منعقد کرده‌اند و سطح کافی از محرمانگی را تضمین می‌کنند، مبادله کنند.

ماده ۷۹. روند رسیدگی در سطح ملی به سامانه‌های هوش مصنوعی که خطر ایجاد می‌کنند

۱. سامانه‌های هوش مصنوعی که خطر ایجاد می‌کنند، در صورتی که برای سلامت یا ایمنی اشخاص یا برای حقوق بنیادین آنان خطر داشته باشند، به‌عنوان *محصول ایجادکنندهٔ خطر*، مطابق تعریف ماده ۳، بند ۱۹ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) تلقی خواهند شد.

۲. هنگامی که مقام ناظر بر بازار یک کشور عضو، دلایل کافی برای آن داشته باشد که یک سامانهٔ هوش مصنوعی خطر ایجاد می‌کند، به معنای مذکور در بند ۱، آن مقام باید ارزیابی سامانهٔ موردنظر را در خصوص انطباق آن با کلیهٔ الزامات و تعهدات مندرج در این قانون انجام دهد. توجه ویژه باید به سامانه‌های هوش مصنوعی که برای گروه‌های آسیب‌پذیر، خطر ایجاد می‌کنند معطوف شود. چنانچه خطراتی برای حقوق بنیادین شناسایی شود، مقام ناظر بر بازار باید همچنین مقام یا نهاد عمومی ملی ذی‌ربط موضوع ماده ۷۷(۱) را مطلع کرده و همکاری کامل با آن‌ها داشته باشد. بهره‌برداران ذی‌ربط باید همکاری‌های لازم را با مقام ناظر بر بازار و دیگر مقامات یا نهادهای عمومی ملی موضوع ماده ۷۷(۱) به عمل آورند.

چنانچه مقام ناظر بر بازار یا حسب مورد، مقام ناظر بر بازار در همکاری با مقام عمومی ملی موضوع ماده ۷۷(۱) در جریان آن ارزیابی احراز کند که سامانهٔ هوش مصنوعی با الزامات و تعهدات این قانون منطبق نیست، باید بدون تأخیر غیرموجه از بهره‌بردار ذی‌ربط بخواهد تمامی اقدامات اصلاحی مناسب را برای ایجاد انطباق یا جمع‌آوری سامانه از بازار یا فراخوانی آن، ظرف مدتی که آن مقام تعیین می‌کند و در هر حال، ظرف مدت کوتاه‌تر از ۱۵ روز کاری یا مدتی که در قوانین هماهنگ اتحادیهٔ اروپا مقرر شده است، به عمل آورد.

مقام ناظر بر بازار باید نهاد ارزیابی انطباق ذی‌ربط را نیز از این امر مطلع کند. ماده ۱۸ قانون۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) در مورد اقدامات مذکور در این بند اعمال خواهد شد.

۳. هر گاه مقام ناظر بر بازار تشخیص دهد که عدم انطباق به قلمرو ملی او محدود نیست، باید بدون تأخیر غیرموجه، کمیسیون و دیگر کشورهای عضو را از نتایج ارزیابی و اقدامات موردنظر که از بهره‌بردار خواسته است اتخاذ کند، مطلع سازد.

۴. بهره‌بردار باید تضمین کند که تمامی اقدامات اصلاحی مناسب در خصوص تمامی سامانه‌های هوش مصنوعی ذی‌ربط که در بازار اتحادیه عرضه کرده است، انجام شود.

۵. چنانچه بهره‌بردار سامانهٔ هوش مصنوعی ظرف مهلت مقرر در بند ۲ اقدامات اصلاحی کافی اتخاذ نکند، مقام ناظر بر بازار باید تمامی اقدامات موقتی مقتضی را برای ممنوع‌کردن یا محدودکردن عرضهٔ سامانه در بازار ملی خود یا بهره‌برداری از آن یا جمع‌آوری آن محصول یا سامانهٔ مستقل از بازار یا فراخوانی آن اتخاذ کند. آن مقام باید بدون تأخیر غیرموجه، کمیسیون و دیگر کشورهای عضو را از این اقدامات مطلع کند.

۶. اطلاع‌رسانی موضوع بند ۵ باید شامل تمامی جزئیات موجود باشد، به‌ویژه اطلاعات لازم برای شناسایی سامانهٔ غیرمنطبق، منشأ سامانه و زنجیرهٔ تأمین آن، ماهیت عدم انطباق ادعایی و خطر موجود، ماهیت و مدت اقدامات ملی اتخاذشده و استدلال‌های ارائه‌شده توسط بهره‌بردار ذی‌ربط. به‌ویژه مقامات ناظر بر بازار باید مشخص کنند که آیا عدم انطباق ناشی از یک یا چند مورد از موارد زیر است:

الف) عدم انطباق با ممنوعیت رویه‌های هوش مصنوعی مذکور در ماده ۵؛

ب) عدم رعایت الزامات مندرج در فصل سوم، بخش ۲ توسط سامانهٔ هوش مصنوعی پرخطر؛

ج) کاستی‌ها در استانداردهای هماهنگ یا مشخصات مشترک موضوع مواد ۴۰ و ۴۱ که دلالت بر انطباق دارند؛

د) عدم انطباق با ماده ۵۰.

۷. مقامات ناظر بر بازار بجز مقام ناظر بر بازار کشور عضو آغازکنندهٔ رویه باید بدون تأخیر غیرموجه، کمیسیون و دیگر کشورهای عضو را از هر گونه اقدام اتخاذشده و هر گونه اطلاعات تکمیلی در اختیار خود در خصوص عدم انطباق سامانهٔ هوش مصنوعی ذی‌ربط مطلع کنند و در صورت مخالفت با اقدام ملی اطلاع‌رسانی‌شده، اعتراض خود را اعلام کنند.

۸. چنانچه ظرف سه ماه از دریافت اطلاع‌رسانی موضوع بند ۵، هیچ اعتراضی از سوی مقام ناظر بر بازار یک کشور عضو یا کمیسیون نسبت به اقدام موقتی اتخاذشده توسط مقام ناظر بر بازار کشور عضو دیگر مطرح نشود، آن اقدام موجه تلقی خواهد شد. این امر بدون خدشه به حقوق آیینی بهره‌بردار ذی‌ربط طبق ماده ۱۸ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) خواهد بود. مهلت سه‌ماههٔ مذکور در این بند در صورت عدم انطباق با ممنوعیت رویه‌های هوش مصنوعی موضوع ماده ۵ این قانون، به ۳۰ روز کاهش می‌یابد.

۹. مقامات ناظر بر بازار باید اطمینان حاصل کنند که اقدامات محدودکنندهٔ مقتضی در خصوص محصول یا سامانهٔ هوش مصنوعی موردنظر، مانند جمع‌آوری آن از بازار، بدون تأخیر غیرموجه اتخاذ شود.

ماده ۸۰. روند رسیدگی به سامانه‌های هوش مصنوعی که توسط ارائه‌دهنده به‌عنوان غیرپرخطر طبقه‌بندی شده‌اند طبق پیوست سوم

۱. هر گاه مقام ناظر بر بازار، دلایل کافی برای آن داشته باشد که سامانهٔ هوش مصنوعی که توسط ارائه‌دهنده طبق ماده ۶(۳) به‌عنوان غیرپرخطر طبقه‌بندی شده است، در واقع پرخطر است، مقام ناظر بر بازار باید ارزیابی سامانهٔ موردنظر را در خصوص طبقه‌بندی آن به‌عنوان سامانهٔ هوش مصنوعی پرخطر بر اساس شرایط مندرج در ماده ۶(۳) و دستورالعمل‌های کمیسیون انجام دهد.

۲. هر گاه مقام ناظر بر بازار در جریان آن ارزیابی احراز کند که سامانهٔ موردنظر پرخطر است، باید بدون تأخیر غیرموجه از ارائه‌دهندهٔ ذی‌ربط بخواهد تمامی اقدامات لازم را برای انطباق سامانهٔ هوش مصنوعی با الزامات و تعهدات مندرج در این قانون و نیز اقدامات اصلاحی مقتضی ظرف مدتی که آن مقام تعیین می‌کند، اتخاذ نماید.

۳. هر گاه مقام ناظر بر بازار تشخیص دهد که استفاده از سامانهٔ موردنظر به قلمرو ملی او محدود نیست، باید بدون تأخیر غیرموجه، کمیسیون و دیگر کشورهای عضو را از نتایج ارزیابی و اقدامات موردنظر که از ارائه‌دهنده خواسته است اتخاذ کند، مطلع سازد.

۴. ارائه‌دهنده باید تضمین کند که تمامی اقدامات لازم برای انطباق سامانهٔ هوش مصنوعی با الزامات و تعهدات مندرج در این قانون انجام شود. چنانچه ارائه‌دهندهٔ سامانهٔ موردنظر ظرف مهلت مذکور در بند ۲ این ماده سامانهٔ هوش مصنوعی را با الزامات و تعهدات یادشده منطبق نکند، مشمول جریمه‌های مقرر در ماده ۹۹ خواهد شد.

۵. ارائه‌دهنده باید تضمین کند که تمامی اقدامات اصلاحی مناسب در خصوص تمامی سامانه‌های هوش مصنوعی ذی‌ربط که در بازار اتحادیه عرضه کرده است، انجام شود.

۶. چنانچه ارائه‌دهندهٔ سامانهٔ موردنظر ظرف مهلت مذکور در بند ۲ این ماده اقدامات اصلاحی کافی اتخاذ نکند، بندهای ۵ تا ۹ ماده ۷۹ اعمال خواهند شد.

۷. هر گاه مقام ناظر بر بازار در جریان ارزیابی موضوع بند ۱ این ماده احراز کند که سامانهٔ هوش مصنوعی توسط ارائه‌دهنده به‌نادرست به‌عنوان غیرپرخطر طبقه‌بندی شده است تا از شمول الزامات فصل سوم، بخش ۲ اجتناب شود، ارائه‌دهنده مشمول جریمه‌های مقرر در ماده ۹۹ خواهد شد.

۸. مقامات ناظر بر بازار در اعمال اختیار خود برای نظارت بر اجرای این ماده و طبق ماده ۱۱ قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا) می‌توانند بررسی‌های مقتضی را، به‌ویژه با درنظرگرفتن اطلاعات ذخیره‌شده در پایگاه دادهٔ اتحادیه، موضوع ماده ۷۱ این قانون انجام دهند.

ماده ۸۱. رویهٔ حفاظتی اتحادیه

۱. هر گاه ظرف سه ماه از تاریخ دریافت اطلاعیهٔ موضوع ماده ۷۹(۵) یا ظرف ۳۰ روز در مورد عدم انطباق با ممنوعیت شیوه‌های هوش مصنوعی موضوع ماده ۵، از سوی مقام ناظر بر بازار، یکی از کشورهای عضو نسبت به اقدام اتخاذشده توسط مقام ناظر بر بازار کشور عضو دیگر ایراد وارد شود یا کمیسیون اقدام را مغایر با حقوق اتحادیه بداند، کمیسیون باید بدون تأخیر غیرموجه وارد مشاوره با مقام ناظر بر بازار کشور عضو ذی‌ربط و نیز با بهره‌بردار یا بهره‌برداران شود و اقدام ملی را ارزیابی کند. بر اساس نتایج این ارزیابی، کمیسیون باید ظرف شش ماه یا ظرف ۶۰ روز در مورد عدم انطباق با ممنوعیت شیوه‌های هوش مصنوعی موضوع ماده ۵، از تاریخ اطلاعیهٔ موضوع ماده ۷۹(۵) تصمیم بگیرد که آیا اقدام ملی موجه است یا خیر و تصمیم خود را به مقام ناظر بر بازار کشور عضو مربوطه اطلاع دهد. کمیسیون همچنین باید تمامی مقامات ناظر بر بازار دیگر کشورها را از تصمیم خود مطلع کند.

۲. هر گاه کمیسیون اقدام اتخاذشده توسط کشور عضو ذی‌ربط را موجه بداند، تمامی کشورهای عضو باید تضمین کنند که اقدامات محدودکنندهٔ مناسب در خصوص سامانهٔ هوش مصنوعی موردنظر اتخاذ می‌شود، ازجمله الزام به جمع‌آوری سامانهٔ هوش مصنوعی از بازارشان بدون تأخیر غیرموجه، و باید کمیسیون را از آن مطلع کنند. هر گاه کمیسیون اقدام ملی را ناموجه بداند، کشور عضو مربوطه باید اقدام خود را مسترد دارد و کمیسیون را آگاه کند.

۳. هر گاه اقدام ملی موجه دانسته شود و عدم انطباق سامانهٔ هوش مصنوعی ناشی از کاستی‌ها در استانداردهای هماهنگ یا مشخصات مشترک موضوع مواد ۴۰ و ۴۱ این قانون باشد، کمیسیون باید رویهٔ مقرر در ماده ۱۱ قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۲/۱۰۲۵ را اعمال کند.

ماده ۸۲. سامانه‌های هوش مصنوعی منطبق که خطر ایجاد می‌کنند

۱. هر گاه مقام ناظر بر بازار یکی از کشورهای عضو، پس از انجام ارزیابی موضوع ماده ۷۹ و پس از مشورت با مقام عمومی ملی ذی‌ربط موضوع ماده ۷۷(۱)، احراز کند که اگرچه یک سامانهٔ هوش مصنوعی پرخطر با قانون حاضر مطابقت دارد، خطری برای سلامت یا ایمنی اشخاص، حقوق بنیادین یا سایر جنبه‌های حمایت از منافع عمومی ایجاد می‌کند، آن مقام باید بهره‌بردار ذی‌ربط را ملزم کند که تمامی تدابیر مقتضی را اتخاذ کند تا اطمینان حاصل شود که سامانهٔ هوش مصنوعی موردنظر، هنگام عرضه در بازار یا بهره‌برداری، بدون تأخیر غیرموجه و در مهلتی که مقام مذکور تعیین می‌کند، دیگر چنین خطری ایجاد نکند.

۲. ارائه‌دهنده یا بهره‌بردار ذی‌ربط باید تضمین کند که اقدام اصلاحی در خصوص تمامی سامانه‌های هوش مصنوعی مربوطه که در بازار اتحادیه در دسترس قرار داده است، در مهلت تعیین‌شده از سوی مقام ناظر بر بازار کشور عضو موضوع بند ۱ انجام گیرد.

۳. کشورهای عضو باید فوراً کمیسیون و دیگر کشورهای عضو را از یافتهٔ موضوع بند ۱ آگاه کنند. این اطلاع باید شامل تمامی جزئیات موجود باشد، به‌ویژه داده‌های لازم برای شناسایی سامانهٔ هوش مصنوعی مربوطه، منشأ و زنجیرهٔ تأمین آن سامانه، ماهیت خطر موجود و نوع و مدت تدابیر ملی اتخاذشده.

۴. کمیسیون باید بدون تأخیر غیرموجه وارد مشاوره با کشورهای عضو ذی‌ربط و بهره‌برداران مربوطه شود و تدابیر ملی اتخاذشده را ارزیابی کند. بر مبنای نتایج آن ارزیابی، کمیسیون باید تصمیم بگیرد که آیا تدبیر مذکور موجه است یا خیر و در صورت لزوم، سایر تدابیر مقتضی را پیشنهاد دهد.

۵. کمیسیون باید فوراً تصمیم خود را به کشورهای عضو ذی‌ربط و بهره‌برداران مربوطه ابلاغ کند. همچنین باید دیگر کشورهای عضو را نیز مطلع کند.

ماده ۸۳. عدم انطباق شکلی

۱. هر گاه مقام ناظر بر بازار یک کشور عضو به یکی از موارد زیر دست یابد، باید ارائه‌دهندهٔ ذی‌ربط را ملزم کند که در مهلتی که ممکن است تعیین کند، به عدم انطباق موردنظر پایان دهد:

الف) علامت CE برخلاف ماده ۴۸ الصاق شده است؛

ب) علامت CE الصاق نشده است؛

پ) اظهارنامهٔ انطباق اتحادیه، موضوع ماده ۴۷ تنظیم نشده است؛

ت) اظهارنامهٔ انطباق اتحادیه، موضوع ماده ۴۷ به‌طور صحیح تنظیم نشده است؛

ث) ثبت در پایگاه دادهٔ اتحادیه، موضوع ماده ۷۱ انجام نشده است؛

ج) در مواردی که لازم است، نمایندهٔ مجاز تعیین نشده است؛

چ) مستندات فنی در دسترس نیست.

۲. در صورتی که عدم انطباق موضوع بند ۱ تداوم یابد، مقام ناظر بر بازار کشور عضو مربوط باید تدابیر مقتضی و متناسبی اتخاذ کند تا از عرضهٔ سامانهٔ هوش مصنوعی پرخطر در بازار جلوگیری یا اطمینان حاصل شود که بدون تأخیر از بازار جمع‌آوری یا بازگردانده شود.

ماده ۸۴. سازوکارهای پشتیبان آزمون اتحادیه برای هوش مصنوعی

۱. کمیسیون یک یا چند سازوکار پشتیبان آزمون اتحادیه در حوزهٔ هوش مصنوعی را تعیین می‌کند تا وظایف مندرج در مادهٔ ۲۱(۶) *قانون (اتحادیهٔ اروپا)* ۱۰۲۰/۲۰۱۹ را در زمینهٔ هوش مصنوعی به انجام رسانند.

۲. بدون لطمه به وظایف مذکور در بند ۱، سازوکارهای پشتیبان آزمون اتحادیه برای هوش مصنوعی همچنین به درخواست هیئت، کمیسیون یا مقامات ناظر بر بازار، مشاورهٔ مستقل فنی یا علمی ارائه خواهند داد.

بخش چهارم. طرق جبران

ماده ۸۵. حق تقدیم شکایت به مرجع نظارت بر بازار

بدون خدشه به سایر طرق اداری یا قضایی جبران، هر شخص حقیقی یا حقوقی که دلیلی برای اعتقاد به وقوع نقض مقررات این قانون داشته باشد، می‌تواند شکایت خود را به مرجع ذی‌صلاح نظارت بر بازار ارائه کند.

مطابق قانون ۲۰۱۹/۱۰۲۰ (اتحادیهٔ اروپا)، چنین شکایاتی برای مقاصد انجام فعالیت‌های نظارت بر بازار مورد توجه قرار گرفته و طبق رویه‌های اختصاصی که توسط مراجع نظارت بر بازار ایجاد شده است، رسیدگی خواهند شد.

ماده ۸۶. حق برخورداری از توضیح در تصمیم‌گیری فردی

۱. هر شخص ذی‌نفع که مشمول تصمیمی شود که توسط بهره‌بردار بر اساس خروجی یک سامانهٔ هوش مصنوعی پرخطر (مندرج در پیوست سوم به استثنای سامانه‌های مندرج در بند ۲ همان پیوست) اتخاذ شده و آن تصمیم دارای آثار حقوقی باشد یا به نحوی مشابه به‌طور چشمگیر بر آن شخص اثر گذارد، به گونه‌ای که وی آن را برای سلامت، ایمنی یا حقوق بنیادین خود زیان‌بار تلقی کند، حق خواهد داشت که از بهره‌بردار، توضیحات روشن و معناداری در خصوص نقش سامانهٔ هوش مصنوعی در فرآیند تصمیم‌گیری و عناصر اصلی تصمیم اتخاذشده دریافت کند.

۲. بند ۱ شامل مواردی نمی‌شود که استفاده از سامانه‌های هوش مصنوعی به موجب حقوق اتحادیه یا حقوق ملی، در انطباق با حقوق اتحادیه، مشمول استثنائات یا محدودیت‌هایی نسبت به الزام مقرر در آن بند باشد.

۳. این ماده صرفاً در صورتی اعمال می‌شود که حقی که در بند ۱ بدان اشاره شده است، به نحو دیگری تحت حقوق اتحادیه پیش‌بینی نشده باشد.

ماده ۸۷. گزارش‌دهی تخلفات و حمایت از گزارش‌دهندگان

دستورالعمل ۱۹۳۷/۲۰۱۹ (اتحادیهٔ اروپا) در خصوص گزارش‌دهی تخلفات از این قانون و حمایت از اشخاصی که چنین تخلفاتی را گزارش می‌دهند، اعمال خواهد شد.

بخش پنجم. نظارت، تحقیق، اجرا و پایش در خصوص ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی

ماده ۸۸. اجرای تعهدات ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی

۱. کمیسیون دارای صلاحیت انحصاری برای نظارت و اجرای فصل پنجم خواهد بود، با رعایت تضمین‌های شکلی مقرر در ماده ۹۴. کمیسیون انجام این وظایف را به *دفتر هوش مصنوعی* محول خواهد کرد، بدون لطمه به اختیارات سازمان‌دهی کمیسیون و تقسیم صلاحیت‌ها میان کشورهای عضو و اتحادیه بر اساس معاهدات.

۲. بدون خدشه به ماده ۷۵(۳)، مقامات نظارت بر بازار می‌توانند، در مواردی که برای کمک به انجام وظایف آنان ذیل این قانون ضروری و متناسب باشد، از کمیسیون درخواست کنند تا از اختیارات مقرر در این بخش استفاده کند.

ماده ۸۹. اقدامات پایشی

۱. *دفتر هوش مصنوعی* به منظور انجام وظایفی که در این بخش به آن محول شده است، می‌تواند اقدامات لازم را برای پایش اجرای مؤثر و رعایت این قانون توسط ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عمومی، ازجمله پایبندی آنان به کُدهای رفتاری مورد تأیید، اتخاذ کند.

۲. ارائه‌دهندگان پایین‌دستی حق دارند شکایتی مبنی بر نقض این قانون مطرح کنند. شکایت باید به‌طور مستدل ارائه شود و حداقل شامل موارد زیر باشد:

الف) اطلاعات تماس ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی مربوطه؛

ب) شرح حقایق مربوطه، مقررات این قانون که نقض شده‌اند، و دلیل اینکه چرا ارائه‌دهندهٔ پایین‌دستی بر این باور است که ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی قانون را نقض کرده است؛

ج) هر گونه اطلاعات دیگری که ارائه‌دهندهٔ پایین‌دستیِ ارسال‌کنندهٔ درخواست، آن را مرتبط می‌داند، ازجمله، در صورت اقتضا، اطلاعاتی که به ابتکار خود گردآوری کرده باشد.

ماده ۹۰. هشدارهای ریسک‌های نظام‌مند توسط هیئت علمی

۱. هیئت علمی می‌تواند هشدار واجد شرایطی به *دفتر هوش مصنوعی* ارائه دهد، هر گاه دلیلی برای ظن داشته باشد که:

الف) یک مدل هوش مصنوعی با هدف عمومی، ریسک مشخص و قابل شناسایی در سطح اتحادیه ایجاد می‌کند؛ یا

ب) یک مدل هوش مصنوعی با هدف عمومی، شرایط اشاره‌شده در ماده ۵۱ را برآورده می‌کند.

۲. پس از چنین هشدار واجد شرایطی، کمیسیون از طریق *دفتر هوش مصنوعی* و پس از اطلاع‌رسانی به هیئت، می‌تواند از اختیارات مقرر در این بخش به منظور ارزیابی موضوع استفاده کند. *دفتر هوش مصنوعی* هر گونه اقدام مطابق مواد ۹۱ تا ۹۴ را به هیئت اطلاع خواهد داد.

۳. هشدار واجد شرایط باید مستدل و دست‌کم شامل موارد زیر باشد:

الف) اطلاعات تماس ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی که ریسک نظام‌مند دارد؛

ب) شرح حقایق مربوطه و دلایل هشدار توسط هیئت علمی؛

ج) هر گونه اطلاعات دیگری که هیئت علمی آن را مرتبط بداند، ازجمله، در صورت اقتضا، اطلاعاتی که به ابتکار خود گردآوری کرده باشد.

ماده ۹۱. اختیار درخواست مستندات و اطلاعات

۱. کمیسیون می‌تواند از ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومیِ مربوطه درخواست کند تا مستنداتی را که طبق مواد ۵۳ و ۵۵ تهیه کرده است، یا هر گونه اطلاعات تکمیلی که برای ارزیابی انطباق ارائه‌دهنده با این قانون لازم باشد، ارائه دهد.

۲. *دفتر هوش مصنوعی* می‌تواند پیش از ارسال درخواست اطلاعات، گفتگویی ساختاریافته با ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی آغاز کند.

۳. بنا بر یک درخواست مستند و دارای توجیه کافی از سوی هیئت علمی، در مواردی که دسترسی به اطلاعات برای انجام وظایف هیئت علمی طبق ماده ۶۸(۲) لازم و متناسب باشد، کمیسیون می‌تواند از ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی درخواست اطلاعات کند.

۴. درخواست اطلاعات باید مبنای قانونی و هدف از درخواست را بیان و مشخص کند که چه اطلاعاتی مورد نیاز است، مهلتی برای ارائهٔ اطلاعات تعیین، و همچنین به جریمه‌های مقرر در ماده ۱۰۱ برای ارائهٔ اطلاعات نادرست، ناقص یا گمراه‌کننده اشاره کند.

۵. ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی مربوطه یا نمایندهٔ او باید اطلاعات درخواستی را ارائه دهد. در مورد اشخاص حقوقی، شرکت‌ها یا مؤسسات، یا در صورتی که ارائه‌دهنده شخصیت حقوقی نداشته باشد، اشخاصی که طبق قانون یا اساسنامه‌هایشان مجاز به نمایندگی هستند، باید اطلاعات درخواستی را به جای ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی مربوطه ارائه کنند. وکلایی که به‌طور رسمی اختیار دارند می‌توانند اطلاعات را به نمایندگی از موکلان خود ارائه دهند. با این حال، مسئولیت کامل در صورت ناقص، نادرست یا گمراه‌کننده‌بودن اطلاعات، همچنان بر عهدهٔ موکل باقی می‌ماند.

ماده ۹۲. اختیار انجام ارزیابی‌ها

۱. دفتر هوش مصنوعی، پس از مشورت با هیئت، می‌تواند ارزیابی‌هایی از مدل هوش مصنوعی با هدف عمومیِ مربوطه انجام دهد:

الف) به منظور سنجش انطباق ارائه‌دهنده با تعهدات مندرج در این قانون، در صورتی که اطلاعات گردآوری‌شده طبق ماده ۹۱ کافی نباشد؛ یا

ب) به منظور بررسی خطرات نظام‌مند در سطح اتحادیه، ناشی از مدل‌های هوش مصنوعی با هدف عمومی که دارای خطر نظام‌مند هستند، به‌ویژه پس از دریافت هشدار واجد شرایط از سوی هیئت علمی مطابق ماده ۹۰(۱)(الف).

۲. کمیسیون می‌تواند تصمیم بگیرد که کارشناسان مستقل را برای انجام ارزیابی‌ها به نمایندگی از خود منصوب کند، ازجمله از میان اعضای هیئت علمی که به موجب ماده ۶۸ تشکیل شده است. کارشناسان مستقلی که برای این وظیفه منصوب می‌شوند باید معیارهای مندرج در ماده ۶۸(۲) را رعایت کنند.

۳. برای مقاصد بند ۱، کمیسیون می‌تواند درخواست دسترسی به مدل هوش مصنوعی با هدف عمومیِ مربوطه از طریق APIها یا سایر ابزارها و وسایل فنی مناسب، ازجمله کد منبع داشته باشد.

۴. درخواست دسترسی باید مبنای قانونی، هدف و دلایل درخواست را بیان کند، مهلتی برای فراهم‌کردن دسترسی تعیین کند، و به جریمه‌های مقرر در ماده ۱۰۱ بابت امتناع از فراهم‌کردن دسترسی اشاره کند.

۵. ارائه‌دهندگان مدل هوش مصنوعی با هدف عمومیِ مربوطه یا نمایندگان آنان باید دسترسی درخواستی را فراهم کنند. در مورد اشخاص حقوقی، شرکت‌ها یا مؤسسات، یا در صورتی که ارائه‌دهنده شخصیت حقوقی نداشته باشد، اشخاصی که طبق قانون یا اساسنامه‌هایشان مجاز به نمایندگی هستند، باید دسترسی درخواستی را به جای ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی فراهم کنند.

۶. کمیسیون آیین‌نامه‌های اجرایی را برای تعیین ترتیبات تفصیلی و شرایط انجام ارزیابی‌ها تصویب خواهد کرد؛ ازجمله ترتیبات مربوط به مشارکت کارشناسان مستقل و رویهٔ انتخاب آنان. این آیین‌نامه‌های اجرایی مطابق رویهٔ بررسی مندرج در ماده ۹۸(۲) تصویب خواهند شد.

۷. پیش از درخواست دسترسی به مدل هوش مصنوعی با هدف عمومیِ مربوطه، دفتر هوش مصنوعی می‌تواند گفتگویی ساختاریافته با ارائه‌دهندهٔ مدل آغاز کند تا اطلاعات بیشتری دربارهٔ آزمون‌های داخلی مدل، تدابیر احتیاطی داخلی برای پیشگیری از خطرات نظام‌مند، و سایر رویه‌ها و اقداماتی که ارائه‌دهنده برای کاهش چنین خطراتی اتخاذ کرده است، گردآوری کند.

ماده ۹۳. اختیار درخواست اقدامات

۱. هر گاه ضروری و مناسب باشد، کمیسیون می‌تواند از ارائه‌دهندگان بخواهد که:

الف) تدابیر مقتضی را برای رعایت تعهدات مقرر در مواد ۵۳ و ۵۴ اتخاذ کنند؛

ب) در صورتی که ارزیابی انجام‌شده طبق ماده ۹۲ موجب نگرانی جدی و مستند از وجود خطر نظام‌مند در سطح اتحادیه شده باشد، اقدامات کاهنده را اجرا کنند؛

ج) عرضه در بازار را محدود، یا مدل را از بازار خارج یا فراخوان کنند.

۲. پیش از آنکه اقدامی درخواست شود، دفتر هوش مصنوعی می‌تواند گفتگویی ساختاریافته با ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومی آغاز کند.

۳. اگر در جریان گفتگوی ساختاریافتهٔ مذکور در بند ۲، ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عمومیِ دارای خطر نظام‌مند، تعهداتی برای اجرای اقدامات کاهنده جهت رفع خطر نظام‌مند در سطح اتحادیه ارائه دهد، کمیسیون می‌تواند با اتخاذ تصمیم، آن تعهدات را الزام‌آور کند و اعلام کند که دیگر هیچ دلیلی برای اقدام بیشتر وجود ندارد.

ماده ۹۴. حقوق آیین دادرسیِ فعالان اقتصادیِ مدل هوش مصنوعی با هدف عمومی

مادهٔ ۱۸ قانون (اتحادیهٔ اروپا) ۱۰۲۰/۲۰۱۹ به نحو لازم و متناسب در مورد ارائه‌دهندگان مدل

هوش مصنوعی با هدف عمومی تغییر یافته و اعمال خواهد شد، بدون آنکه به حقوق شکلیِ خاص‌ترِ پیش‌بینی‌شده در این قانون لطمه‌ای وارد آید.

فصل دهم. آیین‌های رفتاری و رهنمودها

ماده ۹۵. آیین‌های رفتاری برای اجرای داوطلبانهٔ الزامات مشخص

۱. دفتر هوش مصنوعی و کشورهای عضو باید تهیهٔ آیین‌های رفتاری، ازجمله سازوکارهای حکمرانی مرتبط را تشویق و تسهیل کنند؛ آیین‌هایی که هدفشان ترویج اجرای داوطلبانهٔ برخی یا تمام الزامات مندرج در فصل سوم، بخش دوم در خصوص سامانه‌های هوش مصنوعی، به استثنای سامانه‌های پرخطر باشد؛ با درنظرگرفتن راه‌حل‌های فنی موجود و بهترین رویه‌های صنعتی که امکان اجرای آن الزامات را فراهم می‌کند.

۲. دفتر هوش مصنوعی و کشورهای عضو باید تسهیل‌گر تهیهٔ آیین‌های رفتاری دربارهٔ اجرای داوطلبانهٔ الزامات مشخص ازجمله توسط بهره‌برداران در خصوص همهٔ سامانه‌های هوش مصنوعی باشند، بر مبنای اهداف روشن و شاخص‌های کلیدی عملکرد برای سنجش تحقق آن اهداف، شامل عناصری همچون، اما نه محدود به:

الف) عناصر قابل اعمال پیش‌بینی‌شده در *رهنمودهای اخلاقی اتحادیه برای هوش مصنوعی قابل اعتماد*؛

ب) ارزیابی و به‌حداقل‌رساندن تأثیر سامانه‌های هوش مصنوعی بر پایداری زیست‌محیطی، ازجمله در زمینهٔ برنامه‌نویسی کارآمد از نظر انرژی و فنون طراحی، آموزش و بهره‌برداری کارآمد از هوش مصنوعی؛

ج) ارتقاء سواد هوش مصنوعی، به‌ویژه در میان اشخاصی که در توسعه، بهره‌برداری و استفاده از هوش مصنوعی مشارکت دارند؛

د) تسهیل طراحی فراگیر و متنوع سامانه‌های هوش مصنوعی، ازجمله از طریق تشکیل تیم‌های توسعهٔ فراگیر و متنوع و ترویج مشارکت ذی‌نفعان در آن فرآیند؛

هـ) ارزیابی و پیشگیری از تأثیر منفی سامانه‌های هوش مصنوعی بر اشخاص آسیب‌پذیر یا گروه‌های آسیب‌پذیر، ازجمله در زمینهٔ دسترس‌پذیری برای اشخاص دارای معلولیت، و نیز بر برابری جنسیتی.

۳. آیین‌های رفتاری می‌توانند توسط ارائه‌دهندگان منفرد یا بهره‌برداران سامانه‌های هوش مصنوعی، یا توسط سازمان‌های نمایندگی‌کنندهٔ آنان، یا توسط هر دو گروه، ازجمله با مشارکت هر ذی‌نفع علاقه‌مند و سازمان‌های نمایندگی‌کنندهٔ آن‌ها، شامل سازمان‌های جامعهٔ مدنی و نهادهای دانشگاهی تهیه شوند. آیین‌های رفتاری می‌توانند با لحاظ‌کردن شباهت در هدف موردنظر سامانه‌های مربوطه،

یک یا چند سامانهٔ هوش مصنوعی را پوشش دهند.

۴. دفتر هوش مصنوعی و کشورهای عضو، هنگام تشویق و تسهیل تهیهٔ آیین‌های رفتاری باید منافع و نیازهای ویژهٔ بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا را در نظر بگیرند.

ماده ۹۶. رهنمودهای کمیسیون در خصوص اجرای این قانون

۱. کمیسیون به‌ویژه دربارهٔ موارد زیر باید رهنمودهایی در خصوص اجرای عملی این قانون تهیه کند:

الف) اعمال الزامات و تعهدات مندرج در مواد ۸ تا ۱۵ و ماده ۲۵؛

ب) رویه‌های ممنوع‌شدهٔ مندرج در ماده ۵؛

ج) اجرای عملی مقررات مربوط به تغییرات اساسی؛

د) اجرای عملی تعهدات شفافیت مندرج در ماده ۵۰؛

هـ) اطلاعات تفصیلی دربارهٔ رابطهٔ این قانون با قوانین هماهنگ‌سازی اتحادیهٔ ذکرشده در پیوست یک، همچنین با دیگر قوانین مرتبط اتحادیه، ازجمله در خصوص انسجام در اجرای آن‌ها؛

و) اعمال تعریف *سامانهٔ هوش مصنوعی* همان گونه که در ماده ۳، بند (۱) آمده است.

هنگام صدور این رهنمودها، کمیسیون باید به نیازهای بنگاه‌های کوچک و متوسط، ازجمله شرکت‌های نوپا، مقامات عمومی محلی و بخش‌هایی که بیشترین احتمال تأثیرپذیری از این قانون را دارند، توجه ویژه‌ای داشته باشد.

رهنمودهای مذکور در بند نخست این پاراگراف باید به‌طور مقتضی به سطح دانش فنیِ عموماً شناخته‌شده در حوزهٔ هوش مصنوعی، همچنین به استانداردهای هماهنگ و مشخصات مشترک ارجاع‌شده در مواد ۴۰ و ۴۱ یا به استانداردها و مشخصات فنی مندرج ذیل حقوق هماهنگ‌سازی اتحادیه توجه کنند.

۲. بنا به درخواست کشورهای عضو یا دفتر هوش مصنوعی، یا به ابتکار خود، کمیسیون باید در صورت ضرورت، رهنمودهای پیش‌تر تصویب‌شده را به‌روزرسانی کند.

فصل یازدهم. تفویض اختیار و رویهٔ کمیته

ماده ۹۷. اعمال اختیار تفویض‌شده

۱. اختیار تصویبِ *اعمال تفویضی* مشروط بر شرایط مقرر در این ماده، به کمیسیون اعطا می‌شود.

۲. اختیار تصویب اعمال تفویضی که در ماده ۶(۶) و (۷)، ماده ۷(۱) و (۳)، ماده ۱۱(۳)، ماده ۴۳(۵) و (۶)، ماده ۴۷(۵)، ماده ۵۱(۳)، ماده ۵۲(۴) و ماده ۵۳(۵) و (۶) به آن اشاره شده است، برای مدت پنج سال از اول اوت ۲۰۲۴ به کمیسیون اعطا می‌شود. کمیسیون باید حداکثر نه ماه پیش از پایان این دورهٔ پنج‌ساله، گزارشی در خصوص تفویض اختیار تهیه کند. تفویض اختیار به‌طور ضمنی برای دوره‌هایی با مدت مشابه تمدید خواهد شد، مگر آنکه پارلمان اروپا یا شورا حداکثر سه ماه پیش از پایان هر دوره با چنین تمدیدی مخالفت کنند.

۳. تفویض اختیار مذکور در ماده ۶(۶) و (۷)، ماده ۷(۱) و (۳)، ماده ۱۱(۳)، ماده ۴۳(۵) و (۶)، ماده ۴۷(۵)، ماده ۵۱(۳)، ماده ۵۲(۴) و ماده ۵۳(۵) و (۶) در هر زمان می‌تواند از سوی پارلمان اروپا یا شورا لغو شود. تصمیم به لغو، به تفویض اختیار مشخص‌شده در همان تصمیم خاتمه می‌دهد. این تصمیم از روز پس از انتشار آن در *روزنامهٔ رسمی اتحادیهٔ اروپا* یا در تاریخی بعد که در آن قید شود، نافذ خواهد شد. لغو تفویض اختیار بر اعتبار اعمال تفویضی که پیش‌تر لازم‌الاجرا شده‌اند تأثیری نخواهد داشت.

۴. کمیسیون پیش از تصویب یک عمل تفویضی باید با کارشناسانی که هر یک از کشورهای عضو معرفی کرده‌اند و مطابق اصول مندرج در *توافقنامهٔ بین‌نهادی مورخ ۱۳ آوریل ۲۰۱۶ دربارهٔ قانونگذاری بهتر*، مشورت کند.

۵. به‌محض تصویب یک عمل تفویضی، کمیسیون باید آن را هم‌زمان به پارلمان اروپا و شورا اطلاع دهد.

۶. هر عمل تفویضی که به موجب ماده ۶(۶) یا (۷)، ماده ۷(۱) یا (۳)، ماده ۱۱(۳)، ماده ۴۳(۵) یا (۶)، ماده ۴۷(۵)، ماده ۵۱(۳)، ماده ۵۲(۴) یا ماده ۵۳(۵) یا (۶) تصویب شود، تنها در صورتی لازم‌الاجرا خواهد شد که هیچ‌یک از پارلمان اروپا یا شورا ظرف سه ماه از تاریخ اطلاع‌رسانی آن به پارلمان و شورا، مخالفتی اعلام نکرده باشند یا آنکه پیش از انقضای این مهلت، هر دو نهاد به کمیسیون اطلاع دهند که اعتراضی نخواهند داشت. این مهلت به ابتکار عمل پارلمان اروپا یا شورا به مدت سه ماه دیگر قابل تمدید است.

ماده ۹۸. رویهٔ کمیته

۱. کمیسیون به وسیلهٔ یک کمیته یاری خواهد شد. این کمیته در معنای مندرج در قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۱/۱۸۲، یک *کمیته* محسوب می‌شود.

۲. هر گاه به این بند ارجاع داده شود، ماده ۵ قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۱/۱۸۲ اعمال خواهد شد.

فصل دوازدهم. ضمانت‌های اجرا

ماده ۹۹. مجازات‌ها

۱. مطابق شرایط و ترتیبات مقرر در این قانون، کشورهای عضو باید قواعد مربوط به مجازات‌ها و سایر تدابیر اجرایی را که می‌تواند شامل اخطارها و تدابیر غیرمالی نیز باشد، قابل اعمال بر نقض این قانون توسط عاملان اقتصادی وضع کرده و تمامی تدابیر لازم را برای تضمین اجرای صحیح و مؤثر آن‌ها اتخاذ کنند. در این راستا باید رهنمودهای کمیسیون به موجب ماده ۹۶ نیز مدنظر قرار گیرد. مجازات‌های مقرر باید مؤثر، متناسب و بازدارنده باشند و همچنین منافع شرکت‌های کوچک و متوسط، ازجمله شرکت‌های نوپا، و امکان بقای اقتصادی آن‌ها لحاظ شود.

۲. کشورهای عضو باید بی‌درنگ و حداکثر تا تاریخ آغاز اجرای قانون، قواعد مربوط به مجازات‌ها و سایر تدابیر اجرایی موضوع بند ۱ را به کمیسیون اطلاع دهند و هر گونه اصلاح بعدی در این زمینه را نیز بدون تأخیر به آن ابلاغ کنند.

۳. عدم رعایت ممنوعیت شیوه‌های هوش مصنوعی موضوع ماده ۵ مشمول جریمه‌های اداری تا سقف ۳۵.۰۰۰.۰۰۰ یورو یا، در صورتی که متخلف یک شرکت باشد، تا ۷٪ از کل گردش مالی سالانهٔ جهانی آن در سال مالی پیشین ـ هر کدام که بیشتر باشد ـ خواهد شد.

۴. عدم رعایت هر یک از مقررات زیر که مربوط به عاملان اقتصادی یا نهادهای اعلام‌شده است، غیر از موارد مقرر در ماده ۵ مشمول جریمه‌های اداری تا سقف ۱۵.۰۰۰.۰۰۰ یورو یا، در صورتی که متخلف یک شرکت باشد، تا ۳٪ از کل گردش مالی سالانهٔ جهانی آن در سال مالی پیشین ـ هرکدام که بیشتر باشد ـ خواهد شد:

الف) تعهدات ارائه‌دهندگان طبق ماده ۱۶؛

ب) تعهدات نمایندگان مجاز طبق ماده ۲۲؛

پ) تعهدات واردکنندگان طبق ماده ۲۳؛

ت) تعهدات توزیع‌کنندگان طبق ماده ۲۴؛

ث) تعهدات بهره‌برداران/به‌کارگیرندگان طبق ماده ۲۶؛

ج) الزامات و تعهدات نهادهای اعلام‌شده طبق ماده ۳۱، ماده ۳۳(۱)، (۳) و (۴) یا ماده ۳۴؛

چ) تعهدات شفافیت برای ارائه‌دهندگان و بهره‌برداران طبق ماده ۵۰.

۵. ارائهٔ اطلاعات نادرست، ناقص یا گمراه‌کننده به نهادهای اعلام‌شده یا مقامات صلاحیت‌دار ملی در پاسخ به درخواست، مشمول جریمه‌های اداری تا سقف ۷.۵۰۰.۰۰۰ یورو یا، در صورتی که متخلف یک شرکت باشد، تا ۱٪ از کل گردش مالی سالانهٔ جهانی آن در سال مالی پیشین ـ هر کدام که بیشتر باشد ـ خواهد شد.

۶. در مورد شرکت‌های کوچک و متوسط، ازجمله شرکت‌های نوپا، سقف هر جریمهٔ مندرج در این ماده برابر خواهد بود با درصدها یا مبالغ مذکور در بندهای ۳، ۴ و ۵ ـ هرکدام که پایین‌تر باشد.

۷. هنگام تصمیم‌گیری در خصوص اعمال جریمهٔ اداری و تعیین میزان آن در هر پروندهٔ مشخص، تمامی اوضاع و احوال مرتبط باید مدنظر قرار گیرد و حسب مورد توجه ویژه‌ای به موارد زیر بشود:

الف) ماهیت، شدت و مدت تخلف و پیامدهای آن، با لحاظ هدف سامانهٔ هوش مصنوعی و، در صورت لزوم، تعداد افراد آسیب‌دیده و سطح زیان وارده به آن‌ها؛

ب) اینکه آیا پیش‌تر جریمه‌های اداری توسط سایر مراجع نظارت بر بازار برای همان تخلف علیه همان عامل اقتصادی اعمال شده است یا خیر؛

پ) اینکه آیا پیش‌تر جریمه‌های اداری توسط سایر مراجع برای تخلفات دیگر از حقوق اتحادیه یا حقوق ملی علیه همان عامل اقتصادی اعمال شده است، در صورتی که آن تخلفات ناشی از همان اقدام یا ترک فعلی باشد که تخلف مربوط به این قانون را تشکیل می‌دهد؛

ت) اندازه، گردش مالی سالانه و سهم بازار عامل اقتصادی مرتکب تخلف؛

ث) هر عامل تشدیدکننده یا تخفیف‌دهندهٔ دیگری که به اوضاع پرونده مربوط باشد، مانند منافع مالی کسب‌شده یا زیان‌های اجتناب‌شده به‌طور مستقیم یا غیرمستقیم از طریق تخلف؛

ج) میزان همکاری با مقامات صلاحیت‌دار ملی برای رفع تخلف و کاهش آثار زیانبار احتمالی آن؛

چ) درجهٔ مسئولیت عامل اقتصادی با توجه به تدابیر فنی و سازمانی اتخاذشده توسط وی؛

ح) نحوهٔ آگاهی مقامات صلاحیت‌دار ملی از تخلف، به‌ویژه اینکه آیا و تا چه حد عامل اقتصادی خود تخلف را گزارش کرده است؛

خ) عمدی یا سهل‌انگارانه‌بودن تخلف؛

د) هر اقدامی که توسط عامل اقتصادی برای جبران خسارات وارده به افراد آسیب‌دیده اتخاذ شده باشد.

۸. هر کشور عضو باید قواعدی را وضع کند که مشخص کند تا چه حد می‌توان جریمه‌های اداری را بر مراجع و نهادهای عمومی مستقر در آن کشور اعمال کرد.

۹. بسته به نظام حقوقی کشورهای عضو، ممکن است قواعد مربوط به جریمه‌های اداری به نحوی اجرا شوند که جریمه‌ها توسط دادگاه‌های ملی صلاحیت‌دار یا توسط سایر نهادها، حسب مورد در هر کشور عضو، اعمال شود. اجرای این قواعد در کشورهای عضو باید اثر معادل داشته باشد.

۱۰. اعمال اختیارات به موجب این ماده باید مشمول تضمین‌های آیین دادرسی مناسب، مطابق حقوق اتحادیه و حقوق ملی باشد، ازجمله تضمین دسترسی به طرق مؤثر جبران قضایی و رعایت دادرسی منصفانه.

۱۱. کشورهای عضو باید سالانه به کمیسیون گزارش دهند که در طول آن سال، چه جریمه‌های اداری طبق این ماده اعمال کرده‌اند و همچنین دربارهٔ هر گونه دعوا یا رسیدگی قضایی مرتبط اطلاع‌رسانی کنند.

ماده ۱۰۰. جریمه‌های اداری علیه نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه

۱. ناظر اروپایی حفاظت از داده‌ها می‌تواند بر نهادها، ارگان‌ها، دفاتر و آژانس‌های اتحادیه که مشمول این قانون هستند، جریمه‌های اداری اعمال کند. هنگام تصمیم‌گیری در خصوص اعمال جریمهٔ اداری و تعیین میزان آن در هر پروندهٔ مشخص، باید تمامی اوضاع و احوال مرتبط در نظر گرفته شده و توجه ویژه‌ای به موارد زیر معطوف شود:

الف) ماهیت، شدت و مدت تخلف و پیامدهای آن، با لحاظ هدف سامانهٔ هوش مصنوعی مربوطه و در صورت لزوم، تعداد افراد آسیب‌دیده و میزان خسارت وارده به آنان؛

ب) درجهٔ مسئولیت نهاد، ارگان، دفتر یا آژانس اتحادیه، با توجه به تدابیر فنی و سازمانی اتخاذشده؛

پ) اقداماتی که توسط نهاد، ارگان، دفتر یا آژانس اتحادیه برای جبران خسارت افراد آسیب‌دیده اتخاذ شده است؛

ت) میزان همکاری با ناظر اروپایی حفاظت از داده‌ها برای رفع تخلف و کاهش پیامدهای منفی احتمالی آن، ازجمله رعایت تدابیری که پیش‌تر توسط ناظر اروپایی حفاظت از داده‌ها علیه نهاد، ارگان، دفتر یا آژانس مربوطه در خصوص همان موضوع مقرر شده است؛

ث) تخلفات مشابه پیشین توسط نهاد، ارگان، دفتر یا آژانس اتحادیه؛

ج) نحوهٔ آگاهی ناظر اروپایی حفاظت از داده‌ها از تخلف، به‌ویژه اینکه آیا و تا چه حد نهاد، ارگان، دفتر یا آژانس اتحادیه تخلف را گزارش کرده است؛

چ) بودجهٔ سالانهٔ نهاد، ارگان، دفتر یا آژانس اتحادیه.

۲. عدم رعایت ممنوعیت شیوه‌های هوش مصنوعی موضوع ماده ۵ مشمول جریمه‌های اداری تا سقف ۱.۵۰۰.۰۰۰یورو خواهد بود.

۳. عدم انطباق سامانهٔ هوش مصنوعی با هر یک از الزامات یا تعهدات مندرج در این قانون، بجز موارد مقرر در ماده ۵ مشمول جریمه‌های اداری تا سقف ۷۵۰.۰۰۰ یورو خواهد بود.

۴. پیش از اتخاذ تصمیمات به موجب این ماده، ناظر اروپایی حفاظت از داده‌ها باید به نهاد، ارگان، دفتر یا آژانس اتحادیه‌ای که موضوع رسیدگی است، فرصت استماع در خصوص تخلف احتمالی بدهد. تصمیمات ناظر باید صرفاً بر مبنای عناصر و اوضاع و احوالی استوار باشد که طرف‌های ذی‌ربط توانسته‌اند نسبت به آن اظهارنظر کنند. شاکیان احتمالی نیز باید در جریان رسیدگی‌ها به‌طور نزدیک

مشارکت داده شوند.

۵. باید حقوق دفاع طرف‌های ذی‌ربط در جریان رسیدگی‌ها کاملاً رعایت شود. این طرف‌ها حق خواهند داشت به پروندهٔ ناظر اروپایی حفاظت از داده‌ها دسترسی داشته باشند، مشروط بر اینکه منافع مشروع اشخاص یا شرکت‌ها در حفاظت از داده‌های شخصی یا اسرار تجاری آن‌ها مخدوش نشود.

۶. وجوهی که از محل اعمال جریمه‌ها به موجب این ماده وصول می‌شود باید به بودجهٔ عمومی اتحادیه واریز شود. این جریمه‌ها نباید بر کارکرد مؤثر نهاد، ارگان، دفتر یا آژانس اتحادیهٔ جریمه‌شده اثر بگذارد.

۷. ناظر اروپایی حفاظت از داده‌ها باید سالانه کمیسیون را از جریمه‌های اداری که به موجب این ماده اعمال کرده و همچنین از هر گونه دعوا یا رسیدگی قضایی مرتبط مطلع کند.

ماده ۱۰۱. جریمه‌ها برای ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عام

۱. کمیسیون می‌تواند بر ارائه‌دهندگان مدل‌های هوش مصنوعی با هدف عام، جریمه‌هایی اعمال کند که از ۳٪ از گردش مالی کل جهانی سالانهٔ آنان در سال مالی پیشین یا ۱۵.۰۰۰.۰۰۰ یورو ـ هرکدام که بیشتر باشد ـ تجاوز نکند، در صورتی که کمیسیون احراز کند ارائه‌دهنده عمداً یا از روی تقصیر:

الف) مقررات قانون را نقض کرده است؛

ب) از تبعیت با درخواست ارائهٔ یک سند یا اطلاعات طبق ماده ۹۱ خودداری کرده یا اطلاعات نادرست، ناقص یا گمراه‌کننده ارائه کرده است؛

ج) از تبعیت با اقدام درخواستی طبق ماده ۹۳ خودداری کرده است؛

د) دسترسی به مدل هوش مصنوعی با هدف عام یا مدل هوش مصنوعی با هدف عام همراه با ریسک نظام‌مند را برای کمیسیون به منظور انجام ارزیابی طبق ماده ۹۲ فراهم نکرده است.

در تعیین میزان جریمه یا جریمهٔ روزانه باید به ماهیت، شدت و مدت تخلف توجه و اصول تناسب و مناسبت رعایت شود. همچنین کمیسیون باید به تعهداتی که طبق ماده ۹۳(۳) یا در کدهای رفتاری مربوطه طبق ماده ۵۶ ارائه شده‌اند نیز توجه کند.

۲. پیش از اتخاذ تصمیم طبق بند ۱، کمیسیون باید یافته‌های مقدماتی خود را به ارائه‌دهندهٔ مدل هوش مصنوعی با هدف عام ابلاغ کرده و به او فرصت شنیده‌شدن بدهد.

۳. جریمه‌های اعمال‌شده طبق این ماده باید مؤثر، متناسب و بازدارنده باشند.

۴. اطلاعات مربوط به جریمه‌های اعمال‌شده طبق این ماده، حسب مورد به هیئت نیز ابلاغ خواهد شد.

۵. دیوان دادگستری اتحادیهٔ اروپا دارای صلاحیت نامحدود برای بازبینی تصمیمات کمیسیون در خصوص تعیین جریمه به موجب این ماده خواهد بود. دیوان می‌تواند جریمهٔ اعمال‌شده را لغو کند، کاهش یا افزایش دهد.

۶. کمیسیون باید اعمال اجرایی را با محتوای ترتیبات تفصیلی و تضمین‌های آیین دادرسی برای رسیدگی‌هایی که ممکن است به تصمیمات موضوع بند ۱ منجر شود، تصویب کند. این اعمال اجرایی باید مطابق روش بررسی مذکور در ماده ۹۸(۲) به تصویب برسند.

فصل سیزدهم. مفاد نهایی

ماده ۱۰۲. اصلاح قانون شمارهٔ ۲۰۰۸/۳۰۰ (اتحادیهٔ اروپا)

در بند ۳ ماده ۴ قانون شمارهٔ ۲۰۰۸/۳۰۰ (اتحادیهٔ اروپا)، بند فرعی زیر اضافه می‌شود:

«هنگام تصویب تدابیر تفصیلی مربوط به مشخصات فنی و رویه‌های مربوط به تأیید و استفاده از تجهیزات امنیتی مرتبط با سامانه‌های هوش مصنوعی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) پارلمان و شورای اروپا (*)، الزامات مندرج در فصل سوم، بخش دوم آن قانون باید مدنظر قرار گیرند».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

ماده ۱۰۳. اصلاح قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۳/۱۶۷

در بند ۵ ماده ۱۷ قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۳/۱۶۷، بند فرعی زیر اضافه می‌شود:

«هنگام تصویب اعمال تفویضی مطابق بند فرعی نخست، مربوط به سامانه‌های هوش مصنوعی که جزء مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا (*) محسوب می‌شوند، الزامات مندرج در فصل سوم، بخش دوم آن قانون باید مدنظر قرار گیرند».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷

(اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

ماده ۱۰۴. اصلاح قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۳/۱۶۸

در بند ۵ ماده ۲۲ قانون (اتحادیهٔ اروپا) شمارهٔ ۲۰۱۳/۱۶۸، بند فرعی زیر اضافه می‌شود:

«هنگام تصویب اعمال تفویضی مطابق بند فرعی نخست، مربوط به سامانه‌های هوش مصنوعی که جزء مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا (*) محسوب می‌شوند، الزامات مندرج در فصل سوم، بخش دوم آن قانون باید مدنظر قرار گیرند».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

ماده ۱۰۵. اصلاح دستورالعمل EU/۹۰/۲۰۱۴

در ماده ۸ دستورالعمل EU/۹۰/۲۰۱۴، بند زیر اضافه می‌شود:

«۵ـ در مورد سامانه‌های هوش مصنوعی که جزء مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا (*) محسوب می‌شوند، کمیسیون هنگام انجام فعالیت‌های خود مطابق بند ۱ و هنگام تصویب مشخصات فنی و استانداردهای آزمون مطابق بندهای ۲ و ۳، الزامات مندرج در فصل سوم، بخش دوم آن قانون را مدنظر قرار خواهد داد».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

ماده ۱۰۶. اصلاح دستورالعمل ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا)

در ماده ۵ دستورالعمل ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) بند زیر اضافه می‌شود:

«۱۲ـ هنگام تصویب اقدامات تفویضی طبق بند ۱ و اقدامات اجرایی طبق بند ۱۱ که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا (*) هستند، الزامات مندرج در فصل سوم، بخش دوم آن قانون مدنظر قرار خواهد گرفت».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

ماده ۱۰۷. اصلاح قانون ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)

در ماده ۵ قانون ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، بند زیر اضافه می‌شود:

«۴ـ هنگام تصویب اقدامات تفویضی طبق بند ۳ که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) پارلمان و شورای اروپا (*) هستند، الزامات مندرج در فصل سوم، بخش دوم آن قانون مدنظر قرار خواهد گرفت».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

ماده ۱۰۸. اصلاحات قانون ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا)

قانون ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) به شرح زیر اصلاح می‌شود:

۱. در ماده ۱۷، بند زیر اضافه می‌شود:

«۳ـ بدون خدشه به بند ۲، هنگام تصویب اقدامات اجرایی طبق بند ۱ که مربوط به سامانه‌های

هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا (*) هستند، الزامات مندرج در بخش دوم از فصل سوم آن قانون مدنظر قرار خواهد گرفت».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

۲. در ماده ۱۹، بند زیر اضافه می‌شود:

«۴ـ هنگام تصویب اقدامات تفویضی طبق بندهای ۱ و ۲ که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) هستند، الزامات مندرج در بخش دوم از فصل سوم آن قانون مدنظر قرار خواهد گرفت».

۳. در ماده ۴۳، بند زیر اضافه می‌شود:

«۴ـ هنگام تصویب اقدامات اجرایی طبق بند ۱ که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) هستند، الزامات مندرج در بخش دوم از فصل سوم آن قانون مدنظر قرار خواهد گرفت».

۴. در ماده ۴۷، بند زیر اضافه می‌شود:

«۳ـ هنگام تصویب اقدامات تفویضی طبق بندهای ۱ و ۲ که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) هستند، الزامات مندرج در بخش دوم از فصل سوم آن قانون مدنظر قرار خواهد گرفت».

۵. در ماده ۵۷، بند فرعی زیر اضافه می‌شود:

«هنگام تصویب آن اقدامات اجرایی که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) هستند، الزامات مندرج در بخش دوم از فصل سوم آن قانون مدنظر قرار خواهد گرفت».

۶. در ماده ۵۸، بند زیر اضافه می‌شود:

«۳ـ هنگام تصویب اقدامات تفویضی طبق بندهای ۱ و ۲ که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) هستند، الزامات مندرج در بخش دوم از فصل سوم آن قانون مدنظر قرار خواهد گرفت».

ماده ۱۰۹. اصلاح قانون ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا)

در ماده ۱۱ قانون ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا)، بند زیر اضافه می‌شود:

«۳ـ هنگام تصویب اقدامات تفویضی طبق بند ۲ که مربوط به سامانه‌های هوش مصنوعی به‌عنوان مؤلفه‌های ایمنی در معنای قانون ۲۰۲۴/۱۶۸۹ (اتحادیهٔ اروپا) هستند، الزامات مندرج در بخش دوم از فصل سوم آن قانون مدنظر قرار خواهد گرفت».

(*) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

ماده ۱۱۰. اصلاح دستورالعمل ۲۰۲۰/۱۸۲۸

در پیوست اول دستورالعمل ۲۰۲۰/۱۸۲۸ پارلمان و شورای اروپا،[۱۹۲] نکتهٔ زیر اضافه می‌شود:

«(۶۸) قانون ۲۰۲۴/۱۶۸۹ پارلمان و شورای اروپا، مورخ ۱۳ ژوئن ۲۰۲۴ در خصوص وضع قواعد هماهنگ در زمینهٔ هوش مصنوعی و اصلاح مقررات شمارهٔ ۲۰۰۸/۳۰۰، شمارهٔ ۲۰۱۳/۱۶۷ (اتحادیهٔ اروپا)، شمارهٔ ۲۰۱۳/۱۶۸، ۲۰۱۸/۸۵۸ (اتحادیهٔ اروپا)، ۲۰۱۸/۱۱۳۹ (اتحادیهٔ اروپا) و ۲۰۱۹/۲۱۴۴ (اتحادیهٔ اروپا) و دستورالعمل‌های EU/۹۰/۲۰۱۴، ۲۰۱۶/۷۹۷ (اتحادیهٔ اروپا) و ۲۰۲۰/۱۸۲۸ (اتحادیهٔ اروپا) (قانون هوش مصنوعی) (روزنامهٔ رسمی ۱۶۸۹/۲۰۲۴، ۱۲ ژوئیهٔ ۲۰۲۴، ELI: http://data.europa.eu/eli/reg/2024/1689/oj)».

ماده ۱۱۱. سامانه‌های هوش مصنوعی که پیش‌تر در بازار عرضه یا به کار گرفته شده‌اند و مدل‌های هوش مصنوعی با کاربری عام که پیش‌تر در بازار عرضه شده‌اند

۱. بدون خدشه به اعمال ماده ۵ به شرح مذکور در ماده ۱۱۳(۳)، بند (الف)، سامانه‌های هوش مصنوعی که جزء سامانه‌های فناوری اطلاعات کلان هستند و به موجب اسناد حقوقی مندرج در پیوست دهم تأسیس شده‌اند و پیش از ۲ اوت ۲۰۲۷ در بازار عرضه یا به کار گرفته شده‌اند، باید تا ۳۱ دسامبر ۲۰۳۰ با این قانون منطبق شوند.

۱۹۲. دستورالعمل ۲۰۲۰/۱۸۲۸ پارلمان اروپا و شورای ۲۵ نوامبر ۲۰۲۰ در مورد اقدامات نمایندگی برای حفاظت از منافع جمعی مصرف‌کنندگان و لغو دستورالعمل EC/۲۲/۲۰۰۹ (روزنامهٔ رسمی ۴۰۹، ۴.۱۲.۲۰۲۰، ص ۱).

الزامات مقرر در این قانون در ارزیابی هر سامانهٔ فناوری اطلاعات کلان که به موجب اسناد حقوقی مندرج در پیوست دهم تأسیس شده و مطابق آن اسناد ارزیابی می‌شود، و نیز در مواردی که آن اسناد حقوقی جایگزین یا اصلاح شوند، باید مدنظر قرار گیرد.

۲. بدون خدشه به اعمال ماده ۵ به شرح مذکور در ماده ۱۱۳(۳)، بند (الف)، این قانون بر بهره‌برداران سامانه‌های پرخطر هوش مصنوعی (غیر از سامانه‌های مذکور در بند ۱ این ماده) که پیش از ۲ اوت ۲۰۲۶ در بازار عرضه یا به کار گرفته شده‌اند، صرفاً در صورتی اعمال می‌شود که از آن تاریخ به بعد، تغییرات اساسی در طراحی آن‌ها صورت گیرد. در هر حال، ارائه‌دهندگان و بهره‌برداران سامانه‌های پرخطر هوش مصنوعی که برای استفاده توسط مقامات عمومی در نظر گرفته شده‌اند، باید تا ۲ اوت ۲۰۳۰ اقدامات لازم را برای رعایت الزامات و تعهدات این قانون انجام دهند.

۳. ارائه‌دهندگان مدل‌های هوش مصنوعی با کاربری عام که پیش از ۲ اوت ۲۰۲۵ در بازار عرضه شده‌اند، باید اقدامات لازم را برای رعایت تعهدات مقرر در این قانون تا ۲ اوت ۲۰۲۷ انجام دهند.

ماده ۱۱۲. ارزیابی و بازنگری

۱. کمیسیون باید ضرورت اصلاح فهرست مندرج در پیوست سوم و فهرست شیوه‌های ممنوع هوش مصنوعی مقرر در ماده ۵ را، از زمان لازم‌الاجراشدن این قانون، سالی یک بار و تا پایان دورهٔ تفویض اختیار مقرر در ماده ۹۷ ارزیابی کند. کمیسیون نتایج این ارزیابی را به پارلمان اروپا و شورا ارائه خواهد داد.

۲. تا ۲ اوت ۲۰۲۸ و سپس هر چهار سال یک بار، کمیسیون باید موارد زیر را ارزیابی و گزارشی در این خصوص به پارلمان اروپا و شورا ارائه کند:

الف) ضرورت اصلاحاتی برای گسترش عناوین حوزه‌های موجود یا افزودن عناوین حوزه‌های جدید در پیوست سه؛

ب) اصلاحات در فهرست سامانه‌های هوش مصنوعی که نیازمند تدابیر شفافیت اضافی مطابق ماده ۵۰ هستند؛

ج) اصلاحاتی برای ارتقاء اثربخشی نظام نظارت و حکمرانی.

۳. تا ۲ اوت ۲۰۲۹ و سپس هر چهار سال یک بار، کمیسیون باید گزارشی دربارهٔ ارزیابی و بازنگری این قانون به پارلمان اروپا و شورا ارائه کند. این گزارش باید شامل ارزیابی ساختار اجرای قانون و نیاز احتمالی به یک نهاد اتحادیه‌ای برای رفع کاستی‌های شناسایی‌شده باشد. بر اساس یافته‌ها، این گزارش، در صورت اقتضا، همراه با پیشنهاد اصلاح قانون خواهد بود. این گزارش‌ها باید علنی شوند.

۴. گزارش‌های مذکور در بند ۲ باید توجه ویژه‌ای به موارد زیر داشته باشند:

الف) وضعیت منابع مالی، فنی و انسانی مقامات صلاحیت‌دار ملی برای اجرای مؤثر وظایف محوله ذیل این قانون؛

ب) وضعیت مجازات‌ها، به‌ویژه جریمه‌های اداری موضوع ماده ۹۹(۱) که توسط دولت‌های عضو برای نقض قانون اعمال می‌شوند؛

ج) استانداردهای هماهنگ و مشخصات مشترکی که در حمایت از این قانون تدوین شده‌اند؛

د) تعداد بنگاه‌هایی که پس از لازم‌الاجراشدن این قانون وارد بازار شده‌اند، و میزان سهم بنگاه‌های کوچک و متوسط از میان آن‌ها.

۵. تا ۲ اوت ۲۰۲۸، کمیسیون باید عملکرد دفتر هوش مصنوعی را ارزیابی کند، ازجمله اینکه آیا این دفتر اختیارات و صلاحیت‌های کافی برای انجام وظایف خود داشته و آیا ارتقاء جایگاه آن و افزایش صلاحیت‌های اجرایی و منابعش برای اجرای درست این قانون لازم است یا خیر. کمیسیون باید گزارشی از این ارزیابی به پارلمان اروپا و شورا ارائه کند.

۶. تا ۲ اوت ۲۰۲۸ و سپس هر چهار سال یک بار، کمیسیون باید گزارشی دربارهٔ بازنگری پیشرفت در تدوین اسناد استانداردسازی مرتبط با توسعهٔ مدل‌های هوش مصنوعی با کاربری عام ارائه و نیاز به اقدامات بیشتر، ازجمله اقدامات الزام‌آور را ارزیابی کند. این گزارش باید به پارلمان اروپا و شورا ارائه و علنی شود.

۷. تا ۲ اوت ۲۰۲۸ و سپس هر سه سال یک بار، کمیسیون باید اثر و کارآیی آیین‌نامه‌های رفتاری داوطلبانه را در جهت تقویت اجرای الزامات مقرر در بخش دوم از فصل سوم برای سامانه‌های غیرپرخطر هوش مصنوعی و نیز الزامات اضافی احتمالی برای سامانه‌های غیرپرخطر، ازجمله در زمینهٔ پایداری زیست‌محیطی، ارزیابی کند.

۸. برای اهداف بندهای ۱ تا ۷، هیئت، دولت‌های عضو و مقامات صلاحیت‌دار ملی باید بنا به درخواست کمیسیون و بدون تأخیر ناموجه، اطلاعات لازم را در اختیار کمیسیون قرار دهند.

۹. کمیسیون در انجام ارزیابی‌ها و بازنگری‌های مذکور در بندهای ۱ تا ۷، باید مواضع و یافته‌های هیئت، پارلمان اروپا، شورا و سایر نهادها یا منابع مرتبط را مدنظر قرار دهد.

۱۰. کمیسیون در صورت لزوم، باید به‌ویژه با توجه به تحولات فناوری، آثار سامانه‌های هوش مصنوعی بر سلامت و ایمنی و حقوق بنیادین، و در پرتو سطح پیشرفت جامعهٔ اطلاعاتی، پیشنهادهای مقتضی برای اصلاح این قانون ارائه کند.

۱۱. به منظور هدایت ارزیابی‌ها و بازنگری‌های مذکور در بندهای ۱ تا ۷، دفتر هوش مصنوعی

باید متعهد شود که روشی عینی و مشارکتی برای ارزیابی سطح ریسک‌ها بر اساس معیارهای مقرر در مواد مربوطه و برای شمول سامانه‌های جدید در موارد زیر توسعه دهد:

الف) فهرست مندرج در پیوست سوم، شامل گسترش عناوین حوزه‌های موجود یا افزودن حوزه‌های جدید؛

ب) فهرست شیوه‌های ممنوع مندرج در ماده ۵؛

ج) فهرست سامانه‌های هوش مصنوعیِ نیازمند تدابیر شفافیت اضافی مطابق ماده ۵۰.

۱۲. هر گونه اصلاح این قانون مطابق بند ۱۰ یا اعمال حقوق تفویضی یا اجرایی مرتبط که به قوانین هماهنگ‌سازی بخشی اتحادیه در بخش (ب) پیوست اول مربوط است، باید ویژگی‌های مقرراتی هر بخش و نیز سازوکارهای موجود در زمینهٔ حکمرانی، ارزیابی انطباق و اجرا و مقامات مستقر در آن‌ها را در نظر گیرد.

۱۳. تا ۲ اوت ۲۰۳۱، کمیسیون باید ارزیابی‌ای از اجرای این قانون انجام دهد و گزارشی از آن را با لحاظ سال‌های نخستین اجرای قانون، به پارلمان اروپا، شورا و کمیتهٔ اقتصادی و اجتماعی اروپا ارائه کند. بر اساس یافته‌ها، آن گزارش، در صورت اقتضا باید همراه با پیشنهاد اصلاح قانون در خصوص ساختار اجرای آن و ضرورت وجود یک نهاد اتحادیه‌ای برای رفع کاستی‌های شناسایی‌شده باشد.

ماده ۱۱۳. لازم‌الاجراشدن و آغاز اجرا

این قانون در بیستمین روز پس از انتشار آن در روزنامهٔ رسمی اتحادیهٔ اروپا لازم‌الاجرا خواهد شد.

این قانون از ۲ اوت ۲۰۲۶ لازم‌الاجرا خواهد بود.

با این حال:

الف) فصل‌های اول و دوم از ۲ فوریهٔ ۲۰۲۵ لازم‌الاجرا خواهند بود؛

ب) فصل سوم بخش ۴، فصل پنج، فصل هفت و فصل دوازده و ماده ۷۸ از ۲ اوت ۲۰۲۵ لازم‌الاجرا خواهند بود، به استثنای ماده ۱۰۱؛

ج) ماده ۶(۱) و تعهدات متناظر در این قانون از ۲ اوت ۲۰۲۷ لازم‌الاجرا خواهند بود.

این قانون در کلیت خود لازم‌الاجرا و مستقیماً در تمامی دولت‌های عضو قابل اعمال است.

تنظیم‌شده در بروکسل، ۱۳ ژوئن ۲۰۲۴.

برای پارلمان اروپا، رئیس متسولا

برای شورا، رئیس میشل

پیوست اول. فهرست قوانین هماهنگ‌شدهٔ اتحادیه

بخش الف. فهرست قوانین هماهنگ‌شدهٔ اتحادیه مبتنی بر *چارچوب قانونگذاری جدید*

۱. دستورالعمل ۴۲/ ۲۰۰۶ پارلمان و شورای اروپا اتحادیهٔ اروپا، مورخ ۱۷ مه ۲۰۰۶ دربارهٔ ماشین‌آلات، و اصلاح دستورالعمل۱۶/ ۹۵ (روزنامهٔ رسمی، مورخ ۹ ژوئن ۲۰۰۶، ص ۲۴)؛

۲. دستورالعمل ۴۸/ ۲۰۰۹ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۱۸ ژوئن ۲۰۰۹ دربارهٔ ایمنی اسباب‌بازی‌ها (روزنامهٔ رسمی، مورخ ۳۰ ژوئن ۲۰۰۹، ص ۱)؛

۳. دستورالعمل۵۳/ ۲۰۱۳ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۲۰ نوامبر ۲۰۱۳ دربارهٔ وسایل نقلیهٔ تفریحی و آبی شخصی و لغو دستورالعمل ۳۵۴/۲۵/۹۴ (روزنامهٔ رسمی مورخ ۲۸ دسامبر ۲۰۱۳، ص ۹۰)؛

۴. دستورالعمل ۳۳/ ۲۰۱۴ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۲۶ فوریهٔ ۲۰۱۴ دربارهٔ همسوسازی قوانین کشورهای عضو در خصوص آسانسورها و اجزای ایمنی آن‌ها (روزنامهٔ رسمی ۹۶، مورخ ۲۹ مارس ۲۰۱۴، ص ۲۵۱)؛

۵. دستورالعمل ۳۴/ ۲۰۱۴ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۲۶ فوریهٔ ۲۰۱۴ دربارهٔ همسوسازی قوانین کشورهای عضو در مورد تجهیزات و سامانه‌های حفاظتی مورد استفاده در محیط‌های بالقوه انفجاری (روزنامهٔ رسمی ۹۶، مورخ ۲۹ مارس ۲۰۱۴، ص ۳۰۹)؛

۶. دستورالعمل ۵۳/ ۲۰۱۴ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۱۶ آوریل ۲۰۱۴ دربارهٔ همسوسازی قوانین کشورهای عضو در زمینهٔ عرضهٔ تجهیزات رادیویی در بازار و لغو دستورالعمل ۵/۱۹۹۹/ ۱۵۳، (روزنامهٔ رسمی مورخ ۲۲ مه ۲۰۱۴، ص ۶۲)؛

۷. دستورالعمل ۶۸/ ۲۰۱۴ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۱۵ مه ۲۰۱۴ دربارهٔ همسوسازی قوانین کشورهای عضو در خصوص تجهیزات تحت فشار (روزنامهٔ رسمی ۱۸۹، مورخ ۲۷ ژوئن ۲۰۱۴، ص ۱۶۴)؛

۸. مقررات شمارهٔ ۲۰۱۶/۴۲۴ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۹ مارس ۲۰۱۶ دربارهٔ تأسیسات کابلی و لغو دستورالعمل ۹/ ۲۰۰۰، (روزنامهٔ رسمی ۸۱ مورخ ۳۱ مارس ۲۰۱۶، ص ۱)؛

۹. قانون شمارهٔ ۴۲۵/ ۲۰۱۶ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۹ مارس ۲۰۱۶ دربارهٔ تجهیزات حفاظت فردی و لغو دستورالعمل شورای ۶۸۶/ ۸۹ جامعهٔ اقتصادی اروپا، (روزنامهٔ رسمی ۸۱، مورخ ۳۱ مارس ۲۰۱۶، ص ۵۱)؛

۱۰. مقررات شمارهٔ ۴۲۶/ ۲۰۱۶ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۹ مارس ۲۰۱۶ دربارهٔ وسایل گازسوز و لغو دستورالعمل ۲۰۰۹/۱۴۲ (روزنامهٔ رسمی ۸۱، مورخ ۳۱ مارس ۲۰۱۶، ص ۹۹)؛

۱۱. مقررات شمارهٔ ۲۰۱۷/۷۴۵ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۵ آوریل ۲۰۱۷ دربارهٔ تجهیزات پزشکی و اصلاح مقررات و دستورالعمل‌های متعدد ازجمله لغو دستورالعمل‌های ۹۰/۳۸۵ و ۴۲/۹۳ جامعهٔ اقتصادی اروپا، (روزنامهٔ رسمی، مورخ ۵ مه ۲۰۱۷، ص ۱)؛

۱۲. قانون شمارهٔ ۲۰۱۷/۷۴۶ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۵ آوریل ۲۰۱۷ دربارهٔ تجهیزات پزشکی تشخیصی درون‌کشتگاهی و لغو دستورالعمل ۹۸/۷۹ و تصمیم ۲۰۱۰/۲۲۷ کمیسیون (روزنامهٔ رسمی ۱۱۷، مورخ ۵ مه ۲۰۱۷، ص ۱۷۶).

بخش ب. فهرست سایر قوانین هماهنگ‌شدهٔ اتحادیه

۱۳. مقررات شمارهٔ ۳۰۰/۲۰۰۸ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۱۱ مارس ۲۰۰۸ دربارهٔ قواعد مشترک در حوزهٔ امنیت هوانوردی غیرنظامی و لغو مقررات ۲۰۰۲/۲۳۲۰، (روزنامهٔ رسمی ۹۷، مورخ ۹ آوریل ۲۰۰۸، ص ۷۲)؛

۱۴. مقررات شمارهٔ ۲۰۱۳/۱۶۸ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۱۵ ژانویهٔ ۲۰۱۳ دربارهٔ تأیید و پایش بازار وسایل نقلیهٔ دو یا سه‌چرخ و چهارچرخ (روزنامهٔ رسمی ۶۰، مورخ ۲ مارس ۲۰۱۳، ص ۵۲)؛

۱۵. مقررات شمارهٔ ۲۰۱۳/۱۶۷ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۵ فوریهٔ ۲۰۱۳ دربارهٔ تأیید و پایش بازار وسایل نقلیهٔ کشاورزی و جنگلی (روزنامهٔ رسمی ۶۰، مورخ ۲ مارس ۲۰۱۳، ص ۱)؛

۱۶. دستورالعمل ۲۰۱۴/۹۰ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۲۳ ژوئیهٔ ۲۰۱۴ دربارهٔ تجهیزات دریایی و لغو دستورالعمل شورای ۹۸/۹۶ (روزنامهٔ رسمی ۲۵۷، مورخ ۲۸ اوت ۲۰۱۴، ص ۱۴۶)؛

۱۷. دستورالعمل ۲۰۱۶/۷۹۷ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۱۱ مه ۲۰۱۶ دربارهٔ قابلیت همکاری سامانهٔ ریلی در اتحادیهٔ اروپا (روزنامهٔ رسمی ۱۳۸، مورخ ۲۶ مه ۲۰۱۶، ص ۴۴)؛

۱۸. مقررات شمارهٔ ۲۰۱۸/۸۵۸ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۳۰ مه ۲۰۱۸ دربارهٔ تأیید و پایش بازار وسایل نقلیهٔ موتوری و تریلرها و اجزای فنی مربوط، و اصلاح و لغو چندین مقررات و دستورالعمل (روزنامهٔ رسمی ۱۵۱، مورخ ۱۴ ژوئن ۲۰۱۸، ص ۱)؛

۱۹. مقررات شمارهٔ ۲۰۱۹/۲۱۴۴ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۲۷ نوامبر ۲۰۱۹ دربارهٔ الزامات تأیید نوع وسایل نقلیهٔ موتوری، تریلرها، اجزا و واحدهای فنی جداگانهٔ مرتبط با ایمنی

عمومی و حفاظت از سرنشینان و کاربران آسیب‌پذیر جاده، و لغو مقررات و مقررات اجرایی متعدد (روزنامهٔ رسمی ۳۲۵، مورخ ۱۶ دسامبر ۲۰۱۹، ص ۱)؛

۲۰. مقررات شمارهٔ ۲۰۱۸/۱۱۹۳ پارلمان و شورای اتحادیهٔ اروپا، مورخ ۴ ژوئیهٔ ۲۰۱۸ دربارهٔ قواعد مشترک در حوزهٔ هوانوردی غیرنظامی و تأسیس آژانس ایمنی هوانوردی اتحادیهٔ اروپا[۱۹۳] و اصلاح یا لغو مقررات و دستورالعمل‌های متعدد، به‌ویژه در خصوص طراحی، تولید و عرضهٔ هواپیماها و پهپادهای بدون سرنشین و اجزای کنترل از راه دور آن‌ها (روزنامهٔ رسمی ۲۱۲، مورخ ۲۲ اوت ۲۰۱۸، ص ۱).

پیوست دوم. فهرست جرایم کیفری مذکور در بند (۱) ماده ۵، بند فرعی نخست، جزء (ح)

جرایم کیفری مذکور در بند (۱) ماده ۵، بند فرعی نخست، جزء (ح) عبارت‌اند از:

- تروریسم،
- قاچاق انسان،
- بهره‌کشی جنسی از کودکان و هرزه‌نگاری کودکان،
- قاچاق غیرقانونی مواد مخدر یا مواد روان‌گردان،
- قاچاق غیرقانونی سلاح، مهمات یا مواد منفجره،
- قتل یا ایراد صدمهٔ شدید بدنی،
- تجارت غیرقانونی اعضا یا بافت‌های انسانی،
- قاچاق غیرقانونی مواد هسته‌ای یا رادیواکتیو،
- آدم‌ربایی، بازداشت غیرقانونی یا گروگان‌گیری،
- جرایمی که در صلاحیت دیوان کیفری بین‌المللی قرار دارند،
- تصرف غیرقانونی هواپیما یا کشتی،
- تجاوز جنسی،
- جرم علیه محیط‌زیست،
- سرقت سازمان‌یافته یا مسلحانه،
- خرابکاری،
- مشارکت در سازمان جنایی که در یک یا چند مورد از جرایم فوق‌الذکر فعالیت دارد.

193. EASA

پیوست سوم. سامانه‌های هوش مصنوعی با ریسک بالا (موضوع بند ۲ ماده ۶)

سامانه‌های هوش مصنوعی پرخطر بر اساس بند (۲) ماده (۶)، شامل سامانه‌های هوش مصنوعی در هر یک از حوزه‌های زیر می‌شوند:

۱. زیست‌سنجی (در حدودی که استفاده از آن طبق حقوق اتحادیه یا قوانین ملی مجاز باشد):

الف) سیستم‌های شناسایی زیست‌سنجی از راه دور.

(این مورد شامل سامانه‌های هوش مصنوعی مورد استفاده برای تأیید هویت زیست‌سنجی با هدف صرفِ اطمینان از اینکه شخص طبیعی مشخص، همان کسی که ادعا می‌کند، نمی‌شود).

ب) سامانه‌های هوش مصنوعی مورد استفاده برای دسته‌بندی زیست‌سنجی بر اساس ویژگی‌ها یا صفات حساس یا تحت حمایت که این دسته‌بندی بر مبنای استنتاج آن ویژگی‌ها یا صفات انجام می‌شود.

پ) سامانه‌های هوش مصنوعی مورد استفاده برای شناسایی احساسات.

۲. زیرساخت‌های حیاتی:

سامانه‌های هوش مصنوعی که به‌عنوان مؤلفه‌های ایمنی در مدیریت و بهره‌برداری از زیرساخت‌های حیاتی دیجیتال، ترافیک جاده‌ای، یا تأمین آب، گاز، گرمایش یا برق به کار می‌روند.

۳. آموزش و پرورش حرفه‌ای:

الف) سامانه‌های هوش مصنوعی مورد استفاده برای تعیین دسترسی یا پذیرش اشخاص به مؤسسات آموزشی یا حرفه‌ای در هر سطح؛

ب) سامانه‌های هوش مصنوعی مورد استفاده برای ارزیابی نتایج یادگیری، ازجمله هنگامی که این نتایج برای هدایت فرآیند یادگیری افراد در مؤسسات آموزشی یا حرفه‌ای در هر سطح به کار می‌رود؛

پ) سامانه‌های هوش مصنوعی مورد استفاده برای ارزیابی سطح مناسب آموزش که فرد باید دریافت کند یا به آن دسترسی داشته باشد در چارچوب یا درون مؤسسات آموزشی یا حرفه‌ای در هر سطح؛

ت) سامانه‌های هوش مصنوعی مورد استفاده برای پایش و شناسایی رفتارهای ممنوعهٔ دانش‌آموزان در جریان آزمون‌ها در چارچوب یا درون مؤسسات آموزشی یا حرفه‌ای در هر سطح.

۴. اشتغال، مدیریت کارکنان و دسترسی به خوداشتغالی:

الف) سامانه‌های هوش مصنوعی مورد استفاده در فرآیند استخدام یا گزینش اشخاص به‌ویژه برای نمایش آگهی‌های شغلی هدفمند، تحلیل و فیلترکردن درخواست‌های استخدام و ارزیابی داوطلبان؛

ب) سامانه‌های هوش مصنوعی مورد استفاده برای تصمیم‌گیری در خصوص شرایط روابط شغلی،

ارتقا یا خاتمهٔ روابط قراردادی کاری، تخصیص وظایف بر اساس رفتار فردی یا ویژگی‌ها و خصوصیات شخصی یا نظارت و ارزیابی عملکرد و رفتار افراد در چنین روابطی.

۵. دسترسی به خدمات ضروری خصوصی و عمومی و بهره‌مندی از آن‌ها:

الف) سامانه‌های هوش مصنوعی مورد استفاده توسط مقامات عمومی یا به نیابت از آنان برای ارزیابی صلاحیت اشخاص در بهره‌مندی از مزایا و خدمات عمومی ضروری ازجمله خدمات بهداشتی، و نیز اعطا، کاهش، لغو یا بازپس‌گیری آن مزایا و خدمات؛

ب) سامانه‌های هوش مصنوعی مورد استفاده برای ارزیابی اعتبار مالی اشخاص یا تعیین امتیاز اعتباری آنان (به استثنای سامانه‌های هوش مصنوعی مورد استفاده برای کشف تقلب مالی)؛

پ) سامانه‌های هوش مصنوعی مورد استفاده برای ارزیابی ریسک و تعیین نرخ‌ها در ارتباط با اشخاص در حوزهٔ بیمهٔ عمر و سلامت.

ت) سامانه‌های هوش مصنوعی که برای ارزیابی و طبقه‌بندی تماس‌های اضطراری اشخاص یا برای اعزام نیروهای واکنش سریع اضطراری ازجمله پلیس، آتش‌نشانان و امداد پزشکی یا برای تعیین اولویت در اعزام آن‌ها به کار می‌روند، همچنین سیستم‌های تریاژ بیماران در خدمات فوریت‌های درمانی.

۶. اجرای قانون (در حدودی که استفاده از آن طبق حقوق اتحادیه یا حقوق ملی مجاز باشد):

الف) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات اجرای قانون یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه در حمایت از مقامات اجرای قانون یا به نمایندگی از آن‌ها برای ارزیابی خطر قربانی‌شدن اشخاص در جرایم به کار می‌روند؛

ب) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات اجرای قانون یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه در حمایت از مقامات اجرای قانون به‌عنوان دروغ‌سنج یا ابزارهای مشابه به کار می‌روند؛

پ) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات اجرای قانون یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه در حمایت از مقامات اجرای قانون برای ارزیابی قابلیت اعتماد دلایل و مستندات در جریان تحقیقات یا تعقیب کیفری به کار می‌روند؛

ت) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات اجرای قانون یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه در حمایت از مقامات اجرای قانون برای ارزیابی خطر ارتکاب یا تکرار جرم از سوی اشخاص استفاده می‌شوند، مشروط بر اینکه این ارزیابی صرفاً بر مبنای پروفایل‌سازی اشخاص به معنای ماده ۳(۴) از دستورالعمل شمارهٔ ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) نباشد یا برای ارزیابی ویژگی‌های شخصیتی، خصایص رفتاری یا سوابق کیفری اشخاص یا گروه‌ها به کار روند؛

ث) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات اجرای قانون یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه در حمایت از مقامات اجرای قانون برای پروفایل‌سازی اشخاص به معنای ماده ۳(۴) از دستورالعمل شمارهٔ ۲۰۱۶/۶۸۰ (اتحادیهٔ اروپا) در جریان کشف، تحقیق یا تعقیب جرایم استفاده می‌شوند.

۷. مهاجرت، پناهندگی و مدیریت کنترل مرزها (در حدودی که استفاده از آن طبق حقوق اتحادیه یا حقوق ملی مجاز باشد):

الف) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات عمومی ذی‌صلاح یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه به‌عنوان دروغ‌سنج یا ابزارهای مشابه به کار می‌روند؛

ب) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات عمومی ذی‌صلاح یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه برای ارزیابی خطرات احتمالی ازجمله خطرات امنیتی، مهاجرت غیرقانونی یا خطرات بهداشتی که از سوی شخصی که قصد ورود یا وارد قلمرو یکی از کشورهای عضو اتحادیه می‌شود، استفاده می‌شوند؛

پ) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات عمومی ذی‌صلاح یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه برای یاری‌رساندن به مقامات ذی‌صلاح در بررسی درخواست‌های پناهندگی، روادید یا مجوز اقامت و نیز در رسیدگی به شکایات مربوط به صلاحیت متقاضیان ازجمله برای ارزیابی قابلیت اعتماد مدارک و مستندات ارائه‌شده به کار می‌روند؛

ت) سامانه‌های هوش مصنوعی که توسط یا از جانب مقامات عمومی ذی‌صلاح یا توسط نهادها، سازمان‌ها، دفاتر یا آژانس‌های اتحادیه در زمینهٔ مدیریت مهاجرت، پناهندگی یا کنترل مرزها برای شناسایی، تشخیص یا بازشناسی اشخاص به کار می‌روند، به استثنای مواردی که صرفاً برای تأیید اصالت اسناد مسافرتی استفاده می‌شوند.

۸. ادارهٔ دادگستری و فرآیندهای دموکراتیک:

الف) سامانه‌های هوش مصنوعی که توسط مرجع قضایی یا از جانب آن برای یاری‌رسانی به مرجع قضایی در تحقیق و تفسیر واقعیات و قوانین و در اعمال قانون بر مجموعه‌ای از واقعیات مشخص به کار می‌روند، یا به‌صورت مشابه در فرآیندهای حل و فصل اختلاف جایگزین به کار می‌روند؛

ب) سامانه‌های هوش مصنوعی که برای تأثیرگذاری بر نتیجهٔ انتخابات یا همه‌پرسی یا بر رفتار رأی‌دهندگان در هنگام رأی‌دادن در انتخابات یا همه‌پرسی‌ها استفاده می‌شوند. این مورد شامل سامانه‌های هوش مصنوعی‌ای که اشخاص به‌طور مستقیم در معرض خروجی آن‌ها قرار نمی‌گیرند، مانند ابزارهایی که صرفاً برای سازماندهی، بهینه‌سازی یا ساختاربندی کارزارهای سیاسی از منظر اداری یا لجستیکی به کار می‌روند، نمی‌شود.

پیوست چهارم. مستندات فنی مذکور در ماده ۱۱(۱)

مستندات فنی که در ماده ۱۱(۱) به آن اشاره شده است باید حداقل شامل اطلاعات زیر باشد تا حدی که نسبت به سامانهٔ هوش مصنوعی مربوطه قابل‌اعمال است:

۱. شرح کلی سامانهٔ هوش مصنوعی، شامل:

الف) هدف استفاده از سیستم، نام ارائه‌دهنده و نسخه سیستم (به نحوی که رابطهٔ آن با نسخه‌های قبلی مشخص شود)؛

ب) نحوهٔ تعامل سیستم با سخت‌افزار یا نرم‌افزارهای دیگر (ازجمله سایر سامانه‌های هوش مصنوعی) که جزئی از سیستم نیستند، در صورت وجود؛

پ) نسخه‌های نرم‌افزار یا میان‌افزار[۱۹۴] مرتبط و هر گونه الزامات مربوط به به‌روزرسانی نسخه‌ها؛

ت) توصیف تمام اشکال عرضهٔ سیستم در بازار یا به‌کارگیری آن (مانند بسته‌های نرم‌افزاری تعبیه‌شده در سخت‌افزار، نسخه‌های قابل دانلود، یا رابط برنامه‌نویسی کاربردی (API)؛

ث) توصیف سخت‌افزاری که سیستم برای اجرا بر اساس آن طراحی شده است؛

ج) در صورتی که سیستم بخشی از یک محصول باشد، عکس‌ها یا تصاویر شماتیک از ویژگی‌های ظاهری، نشانه‌گذاری‌ها و آرایش داخلی آن محصول؛

چ) توضیحی کلی دربارهٔ رابط کاربری ارائه‌شده برای بهره‌بردار؛

ح) دستورالعمل‌های استفاده برای بهره‌بردار و توضیحی کلی از رابط کاربری، در صورت وجود.

۲. شرح تفصیلی اجزای سیستم و فرآیند توسعهٔ آن، ازجمله:

الف) روش‌ها و مراحل انجام‌شده در توسعهٔ سیستم، ازجمله در صورت استفاده از سیستم‌ها یا ابزارهای از پیش آموزش‌دیده ارائه‌شده توسط اشخاص ثالث و نحوهٔ استفاده، یکپارچه‌سازی یا اصلاح آن‌ها توسط ارائه‌دهنده؛

ب) مشخصات طراحی سیستم، ازجمله منطق کلی الگوریتم‌ها و سیستم، تصمیمات طراحی کلیدی و دلایل اتخاذ آن‌ها؛ فرضیات انجام‌شده به‌ویژه در مورد گروه‌هایی از اشخاص که سیستم برای استفاده در مورد آنان طراحی شده است؛ انتخاب‌های اصلی در طبقه‌بندی، معیارهای بهینه‌سازی سیستم و اهمیت معیارهای مختلف؛ توصیف خروجی‌های مورد انتظار و کیفیت خروجی‌ها و تصمیمات مربوط به ملاحظات فنی برای رعایت الزامات مندرج در فصل سوم، بخش دوم؛

پ) توصیف معماری سیستم و چگونگی ارتباط و تعامل اجزای نرم‌افزاری با یکدیگر در پردازش کلی؛ منابع محاسباتی مورد استفاده برای توسعه، آموزش، آزمون و اعتبارسنجی سیستم؛

ت) در صورت وجود، الزامات داده‌ای، شامل برگه‌های داده که روش‌ها و داده‌های آموزشی

194. firmware

استفاده‌شده را توصیف می‌کنند، منشأ، دامنه و ویژگی‌های اصلی این داده‌ها، نحوهٔ جمع‌آوری و انتخاب داده‌ها، روش‌های برچسب‌گذاری (برای یادگیری نظارت‌شده) و پاک‌سازی داده‌ها (مانند شناسایی داده‌های ناهنجار یا غیرمعمول)؛

ث) ارزیابی تدابیر نظارت انسانی مورد نیاز مطابق ماده ۱۴، ازجمله ارزیابی تدابیر فنی برای تسهیل تفسیر خروجی‌ها توسط بهره‌برداران طبق ماده ۱۳(۳)(د)؛

ج) در صورت لزوم، شرح مفصل تغییرات از پیش تعیین‌شده در سیستم و عملکرد آن و اطلاعات مرتبط با راه‌حل‌های فنی برای تضمین تداوم انطباق سیستم با الزامات فصل سوم، بخش دوم؛

چ) روش‌های اعتبارسنجی و آزمون، ازجمله داده‌های مورد استفاده برای اعتبارسنجی و آزمون، ویژگی‌های اصلی آن‌ها، شاخص‌های سنجش دقت، استحکام و انطباق با سایر الزامات مربوطه در فصل سوم، بخش دوم، و آثار تبعیض‌آمیز احتمالی؛ گزارش‌ها و سوابق آزمون‌ها با امضا و تاریخ مسئولان مربوط، ازجمله برای تغییرات از پیش تعیین‌شدهٔ موضوع بند (و)؛

ح) تدابیر امنیت سایبری اتخاذشده.

۳. اطلاعات تفصیلی دربارهٔ نظارت، عملکرد و کنترل سیستم، به‌ویژه در خصوص:

توانایی‌ها و محدودیت‌های عملکرد سیستم (ازجمله میزان دقت برای اشخاص یا گروه‌های خاصی که سیستم برای آنان طراحی شده است) و سطح کلی دقت متناسب با هدف موردنظر؛

نتایج ناخواسته قابل پیش‌بینی و منابع خطر برای سلامت و ایمنی، حقوق بنیادین و تبعیض؛

تدابیر نظارت انسانی مطابق ماده ۱۴ ازجمله تدابیر فنی برای تسهیل تفسیر خروجی‌ها توسط بهره‌برداران؛

مشخصات داده‌های ورودی، در صورت اقتضا.

۴. توصیف تناسب *شاخص‌های عملکرد*[۱۹۵] با سیستم خاص.

۵. توصیف تفصیلی نظام مدیریت ریسک مطابق ماده ۹.

۶. توصیف تغییرات انجام‌شده توسط ارائه‌دهنده در طول چرخهٔ عمر سیستم.

۷. فهرست استانداردهای هماهنگ‌شده که به‌طور کامل یا جزئی به کار گرفته شده‌اند و مراجع آن‌ها در *روزنامهٔ رسمی اتحادیهٔ اروپا* منتشر شده است؛ در صورت عدم استفاده از چنین استانداردهایی، شرح تفصیلی راه‌حل‌های جایگزین اتخاذشده برای رعایت الزامات فصل سوم، بخش دوم، شامل فهرستی از سایر استانداردها و مشخصات فنی به‌کاررفته.

۸. یک نسخه از *اعلامیهٔ انطباق اتحادیهٔ اروپا*[۱۹۶] موضوع ماده ۴۷.

---

195. The performance metrics

196. EU declaration of conformity

۹. شرح تفصیلی نظام ارزیابی عملکرد سیستم در مرحلهٔ پس از عرضه در بازار[۱۹۷] مطابق ماده ۷۲، ازجمله برنامهٔ پایش پس از عرضه در بازار مذکور در ماده ۷۲(۳).

پیوست پنجم. اعلامیهٔ انطباق اتحادیهٔ اروپا

اعلامیهٔ انطباق اتحادیهٔ اروپا که در ماده ۴۷ به آن اشاره شده است، باید شامل تمامی اطلاعات زیر باشد:

۱. نام و نوع سامانهٔ هوش مصنوعی و هر گونه شناسهٔ اضافی و روشن که امکان شناسایی و ردیابی دقیق سامانه را فراهم کند؛

۲. نام و نشانی ارائه‌دهنده یا در صورت وجود، نمایندهٔ مجاز او؛

۳. بیانیه‌ای مبنی بر اینکه اعلامیهٔ انطباق اتحادیهٔ اروپا موضوع ماده ۴۷، صرفاً تحت مسئولیت ارائه‌دهنده صادر شده است؛

۴. بیانیه‌ای دال بر انطباق سامانهٔ هوش مصنوعی با مقررات حاضر و در صورت لزوم با سایر قوانین اتحادیهٔ اروپا که صدور اعلامیهٔ انطباق اتحادیهٔ اروپا موضوع ماده ۴۷ را پیش‌بینی کرده‌اند؛

۵. در صورتی که سامانهٔ هوش مصنوعی شامل پردازش داده‌های شخصی باشد، بیانیه‌ای مبنی بر انطباق آن با مقررات ۶۷۹ /۲۰۱۶ و ۱۷۲۵ /۲۰۱۸ و دستورالعمل ۶۸۰ /۲۰۱۶ اتحادیهٔ اروپا؛

۶. ارجاعات به هر گونه استاندارد هماهنگ مرتبط که مورد استفاده قرار گرفته است یا هر مشخصهٔ مشترک دیگری که انطباق با آن اعلام می‌شود؛

۷. در صورت اقتضا، نام و شمارهٔ شناسایی نهاد اعلام‌شده، شرحی از رویهٔ ارزیابی انطباق اجراشده و شناسهٔ گواهی صادره؛

۸. محل و تاریخ صدور اعلامیه، نام و سمت شخص امضاکننده، همچنین ذکر اینکه امضا به نمایندگی از چه شخص یا نهادی انجام شده است، و در پایان امضا.

پیوست ششم. رویهٔ ارزیابی انطباق بر مبنای کنترل داخلی

۱. رویهٔ ارزیابی انطباق بر مبنای کنترل داخلی شامل مراحلی است که در بندهای ۲، ۳ و ۴ زیر آمده است.

197. The post-market

۲. ارائه‌دهنده باید اطمینان حاصل کند که نظام مدیریت کیفیت ایجادشده با الزامات مقرر در ماده ۱۷ مطابقت دارد.

۳. ارائه‌دهنده باید اطلاعات مندرج در مستندات فنی را بررسی کند تا انطباق سامانهٔ هوش مصنوعی با الزامات اساسی مربوطه مندرج در بخش دوم از فصل سوم را ارزیابی کند.

۴. همچنین ارائه‌دهنده باید احراز کند که فرآیند طراحی و توسعهٔ سامانهٔ هوش مصنوعی و نیز نظام پایش پس از عرضهٔ موضوع ماده ۷۲ با مستندات فنی یادشده همخوانی و مطابقت دارد.

پیوست هفتم. ارزیابی انطباق مبتنی بر بررسی نظام مدیریت کیفیت و ارزیابی مستندات فنی

۱. مقدمه

ارزیابی انطباق مبتنی بر بررسی نظام مدیریت کیفیت و ارزیابی مستندات فنی، رویه‌ای برای ارزیابی انطباق است که بر اساس بندهای ۲ تا ۵ انجام می‌شود.

۲. نمای کلی

نظام مدیریت کیفیت تأییدشده برای طراحی، توسعه و آزمون سامانه‌های هوش مصنوعی مطابق ماده ۱۷، طبق بند ۳ بررسی و تحت نظارت مقرر در بند ۵ قرار می‌گیرد. مستندات فنی سامانهٔ هوش مصنوعی طبق بند ۴ بررسی خواهد شد.

۳. نظام مدیریت کیفیت

۳-۱. درخواست ارائه‌دهنده باید شامل موارد زیر باشد:

الف) نام و نشانی ارائه‌دهنده و، در صورت ارائهٔ درخواست از سوی نمایندهٔ مجاز، نام و نشانی او؛

ب) فهرست سامانه‌های هوش مصنوعی مشمول همان نظام مدیریت کیفیت؛

پ) مستندات فنی مربوط به هر سامانهٔ هوش مصنوعی تحت پوشش همان نظام مدیریت کیفیت؛

ت) مستندات مربوط به نظام مدیریت کیفیت که باید تمام جنبه‌های ذکرشده در ماده ۱۷ را پوشش دهد؛

ث) شرح رویه‌های موجود برای اطمینان از کافی و مؤثرماندن نظام مدیریت کیفیت؛

ج) اعلامیهٔ کتبی مبنی بر اینکه همین درخواست به هیچ نهاد اطلاع‌رسان دیگری ارائه نشده است.

۳-۲. نظام مدیریت کیفیت توسط نهاد اطلاع‌رسان ارزیابی می‌شود تا تعیین شود آیا الزامات مذکور در ماده ۱۷ را برآورده می‌کند یا خیر.

تصمیم به ارائه‌دهنده یا نمایندهٔ مجاز او ابلاغ می‌شود.

ابلاغیه باید شامل نتایج ارزیابی نظام مدیریت کیفیت و تصمیم ارزیابی مستدل باشد.

۳-۳. نظام مدیریت کیفیت تأییدشده باید توسط ارائه‌دهنده پیاده‌سازی و نگهداری شود تا همچنان کافی و کارآمد باقی بماند.

۳-۴. هر گونه تغییر موردنظر در نظام مدیریت کیفیت تأییدشده یا فهرست سامانه‌های هوش مصنوعی مشمول آن باید توسط ارائه‌دهنده به اطلاع نهاد اطلاع‌رسان رسانده شود.

تغییرات پیشنهادی توسط نهاد اطلاع‌رسان بررسی می‌شود تا تصمیم بگیرد آیا نظام مدیریت کیفیت اصلاح‌شده همچنان الزامات مذکور در بند ۳.۲ را برآورده می‌کند یا نیاز به ارزیابی مجدد دارد.

نهاد اطلاع‌رسان تصمیم خود را به ارائه‌دهنده ابلاغ می‌کند. ابلاغیه باید شامل نتایج بررسی تغییرات و تصمیم ارزیابی مستدل باشد.

۴. کنترل مستندات فنی

۴-۱. علاوه بر درخواست مذکور در بند ۳، ارائه‌دهنده باید درخواست مستقلی به نهاد اطلاع‌رسان منتخب خود برای ارزیابی مستندات فنی مرتبط با سامانهٔ هوش مصنوعی که قصد دارد در بازار عرضه یا به خدمت گیرد و تحت پوشش نظام مدیریت کیفیت مذکور در بند ۳ قرار دارد، ارائه کند.

۴-۲. درخواست باید شامل موارد زیر باشد:

الف) نام و نشانی ارائه‌دهنده؛

ب) اعلامیهٔ کتبی مبنی بر اینکه همین درخواست به هیچ نهاد اطلاع‌رسان دیگری ارائه نشده است؛

ج) مستندات فنی مذکور در پیوست چهارم.

۴-۳. مستندات فنی توسط نهاد اطلاع‌رسان بررسی خواهد شد. در صورت لزوم، و تا حدی که برای انجام وظایفش ضروری است، باید دسترسی کامل به مجموعه‌داده‌های آموزش، اعتبارسنجی و آزمون فراهم شود؛ ازجمله، در صورت مناسب‌بودن و با رعایت تدابیر امنیتی، از طریق رابط برنامه‌نویسی یا سایر ابزارها و روش‌های فنی مرتبط که امکان دسترسی از راه دور را می‌دهند.

۴-۴. در بررسی مستندات فنی، نهاد اطلاع‌رسان می‌تواند از ارائه‌دهنده بخواهد مدارک بیشتری

ارائه کند یا آزمون‌های بیشتری انجام دهد تا ارزیابی صحیحی از انطباق سامانهٔ هوش مصنوعی با الزامات مندرج در فصل سوم، بخش دوم انجام شود. در صورتی که نهاد اطلاع‌رسان از آزمون‌های انجام‌شده توسط ارائه‌دهنده قانع نشود، خود مستقیماً آزمون‌های مناسب را انجام خواهد داد.

۴-۵. در صورتی که برای ارزیابی انطباق سامانه‌های هوش مصنوعی پرخطر با الزامات مندرج در فصل سوم، بخش دوم ضروری باشد و تمام راه‌های معقول برای تأیید انطباق به کار گرفته و ناکافی تشخیص داده شده باشند، و بنا بر درخواست مستدل، دسترسی به مدل‌های آموزش‌دیده و معیارهای مرتبط نیز باید در اختیار نهاد اطلاع‌رسان قرار گیرد. چنین دسترسی‌ای تابع قوانین اتحادیه در خصوص حمایت از مالکیت فکری و اسرار تجاری خواهد بود.

۴-۶. تصمیم نهاد اطلاع‌رسان باید به ارائه‌دهنده یا نمایندهٔ مجاز او ابلاغ شود. ابلاغیه باید شامل نتایج ارزیابی مستندات فنی و تصمیم ارزیابی مستدل باشد.

چنانچه سامانهٔ هوش مصنوعی با الزامات فصل سوم، بخش دوم منطبق باشد، نهاد اطلاع‌رسان، *گواهی ارزیابی مستندات فنی اتحادیه* صادر می‌کند. گواهی باید نام و نشانی ارائه‌دهنده، نتایج بررسی، شرایط (در صورت وجود) برای اعتبار آن و داده‌های لازم برای شناسایی سامانهٔ هوش مصنوعی را ذکر کند.

گواهی و پیوست‌های آن باید تمام اطلاعات لازم برای ارزیابی انطباق سامانه و امکان کنترل سامانه در حین استفاده (در صورت اقتضا) را دربر داشته باشد.

چنانچه سامانه با الزامات منطبق نباشد، نهاد اطلاع‌رسان از صدور گواهی امتناع و متقاضی را همراه با دلایل مفصل مطلع می‌کند.

چنانچه سامانهٔ هوش مصنوعی با الزامات مربوط به داده‌های آموزشی انطباق نداشته باشد، لازم است پیش از درخواست مجدد برای ارزیابی انطباق، آموزش مجدد انجام گیرد. در این حالت، تصمیم مستدل نهاد اطلاع‌رسان مبنی بر رد صدور گواهی باید حاوی ملاحظات خاص دربارهٔ کیفیت داده‌های آموزشی، به‌ویژه دلایل عدم انطباق باشد.

۴-۷. هر گونه تغییر در سامانهٔ هوش مصنوعی که ممکن است بر انطباق آن با الزامات یا هدف موردنظر اثر بگذارد، باید توسط نهاد اطلاع‌رسان صادرکننده گواهی ارزیابی مستندات فنی اتحادیه ارزیابی شود. ارائه‌دهنده باید نهاد اطلاع‌رسان را از قصد خود برای اعمال تغییرات یا از وقوع چنین تغییراتی مطلع کند. تغییرات پیشنهادی باید توسط نهاد اطلاع‌رسان بررسی شود تا تصمیم بگیرد آیا این تغییرات مستلزم ارزیابی انطباق جدید مطابق ماده ۴۳(۴) هستند یا می‌توانند از طریق الحاقیه به گواهی ارزیابی مستندات فنی اتحادیه پوشش داده شوند. در حالت دوم، نهاد اطلاع‌رسان تغییرات را ارزیابی کرده و تصمیم خود را به ارائه‌دهنده ابلاغ و در صورت تأیید، الحاقیهٔ

گواهی را صادر می‌کند.

۵. نظارت بر نظام مدیریت کیفیت تأییدشده

۵-۱. هدف از نظارت انجام‌شده توسط نهاد اطلاع‌رسان مذکور در بند ۳، اطمینان از رعایت صحیح شرایط نظام مدیریت کیفیت تأییدشده توسط ارائه‌دهنده است.

۵-۲. برای اهداف ارزیابی، ارائه‌دهنده باید اجازهٔ دسترسی نهاد اطلاع‌رسان به محل‌هایی را که طراحی، توسعه و آزمون سامانه‌های هوش مصنوعی در آن انجام می‌شود، بدهد. ارائه‌دهنده همچنین باید تمام اطلاعات لازم را در اختیار نهاد اطلاع‌رسان قرار دهد.

۵-۳. نهاد اطلاع‌رسان باید ممیزی‌های دوره‌ای انجام دهد تا از حفظ و اجرای نظام مدیریت کیفیت توسط ارائه‌دهنده اطمینان یابد و گزارش ممیزی را به او ارائه کند. در چارچوب این ممیزی‌ها، نهاد اطلاع‌رسان می‌تواند آزمون‌های اضافی بر سامانه‌های هوش مصنوعی‌ای که گواهی ارزیابی مستندات فنی اتحادیه برایشان صادر شده است انجام دهد.

پیوست هشتم. اطلاعاتی که باید هنگام ثبت سامانه‌های پرخطر هوش مصنوعی مطابق ماده ۴۹ ارائه شود

بخش الف. اطلاعاتی که باید توسط ارائه‌دهندگان سامانه‌های پرخطر هوش مصنوعی مطابق ماده ۴۹(۱) ارائه شود

اطلاعات زیر باید ارائه و سپس به‌روزرسانی شوند. در خصوص سامانه‌های پرخطر هوش مصنوعی که مطابق ماده ۴۹(۱) ثبت می‌شوند:

۱. نام، نشانی و جزئیات تماس ارائه‌دهنده؛

۲. در صورتی که ارائهٔ اطلاعات توسط شخص دیگری از طرف ارائه‌دهنده انجام شود، نام، نشانی و جزئیات تماس آن شخص؛

۳. نام، نشانی و جزئیات تماس نمایندهٔ مجاز، در صورت وجود؛

۴. نام تجاری سامانهٔ هوش مصنوعی و هر گونه مرجع روشن و غیرمبهم دیگر که امکان شناسایی و ردیابی سامانه را فراهم کند؛

۵. شرح هدف موردنظر از سامانهٔ هوش مصنوعی و اجزاء و کارکردهایی که از طریق آن سامانه پشتیبانی می‌شوند؛

۶. توضیحی پایه‌ای و مختصر از اطلاعات مورد استفادهٔ سامانه (داده‌ها، ورودی‌ها) و منطق عملیاتی آن؛

۷. وضعیت سامانهٔ هوش مصنوعی (در بازار یا در خدمت؛ دیگر در بازار/خدمت قرار ندارد، فراخوانده شده)؛

۸. نوع، شماره و تاریخ انقضای گواهی صادره از نهاد ارزیابی انطباق و نام یا شمارهٔ شناسایی آن نهاد، در صورت وجود؛

۹. یک نسخهٔ اسکن‌شده از گواهی مذکور در بند ۸، در صورت وجود؛

۱۰. هر یک از کشورهای عضو که سامانهٔ هوش مصنوعی در آن‌ها به بازار عرضه شده، به خدمت گرفته شده یا در اتحادیه در دسترس قرار داده شده است؛

۱۱. نسخه‌ای از اعلامیهٔ انطباق اتحادیهٔ اروپا مطابق ماده ۴۷؛

۱۲. دستورالعمل‌های الکترونیکی برای استفاده؛ این اطلاعات نباید برای سامانه‌های پرخطر هوش مصنوعی در حوزه‌های اجرای قانون یا مدیریت مهاجرت، پناهندگی و کنترل مرزها که در پیوست سوم، بندهای ۱، ۶ و ۷ ذکر شده‌اند ارائه شوند؛

۱۳. یک نشانی اینترنتی برای اطلاعات تکمیلی (اختیاری).

بخش ب. اطلاعاتی که باید توسط ارائه‌دهندگان سامانه‌های پرخطر هوش مصنوعی مطابق ماده ۴۹(۲) ارائه شود

اطلاعات زیر باید در خصوص سامانه‌های هوش مصنوعی که مطابق ماده ۴۹(۲) ثبت می‌شوند ارائه و سپس به‌روزرسانی شوند:

۱. نام، نشانی و جزئیات تماس ارائه‌دهنده؛

۲. در صورتی که ارائهٔ اطلاعات توسط شخص دیگری از طرف ارائه‌دهنده انجام شود، نام، نشانی و جزئیات تماس آن شخص؛

۳. نام، نشانی و جزئیات تماس نمایندهٔ مجاز، در صورت وجود؛

۴. نام تجاری سامانهٔ هوش مصنوعی و هر گونه مرجع روشن و غیرمبهم دیگر که امکان شناسایی و ردیابی سامانه را فراهم کند؛

۵. شرح هدف موردنظر از سامانهٔ هوش مصنوعی؛

۶. شرط یا شرایط تحت ماده ۶(۳) که بر اساس آن‌ها سامانهٔ هوش مصنوعی به‌عنوان غیرپرخطر

محسوب می‌شود؛

۷. خلاصه‌ای کوتاه از مبانی بر اساس آن‌ها سامانهٔ هوش مصنوعی در چارچوب فرآیند ماده ۶(۳) به‌عنوان غیرپرخطر تلقی شده است؛

۸. وضعیت سامانهٔ هوش مصنوعی (در بازار یا در خدمت؛ دیگر در بازار/خدمت قرار ندارد، فراخوانده شده)؛

۹. هر یک از کشورهای عضو که سامانهٔ هوش مصنوعی در آن‌ها به بازار عرضه شده، به خدمت گرفته شده یا در اتحادیه در دسترس قرار داده شده است.

بخش ج. اطلاعاتی که باید توسط بهره‌برداران سامانه‌های پرخطر هوش مصنوعی مطابق ماده ۴۹(۳) ارائه شود

اطلاعات زیر باید در خصوص سامانه‌های پرخطر هوش مصنوعی که مطابق ماده ۴۹(۳) ثبت می‌شوند، ارائه و سپس به‌روزرسانی شوند:

۱. نام، نشانی و جزئیات تماس بهره‌بردار؛

۲. نام، نشانی و جزئیات تماس شخصی که اطلاعات را از طرف بهره‌بردار ارائه می‌دهد؛

۳. نشانی اینترنتی مربوط به مدخل سامانهٔ هوش مصنوعی در پایگاه دادهٔ اتحادیهٔ اروپا که توسط ارائه‌دهندهٔ آن ثبت شده است؛

۴. خلاصه‌ای از نتایج ارزیابی تأثیر بر حقوق بنیادین که مطابق ماده ۲۷ انجام شده است؛

۵. خلاصه‌ای از ارزیابی تأثیر بر حفاظت داده‌ها که مطابق ماده ۳۵ قانون (اتحادیهٔ اروپا) ۶۷۹/۲۰۱۶ یا ماده ۲۷ دستورالعمل (اتحادیهٔ اروپا) ۶۸۰/۲۰۱۶ طبق ماده ۲۶(۸) این قانون صورت گرفته است، در صورت وجود.

پیوست نهم. اطلاعاتی که باید هنگام ثبت سامانه‌های پرخطر هوش مصنوعی مندرج در پیوست سوم در رابطه با آزمون در شرایط واقعی مطابق ماده ۶۰ ارائه شود

اطلاعات زیر باید در خصوص آزمون در شرایط واقعی که مطابق ماده ۶۰ ثبت می‌شود، ارائه و سپس به‌روزرسانی شوند:

۱. یک شمارهٔ شناسایی یکتای اتحادیه‌ای برای آزمون در شرایط واقعی؛

۲. نام و جزئیات تماس ارائه‌دهنده یا ارائه‌دهندهٔ بالقوه و بهره‌بردارانی که در آزمون در شرایط واقعی مشارکت دارند؛

۳. شرحی مختصر از سامانهٔ هوش مصنوعی، هدف موردنظر آن و سایر اطلاعات لازم برای شناسایی سامانه؛

۴. خلاصه‌ای از ویژگی‌های اصلی طرح مربوط به آزمون در شرایط واقعی؛

۵. اطلاعات مربوط به تعلیق یا خاتمهٔ آزمون در شرایط واقعی.

پیوست دهم. اسناد تقنینی اتحادیهٔ اروپا دربارهٔ سامانه‌های فناوری اطلاعات در مقیاس بزرگ در حوزهٔ آزادی، امنیت و عدالت

۱. سامانهٔ اطلاعات شنگن[۱۹۸]

الف) قانون ۲۰۱۸/۱۸۶۰ پارلمان و شورای اروپا ۲۸ نوامبر ۲۰۱۸ دربارهٔ استفاده از سامانهٔ اطلاعات شنگن برای بازگرداندن اتباع کشورهای ثالثی که به‌طور غیرقانونی در اتحادیه اقامت دارند (روزنامهٔ رسمی ۳۱۲، ۲۰۱۸/۱۲/۷، ص ۱).

ب) قانون ۲۰۱۸/۱۸۶۱ پارلمان و شورای اروپا ۲۸ نوامبر ۲۰۱۸ دربارهٔ ایجاد، بهره‌برداری و استفاده از سامانهٔ اطلاعات شنگن در حوزهٔ کنترل مرزی و اصلاح کنوانسیون اجرای موافقت‌نامهٔ شنگن و اصلاح و لغو قانون شمارهٔ ۲۰۰۶/۱۹۸۷ (روزنامهٔ رسمی ۳۱۲، ۲۰۱۸/۱۲/۷، ص ۱۴).

ج) قانون ۲۰۱۸/۱۸۶۲ پارلمان و شورای اروپا ۲۸ نوامبر ۲۰۱۸ دربارهٔ ایجاد، بهره‌برداری و استفاده از سامانهٔ اطلاعات شنگن در حوزهٔ همکاری‌های پلیسی و قضایی در امور کیفری، اصلاح و لغو تصمیم شورای JHA/۵۳۳/۲۰۰۷ و لغو قانون شمارهٔ ۲۰۰۶/۱۹۸۶ پارلمان و شورای اروپا و تصمیم کمیسیون EU/۲۶۱/۲۰۱۰ (روزنامهٔ رسمی ۳۱۲، ۲۰۱۸/۱۲/۷، ص ۵۶).

۲. سامانهٔ اطلاعات ویزا[۱۹۹]

الف) قانون ۲۰۲۱/۱۱۳۳ پارلمان و شورای اروپا ۷ ژوئیهٔ ۲۰۲۱ دربارهٔ اصلاح مقررات شمارهٔ ۲۰۱۳/۶۰۳، ۲۰۱۶/۷۹۴، ۲۰۱۸/۱۸۶۲، ۲۰۱۹/۸۱۶ و ۲۰۱۹/۸۱۸ (اتحادیهٔ اروپا) در خصوص ایجاد شرایط دسترسی به سایر سامانه‌های اطلاعاتی اتحادیه برای مقاصد سامانهٔ اطلاعات ویزا (روزنامهٔ رسمی ۲۴۸، ۲۰۲۱/۷/۱۳، ص ۱).

ب) قانون ۲۰۲۱/۱۱۳۴ پارلمان و شورای اروپا ۷ ژوئیهٔ ۲۰۲۱ دربارهٔ اصلاح مقررات شمارهٔ ۲۰۰۸/۷۶۷ و ۲۰۰۹/۸۱۰(EC)، ۲۰۱۶/۳۹۹، ۲۰۱۷/۲۲۲۶، ۲۰۱۸/۱۲۴۰، ۲۰۱۸/۱۸۶۰، ۲۰۱۸/۱۸۶۱، ۲۰۱۹/۸۱۷ و ۲۰۱۹/۱۸۹۶ (اتحادیهٔ اروپا) پارلمان و شورای اروپا و لغو تصمیمات شورای

198. Schengen Information System - SIS
199. Visa Information System - VIS

EC/۵۱۲/۲۰۰۴ و JHA/۶۳۳/۲۰۰۸ برای اصلاح سامانهٔ اطلاعات ویزا (روزنامهٔ رسمی ۲۴۸، ۲۰۲۱/۷/۱۳، ص ۱۱).

۳. پایگاه دادهٔ اروپایی (یوروداک)[۲۰۰]

قانون ۲۰۲۴/۱۳۵۸ پارلمان و شورای اروپا ۱۴ مه ۲۰۲۴ دربارهٔ ایجاد *یوروداک* برای مقایسهٔ داده‌های زیست‌سنجی به منظور اجرای مؤثر مقررات ۲۰۲۴/۱۳۱۵ و ۲۰۲۴/۱۳۵۰ پارلمان و شورای اروپا و دستورالعمل شورای EC/۵۵/۲۰۰۱ و شناسایی اتباع کشورهای ثالث و افراد بی‌تابعیت که به‌طور غیرقانونی در اتحادیه اقامت دارند و نیز دربارهٔ درخواست‌های مقایسه با داده‌های یوروداک توسط مقامات مجری قانون کشورهای عضو و یوروپل برای اهداف اجرای قانون؛ اصلاح مقررات ۲۰۱۸/۱۲۴۰ و ۲۰۱۹/۸۱۸ پارلمان و شورای اروپا و لغو قانون شمارهٔ ۲۰۱۳/۶۰۳ پارلمان اروپا و شورا (روزنامهٔ رسمی ۲۰۲۱/۱۳۵۸، ۲۲.۵.۲۰۲۴، http://data.europa. eu/eli/reg/2024/1358/oj).

۴. سامانهٔ ورود/خروج[۲۰۱]

قانون ۲۰۱۷/۲۲۲۶ پارلمان و شورای اروپا ۳۰ نوامبر ۲۰۱۷ دربارهٔ ایجاد سامانهٔ ورود/خروج برای ثبت داده‌های ورود و خروج و داده‌های ورود اتباع کشورهای ثالثی که از مرزهای خارجی کشورهای عضو عبور می‌کنند و تعیین شرایط دسترسی به سامانهٔ ورود/خروج برای مقاصد اجرای قانون و اصلاح کنوانسیون اجرای موافقت‌نامهٔ شنگن و مقررات شمارهٔ ۲۰۰۸/۷۶۷ و شمارهٔ ۲۰۱۱/۱۰۷۷ (اتحادیهٔ اروپا) (روزنامهٔ رسمی ۳۲۷، ۲۰۱۷/۱۲/۹، ص ۲۰).

۵. سامانهٔ اطلاعات و مجوز سفر اروپا[۲۰۲]

الف) قانون ۲۰۱۸/۱۲۴۰ پارلمان و شورای اروپا ۱۲ سپتامبر ۲۰۱۸ دربارهٔ ایجاد سامانهٔ اطلاعات و مجوز سفر اروپا و اصلاح مقررات شمارهٔ ۲۰۱۱/۱۰۷۷، ۲۰۱۴/۵۱۵، ۲۰۱۶/۳۹۹، ۲۰۱۶/۱۶۲۴و ۲۰۱۷/۲۲۲۶ (اتحادیهٔ اروپا) (روزنامهٔ رسمی ۲۳۶، ۲۰۱۸/۹/۱۹، ص ۱).

ب) قانون ۲۰۱۸۱۲۴۱/۱۲۴۱ پارلمان و شورای اروپا ۱۲ سپتامبر ۲۰۱۸ دربارهٔ اصلاح قانون ۲۰۱۶/۷۹۴ (اتحادیهٔ اروپا) به منظور ایجاد سامانهٔ اطلاعات و مجوز سفر اروپا (روزنامهٔ رسمی ۲۳۶،

۲۰۰. سامانهٔ EURODAC، پایگاه دادهٔ اتحادیهٔ اروپا برای ثبت و مقایسهٔ اثر انگشت متقاضیان پناهندگی و برخی اتباع کشورهای ثالث است.

201. Entry/Exit System - EES

202. European Travel Information and Authorisation System

۲۰۱۸/۹/۱۹، ص ۷۲).

۶. سامانهٔ اطلاعات سوابق کیفری اروپا دربارهٔ اتباع کشورهای ثالث و افراد بی‌تابعیت[۲۰۳]

قانون ۲۰۱۹/۸۱۶ پارلمان و شورای اروپا ۱۷ آوریل ۲۰۱۹ دربارهٔ ایجاد سامانهٔ متمرکز برای شناسایی کشورهای عضو دارندهٔ اطلاعات محکومیت دربارهٔ اتباع کشورهای ثالث و افراد بی‌تابعیت به منظور تکمیل سامانهٔ اطلاعات سوابق کیفری اروپا و اصلاح قانون ۲۰۱۸/۱۷۲۶ (اتحادیهٔ اروپا) (روزنامهٔ رسمی ۱۳۵، ۲۰۱۹/۵/۲۲، ص ۱).

۷. همپوشانی و تعامل سامانه‌ها[۲۰۴]

الف) قانون ۲۰۱۹/۸۱۷ پارلمان و شورای اروپا ۲۰ مه ۲۰۱۹ دربارهٔ ایجاد چارچوبی برای همپوشانی و تعامل میان سامانه‌های اطلاعاتی اتحادیه در حوزهٔ مرزها و روادید و اصلاح مقررات شمارهٔ ۲۰۰۸/۷۶۷، ۲۰۱۶/۳۹۹، ۲۰۱۷/۲۲۲۶، ۲۰۱۸/۱۲۴۰، ۲۰۱۸/۱۷۲۶ و ۲۰۱۸/۱۸۶۱ (اتحادیهٔ اروپا) پارلمان و شورای اروپا و تصمیمات شورای EC/۵۱۲/۲۰۰۴ و JHA/۶۳۳/۲۰۰۸ (روزنامهٔ رسمی ۱۳۵، ۲۰۱۹/۵/۲۲، ص ۲۷).

ب) قانون ۲۰۱۹/۸۱۸ پارلمان و شورای اروپا ۲۰ مه ۲۰۱۹ دربارهٔ ایجاد چارچوبی برای همپوشانی و تعامل میان سامانه‌های اطلاعاتی اتحادیه در حوزهٔ همکاری‌های پلیسی و قضایی، پناهندگی و مهاجرت و اصلاح مقررات ۲۰۱۸/۱۷۲۶، ۲۰۱۸/۱۸۶۲ و ۲۰۱۹/۸۱۶ (اتحادیهٔ اروپا) (روزنامهٔ رسمی ۱۳۵، ۲۰۱۹/۵/۲۲، ص ۸۵).

پیوست یازدهم. مستندات فنی اشاره‌شده در ماده ۵۳(۱)(الف). مستندات فنی برای ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی

بخش یک. اطلاعاتی که باید توسط همهٔ ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی ارائه شود

مستندات فنی موضوع ماده ۵۳(۱)(الف) باید دست‌کم شامل اطلاعات زیر باشد، متناسب با اندازه و نمایهٔ ریسک مدل:

۱. یک توصیف کلی از مدل هوش مصنوعی عمومی، شامل:

203. European Criminal Records Information System on third-country nationals and stateless persons
204. Interoperability

الف) وظایفی که مدل برای انجام آن‌ها طراحی شده و نوع و ماهیت سامانه‌های هوش مصنوعی که می‌تواند در آن‌ها ادغام شود؛

ب) سیاست‌های استفادهٔ قابل قبول؛

ج) تاریخ انتشار و روش‌های توزیع؛

د) معماری و تعداد معیارها؛

هـ) شیوه (مانند متن، تصویر) و قالب ورودی‌ها و خروجی‌ها؛

و) مجوز.

۲. توصیف تفصیلی از عناصر مدل مذکور در بند ۱ و اطلاعات مربوط به فرآیند توسعه، شامل عناصر زیر:

الف) ابزارهای فنی مورد نیاز (مانند دستورالعمل‌های استفاده، زیرساخت‌ها، ابزارها) برای ادغام مدل هوش مصنوعی عمومی در سامانه‌های هوش مصنوعی؛

ب) مشخصات طراحی مدل و فرآیند آموزش، ازجمله روش‌ها و تکنیک‌های آموزشی، انتخاب‌های کلیدی طراحی همراه با منطق و فرضیات اتخاذشده؛ اینکه مدل برای چه چیزی بهینه‌سازی شده و ارتباط معیارهای مختلف در صورت اقتضا؛

پ) اطلاعات دربارهٔ داده‌های مورد استفاده برای آموزش، آزمون و اعتبارسنجی، در صورت اقتضا، ازجمله نوع و منشأ داده‌ها و روش‌های آماده‌سازی (مانند پاک‌سازی، فیلترگذاری و غیره)، تعداد نقاط داده، دامنه و ویژگی‌های اصلی آن‌ها؛ نحوهٔ به‌دست‌آوردن و انتخاب داده‌ها و سایر تدابیر برای تشخیص نامناسب‌بودن منابع داده و روش‌های شناسایی سوگیری‌های قابل تشخیص، در صورت اقتضا؛

ت) منابع محاسباتی مورد استفاده برای آموزش مدل (مانند تعداد عملیات ممیز شناور)، مدت‌زمان آموزش و سایر جزئیات مرتبط با فرآیند آموزش؛

ث) میزان شناخته‌شده یا برآوردی مصرف انرژی مدل.

در خصوص بند (ث)، هر گاه مصرف انرژی مدل ناشناخته باشد، می‌توان آن را بر مبنای اطلاعات مربوط به منابع محاسباتی مورد استفاده برآورد کرد.

بخش دو. اطلاعات تکمیلی که باید توسط ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی دارای خطر نظام‌مند ارائه شود

۱. توصیف تفصیلی راهبردهای ارزیابی، شامل نتایج ارزیابی، بر مبنای پروتکل‌ها و ابزارهای ارزیابی عمومی در دسترس یا در غیر این صورت، سایر روش‌های ارزیابی. راهبردهای ارزیابی باید شامل معیارهای ارزیابی، شاخص‌ها و روش‌شناسی شناسایی محدودیت‌ها باشد.

۲. در صورت اقتضا، توصیف تفصیلی تدابیر اتخاذشده برای انجام آزمون‌های دوطرفه داخلی و/یا خارجی (مانند ردتیمینگ)، سازگاری و تنظیم دقیق مدل.

۳. در صورت اقتضا، توصیف تفصیلی معماری سامانه، توضیح‌دهندهٔ نحوهٔ ساخت یا ارتباط اجزای نرم‌افزاری با یکدیگر و نحوهٔ ادغام آن‌ها در فرآیند کلی پردازش.

پیوست دوازدهم. اطلاعات شفافیت اشاره‌شده در ماده ۵۳(۱)(ب). مستندات فنی برای ارائه‌دهندگان مدل‌های هوش مصنوعی عمومی به ارائه‌دهندگان پایین‌دستی که مدل را در سامانهٔ هوش مصنوعی خود ادغام می‌کنند

اطلاعات موضوع ماده ۵۳(۱)(ب) باید دست‌کم شامل موارد زیر باشد:

۱. توصیف کلی از مدل هوش مصنوعی عمومی، شامل:

الف) وظایفی که مدل برای انجام آن‌ها طراحی شده و نوع و ماهیت سامانه‌های هوش مصنوعی که می‌تواند در آن‌ها ادغام شود؛

ب) سیاست‌های استفادهٔ قابل قبول؛

پ) تاریخ انتشار و روش‌های توزیع؛

ت) چگونگی تعامل مدل، یا امکان استفادهٔ آن برای تعامل، با سخت‌افزار یا نرم‌افزاری که بخشی از خود مدل نیست، در صورت اقتضا؛

ث) نسخه‌های نرم‌افزار مرتبط با استفاده از مدل هوش مصنوعی عمومی، در صورت اقتضا؛

ج) معماری و تعداد معیارها؛

چ) شیوه (مانند متن، تصویر) و قالب ورودی‌ها و خروجی‌ها؛

ح) مجوز مدل.

۲. توصیف عناصر مدل و فرآیند توسعهٔ آن، شامل:

الف) ابزارهای فنی مورد نیاز (مانند دستورالعمل‌های استفاده، زیرساخت‌ها، ابزارها) برای ادغام مدل هوش مصنوعی عمومی در سامانه‌های هوش مصنوعی؛

ب) شیوه (مانند متن، تصویر و غیره) و قالب ورودی‌ها و خروجی‌ها و حداکثر اندازهٔ آن‌ها (مانند طول پنجره متنی و غیره)؛

ج) اطلاعات دربارهٔ داده‌های مورد استفاده برای آموزش، آزمون و اعتبارسنجی، در صورت اقتضا، ازجمله نوع و منشأ داده‌ها و روش‌های آماده‌سازی.

پیوست سیزدهم. معیارهای تعیین مدل‌های هوش مصنوعی عمومی دارای خطر نظام‌مند موضوع ماده ۵۱

به منظور تعیین اینکه یک مدل هوش مصنوعی عمومی دارای توانایی‌ها یا تأثیری معادل موارد مذکور در ماده ۵۱(۱)(الف) است، کمیسیون معیارهای زیر را مدنظر قرار خواهد داد:

الف) تعداد معیارهای مدل؛

ب) کیفیت یا اندازهٔ مجموعهٔ داده، برای نمونه اندازه‌گیری‌شده از طریق تعداد نشانه‌ها؛

پ) میزان محاسبات مورد استفاده برای آموزش مدل، اندازه‌گیری‌شده بر حسب عملیات ممیز شناور یا برآوردشده با ترکیبی از متغیرهای دیگر مانند هزینهٔ برآوردی آموزش، زمان برآوردی لازم برای آموزش یا مصرف انرژی برآوردی برای آموزش؛

ت) شیوه‌های ورودی و خروجی مدل، مانند متن به متن (مدل‌های زبانی بزرگ)، متن به تصویر، چندوجهی و آستانه‌های وضعیت پیشرفته برای تعیین توانایی‌های با تأثیر بالا برای هر شیوه، و نوع خاصی از ورودی‌ها و خروجی‌ها (مانند توالی‌های زیستی)؛

ث) آزمون‌های مرجع و ارزیابی توانایی‌های مدل، ازجمله با درنظرگرفتن تعداد وظایفی که بدون آموزش اضافی انجام می‌دهد، قابلیت سازگاری برای یادگیری وظایف جدید و متمایز، سطح خودمختاری و مقیاس‌پذیری و ابزارهایی که در دسترس دارد؛

ج) اینکه آیا به دلیل دامنهٔ استفاده، اثرگذاری بالایی بر بازار داخلی دارد، که در صورتی مفروض خواهد بود که برای دست‌کم ۱۰.۰۰۰ کاربر تجاری ثبت‌شده مستقر در اتحادیه در دسترس قرار گرفته باشد؛

چ) تعداد کاربران نهایی ثبت‌شده.