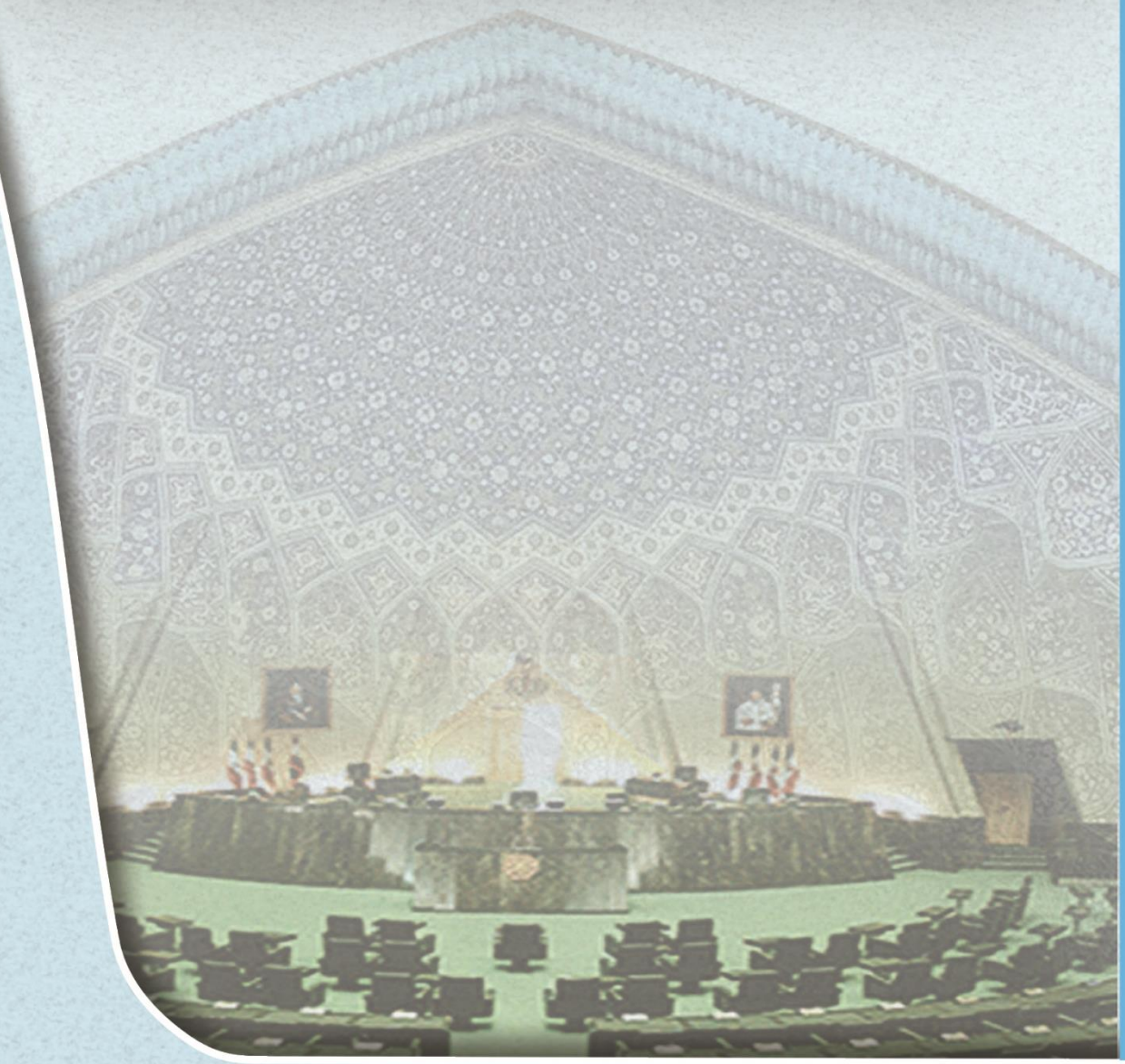
جمهوری اسلامی ایران
مجلس شورای اسلامی
مرکز تحقیقات اسلامی

ترجمه پیش‌نویس قانون
هوش مصنوعی اتحادیه اروپا



مرکز تحقیقات اسلامی
گروه تولیدی و زیربنایی

مرکز تحقیقات اسلامی مجلس شورای اسلامی
گروه تولیدی و زیربنایی

عنوان گزارش:

ترجمه پیش‌نویس قانون
هوش مصنوعی اتحادیه اروپا

شماره ثبت در مرکز:

۰۲/-/۵۸-۶۱۲

تاریخ انتشار:

زمستان ۱۴۰۲

نویسندگان:

حجت‌الاسلام احمد شجاعی‌فر

حجت‌الاسلام یوسف خرم‌پناه

ناظر علمی:

حجت الاسلام دکتر مهدی صمدی

ترجمه پیش‌نویس قانون
هوش مصنوعی اتحادیه اروپا

مرکز تحقیقات اسلامی مجلس شورای اسلامی
گروه تولیدی و زیربنایی

فهرست

خلاصه مدیریتی

متن پیشنهادی کمیسیون اتحادیه اروپا برای قانون‌گذاری در حوزه هوش مصنوعی، پس از چند سال تلاش و مشورت سرانجام در تاریخ ۱ اردیبهشت ۱۴۰۰ (مصادف با ۲۱ آوریل ۲۰۲۱) منتشر شد. این متن دارای ۱۲ بخش و ۸۵ ماده بوده و جامع‌ترین متن قانونی در مورد هوش مصنوعی به‌شمار می‌رود. اگرچه این متن هنوز به تصویب نهایی نرسیده است اما مطالعه آن برای قانون‌گذاران سایر کشورها می‌تواند موجب آشنایی با مشکلات و مسائل مهم در این حوزه گردد. در ادامه گزارش کوتاهی از محتوای این پیش‌نویس را ملاحظه می‌کنید:

بخش ۱ ــ موضوع، محدوده و تعاریف

طبق ماده ۱ هدف این قانون ایجاد قواعدی هماهنگ برای تولید و استفاده از محصولات و خدمات مرتبط با هوش مصنوعی در اتحادیه اروپا است. در همین راستا برخی کاربردها به کلی ممنوع می‌شوند، سیستم‌های هوش مصنوعی پرخطر به‌شدت کنترل می‌شوند و سایر سیستم‌های هوشمند، به عملکرد شفاف در چهارچوب تعیین‌شده متعهد می‌گردند.

طبق ماده ۲ این قانون برای همهٔ توسعه‌دهندگانی که محصولاتشان در اتحادیه اروپا استفاده می‌شود ـ حتی شرکت‌های خارجی ـ لازم‌الاجرا خواهد بود. مخاطب بعدی کاربران داخل کشورهای اتحادیه اروپا هستند. حتی اگر توسعه‌دهنده و کاربر خارجی باشد ولی خروجی سیستم در داخل اتحادیه استفاده شود، باید از قوانین پیروی کند. در انتها برخی سیستم‌های نظامی و مقامات دولتی از این قانون استثنا شده‌اند.

در ماده ۳ تعریف ۴۴ کلیدواژه اصلی بیان شده است که مهم‌ترین آنها همان «سیستم هوش مصنوعی» است. با توجه به پیشرفت سریع تکنولوژی و به‌جهت رعایت اصل بی‌طرفی نسبت به فناوری و سازگاری قانون با تغییرات آینده، این ماده با پیوست ۱ تکمیل شده است. پیوست ۱ شامل فهرستی از رویکردها و تکنیک‌های توسعه هوش مصنوعی است که توسط کمیسیون اروپا تصویب و به‌روزرسانی می‌شود.

در ماده ۴ به‌جهت ضرورت همگام بودن با پیشرفت‌ها، مجوز به روزرسانی پیوست ۱ توسط خود کمیسیون یا به نحو واسپاری صادر شده است.

بخش ۲ ــ کاربردهای ممنوعه هوش مصنوعی

این قانون از رویکرد مبتنی بر ریسک پیروی می‌کند و بین استفاده‌هایی از هوش مصنوعی با ریسک غیرقابل‌قبول، با ریسک بالا، و با ریسک کم یا حداقلی، تفاوت قائل می‌شود. همهٔ کاربردهای ممنوعه ذکرشده در این بخش، مواردی هستند که به‌دلیل نقض ارزش‌های اتحادیه اروپا (مانند حقوق اساسی افراد)، استفاده از آنها موجب ایجاد ریسک غیرقابل‌قبول می‌شود.

طبق ماده ۵ به‌طورکلی استفاده از هوش مصنوعی برای تغییر رفتار انسان‌ها بدون اطلاع آنان با تکنیک‌های نامحسوس یا با استفاده از آسیب‌پذیری خاص افراد (مانند سن، ناتوانی جسمی یا ذهنی و ...) به‌نحوی‌که موجب آسیب جسمی یا روحی بشود یا حتی امکان چنین آسیبی وجود داشته باشد، ممنوع است.

همچنین استفاده از هوش مصنوعی توسط دولت یا نماینده‌اش برای طبقه‌بندی افراد براساس امتیاز اجتماعی آنها (از طریق اطلاعات رفتار یا ویژگی‌های شخصی و شخصیتی) درصورتی‌که منجر به برخورد زیان‌بار یا نامناسب با افراد شود، ممنوع است. ممنوعیت آخر برای استفاده از سیستم‌های شناسایی زیست‌سنجی از راه دور بی‌درنگ در مکان‌های عمومی است که البته استثناها و تبصره‌هایی برای آن بیان شده است.

بخش ۳ ــ سیستم‌های هوش مصنوعی پرخطر

بخش ۳ در مورد سیستم‌های هوش مصنوعی پرخطر است و از لحاظ تعداد فصل‌ها (۵ فصل) و مواد قانونی (۴۶ ماده) بزرگ‌ترین بخش قانون پیشنهادی به‌شمار می‌رود. سیستم‌های پرخطر براساس اهداف و کارکردهای مورد انتظارشان، مطابق با قوانین ایمنی محصول شناسایی می‌شوند. آنها باید از الزامات خاصی پیروی کنند و ارزیابی‌های پیشینی انطباق با استانداردها را پشت سر بگذارند.

فصل ۱ (مواد ۶ و ۷) دو دسته کلی از سیستم‌های پرخطر را معرفی می‌کند: ۱. سیستم‌های هوش مصنوعی که قرار است به‌عنوان جزء ایمنی یک محصول به‌کار گرفته شوند و طبق قانون ملزم به اجرای انطباق‌سنجی با استانداردها توسط شخص ثالث می‌شوند. جزء ایمنی یعنی عملکرد ایمنی آن محصول یا سیستم را برعهده دارد یا اینکه خرابی و عملکرد نادرست آن جزء، سلامت و ایمنی افراد یا دارایی‌ها را به خطر می‌اندازد. ۲. سایر سیستم‌های هوش مصنوعی مستقل که با مفاهیم حقوق اساسی که به‌صراحت در پیوست ۳ فهرست شده‌اند، مغایرت دارد.

پیوست ۳ شامل فهرستی از سیستم‌های هوش مصنوعی پرخطر است که خطرات آنها قبلاً تحقق یافته است یا در آینده نزدیک تحقق می‌یابد. این فهرست ۲۱ مورد از سیستم‌های پرخطر را در قالب ۸ دسته موضوعی تنظیم کرده است. برای اطمینان از پشتیبانی نسبت به فناوری‌های نوظهور و موارد پیش‌بینی‌نشده، کمیسیون می‌تواند براساس برخی معیارها و روش‌های ارزیابی ریسک، پیوست ۳ را گسترش دهد.

فصل ۲ (مواد ۸ تا ۱۵) الزامات قانونی را برای سیستم‌های هوش مصنوعی پرخطر در رابطه با داده‌ها و حاکمیت داده‌ها، مستندسازی و نگهداری اسناد، شفافیت و ارائه اطلاعات به کاربران، نظارت انسانی، استحکام، دقت و امنیت بیان می‌کند.

این فصل، یک سیستم مدیریت خطر برای پایش دائمی چرخه حیات سیستم‌های پرخطر و مدیریت و اطلاع‌رسانی خطرات مربوطه ایجاد می‌کند تا سیستم‌ها همواره در راستای اهداف خود عمل کنند و در این زمینه مورد آزمایش قرار گیرند. در ادامه معیارهای کیفی دقیقی برای داده‌های مورد استفاده مدل‌ها تعیین می‌شود و توسعه‌دهندگان ملزم به رعایت قوانین مربوط به حاکمیت داده‌ها می‌گردند.

آنها باید برای محصول خود مستندات فنی استاندارد (مطابق با پیوست ۴) تهیه کنند و قبل از عرضه در بازار به نهادهای مربوطه ارائه کنند. توسعه‌دهندگان باید به‌طور خودکار، گزارش رویدادهای سیستم را ـ خصوصاً ناظر به خطرهای احتمالی ـ تهیه کنند تا بعداً قابل‌بررسی باشد.

یک محصول هوش مصنوعی باید عملکرد شفاف و قابل‌تفسیر داشته باشد و به همراه راهنمای کاربری به بازار عرضه شود. این محصولات باید به‌طور مؤثری قابلیت نظارت انسانی در فرایندهای خود را فراهم کنند و به‌طور پایدار دارای دقت، استحکام و امنیت سایبری باشند.

الزامات پیشنهادی در این بخش، نتیجه دو سال کار آماده‌سازی مبتنی بر «دستورالعمل‌های اخلاقی برای هوش مصنوعی قابل‌اعتماد» می‌باشد. سند مذکور توسط گروه متخصصان سطح بالا در هوش مصنوعی[1] تهیه شده است. این الزامات حداقلی توسط بیش از ۳۵۰ سازمان به‌صورت آزمایشی اجرا شده است.

فصل ۳ (مواد ۱۶ تا ۲۹) مجموعه‌ای واضح از تعهدات هم‌عرض را برای ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر قرار می‌دهد. همچنین تعهدات متناسبی بر دوش کاربران و سایر نقش‌آفرینان در سراسر زنجیره ارزش هوش مصنوعی (به‌عنوان مثال: واردکنندگان، توزیع‌کنندگان، نمایندگان مجاز) اعمال می‌شود.

ارائه‌کننده باید از رعایت همهٔ الزامات این بخش اطمینان حاصل کند، مستندات فنی را تدوین کند، در مواقع لزوم اقدامات فوری و اصلاحی انجام دهد و به اطلاع مسئولان برساند. او باید یک سیستم مدیریت کیفیت با استانداردهای دوازده‌گانه ایجاد کند و پس از دریافت مجوز و نشان انطباق، آن را منتشر کند. همچنین گزارش‌های خودکار رویدادها باید توسط او برای مدت کافی نگهداری شوند.

ارائه‌دهندگان خارجی باید نماینده مجاز با وکالت‌نامه کتبی معرفی کنند. واردکننده باید مطئمن شود که ارائه‌دهنده همهٔ وظایفش را نسبت به محصول انجام داده است. او باید اطلاعات دقیق شرکت خود را به‌طور عمومی منتشر کند و مدارک لازم را به مقامات مسئول ارائه دهد. توزیع‌کننده نیز باید صحت همهٔ موارد قبل را جویا شود و نشان انطباق و مدارک لازم را در اختیار قرار دهد. کاربران نهایی محصول باید مطابق با دستورالعمل‌ها، از سیستم‌های پرخطر استفاده کند و اگر احتمال بروز خطر وجود داشت استفاده را متوقف کرده و مراتب را به مقامات مربوطه اطلاع دهد. او باید حتی‌الامکان گزارش رویدادها را نگهداری نماید.

1. HLEG

فصل ۴ (مواد ۳۰ تا ۳۹) در مورد فرایندهای اجرایی دریافت مجوز برای سیستم‌های هوش مصنوعی پرخطر است. به طور کلی در اتحادیه اروپا، فرآیند مشخصی برای دریافت گواهی انطباق با استانداردها[1] برای محصولات وجود دارد. در این بخش همان فرایند برای سیستم‌های پرخطر اجرا شده است. ارزیابی انطباق محصولات با استانداردهای قانونی، گاهی توسط سازنده انجام می‌شود، گاهی در تعامل با مشتری صورت می‌گیرد و گاهی نیازمند تأیید شخص ثالث است. به شرکت‌ها و مراکزی که این خدمت را انجام می‌دهند «نهاد انطباق‌سنجی» می‌گویند. شرکت‌های زیادی وجود دارند که چنین خدماتی را عرضه می‌کنند و تولیدکننده حق انتخاب دارد اما همهٔ آنها مورد تأیید رسمی نیستند.

یک مقام و مرجع رسمی در هر کشور عضو اتحادیه، مسئولیت ارزیابی و گزینش و پایش نهادهای انطباق‌سنجی را به عهده دارد و به آنها مجوز انطباق‌سنجی می‌دهد. به آن نهاد رسمی که گزینش می‌کند «مرجع صدور مجوز» و به نهاد انطباق‌سنجی پس از گزینش، «نهاد دارای مجوز» می‌گویند.

فصل ۵ (مواد ۴۰ تا ۵۱) در مورد استانداردها و فرایند انطباق‌سنجی است. در اتحادیه اروپا استانداردهای هماهنگ‌شده‌ای وجود دارد که اگر سیستم پرخطر با آنها مطابق داشته باشد، تا حدودی نسبت به الزامات این قانون کفایت می‌کند. البته در این حالت باید از روش‌های خاص موجود در پیوست ۶ (مبتنی بر کنترل داخلی) یا پیوست ۷ (مبتنی بر ارزیابی سیستم مدیریت کیفیت و مستندات فنی) استفاده کند. اصولاً نوع روش معتبر برای انطباق‌سنجی، براساس دسته‌بندی موجود در پیوست ۳ انجام می‌شود. ایجاد تغییرات اساسی در سیستم‌ها موجب نیاز به انطباق‌سنجی مجدد می‌شود. در پایان انطباق‌سنجی، نهادهای دارای مجوز به شرکت‌های هوش مصنوعی گواهینامه رسمی با اعتبار کمتر از ۵ سال می‌دهند و سپس مرجع صدور مجوز و سایر نهادها را مطلع می‌کنند. گاهی مرجع نظارت بر بازار هم می‌تواند مجوزهایی صادر کند. اگر تا ۱۵ روز اعتراضی به آن مجوزها نشود، موجه تلقی می‌شوند. پس از همهٔ این مراحل، ارائه‌دهنده باید اعلامیه انطباق را تنظیم کند و نشان انطباق را نصب نماید و همهٔ مدارک و سوابق را تا ۱۰ سال نگهداری کند.

1. CE

بخش ۴ – تعهدات شفافیت

بخش ۴ (ماده ۵۲) به سیستم‌های هوش مصنوعی خاص مربوط می‌شود. مانند سیستم‌هایی که: ۱. با انسان‌ها تعامل دارند. ۲. برای شناسایی احساسات یا تعیین ارتباط با مقوله‌های اجتماعی براساس داده‌های بیومتریک استفاده می‌شوند. ۳. برای تولید یا دستکاری محتوا (جعل عمیق) استفاده می‌شوند. این سیستم‌ها باید به‌طور شفاف کاربر را مطلع سازند که در حال تعامل با یک عامل غیرانسانی و هوشمند است؛ خصوصاً اگر محتوایی شبیه محتوای واقعی تولید شود، باید دارای برچسب افشاکننده باشد.[1]

بخش ۵ ــ حمایت از نوآوری

بخش ۵ (مواد ۵۳ تا ۵۵) در مورد روش‌های حمایت از نوآوری در توسعه سیستم‌های هوشمند است. راه‌حل کمیسیون، ایجادهای محیط‌های آزمایشی و ایمن (به اصطلاح سندباکس) است که سیستم‌های هوشمند قبل از عرضه به بازار، درون آنها راه‌اندازی شوند. این ایده با هدف ایجاد یک چارچوب قانونی که نوآوری‌پسند، مقاوم در برابر آینده و مقاوم در برابر اختلال، اجرا می‌شود. محیط‌های مذکور توسط مقامات کشورهای عضو ایجاد می‌شوند و برای آزمایش سیستم‌های هوشمند قبل از انتشار عمومی مفید خواهند بود. درصورتی‌که این سیستم‌ها دارای اهداف مشخص عام‌المنفعه و نوآورانه باشند، اجازه دارند تحت شرایط کنترل‌شده، به جمع‌آوری و استفاده از داده‌های شخصی افراد بپردازند. این بخش همچنین شامل اقداماتی برای کاهش بار نظارتی بر شرکت‌های نوپا، کوچک و متوسط می‌باشد.

بخش ۶ ــ حاکمیت

بخش ۶ (مواد ۵۶ تا ۵۹) طی دو فصل به موضوع سیستم‌های حکمرانی در سطح اتحادیه اروپا و کشورهای عضو پرداخته است. در فصل اول کمیسیون اقدام به تأسیس یک بازوی کمکی به نام «هیئت اروپایی هوش مصنوعی» می‌کند و شرح وظایفش را معیّن می‌کند تا او را در انجام وظایف و هماهنگی بین کشورها و اجرای قانون یاری نماید. در فصل دوم نیز مراجع ذی‌صلاح کشورها که باید متولی اصلی اجرای قانون، نظارت بر آن و ارتباط با کمیسیون باشند، تعیین شده و ضوابط آن بیان می‌گردد.

بخش ۷ ــ پایگاه داده نظارتی

بخش ۷ (ماده ۶۰) به‌دنبال تسهیل نظارت کمیسیون و مقامات ملی، از طریق ایجاد یک پایگاه داده سراسری برای سیستم‌های پرخطر است. این پایگاه داده توسط کمیسیون اداره می‌شود و توسط داده‌های ارائه‌دهندگان سیستم‌های هوش مصنوعی پر می‌شود. آنها باید سیستم‌های خود را قبل از عرضه در بازار یا به‌کارگیری آنها، در این پایگاه داده ثبت کنند.

بخش ۸ ــ رصد پس از فروش و نظارت بر بازار

بخش ۸ (مواد ۶۱ تا ۶۸) دارای سه فصل است. در فصل اول به رصد و نظارت پس از فروش محصولات هوشمند می‌پردازد و ارائه‌دهندگان را ملزم می‌کند تا یک سیستم نظارتی دائمی برای اطمینان از رعایت الزامات این قانون ایجاد کرده و داده‌های استفاده را ذخیره نمایند. این سیستم‌های نظارتی باید براساس یک طرح جامع نظارتی شکل بگیرند و برای سیستم‌های پرخطر شدیدتر باشد.

در فصل دوم ارائه‌دهندگان را ملزم به اطلاع‌رسانی سریع اشکالات و به اشتراک‌گذاری اطلاعات مربوطه می‌کند. این شرکت‌ها باید به‌محض اطلاع از بروز اختلال در سیستم یا حتی احتمال تعدی از الزامات این قانون، آن را به مقامات نظارتی ملی گزارش دهند تا از نقض حقوق بنیادین انسان‌ها جلوگیری شود.

فصل سوم به‌طور مفصل به نحوه اجرای نظارت بر بازار می‌پردازد. در ابتدا این نظارت اقتصادی است یعنی شرکت‌های ارائه‌دهنده باید قوانین رقابت اقتصادی را رعایت کنند و مقام ناظر ملی باید آنها را تحت نظر داشته باشد. این مقام ناظر باید دسترسی کاملی به داده‌های سیستم هوش مصنوعی ـ و حتی در صورت لزوم دسترسی به کد منبع ـ داشته باشد و هر سند درخواستی به او تحویل داده شود.

اگر یک سیستم هوشمند دارای خطری در سطح ملی باشد، نظارت شدیدتری اعمال خواهد شد و حتی در مواقعی منجر به جمع‌آوری محصول از بازار یا از بین بردن آن می‌شود. مقام ناظر باید اقدامات اصلاحی متناسب را اتخاذ کند. درصورتی‌که مخاطرات فراملی باشد، نیازمند همکاری در چهارچوب مشخص‌شده بین کمیسیون و کشورها خواهد بود. حتی طبق ماده ۶۷ اگر یک سیستم هوشمند الزامات این قانون را رعایت کرده باشد، ولی خطرناک تشخیص داده شود، باید از هر طریقی اطمینان مقامات مسئول را نسبت به استفاده امن جلب نماید؛ وگرنه اجازه توزیع نخواهد داشت. در پایان برای شرکت‌هایی که از نشان انطباق جعلی یا نادرست استفاده می‌کنند، قواعدی تعیین شده است.[1]

بخش ۹ ــ آیین‌نامه رفتاری

بخش ۹ (ماده ۶۹) به قواعد محدود رفتاری ـ و نه اخلاقی ـ می‌پردازد. منظور این است که محصولاتی که پرخطر تلقی نمی‌شوند به‌صورت داوطلبانه، الزامات خاص این قانون ـ که برای سیستم‌های پرخطر بود ـ را بپذیرند و اجرا کنند. این آیین‌نامه‌ها می‌تواند توسط ارائه‌دهندگان یا سازمان‌های خاص تدوین شود و قوانین داوطلبانه مفید را شامل شود. کمیسیون و کشورهای عضو، نقش تسهیل‌گری در این موضوع خواهند داشت (تأکید می‌شود که این بخش ربطی به مسئله اخلاق در هوش مصنوعی ندارد).

بخش ۱۰ ــ محرمانگی و مجازات

بخش ۱۰ (مواد ۷۰ تا ۷۲) ناظر به محرمانگی اطلاعات تبادل‌شده در فرایند انطباق‌سنجی، اجرا، نظارت و ... است و الزاماتی را مطرح می‌کند که همهٔ طرف‌های نقش‌آفرین در این فرایندها باید آنها را رعایت نمایند. در ادامه به توصیف جرایم مالی نقض این مقررات می‌پردازد و علاوه‌بر مشخص کردن مقدار جرایم (تا حدود ۳۰ میلیون یورو یا بیشتر)، کشورهای عضور را موظف به وضع قوانین و جریمه‌های اداری متناسب می‌کند. همهٔ این اقدامات و جرایم در راستای تضمین اجرای مؤثر مقررات صورت می‌پذیرد.

بخش ۱۱ ــ تفویض اختیارات

بخش ۱۱ (مواد ۷۳ و ۷۴) به کمیسیون این امکان را می‌دهد تا در راستای انجام بهتر وظایف و رعایت هماهنگی در اجرای یکسان مقررات، بخشی از اختیاراتش را تفویض کند؛ مانند به‌روزرسانی یا تکمیل فهرست‌های موجود در پیوست‌های ۱ تا ۷. مصوبات تفویضی در صورت عدم اعتراض پارلمان و شورا، لازم‌الاجرا خواهند بود. همچنین یک کمیته کمکی هم برای کمیسیون تأسیس می‌شود.

بخش ۱۲ ــ اصلاح قوانین مرتبط و نکات پایانی

بخش ۱۲ (مواد ۷۴ تا ۸۵) ابتدا طی ۸ ماده، قوانین مرتبط به حوزه این قانون را اصلاح می‌کند تا هماهنگی بیشتری بین قوانین ایجاد شود. در ادامه، عدم شمول این قانون نسبت به سیستم‌های هوشمند گذشته را توضیح می‌دهد و سپس تکلیف به‌روزرسانی‌های منظم را برای کمیسیون ضروری می‌داند و در ماده پایانی، روند لازم‌الاجرا شدن این قانون را بیان می‌کند.

مقدمه

نهادهای اصلی اتحادیه اروپا[1] عبارتند از:

۱- کمیسیون اروپایی[2]

۲- پارلمان اروپایی[3]

۳- شورای اروپایی[4]

۴- شورای اتحادیه اروپایی[5]

مشابه: شورای اروپا[6]

1. European Union: EU
2. European Commission: EC
3. European Parliament: EP
4. European Council: EUCO
5. Council of the European Union: The Council
6. Council of Europe: CoE

۵- دیوان دادگستری اتحادیه اروپایی[1]

مشابه: دیوان دادگستری اروپایی[2]

مشابه: دیوان حقوق بشر اروپایی[3]

۶- بانک مرکزی اروپایی[4]

۷- دادگاه اروپایی حسابرسان[5]

سیر تلاش‌های اتحادیه اروپا برای قانون‌گذاری در مورد هوش مصنوعی بدین شرح است:

۱- در تاریخ ۳۰ بهمن ۱۳۹۸ کمیسیون اروپایی[6] سپیدنامه هوش مصنوعی را منتشر کرد.

۲- در تاریخ ۲۰ شهریور ۱۳۹۹ (۱۰ سپتامبر ۲۰۲۰) بازه زمانی مربوط به ارزیابی تأثیر اولیه[7] به پایان رسید. این بازه از ۲ مرداد (۲۳ جولای ۲۰۲۰) شروع شده بود. در این مدت حدود ۱۳۳ بازخورد جمع‌آوری شد.

۳- در تاریخ ۱ اردیبهشت ۱۴۰۰ (۲۱ آوریل ۲۰۲۱) کمیسیون اروپایی یک متن پیشنهادی برای قانون‌گذاری در زمینه هوش مصنوعی منتشر کرد. عنوان دقیق این سند «پیشنهاد برای مقررات پارلمان اروپا و شورای اروپا؛ تعیین قوانین هماهنگ در مورد هوش مصنوعی (قانون هوش مصنوعی) و اصلاح برخی از قوانین اتحادیه» قرار داده شد. این سند در حکم لایحه‌ای است که بخش اجرایی اتحادیه اروپا پیشنهاد کرده است تا نهادهای قانون‌گذاری آن را بررسی کنند.

۴- در تاریخ ۲۹ تیر ۱۴۰۰ (۲۰ جولای ۲۰۲۱) ریاست اسلوونیایی شورای اتحادیه اروپایی[8] یک گردهمایی مجازی با موضوع «تنظیم‌گری هوش مصنوعی؛ اصول اخلاقی و حقوق بنیادی» برگزار کرد.

۵- در تاریخ ۱۵ مرداد ۱۴۰۰ (۶ آگوست ۲۰۲۱) بازه زمانی مربوط به مشاوره عمومی[9] به اتمام رسید. این دوره ۴ روز پس از انتشار متن پیشنهادی شروع شده بود. در مجموع ۳۰۴ بازخورد توسط کمیسیون دریافت شد.

1. Court of Justice of the European Union: The Court
2. European Court of Justice
3. European Court of Human Rights
4. European Central Bank: ECB
5. European Court of Auditors - ECA
6. European Commission
7. Inception impact assessment
8. The Council
9. public consultation

از سوی دیگر به درخواست کمیته دادخواست‌ها[1] و کمیته امور قانونی[2] از زیرمجموعه‌های پارلمان اروپا، مطالعه‌ای با عنوان «شناسایی زیست‌سنجی و تشخیص رفتاری، ارزیابی جنبه‌های اخلاقی» توسط اداره حقوق شهروندی و امور قانون اساسی انجام گرفت که نتیجه آن در همین روز منتشر شد.

۶- در تاریخ ۸ آذر ۱۴۰۰ (۲۹ نوامبر ۲۰۲۱) ریاست اسلوونیایی شورای اتحادیه اروپایی اصلاحیه اساسی و مفصلی را بر متن پیشنهادی منتشر کرد که بیشتر متمرکز بر اعتبار اجتماعی، شناسایی زیست‌سنجی و کاربردهای پرخطر بود.

۷- در تاریخ ۵ بهمن ۱۴۰۰ (۲۵ ژانویه ۲۰۲۲) کمیته‌های «بازار داخلی و حمایت از مصرف‌کننده»[3] و «آزادی‌های مدنی، عدالت و امور داخلی»[4] از زیرمجموعه‌های پارلمان اروپا، گفتگوی مشترکی روی متن پیشنهادی داشتند و این‌گونه کارهای پارلمانی آغاز شد.

۸- در تاریخ ۱۴ بهمن ۱۴۰۰ (۳ فوریه ۲۰۲۲) ریاست فرانسوی شورای اتحادیه اروپایی یک متن اصلاحی راجع‌به مواد ۱۶ تا ۲۹ منتشر کرد. همچنین او پس از مدتی متن اصلاحی دوم را ناظر به مواد ۴۰ تا ۵۲ منتشر کرد.

۹- در تاریخ ۱۱ اسفند ۱۴۰۰ (۲ مارس ۲۰۲۲) کمیته امور قانونی از زیرمجموعه‌های پارلمان اروپا، یک متن اصلاحی جدید منتشر کرد و روز بعد هم کمیته صنعت، تحقیقات و انرژی[5] اظهارنظر اصلاحی خود را منتشر کرد.

۱۰- در تاریخ ۳۱ فروردین ۱۴۰۱ (۲۰ آوریل ۲۰۲۲) کمیته‌های «بازار داخلی و حمایت از مصرف‌کننده» و «آزادی‌های مدنی، عدالت و امور داخلی» نتایج گفتگوهای خود را در قالب یک متن اصلاحی منتشر کردند.

۱۱- در تاریخ ۲۳ اردیبهشت ۱۴۰۱ (۱۳ می۲۰۲۲) ریاست فرانسوی شورای اتحادیه اروپایی یک متن اصلاحی جدید راجع‌به ماده ۴ بخش اول منتشر کرد.

۱۲- در تاریخ ۱۱ خرداد ۱۴۰۱ (۱ ژوئن ۲۰۲۲) مهلت گروه‌های سیاسی در پارلمان اروپا برای ارائه اصلاحیه بر متن پیشنهادی کمیسیون به اتمام رسید. تا این زمان هزاران اصلاحیه برای متن پیشنهادی به کمیسیون ارسال شد.

۱۳- در تاریخ ۲۵ خرداد ۱۴۰۱ (۱۵ ژوئن ۲۰۲۲) ریاست فرانسوی شورای اتحادیه اروپایی آخرین اصلاحیه خود را قبل از تغییر ریاست منتشر کرد.

---

1. PETI
2. JURI
3. IMCO
4. LIBE
5. ITRE

۱۴- در تاریخ ۲۷ خرداد ۱۴۰۱ (۱۷ ژوئن ۲۰۲۲) ریاست جدید شورای اتحادیه اروپایی که به دست کشور چک بود، اولویت‌های خود را برای قانون‌گذاری در مورد هوش مصنوعی به کشورهای عضو اتحادیه اروپا ارسال کرد.

۱۵- در تاریخ ۱۴ شهریور ۱۴۰۱ (۵ سپتامبر ۲۰۲۲) کمیته امور قانونی به‌عنوان آخرین کمیته در پارلمان اروپا، نظرات خود را نسبت به متن کمیسیون به تصویب رساند.

۱۶- در تاریخ ۶ مهر ۱۴۰۱ (۲۸ سپتامبر ۲۰۲۲) کمیسیون اروپایی یک هماهنگ‌سازی هدفمند را برای قوانین مسئولیت ملی در مورد هوش مصنوعی پیشنهاد کرد. این دستورالعمل، دریافت غرامت برای قربانیان آسیب‌های مرتبط با هوش مصنوعی را آسان‌تر می‌کرد.

۱۷- در تاریخ ۱۵ آذر ۱۴۰۱ (۶ دسامبر ۲۰۲۲) کمیسیون اروپایی نسخه جدیدی و کامل‌تری از متن پیشنهادی را تحت عنوان «رویکرد کلی»[1] منتشر کرد و آماده مذاکره با پارلمان شد.

۱۸- در تاریخ ۲۴ خرداد ۱۴۰۲ (۱۴ ژوئن ۲۰۲۳) پارلمان اروپایی[2] نیز ۷۷۱ اصلاحیه را نسبت به متن پیشنهادی تصویب کرد و برای مذاکره با کمیسیون آماده شد.

۱۹- در تاریخ ۱۸ آذر ۱۴۰۲ (۹ دسامبر ۲۰۲۳) نمایندگان پارلمان اروپایی و شورای اروپایی به یک توافق سیاسی و موقت رسیدند.

1. general approach
2. European Parliament

بخش اول: تمهیدات عمومی

ماده ۱: موضوع اصلی

این مقررات موارد زیر را مطرح می‌کند:

(الف) قواعدی هماهنگ برای عرضه به بازار، ارائه خدمت و استفاده از سیستم‌های هوش مصنوعی در اتحادیه اروپا؛

(ب) ممنوعیت برخی از کاربردهای هوش مصنوعی؛

(ج) الزامات خاص برای سیستم‌های هوش مصنوعی پرخطر و تعهداتی برای متصدی آنها؛

(د) قواعد هماهنگ شفافیت برای سیستم‌های هوش مصنوعی که می‌خواهند با افراد حقیقی، سیستم‌های تشخیص احساسات و سیستم‌های طبقه‌بندی زیست‌سنجی تعامل کنند و همچنین سیستم‌های هوش مصنوعی که برای تولید یا دستکاری محتوای تصویری، صوتی یا ویدیویی استفاده می‌شوند؛

(ه) قواعدی مربوط به پایش و نظارت بر بازار.

ماده ۲: محدوده

۱. این مقررات در موارد زیر اعمال می‌شود:

(الف) ارائه‌دهندگانی که سیستم‌های هوش مصنوعی را در بازار اتحادیه اروپا عرضه می‌کنند یا به ارائه خدمت می‌پردازند، صرف‌نظر از اینکه آن ارائه‌دهندگان در داخل اتحادیه تأسیس شده‌اند یا در یک کشور ثالث.

(ب) کاربران سیستم‌های هوش مصنوعی که داخل اتحادیه اروپا قرار دارند.

(ج) ارائه‌دهندگان و کاربران سیستم‌های هوش مصنوعی که در کشور ثالثی قرار دارند، ولی خروجی تولیدشده توسط آن سیستم در اتحادیه اروپا استفاده می‌شود.

۲. سیستم‌های هوش مصنوعی پرخطری که اجزای ایمنی محصولات یا سیستم‌ها هستند یا اینکه خودشان محصول یا سیستم هستند، اگر مشمول مصوبات زیر قرار گیرند، فقط ماده ۸۴ روی آنها اعمال می‌شود:

(الف) مقررات (EC) ۳۰۰/۲۰۰۸

(ب) مقررات (EU) ۲۰۱۳/۱۶۷

(ج) مقررات (EU) ۱۶۸/۲۰۱۳

(د) دستورالعمل (EU) ۲۰۱۴/۹۰

(ه) دستورالعمل (EU) ۷۹۷/۲۰۱۶

(و) مقررات (EU) ۸۵۸/۲۰۱۸

(ز) مقررات (EU) ۱۱۳۹/۲۰۱۸

۳. این مقررات برای سیستم‌های هوش مصنوعی که صرفاً برای مقاصد نظامی توسعه یافته‌اند یا استفاده می‌شوند، اعمال نمی‌گردد.

۴. این مقررات در مورد مقامات دولتی مستقر در یک کشور ثالث یا سازمان‌های بین المللی که مطابق بند ۱ در محدوده این مقررات قرار می‌گیرند، اعمال نمی‌شود؛ البته درصورتی‌که آن مقامات یا سازمان‌ها از سیستم‌های هوش مصنوعی در چارچوب موافقت‌نامه‌های بین‌المللی برای اجرای قانون و همکاری قضایی با اتحادیه یا با یک یا چند کشور عضو استفاده می‌کنند.

۵. این مقررات بر اعمال مفاد مربوط به «مسئولیت ارائه‌دهندگان خدمات واسطه» مندرج در فصل ۲ بخش ۴ دستورالعمل (EC)/۲۰۰۰/۳۱ پارلمان اروپا و شورای اروپا تأثیری نخواهد داشت[1] [چنانچه با مفاد مربوطه از قانون خدمات دیجیتال جایگزین می‌شود].

ماده ۳: تعاریف

تعاریف زیر برای این مقررات اعمال می‌شود:

(۱) «سیستم هوش مصنوعی» به معنای نرم‌افزاری است که با یک یا چند تکنیک و رویکرد ذکرشده در پیوست ۱ توسعه یافته و می‌تواند برای مجموعه معیّنی از اهداف تعریف‌شده توسط انسان، خروجی‌هایی مانند محتوا، پیش‌بینی، توصیه یا تصمیم ـ تحت تأثیر محیطی که با آن تعامل دارد ـ تولید کند.

(۲) «ارائه‌دهنده» به معنای شخص حقیقی یا حقوقی، مقام دولتی، آژانس یا هر نهاد دیگری است که یک سیستم هوش مصنوعی را توسعه می‌دهد یا یک سیستم هوش مصنوعی دارد که با نگاه عرضه در بازار یا ارائه خدمت آن، به نام خود یا یک نشان تجاری توسعه داده شده است؛ چه به‌صورت پولی و چه به‌صورت رایگان.

(۳) «ارائه‌دهنده کوچک‌مقیاس» به معنای ارائه‌دهنده‌ای است که خودش یک واحد تجاری خیلی کوچک یا کوچک ـ طبق معنای مدنظر در توصیه‌نامه کمیسیون EC/۲۰۰۳/۳۶۱ ـ است.[2]

(۴) «کاربر» به معنای هر شخص حقیقی یا حقوقی، مقام دولتی، آژانس یا هر نهاد دیگری است که از یک سیستم هوش مصنوعی تحت اختیار خود استفاده می‌کند؛ به استثنای مواردی که سیستم هوش مصنوعی در جریان یک فعالیت شخصی غیرحرفه‌ای استفاده می‌شود.

---

۱. دستورالعمل (EC) ۲۰۰۰/۳۱ پارلمان اروپا و شورای اروپا مصوب ۸ ژوئن ۲۰۰۰ درباره برخی جنبه‌های حقوقی خدمات جامعه اطلاعاتی، به‌ویژه تجارت الکترونیکی در بازار داخلی (دستورالعمل تجارت الکترونیک) (OJL 178, 17.7.2000, p1).

۲. توصیه‌نامه کمیسیون اروپا مصوب ۶ می ۲۰۰۳ در مورد تعریف شرکت‌های خیلی کوچک، کوچک و متوسط (OJL 124, 20.5.2003, p36).

(۵) «نماینده مجاز» به معنای هر شخص حقیقی یا حقوقی تأسیس‌شده در اتحادیه اروپا است که از یک ارائه‌دهنده سیستم هوش مصنوعی دستور کتبی دریافت کرده تا از طرف او تعهدات و رویه‌های تعیین‌شده در این مقررات را به‌ترتیب اجرا کرده و انجام دهد.

(۶) «واردکننده» به معنای هر شخص حقیقی یا حقوقی تاسیس‌شده در اتحادیه اروپا است که یک سیستم هوش مصنوعی را به بازار عرضه کند یا در خدمت بگذارد که نام یا نشان تجاری یک شخص حقیقی یا حقوقی تاسیس‌شده در خارج از اتحادیه را با خود دارد.

(۷) «توزیع‌کننده» به معنای هر شخص حقیقی یا حقوقی ـ غیر از ارائه‌دهنده یا واردکننده ـ در زنجیره تأمین است که یک سیستم هوش مصنوعی را بدون تأثیر بر ویژگی‌های آن، در بازار اتحادیه اروپا در دسترس قرار می‌دهد.

(۸) «متصدی» به معنای ارائه‌دهنده، کاربر، نماینده مجاز، واردکننده و توزیع‌کننده است.

(۹) «عرضه در بازار» به معنای اولین موجود کردن یک سیستم هوش مصنوعی در بازار اتحادیه است.

(۱۰) «موجود کردن در بازار» به معنای هرگونه عرضه یک سیستم هوش مصنوعی برای توزیع یا استفاده در بازار اتحادیه در جریان یک فعالیت تجاری است؛ خواه در ازای پرداخت پول باشد و خواه رایگان.

(۱۱) «ارائه خدمت» به معنای عرضه مستقیم یک سیستم هوش مصنوعی به کاربر برای اولین استفاده یا جهت استفاده شخصی در بازار اتحادیه برای هدف موردنظر است.

(۱۲) «هدف موردنظر» به معنای استفاده‌ای است که توسط ارائه‌دهنده برای یک سیستم هوش مصنوعی در نظر گرفته شده؛ ازجمله زمینه خاص و شرایط استفاده، همان‌طور که علاوه بر مستندات فنی در اطلاعات عرضه شده توسط ارائه‌دهنده در دستورالعمل‌های استفاده، محتواها و ادعاهای تبلیغاتی یا هنگام فروش مشخص شده است.

(۱۳) «سوءاستفاده قابل پیش‌بینی معقول» به معنای استفاده از یک سیستم هوش مصنوعی به روشی است که با هدف موردنظر آن مطابقت ندارد، اما ممکن است ناشی از رفتار قابل‌پیش‌بینی معقول انسانی یا تعامل با سایر سیستم‌ها باشد.

(۱۴) «جزء ایمنی یک محصول یا سیستم» به معنای جزئی از یک محصول یا سیستم است که عملکرد ایمنی آن محصول یا سیستم را برعهده دارد یا اینکه خرابی یا عملکرد نادرست آن جزء، سلامت و ایمنی افراد یا دارایی‌ها را به خطر می‌اندازد.

(۱۵) «دستورالعمل‌های استفاده» به معنی اطلاعات ارائه‌شده توسط ارائه‌دهنده برای اطلاع دادن به کاربر، خصوصاً درباره هدف موردنظر سیستم هوش مصنوعی و استفاده مناسب از آن است که شامل تنظیمات جغرافیایی، رفتاری یا کاربردی خاص ـ در زمینه‌ای که قرار است سیستم هوش مصنوعی پرخطر در آن استفاده شود ـ می‌باشد.

(۱۶) «جمع‌آوری یک سیستم هوش مصنوعی» به معنای هر اقدامی است که با هدف دستیابی به عودت به ارائه‌دهنده یک سیستم هوش مصنوعی در دسترس کاربران صورت می‌گیرد.

(۱۷) «توقف یک سیستم هوش مصنوعی» به معنای هرگونه اقدامی است که با هدف جلوگیری از توزیع، نمایش و ارائه یک سیستم هوش مصنوعی انجام می‌شود.

(۱۸) «عملکرد یک سیستم هوش مصنوعی» به معنای توانایی یک سیستم هوش مصنوعی برای دستیابی به هدف موردنظرش است.

(۱۹) «مرجع صدور مجوز» به معنای یک مقام ملی است که مسئول ایجاد و اجرای رویه‌های لازم برای ارزیابی، گزینش و صدور مجوز به نهادهای انطباق‌سنجی و پایش آن نهادهاست.

(۲۰) «انطباق‌سنجی» به معنای فرایند تأیید تحقق الزامات فصل ۲ از بخش سوم این مقررات نسبت به یک سیستم هوش مصنوعی است.

(۲۱) «نهاد انطباق‌سنجی» به معنای نهادی است که فعالیت‌های انطباق‌سنجی شخص ثالث ـ ازجمله آزمایش، صدور گواهینامه و بازرسی ـ را انجام می‌دهد.

(۲۲) «نهاد دارای مجوز» به معنای یک نهاد انطباق‌سنجی است که طبق این مقررات و سایر قوانین هماهنگ‌سازی اتحادیه اروپا گزینش و تعیین شده است.

(۲۳) «اصلاح اساسی» به معنای ایجاد تغییر در سیستم هوش مصنوعی پس از عرضه به بازار یا ارائه خدمت آن است که بر پای‌بندی سیستم هوش مصنوعی به الزامات فصل ۲ از عنوان سوم این مقررات تأثیر می‌گذارد یا منجر به اصلاح در هدف موردنظر ـ که سیستم هوش مصنوعی برای آن ساخته شده ـ می‌شود.

(۲۴) «علامت انطباق CE» (یا علامت CE) به معنی علامتی است که با آن یک ارائه‌دهنده نشان می‌دهد که سیستم هوش مصنوعی با الزامات فصل ۲ از عنوان سوم این مقررات و سایر قوانین قابل‌اعمال اتحادیه اروپا ـ که شرایط را برای بازاریابی محصولات هماهنگ می‌کنند («هماهنگ‌سازی قانون اتحادیه») ـ مطابقت دارد. مشروط بر اینکه آن قوانین الصاق شده باشند.

(۲۵) «نظارت پس از بازار» به معنای کلیه فعالیت‌هایی است که توسط ارائه‌دهندگان سیستم‌های هوش مصنوعی برای جمع‌آوری و بازبینی فعالانه تجربیات استفاده از سیستم‌های هوش مصنوعی که آنها در بازار عرضه می‌کنند یا در خدمت می‌گذارند ـ با هدف شناسایی هرگونه نیاز فوری به اعمال هرگونه اقدامات اصلاحی یا پیشگیرانه لازم ـ انجام می‌شود.

(۲۶) «مرجع نظارت بر بازار» به معنای مقام ملی است که طبق مقررات (EU) ۱۰۲۰/۲۰۱۹ فعالیت‌ها را انجام دهد و تدابیری اتخاذ کند.

(۲۷) «استاندارد هماهنگ» به معنای یک استاندارد اروپایی است که در ماده ۲ (۱) (ج) مقررات (EU) ۲۰۱۲/۱۰۲۵ تعریف شده است.

(۲۸) «مشخصات مشترک» به معنای یک سند ـ متفاوت از یک استاندارد ـ حاوی راه‌حل‌های فنی است که وسیله‌ای برای انطباق با برخی الزامات و تعهدات تعیین‌شده در این مقررات ارائه می‌کند.

(۲۹) «داده‌های آموزشی» به معنای داده‌هایی است که برای آموزش یک سیستم هوش مصنوعی از طریق برازش پارامترهای قابل‌یادگیری آن ـ ازجمله وزن‌های یک شبکه عصبی ـ استفاده می‌شوند.

(۳۰) «داده‌های اعتبارسنجی» به معنای داده‌هایی است که برای ارزیابی سیستم هوش مصنوعی آموزش‌دیده و تنظیم پارامترهای غیرقابل‌یادگیری و فرایند یادگیری آن ـ ازجمله به‌منظور جلوگیری از بیش برازش ـ استفاده می‌شوند. درحالی‌که مجموعه داده اعتبارسنجی می‌تواند یک مجموعه داده جداگانه یا بخشی از مجموعه‌داده آموزشی باشد، چه به‌صورت یک تقسیم ثابت باشد و چه متغیر.

(۳۱) «داده‌های آزمایشی» به معنای داده‌هایی است که برای ارائه ارزیابی مستقل از سیستم هوش مصنوعی آموزش‌دیده و اعتبارسنجی‌شده به‌منظور تأیید عملکرد مورد انتظار آن سیستم قبل از عرضه به بازار یا ارائه خدمت استفاده می‌شود.

(۳۲) «داده‌های ورودی» به معنای داده‌هایی است که به یک سیستم هوش مصنوعی ارائه می‌شود یا مستقیماً توسط آن به‌دست می‌آید که سیستم براساس آن یک خروجی تولید می‌کند.

(۳۳) «داده‌های زیست‌سنجی» به معنای داده‌های شخصی ناشی از پردازش فنی خاص ـ مربوط به ویژگی‌های جسمانی، فیزیولوژیکی یا رفتاری یک شخص حقیقی ـ است که امکان شناسایی منحصربه‌فرد آن شخص حقیقی را فراهم یا تأیید می‌کند؛ مانند تصاویر چهره یا داده‌های انگشت‌نگاری.

(۳۴) «سیستم تشخیص احساسات» به معنای یک سیستم هوش مصنوعی است که هدفش شناسایی یا استنباط احساسات یا مقاصد افراد حقیقی بر اساس داده‌های زیست‌سنجی آنهاست.

(۳۵) «سیستم طبقه‌بندی زیست‌سنجی» به معنای یک سیستم هوش مصنوعی است که هدفش انتساب افراد حقیقی به دسته‌های خاص مانند جنسیت، سن، رنگ مو، رنگ چشم، خالکوبی، منشأ قومیتی یا گرایش جنسی یا سیاسی، براساس داده‌های زیست‌سنجی آنهاست.

(۳۶) «سیستم شناسایی زیست‌سنجی از راه دور» به معنای یک سیستم هوش مصنوعی است که هدفش شناسایی افراد حقیقی از راه دور از طریق مقایسه داده‌های زیست‌سنجی یک فرد با داده‌های زیست‌سنجی موجود در پایگاه داده مرجع، و بدون اطلاع قبلی از کاربر سیستم هوش مصنوعی که آیا شخص حاضر خواهد بود و قابل‌شناسایی است یا خیر.

(۳۷) «سیستم شناسایی زیست‌سنجی از راه‌دور بی‌درنگ» به معنای یک سیستم شناسایی زیست‌سنجی از راه دور است که به‌موجب آن جمع‌آوری داده‌های زیست‌سنجی، مقایسه و شناسایی همگی بدون تأخیر قابل‌توجه انجام می‌شود. این تعریف نه‌تنها شامل شناسایی فوری می‌شود، بلکه برای جلوگیری از سرپیچی، شامل تأخیرهای کوتاه محدود نیز می‌شود.

(۳۸) «سیستم شناسایی زیست‌سنجی از راه دور با تأخیر» به معنای یک سیستم شناسایی زیست‌سنجی از راه دور، به غیر از سیستم شناسایی زیست‌سنجی از راه دور بی‌درنگ است.

(۳۹) «فضای قابل‌دسترس عموم» به معنای هر مکان فیزیکی قابل‌دسترسی برای عموم است؛ صرف‌نظر از شرایط خاصی که ممکن است برای دسترسی اعمال شود.

(۴۰) «مرجع اجرای قانون» به این معنی است:

الف) هر مقام دولتی که برای پیشگیری، تحقیق، شناسایی یا تعقیب جرایم جنایی یا اجرای مجازات‌های کیفری، ازجمله محافظت در برابر تهدیدات امنیت عمومی و جلوگیری از آن صلاحیت دارد. یا

(ب) هر نهاد یا سازمان دیگری که توسط قانون کشور عضو برای اعمال اقتدار و قدرت عمومی به‌منظور پیشگیری، تحقیق، شناسایی یا تعقیب جرایم جنایی یا اجرای مجازات‌های کیفری، ازجمله محافظت در برابر تهدید امنیت عمومی و جلوگیری از آن، واسپاری شده است.

(۴۱) «اجرای قانون» به فعالیت‌هایی اطلاق می‌شود که توسط مرجع اجرای قانون برای پیشگیری، تحقیق، شناسایی یا تعقیب جرایم جنایی یا اجرای مجازات‌های کیفری، ازجمله محافظت در برابر تهدید امنیت عمومی و جلوگیری از آن انجام می‌شود.

(۴۲) «مقام ناظر ملی» به مرجعی اطلاق می‌شود که یک کشور عضو، مسئولیت اجرا و به‌کارگیری این مقررات را برای هماهنگ‌سازی فعالیت‌های محول‌شده به آن کشور عضو، جهت عمل کردن به‌عنوان نقطه تماس منفرد برای کمیسیون، و برای نمایندگی کشور عضو در هیئت هوش مصنوعی اروپا به او می‌سپارد.

(۴۳) «مرجع ذی‌صلاح ملی» به معنای مقام ناظر ملی، مقام مجوزدهنده و مرجع نظارت بر بازار است.

(۴۴) «حادثه جدی» به معنای هر حادثه‌ای است که به‌طور مستقیم یا غیرمستقیم به هریک از موارد زیر منجر می‌شود، ممکن است منجر شده باشد یا ممکن است منجر شود:

(الف) مرگ یک فرد یا آسیب جدی به سلامتی، دارایی‌ها یا محیط‌زیست یک شخص؛

(ب) اختلال جدی و غیرقابل‌برگشت در مدیریت و بهره‌برداری از زیرساخت‌های حیاتی.

ماده ٤: اصلاحات پیوست ۱

کمیسیون اختیار دارد طبق ماده ۷۳ برای اصلاح فهرست تکنیک‌ها و رویکردهای ذکرشده در پیوست ۱، جهت به‌روزرسانی آن فهرست نسبت به بازار و پیشرفت‌های فناورانه ـ براساس ویژگی‌هایی مشابه همان تکنیک‌ها و رویکردها ـ اقدامات تفویضی انجام دهد.

بخش دوم: کاربردهای ممنوعه هوش مصنوعی

ماده ۵

۱. کاربرد هوش مصنوعی برای موارد زیر ممنوع است:

(الف) عرضه به بازار، ارائه خدمت یا استفاده از یک سیستم هوش مصنوعی که تکنیک‌های نامحسوس را بدون آگاهی شخص به‌کار می‌گیرد تا رفتار او را به‌طور قابل‌توجهی منحرف کند، به‌نحوی‌که موجب آسیب جسمی یا روانی به آن شخص یا شخص دیگری شود یا احتمال آن وجود داشته باشد.

(ب) عرضه به بازار، ارائه خدمت یا استفاده از یک سیستم هوش مصنوعی که از آسیب‌پذیری‌های گروه خاصی از افراد به‌دلیل سن، ناتوانی جسمی یا ذهنی آنها سوءاستفاده می‌کند، تا به‌طور قابل‌توجهی رفتار یک شخص متعلق به آن گروه را منحرف کند؛ به‌نحوی‌که موجب آسیب جسمی یا روانی به آن شخص یا شخص دیگری شود یا احتمال آن وجود داشته باشد.

ج) عرضه به بازار، ارائه خدمت یا استفاده از یک سیستم هوش مصنوعی توسط مقامات دولتی یا از طرف آنها برای ارزیابی یا طبقه‌بندی قابلیت اعتماد به اشخاص حقیقی با امتیاز اجتماعی در یک دوره زمانی معیّن، براساس رفتار اجتماعی یا ویژگی‌های شخصی یا شخصیتی شناخته‌شده یا پیش‌بینی‌شده آنها، که منجر به یک یا هر دو مورد زیر می‌شود:

(۱) برخورد زیان‌بار یا نامناسب با افراد حقیقی خاص یا گروه‌هایی از آنها، در زمینه‌های اجتماعی که داده‌های تولیدشده یا جمع‌آوری‌شده ربطی به آن زمینه‌ها ندارند.

(۲) برخورد زیان‌بار یا نامناسب با افراد حقیقی خاص یا گروه‌هایی از آنها که نسبت به رفتار اجتماعی‌شان یا اهمیت ماجرا، غیرقابل‌توجیه و نامتناسب باشد.

(د) استفاده از سیستم‌های شناسایی زیست‌سنجی از راه دور بی‌درنگ در مکان‌های در دسترس عموم به‌منظور اجرای قانون، مگر اینکه و تا آنجایی که این استفاده برای یکی از اهداف زیر کاملاً ضروری باشد:

(۱) جستجوی هدفمند برای قربانیان احتمالی خاص در یک جنایت، ازجمله کودکان گم‌شده.

(۲) جلوگیری از یک تهدید خاص، اساسی و قریب‌الوقوع برای جان یا ایمنی فیزیکی افراد حقیقی یا برای یک حمله تروریستی.

(۳) کشف، موقعیت‌یابی، شناسایی یا تعقیب یک مجرم یا مظنون به جرم کیفری ـ که در بند ۲ از ماده ۲ تصمیم اساسی شورای اروپا[1](2002/584/JHA) به آن اشاره شده است ـ به‌طوری‌که در قانون کشور عضو مربوطه مجازات آن با حکم حبس یا قرار بازداشت ـ با قاعده مرور زمان سه سال به بالا ـ تعیین شده باشد.

---

۱. تصمیم اساسی شورای اروپا (2002/584/JHA) مصوب ۱۳ ژوئن ۲۰۰۲ در مورد حکم بازداشت اروپاییان و رویه‌های تسلیم کردن بین کشورهای عضو (OJ L 190, 18.7.2002, p1)

۲. استفاده از سیستم‌های شناسایی زیست‌سنجی از راه دور بی‌درنگ در مکان‌های در دسترس عموم به‌منظور اجرای قانون، برای هریک از اهداف ذکرشده در بند ۱ قسمت «د» باید مؤلفه‌های زیر را در نظر بگیرد:

(الف) ماهیت وضعیتی که منجر به استفاده احتمالی می‌شود؛ به‌ویژه وخامت، احتمال وقوع و مقیاس آسیب ناشی از عدم استفاده از سیستم.

(ب) پیامدهای استفاده از سیستم برای حقوق و آزادی‌های همه افراد مرتبط، به‌ویژه وخامت، احتمال وقوع و مقیاس آن پیامدها.

علاوه‌بر این، استفاده از سیستم‌های شناسایی زیست‌سنجی از راه دور بی‌درنگ در مکان‌های در دسترس عموم به‌منظور اجرای قانون، برای هریک از اهداف ذکرشده در بند ۱ قسمت «د» باید مطابق با پادمان‌ها و شرایط متناسب و ضروری مربوط به استفاده، به‌ویژه از لحاظ محدودیت‌های زمانی، جغرافیایی و شخصی باشد.

۳. با توجه به بند ۱ قسمت «د» و بند ۲، هرگونه استفاده فردی به‌منظور اجرای قانون از یک سیستم شناسایی زیست‌سنجی از راه دور بی‌درنگ در مکان‌های در دسترس عموم، منوط به مجوز قبلی صادرشده توسط مقام قضایی خواهد بود یا مجوزی که توسط یک مقام اداری مستقل کشور عضوی که قرار است استفاده در آن صورت گیرد، و بنا به درخواست مستدل و مطابق با قواعد تفصیلی قانون ملی مذکور در بند ۴ صادر شده است. بااین‌حال، در وضعیت اضطراری کاملاً موجه، استفاده از سیستم می‌تواند بدون مجوز آغاز گشته و مجوز فقط در حین یا بعد از استفاده درخواست شود.

مقام قضایی یا اداری ذی‌صلاح فقط در صورتی مجوز می‌دهد که براساس شواهد عینی یا قرائن روشن ارائه‌شده به خود، متقاعد شود که استفاده از سیستم شناسایی زیست‌سنجی از راه دور بی‌درنگ در آن موضوع برای رسیدن به اهداف ذکرشده در بند ۱ قسمت «د» ضروری و متناسب است. همان‌طور که در درخواست ارائه‌شده نیز آمده است، برای تصمیم‌گیری در مورد درخواست، مقام قضایی یا اداری ذی‌صلاح باید مؤلفه‌های مذکور در بند ۲ را در نظر بگیرد.

۴. یک کشور عضو می‌تواند تصمیم بگیرد که امکان ارائه مجوز کامل یا جزئی برای استفاده از سیستم‌های شناسایی زیست‌سنجی از راه دور بی‌درنگ در مکان‌های در دسترس عموم به‌منظور اجرای قانون، تحت محدودیت‌ها و شرایط ذکرشده در بند ۱ قسمت «د» و بند ۲ و ۳ را فراهم کند.

آن کشور عضو باید در قانون ملی خود قواعد تفصیلی لازم را برای درخواست، صدور و کاربرد و همچنین نظارت مربوط به مجوزهای ذکرشده در بند ۳ را وضع نماید.

آن قوانین همچنین باید مشخص کنند که در رابطه با کدام‌یک از اهداف ذکرشده در بند ۱ قسمت «د» ـ ازجمله کدام‌یک از جرایم کیفری مندرج در شماره ۳ از قسمت «د» ـ مقامات ذی‌صلاح می‌توانند مجاز به استفاده از این سیستم‌ها به‌منظور اجرای قانون باشند.

بخش سوم: سیستم‌های هوش مصنوعی پرخطر

فصل ۱: طبقه‌بندی سیستم‌های هوش مصنوعی به‌عنوان پرخطر

ماده ٦: قواعد طبقه‌بندی سیستم‌های هوش مصنوعی پرخطر

۱. صرف‌نظر از اینکه یک سیستم هوش مصنوعی به‌طور مستقل از محصولات ذکرشده در بندهای (الف) و (ب) در بازار عرضه می‌شود یا ارائه خدمت می‌کند، آن سیستم هوش مصنوعی درصورتی‌که هر دو شرط زیر برآورده شده باشد، پرخطر محسوب می‌شود:

(الف) سیستم هوش مصنوعی برای استفاده به‌عنوان جزء ایمنی یک محصول در نظر گرفته شده یا خودْ محصولی است که تحت پوشش قانون هماهنگ‌سازی اتحادیه اروپا ـ که در پیوست ۲ آمده ـ قرار دارد.

(ب) محصولی که سیستم هوش مصنوعی، جزء ایمنی آن است یا سیستم هوش مصنوعی خودش به‌عنوان یک محصول، ملزم به انجام انطباق‌سنجی شخص ثالث با نگاه عرضه به بازار یا در خدمت گذاشتن آن محصول براساس قانون هماهنگ‌سازی اتحادیه ـ که در پیوست۲ آمده ـ می‌باشد.

۲. علاوه‌بر سیستم‌های هوش مصنوعی پرخطر ذکرشده در بند ۱، سیستم‌های هوش مصنوعی مذکور در پیوست ۳ نیز پرخطر محسوب می‌شوند.

ماده ۷: اصلاحات پیوست ۳

۱. کمیسیون اختیار دارد که طبق ماده ۷۳ برای به‌روزرسانی لیست پیوست ۳ از طریق افزودن سیستم‌های هوش مصنوعی پرخطری که هر دو شرط زیر را برآورده کنند، اقدامات تفویضی انجام دهد:

(الف) سیستم‌های هوش مصنوعی که قرار است در هریک از زمینه‌های ذکرشده در نکات ۱ تا ۸ پیوست ۳ استفاده شوند.

(ب) سیستم‌های هوش مصنوعی که خطر آسیب به سلامت و ایمنی یا خطر تأثیر نامطلوب بر حقوق اساسی را ایجاد می‌کنند، خطری که از نظر شدت و احتمال وقوع، معادل یا بیشتر از خطر آسیب یا آثار نامطلوب ناشی از سیستم‌های هوش مصنوعی پرخطر ـ ذکرشده در پیوست ۳ ـ باشد.

۲. هنگام ارزیابی برای اهداف بند ۱ (اینکه آیا یک سیستم هوش مصنوعی، خطر آسیب به سلامت و ایمنی یا خطر تأثیر نامطلوب بر حقوق اساسی را دارد، به‌طوری‌که معادل یا بیشتر از خطر آسیب ناشی از سیستم‌های هوش مصنوعی پرخطر ذکرشده در پیوست ۳ باشد) کمیسیون باید معیارهای زیر را در نظر بگیرد:

(الف) هدف تعیین‌شده برای سیستم هوش مصنوعی.

(ب) میزان استفاده ـ یا احتمال استفاده ـ از سیستم هوش مصنوعی.

(ج) میزانی که استفاده از یک سیستم هوش مصنوعی باعث آسیب به سلامت و ایمنی شده یا تأثیر نامطلوب بر حقوق اساسی ایجاد کرده یا نگرانی‌های قابل‌توجهی در رابطه با تحقق چنین آسیب یا تأثیر نامطلوبی ایجاد کرده که با گزارش‌ها یا ادعاهای مستند ارائه‌شده به مقامات ذی‌صلاح ملی نشان داده شده است.

(د) میزان بالقوه چنین آسیب یا تأثیر نامطلوبی، به‌ویژه از نظر شدت و توانایی آن برای تأثیرگذاری بر اکثریت نسبی افراد.

(ه) میزان وابستگی افرادی که احتمالاً آسیب دیده‌اند یا تحت تأثیر نامطلوب قرار گرفته‌اند به نتیجه حاصل از یک سیستم هوش مصنوعی، خصوصاً وقتی که به دلایل عملی یا قانونی، امکان انصراف از آن نتیجه وجود ندارد.

(و) میزان که افراد احتمالاً آسیب‌دیده یا تحت تأثیر نامطلوب قرار گرفته، در نسبت با یک کاربر سیستم هوش مصنوعی آسیب‌پذیر هستند، به‌ویژه به‌دلیل عدم تعادل قدرت، دانش، شرایط اقتصادی یا اجتماعی یا سن.

(ز) میزانی که نتیجه تولیدشده با یک سیستم هوش مصنوعی به‌راحتی قابل‌برگشت است، که به‌موجب آن نتایجی که بر سلامت یا ایمنی افراد تأثیر می‌گذارد، نباید به‌راحتی قابل‌برگشت در نظر گرفته شوند.

(ح) میزانی که قوانین موجود اتحادیه برای موارد زیر آماده‌سازی می‌کند:

(۱) اقدامات مؤثر جبران خسارت در رابطه با خطرات ناشی از یک سیستم هوش مصنوعی، به استثنای ادعای خسارت؛

(۲) اقدامات مؤثر برای جلوگیری یا به حداقل رساندن قابل‌ملاحظه آن خطرات.

فصل ۲: الزامات سیستم‌های هوش مصنوعی پرخطر

ماده ۸: پیروی از الزامات

۱. سیستم‌های هوش مصنوعی پرخطر باید از الزامات مقررشده در این فصل پیروی کنند.

۲. هدف موردنظر سیستم هوش مصنوعی پرخطر و سیستم مدیریت خطر ـ مذکور در ماده ۹ ـ باید هنگام حصول اطمینان از انطباق با الزامات در نظر گرفته شود.

ماده ۹: سیستم مدیریت خطر

۱. در رابطه با سیستم‌های هوش مصنوعی پرخطر، باید یک سیستم مدیریت خطر ایجاد، اجرا، مستندسازی و نگهداری شود.

۲. سیستم مدیریت خطر باید متشکل از یک فرایند تکرارشونده مستمر باشد که در کل چرخه حیات یک سیستم هوش مصنوعی پرخطر اجرا می‌شود و مستلزم به‌روزرسانی منظم و قاعده‌مند است. این سیستم مدیریت خطر باید شامل موارد زیر باشد:

(الف) شناسایی و تحلیل خطرات شناخته‌شده و قابل‌پیش‌بینی مرتبط با هر سیستم هوش مصنوعی پرخطر؛

(ب) برآورد و ارزیابی خطراتی که ممکن است هنگام استفاده از سیستم هوش مصنوعی پرخطر ـ با رعایت هدف موردنظر خود و در شرایط سوءاستفاده معقول و قابل‌پیش‌بینی ـ پدیدار شود.

(ج) ارزیابی سایر خطرات احتمالی ناشی از تجزیه و تحلیل داده‌های جمع‌آوری‌شده از سیستم نظارت پس از بازار (ماده ۶۱).

(د) اتخاذ تدابیر مدیریت خطر مناسب مطابق با مفاد بندهای زیر.

۳. اقدامات مدیریت خطر مذکور در بند (د) از شماره ۲ باید به آثار و تعاملات احتمالی ناشی از کاربرد ترکیبی الزامات مندرج در فصل ۲ توجه کافی را داشته باشد. این اقدامات باید آخرین پیشرفت‌های عموماً پذیرفته‌شده را در نظر بگیرد؛ ازجمله آنچه در استانداردهای هماهنگ مرتبط یا گزارش‌های جزئی متداول، منعکس شده است.

۴. اقدامات مدیریت خطر ـ مذکور در بند (د) از شماره ۲ ـ باید به‌گونه‌ای باشد که هرگونه خطر باقیمانده مرتبط با هر امر آسیب‌زا و همچنین خطر باقیمانده کلی سیستم‌های هوش مصنوعی پرخطر قابل‌قبول ارزیابی شود، مشروط بر اینکه سیستم هوش مصنوعی پرخطر مطابق با هدف موردنظر خود یا در شرایط سوءاستفاده معقول و قابل‌پیش‌بینی استفاده شود. آن خطرهای باقیمانده باید به کاربر اطلاع داده شوند. جهت شناسایی مناسب‌ترین اقدامات مدیریت خطر، باید از موارد زیر اطمینان حاصل کرد:

(الف) حذف یا کاهش خطرات تا آنجا که ممکن است از طریق طراحی و توسعه قابل‌قبول.

(ب) در صورت لزوم، به‌کارگیری اقدامات کاهشی و کنترلی قابل‌قبول در رابطه با خطراتی که قابل‌حذف نیستند.

(ج) تأمین اطلاعات قابل‌قبول طبق ماده ۱۳، به‌ویژه در مورد خطرات مذکور در بند (ب) از شماره ۲ این ماده، و در صورت لزوم، آموزش دادن به کاربران.

در حذف یا کاهش خطرات مربوط به استفاده از سیستم هوش مصنوعی پرخطر، باید به دانش فنی، تجربه، آموزش، تمرین مورد انتظار کاربر و محیطی که قرار است سیستم در آن استفاده شود، توجه کافی به عمل آید.

۵. سیستم‌های هوش مصنوعی پرخطر باید به‌منظور شناسایی مناسب‌ترین اقدامات مدیریت خطر، آزمایش شوند. آزمایش باید اطمینان حاصل کند که سیستم‌های هوش مصنوعی پرخطر به‌طور مداوم در راستای هدف موردنظر خود عمل می‌کنند و با الزامات مندرج در این فصل مطابقت دارند.

۶. روش‌های آزمایش باید برای دستیابی به هدف موردنظر سیستم هوش مصنوعی مناسب باشد و نیازی به فراتر رفتن از آنچه برای دستیابی به آن هدف ضروری است نباشد.

۷. آزمایش سیستم‌های هوش مصنوعی پرخطر باید در هر نقطه‌ای از زمان در طول فرایند توسعه و در هر صورت قبل از عرضه به بازار یا در خدمت گذاشتن، در صورت لزوم انجام شود. آزمایش باید براساس معیارهای ازپیش‌تعریف‌شده و آستانه‌های احتمالی که با هدف موردنظر سیستم هوش مصنوعی پرخطر مناسب هستند، انجام شود.

۸. هنگام به‌کارگیری سیستم مدیریت خطر ـ که در شماره‌های ۱ تا ۷ شرح داده شد ـ باید توجه ویژه‌ای به این موضوع صورت گیرد که آیا سیستم هوش مصنوعی پرخطر احتمالاً توسط کودکان قابل‌دسترسی است یا بر آنها تأثیر می‌گذارد یا خیر.

۹. برای مؤسسات اعتباری تحت نظارت دستورالعمل ۲۰۱۳/۳۶/EU جنبه‌های شرح داده‌شده در بندهای ۱ تا ۸ باید بخشی از رویه‌های مدیریت خطر ـ که توسط آن مؤسسات براساس ماده ۷۴ آن دستورالعمل ایجاد شده ـ باشد.

ماده ۱۰: داده و حاکمیت داده

۱. سیستم‌های هوش مصنوعی پرخطری که از تکنیک‌های مربوط به آموزش مدل‌ها با داده استفاده می‌کنند، باید براساس آموزش، اعتبارسنجی و آزمایش مجموعه داده‌هایی توسعه داده شوند که معیارهای کیفی ذکرشده در بندهای ۲ تا ۵ را برآورده می‌کنند.

۲. مجموعه داده‌های آموزشی، اعتبارسنجی و آزمایشی باید تابع شیوه‌های حاکمیت و مدیریت داده مناسب باشد. این شیوه‌ها باید به‌طور ویژه به موارد زیر توجه کنند:

(الف) «انتخاب‌های طراحی» مربوطه؛

(ب) جمع‌آوری داده؛

(ج) عملیات پردازش برای آماده‌سازی داده‌های مربوطه، مانند حاشیه‌نویسی، برچسب‌گذاری، تمیز کردن، غنی‌سازی و تجمیع؛

(د) فرمول‌بندی مفروضات مربوطه، به‌ویژه با توجه به اطلاعاتی که قرار است داده‌ها اندازه‌گیری کنند و نشان دهند؛

(ه) ارزیابی قبلی از دسترس‌پذیری، کمیت و مناسب بودن مجموعه داده‌های مورد نیاز؛

(و) امتحان کردن از دیدگاه سوگیری‌های احتمالی؛

(ز) شناسایی هرگونه شکاف یا کاستی احتمالی در داده‌ها و چگونگی رسیدگی به آنها.

۳. مجموعه داده‌های آموزشی، اعتبارسنجی و آزمایشی باید مرتبط، نماینده، عاری از خطا و کامل باشند. آنها باید دارای ویژگی‌های آماری مناسب باشند؛ ازجمله ـ در صورت لزوم ـ در مورد افراد یا گروه‌هایی از افراد که قرار است از سیستم هوش مصنوعی پرخطر بر روی آنها استفاده شود. این ویژگی‌های مجموعه داده‌ها ممکن است در سطح مجموعه داده‌های فردی یا ترکیبی از آنها برآورده شود.

۴. مجموعه داده‌های آموزشی، اعتبارسنجی و آزمایشی باید تا حدی که هدف موردنظر اقتضا می‌کند، ویژگی‌ها یا عناصری را که به محیط جغرافیایی، رفتاری یا عملکردی خاص مربوط‌اند و قرار است سیستم هوش مصنوعی پرخطر در آن استفاد شود، در نظر بگیرد.

۵. ارائه‌دهندگان چنین سیستم‌هایی می‌توانند ـ تا حدی که برای اطمینان از پایش، تشخیص و اصلاح سوگیری در رابطه با سیستم‌های هوش مصنوعی پرخطر کاملاً ضروری باشد ـ دسته‌های خاصی از داده‌های شخصی را پردازش کنند ـ اشاره‌شده در شماره ۱ از ماده ۹ مقررات (EU) ۶۷۹/۲۰۱۶، ماده ۱۰ دستورالعمل (EU) ۶۸۰/۲۰۱۶ و شماره ۱ از ماده ۱۰ مقررات (EU) ۱۷۲۵/۲۰۱۸ ـ مشروط به رعایت ضمانت‌های مناسب برای حق‌ها و آزادی‌های اساسی افراد حقیقی ازجمله محدودیت‌های فنی در استفاده مجدد و استفاده از اقدامات پیشرفته امنیتی و حفظ حریم خصوصی مانند نام مستعارسازی یا رمزگذاری (که در آن ناشناس‌سازی ممکن است به‌طور قابل‌توجهی بر هدف دنبال‌شده تأثیر بگذارد).

۶. شیوه‌های حاکمیت و مدیریت داده مناسب باید برای توسعه سیستم‌های هوش مصنوعی پرخطر ـ به‌جز سیستم‌هایی که از تکنیک‌های مربوط به آموزش مدل‌ها استفاده می‌کنند ـ اعمال شود تا اطمینان حاصل شود که آن سیستم‌های هوش مصنوعی پرخطر با شماره ۲ مطابقت دارند.

ماده ۱۱: مستندات فنی

۱. مستندات فنی یک سیستم هوش مصنوعی پرخطر باید قبل از عرضه به بازار یا ارائه خدمت آن، تدوین شده و به‌روز نگه داشته شود. مستندات فنی باید به‌گونه‌ای تنظیم شود که نشان دهد سیستم هوش مصنوعی پرخطر با الزامات مندرج در این فصل مطابقت دارد و تمام اطلاعات لازم را برای انطباق‌سنجی سیستم هوش مصنوعی با الزامات مذکور به مرجع ذی‌صلاح ملی و نهادهای اعلام‌شده ارائه می‌کند. این مستندات فنی حداقل باید شامل عناصر مندرج در پیوست ۴ باشد.

۲. هنگامی که یک سیستم هوش مصنوعی پرخطر مربوط به یک محصول ـ که اقدامات قانونی مندرج در پیوست ۲ بخش اول در مورد آن اعمال می‌شود ـ در بازار عرضه گردد یا ارائه خدمت کند، باید یک سند فنی واحد تهیه شود که حاوی تمام اطلاعات تعیین‌شده در پیوست ۴ و همچنین اطلاعات مورد نیاز آن اسناد قانونی باشد.

۳. کمیسیون اختیار دارد طبق ماده ۷۳ در صورت لزوم برای اصلاح پیوست ۴ اقدامات تفویضی انجام دهد تا اطمینان حاصل کند که در پرتو پیشرفت فنی، اسناد فنی تمام اطلاعات لازم را برای انطباق‌سنجی سیستم با الزامات مندرج در این فصل ارائه می‌دهد.

ماده ۱۲: نگهداری گزارش فعالیت‌ها

۱. سیستم‌های هوش مصنوعی پرخطر باید به‌گونه‌ای طراحی و توسعه داده شوند که امکان ثبت خودکار رویدادها (گزارش فعالیت‌ها) را در حین کار کردن داشته باشند. این قابلیت‌ها باید با استانداردهای تعیین‌شده یا مشخصات مشترک مطابقت داشته باشد.

۲. قابلیت‌های ثبت گزارش فعالیت‌ها باید سطحی از ردیابی عملکرد سیستم هوش مصنوعی را در طول چرخه عمر آن تضمین کنند که متناسب با هدف موردنظر سیستم باشد.

۳. به‌طور خاص، قابلیت‌های ثبت گزارش فعالیت‌ها باید رصد عملکرد سیستم هوش مصنوعی پرخطر را با توجه به وقوع رویدادهایی که ممکن است منجر به ایجاد خطر در سیستم هوش مصنوعی، به معنایی که در ماده ۶۵ (۱) تعریف شده است، گردد، یا منجر به تغییرات اساسی شود، امکان‌پذیر کند و همچنین نظارت پس از عرضه به بازار را که در ماده ۶۱ ذکر شده است تسهیل نماید.

۴. قابلیت‌های ثبت گزارش فعالیت‌ها حداقل باید موارد زیر را برای سیستم‌های هوش مصنوعی پرخطر ذکرشده در بند ۱ بخش الف از ضمیمه ۳ فراهم کنند:

(الف) ثبت دوره هر استفاده از سیستم (تاریخ و زمان شروع و تاریخ و زمان پایان هر استفاده).

(ب) پایگاه دادهٔ مرجعی که سیستم، داده‌های ورودی را با مقابله با داده‌های آن پایگاه بررسی می‌کند.

(ج) داده‌های ورودی ای که جستجو منتهی به یک تطابق شده است.

(د) شناسایی اشخاص حقیقی دخیل در راستی‌آزمایی نتایج، مطابق ماده (5) 14.

ماده ۱۳: شفافیت و ارائه اطلاعات به کاربران

۱. سیستم‌های هوش مصنوعی پرخطر باید به‌گونه‌ای طراحی و توسعه داده شوند که اطمینان حاصل شود عملکرد آنها به اندازه کافی شفاف است که کاربران می‌توانند خروجی سیستم را تفسیر کرده و به‌طور مناسب از آن استفاده کنند. باید از نوع و میزان شفافیت، در راستای دستیابی به انطباق با وظایف مربوطه کاربر و ارائه‌دهنده مندرج در فصل ۳ از همین بخش اطمینان حاصل شود.

۲. سیستم‌های هوش مصنوعی پرخطر باید همراه با دستورالعمل‌های دیجیتالی برای استفاده باشند یا در غیر این صورت باید به شکلی قابل‌دسترس و روشن، حاوی اطلاعات مختصر، کامل، صحیح و واضحی باشد.

۳. اطلاعات اشاره‌شده در بند ۲ باید این موارد را مشخص کنند:

(الف) اطلاعات هویتی و جزئیات راه ارتباطی با ارائه‌دهنده و در صورت امکان نماینده قانونی؛

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

(۱) هدف موردنظر.

(۲) سطح دقت، استحکام و امنیت سایبری ذکرشده در ماده ۱۵ که سیستم هوش مصنوعی پرخطر در نسبت به آنها آزمایش و تأیید شده است و چنین ویژگی‌هایی را می‌توان از آن انتظار داشت و هر شرایط شناخته‌شده و قابل‌پیش‌بینی که ممکن است بر آن سطح مورد انتظار از دقت، استحکام و امنیت سایبری تأثیر بگذارد.

(۳) هر شرایط شناخته‌شده یا قابل‌پیش‌بینی مربوط به استفاده در راستای هدف موردنظر یا سوءاستفاده در راستای اهداف قابل‌پیش‌بینی و معقول، از سیستم هوش مصنوعی که ممکن است منجر به خطراتی برای سلامتی و ایمنی یا حقوق اساسی شود.

(۴) عملکرد آن در رابطه با افراد یا گروه‌هایی از افراد که هدف، استفاده سیستم بر روی آنهاست.

(۵) در صورت امکان، مشخصات داده‌های ورودی یا هر اطلاعات مرتبط دیگری از نظر آموزش، اعتبارسنجی و مجموعه داده‌های آزمایشی مورد استفاده، با در نظر گرفتن هدف موردنظر سیستم هوش مصنوعی.

(ج) تغییرات سیستم هوش مصنوعی پرخطر و کارکرد آن که در لحظه انطباق‌سنجی اولیه توسط ارائه‌دهنده از قبل تعیین شده است؛ البته در صورت وجود.

(د) تدابیری جهت نظارت انسانی ذکرشده در ماده ۱۴، ازجمله اقدامات فنی که برای تسهیل تفسیر خروجی‌های سیستم‌های هوش مصنوعی توسط کاربران ایجاد شده است.

(ه) عمر متوسط سیستم هوش مصنوعی پرخطر و هرگونه اقدامات لازم جهت نگهداری و مراقبت برای اطمینان از عملکرد صحیح، ازجمله به‌روزرسانی نرم‌افزار.

ماده ١٤: نظارت انسانی

۱. سیستم‌های هوش مصنوعی پرخطر باید به‌گونه‌ای طراحی شوند و توسعه یابند ـ ازجمله با ابزارهای واسط انسان و ماشین مناسب ـ که امکان داشته باشد به‌طور مؤثری توسط اشخاص حقیقی در طول دوره‌ای که از سیستم هوش مصنوعی استفاده می‌شود، نظارت شوند.

۲. نظارت انسانی باید با هدف جلوگیری یا به حداقل رساندن خطرات برای سلامت، ایمنی یا حقوق اساسی‌ای انجام شود که ممکن است هنگام استفاده از یک سیستم هوش مصنوعی پرخطر مطابق با هدف موردنظر خود یا در شرایط سوءاستفاده قابل‌پیش‌بینی معقول ظاهر شود؛ به‌ویژه هنگامی که این خطرات با وجود اعمال سایر الزامات مندرج در این فصل همچنان وجود دارند.

۳. نظارت انسانی باید از طریق یکی یا همه اقدامات زیر تضمین شود:

(الف) در صورت امکان فنی، در سیستم هوش مصنوعی پرخطر، توسط ارائه‌دهنده، قبل از عرضه به بازار یا به خدمت گذاشتن، شناسایی و ساخته شود.

(ب) قبل از عرضه سیستم هوش مصنوعی پرخطر در بازار یا به خدمت گذاردن آن، توسط ارائه‌دهنده شناسایی شده و برای اجرا توسط کاربر مناسب باشد.

۴. اقدامات ذکرشده در بند ۳، باید به افرادی که نظارت انسانی به آنها محول شده است، این امکان را بدهد که متناسب با شرایط، موارد زیر را انجام دهند:

(الف) ظرفیت‌ها و محدودیت‌های سیستم هوش مصنوعی پرخطر را به‌طور کامل درک کرده و قادر به نظارت مناسب بر عملکرد آن باشد؛ به‌طوری‌که علائم ناهنجاری، اختلال در عملکرد و عملکرد غیرمنتظره را بتوان در اسرع وقت شناسایی و برطرف کرد.

(ب) از تمایل احتمالی اتکا یا تکیه بیش از حد خودکار به خروجی تولیدشده توسط یک سیستم هوش مصنوعی پرخطر (سوگیری خودکارسازی) آگاه باشد؛ به‌ویژه نسبت به سیستم‌های هوش مصنوعی پرخطر که برای ارائه اطلاعات یا توصیه‌هایی برای تصمیم‌گیری توسط اشخاص حقیقی استفاده می‌شود.

(ج) قادر به تفسیر صحیح خروجی سیستم هوش مصنوعی پرخطر، به‌ویژه با در نظر گرفتن ویژگی‌های سیستم و ابزارها و روش‌های تفسیری موجود باشد.

(د) قادر باشد در هر موقعیت خاص تصمیم بگیرد که از سیستم هوش مصنوعی پرخطر استفاده نکند یا خروجی سیستم هوش مصنوعی پرخطر را نادیده بگیرد، باطل یا معکوس کند.

(ه) قادر به مداخله در عملکرد سیستم هوش مصنوعی پرخطر یا قطع کردن سیستم از طریق دکمه «توقف» یا روشی مشابه باشد.

۵. برای سیستم‌های هوش مصنوعی پرخطر ذکرشده در بند ۱ (الف) ضمیمه ۳، اقدامات ذکرشده در بند ۳ باید به‌گونه‌ای باشد که اطمینان حاصل شود که علاوه‌بر آن موارد، هیچ اقدام یا تصمیمی توسط کاربر براساس شناسایی حاصل از سیستم اتخاذ نمی‌شود، مگر اینکه حداقل توسط دو شخص حقیقی وارسی و تأیید گردد.

ماده ۱۵: دقت، استحکام و امنیت سایبری

۱. سیستم‌های هوش مصنوعی پرخطر باید به‌گونه‌ای طراحی و توسعه داده شوند که در راستای هدف موردنظر خود، به سطح مناسبی از دقت، استحکام و امنیت سایبری دست یابند و در طول چرخه عمر خود از این جنبه‌ها به‌طور ثابت برخوردار باشند.

۲. سطوح دقت و معیارهای دقت مربوطه در سیستم‌های هوش مصنوعی پرخطر باید در دستورالعمل‌های استفاده همراه اعلام شود.

۳. سیستم‌های هوش مصنوعی پرخطر باید نسبت به خطاها، اشتباهات یا ناسازگاری‌هایی که ممکن است در داخل سیستم یا محیطی که سیستم در آن کار می‌کند رخ دهد، به‌ویژه به‌دلیل تعامل با افراد حقیقی یا سایر سیستم‌ها، مقاوم و پایدار باشند.

استحکام سیستم‌های هوش مصنوعی پرخطر ممکن است از طریق راه‌حل‌های افزونگی فنی، که ممکن است شامل برنامه‌های پشتیبان یا مصون از خرابی باشد، به دست آید.

سیستم‌های هوش مصنوعی پرخطر که پس از عرضه در بازار یا به خدمت گذاردن همچنان به یادگیری ادامه می‌دهند، باید به‌گونه‌ای توسعه داده شوند تا اطمینان حاصل شود که خروجی‌های احتمالی جانبدارانه ناشی از خروجی‌هایی که به‌عنوان ورودی برای عملیات‌های آینده استفاده می‌شوند (حلقه‌های بازخورد)، با اقدامات کاهشی مناسب، به‌درستی مورد بررسی قرار می‌گیرند.

۴. سیستم‌های هوش مصنوعی پرخطر باید نسبت به تلاش‌های اشخاص ثالث غیرمجاز که با بهره‌جویی از آسیب‌پذیری‌های سیستم، درصدد تغییر استفاده یا عملکرد آن هستند، مقاوم و پایدار باشند.

راه‌حل‌های فنی با هدف تضمین امنیت سایبری سیستم‌های هوش مصنوعی پرخطر باید متناسب با شرایط و خطرات مربوطه باشد.

راه‌حل‌های فنی برای رسیدگی به آسیب‌پذیری‌های خاص هوش مصنوعی، در هر مورد به تناسب، باید شامل اقداماتی برای جلوگیری و کنترل این موارد باشد: حملاتی که سعی در دستکاری مجموعه داده آموزشی («مسمومیت داده») دارند، ورودی‌های طراحی‌شده برای ایجاد اشتباه در مدل («مثال‌های متخاصم») یا نقص‌های مدل.

فصل ۳: وظایف ارائه‌دهندگان، استفاده‌کنندگان و سایر افراد در سیستم‌های هوش مصنوعی پرخطر

ماده ۱۶: وظایف ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر

ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر باید:

(الف) اطمینان حاصل کنند که سیستم‌های هوش مصنوعی پرخطر آنها با الزامات بیان‌شده در بخش ۲ مطابقت دارد.

(ب) دارای سیستم مدیریت کیفیت آماده به‌کار باشند که مطابق با ماده ۱۷ باشد.

(ج) مستندات فنی سیستم‌های هوش مصنوعی پرخطر را تدوین کنند.

(د) زمانی که اختیارش را دارند باید گزارش‌هایی را که سیستم هوش مصنوعی پرخطر از فعالیتش به‌صورت خودکار تولید می‌کند، نگهداری کنند.

(د) اطمینان حاصل کنند که سیستم‌های هوش مصنوعی پرخطر قبل از عرضه به بازار یا ارائه خدمت، مراحل انطباق‌سنجی مربوطه را طی می‌کند.

(ه) مطابق با وظایف مربوط به ثبت، مندرج در ماده ۵۱، عمل کنند.

(و) در صورت عدم مطابقت سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از همین بخش، اقدامات اصلاحی ضروری را انجام دهند.

(ز) هرگونه اقدام اصلاحی انجام‌شده را به اطلاع مقامات ذی‌صلاح ملی کشورهای عضوی که در آن سیستم هوش مصنوعی را در دسترس قرار داده یا به خدمت گذاشته‌اند، و در صورت امکان به اطلاع نهاد دارای مجوز برسانند.

(ح) در صورت درخواست یک مقام ذی‌صلاح ملی، مطابقت سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از همین بخش را اثبات کنند.

ماده ۱۷: سیستم مدیریت کیفیت

۱. ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر باید یک سیستم مدیریت کیفیت ایجاد کنند که انطباق با این مقرره را تضمین کند. سیستم مذکور باید به شیوه‌ای نظام‌مند و منظم در قالب راهبردها، روندها و دستورالعمل‌های مکتوب مستند شود و حداقل شامل ابعاد زیر باشد:

(الف) استراتژی مشخصی برای مطابقت با مقررات، ازجمله مطابقت با روندهای انطباق‌سنجی و مدیریت تغییرات در سیستم هوش مصنوعی پرخطر.

(ب) راهکارها، روندها و اقدامات نظام‌مندی که برای طراحی، کنترل طراحی و تأیید طراحی سیستم هوش مصنوعی پرخطر استفاده شوند.

(ج) تکنیک‌ها، روندها و اقدامات نظام‌مندی که برای توسعه، کنترل کیفیت و تضمین کیفیت سیستم هوش مصنوعی پرخطر استفاده شوند.

(د) بررسی‌ها، آزمودن‌ها و اعتبارسنجی‌هایی که باید قبل، حین و بعد از توسعه سیستم هوش مصنوعی پرخطر انجام شود و تعداد دفعاتی که این موارد باید انجام پذیرد.

(ه) مشخصات فنی، ازجمله استانداردهایی که باید اعمال شوند و در مواردی که استانداردهای هماهنگ مربوطه به‌طور کامل اعمال نمی‌شوند، ابزارهایی به‌کار روند که برای اطمینان از مطابقت سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ بخش به‌کار می‌روند.

(و) سیستم‌ها و روندهای مدیریت داده‌ها، که شامل جمع‌آوری داده‌ها، تجزیه و تحلیل داده‌ها، برچسب‌گذاری داده‌ها، ذخیره‌سازی داده‌ها، فیلتر کردن داده‌ها، داده‌کاوی، تجمیع داده‌ها، نگهداری داده‌ها و هر عملیات دیگری در رابطه با داده‌ها که از قبل به‌منظور عرضه یا به خدمت گذاشتن سیستم‌های هوش مصنوعی پرخطر انجام می‌شود.

(ز) سیستم مدیریت خطر که در ماده ۹ بدان اشاره شده است.

(ح) ایجاد، اجرا و نگهداری سیستم نظارت پس از عرضه مطابق ماده ۶۱.

(ط) روندهای مرتبط با گزارش رخدادهای خطیر و مهم و همچنین اختلال در عملکرد مطابق ماده ۶۲.

(ی) رسیدگی به ارتباط با مقامات ذی‌صلاح ملی، مقامات ذی‌صلاح، ازجمله مقامات منطقه‌ای، ارائه یا پشتیبانی از دسترسی به داده‌ها، نهادهای دارای مجوز، سایر اپراتورها، مشتریان یا سایر گروه‌های ذی‌نفع.

(ک) سیستم‌ها و روندهایی جهت نگهداری سوابق کلیه اسناد و اطلاعات مربوطه.

(ل) یک ساختار پاسخگویی که مسئولیت‌های مدیر و سایر کارکنان را نسبت به تمام ابعاد فهرست‌شده در این بند تعیین کند.

۲. اجرا و عملیاتی شدن تمام ابعاد اشاره‌شده در بند ۱ باید متناسب با اندازه سازمان ارائه‌دهنده باشد.

۳. برای ارائه‌دهندگانی که مؤسسه اعتباریِ تحت دستورالعمل EU ۲۰۱۳/۳۶ هستند، وظیفهٔ برقرار ساختن سیستم مدیریت کیفیت باید در راستای قواعد مرتبط با ترتیبات، فرایندها و سازوکارهای اداری داخلی باشد که در ماده ۷۴ از آن دستورالعمل بدانها اشاره شده است. در این حوزه، همهٔ استانداردهای همگون‌شدهٔ مورد اشاره در ماده ۴۰ این قانون باید مدنظر قرار گیرد.

ماده ۱۸: وظایف مربوط به تدوین مستندات فنی

۱. ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر باید مستندات فنی ذکرشده در ماده ۱۱ را مطابق با پیوست ۴ تدوین کنند.

۲. ارائه‌دهندگانی که مؤسسه اعتباریِ تحت دستورالعمل EU ۲۰۱۳/۳۶ هستند باید مستندات فنی را تحت عنوان بخشی از مستندات مرتبط با ترتیبات، فرایندها و مکانیسم‌های اداری داخلی، پیرو ماده ۷۴ از آن دستورالعمل، نگهداری کنند.

ماده ۱۹: انطباق‌سنجی

۱. ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر باید اطمینان حاصل کنند که سیستم‌های آنها، قبل از عرضه به بازار یا ارائه خدمت، مراحل انطباق‌سنجی مربوطه را مطابق ماده ۴۳ طی می‌کند. درصورتی‌که پس از انطباق‌سنجی، مطابقت سیستم‌های هوش مصنوعی با الزامات مندرج در فصل ۲ از همین بخش به اثبات رسد، ارائه‌دهندگان باید اعلامیه انطباق اتحادیه اروپا را مطابق با ماده ۴۸ تنظیم نموده و علامت انطباق CE را مطابق با ماده ۴۹ الصاق کنند.

۲. برای سیستم‌های هوش مصنوعی پرخطر اشاره‌شده در قسمت ۵ (ب) از ضمیمه ۳ که توسط مؤسسات اعتباری مشمول دستورالعمل در بازار عرضه می‌شوند یا در خدمت قرار می‌گیرند، انطباق‌سنجی باید به‌عنوان بخشی از روند مذکور در مواد ۹۷ تا ۱۰۱ آن دستورالعمل انجام گردد.

ماده ۲۰: گزارش‌های فعالیت تولیدشده به‌صورت خودکار

۱. ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر باید گزارش‌هایی را که به‌طور خودکار توسط سیستم‌های هوش مصنوعی پرخطر تولید می‌شوند، نگهداری کنند تا این گزارش‌ها به‌موجب توافق قراردادی یا اگر توافقی نبود به‌موجب قانون، تحت کنترل آنها باشد. مدت نگهداری گزارش‌ها باید به‌گونه‌ای باشد که با توجه به هدف موردنظر سیستم هوش مصنوعی پرخطر و وظایف قانونی قابل‌اعمال تحت قوانین اتحادیه یا قوانین ملی مناسب باشد.

۲. ارائه‌دهندگانی که مؤسسه اعتباریِ مشمول دستورالعمل EU ۲۰۱۳/۳۶ هستند باید گزارش‌های فعالیتی را که توسط سیستم هوش مصنوعی به‌صورت خودکار تولید شده‌اند، تحت عنوان بخشی از مستندات مرتبط با ماده ۷۴ از آن دستورالعمل، نگهداری کنند.

ماده ۲۱: اقدامات اصلاحی

ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر که فکر می‌کنند یا دلایلی دارند که فکر کنند که سیستم‌های پرخطر هوش مصنوعی که به بازار عرضه کرده یا به خدمت گذاشته‌اند مطابقت با این قوانین ندارند، باید فوراً اقدامات اصلاحی لازم را برای انطباق آن سیستم، پس گرفتن یا فراخوانی آن به تناسب، انجام دهند. آنها باید به توزیع‌کنندگان سیستم هوش مصنوعی پرخطر موردنظر و در صورت امکان، نماینده مجاز و واردکنندگان اطلاع دهند.

ماده ۲۲: تکالیف اطلاع رسانی

درصورتی‌که سیستم هوش مصنوعی پرخطر، خطری ـ به معنایی که در ماده ۶۵(۱) تعریف شده است – ایجاد کند و این خطر برای ارائه‌دهنده سیستم شناخته شده باشد، آن ارائه‌دهنده باید بلافاصله مقامات ذی‌صلاح ملی کشورهای عضوی را که سیستم را در آنها در دسترس قرار داده است، مطلع کند. همچنین در صورت امکان، نهاد دارای مجوز را که گواهی برای سیستم هوش مصنوعی پرخطر صادر کرده است، به‌ویژه از عدم انطباق و هرگونه اقدام اصلاحی انجام‌شده، مطلع سازد.

ماده ۲۳: همکاری با مراجع ذی‌صلاح

ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر، درصورت درخواست یک مقام ذی‌صلاح ملی، باید تمام اطلاعات و مدارک لازم برای اثبات انطباق سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از همین بخش را در اختیار آن مرجع قرار دهند. این اطلاعات و مدارک باید به زبان رسمی اتحادیه که توسط کشور عضو مربوطه تعیین شده، باشد.

ماده ۲٤: وظایف سازندگان محصولات

اگر سیستم هوش مصنوعی پرخطری مربوط به محصولاتی که مشمول قوانین مندرج در ضمیمه ۲، بخش الف هستند، همراه با محصولی تولیدشده مطابق با آن قوانین و تحت عنوان سازنده محصول، در بازار عرضه گردد یا به خدمت گذاشته شود، سازنده باید مسئولیت انطباق سیستم هوش مصنوعی پرخطر با این قوانین را برعهده بگیرد و تا آنجا که به سیستم هوش مصنوعی مربوط می‌شود، همان وظایفی را که توسط این آیین‌نامه متوجه ارائه‌دهنده است، متوجه سازنده نیز هست.

ماده ۲۵: نمایندگان مجاز

۱. در مواردی که یک واردکننده قابل‌شناسایی نباشد، ارائه‌دهندگان مستقر در خارج از اتحادیه، قبل از موجود کردن سیستم‌های خود در بازار اتحادیه، باید با وکالت‌نامهٔ کتبی، نماینده مجاز مستقر در اتحادیه را تعیین کنند.

۲. نماینده ذی‌صلاح باید وظایفی را که در وکالت‌نامهٔ دریافت‌شده از ارائه‌دهنده مشخص گردیده، انجام دهد. این وکالت‌نامه باید به نماینده مجاز برای انجام وظایف زیر اختیار دهد:

(الف) یک نسخه از اعلامیه انطباق اتحادیه اروپا و اسناد فنی را برای در اختیارِ مقامات ذی‌صلاح ملی و مقامات ملی ذکرشده در ماده ۶۳ (۷) نگهداری کنند.

(ب) در صورت درخواست مستدل، تمام اطلاعات و مدارک لازم برای اثبات انطباق سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از همین بخش را به یک مقام صلاحیتدار ملی ارائه دهند. این اطلاعات شامل گزارش‌های فعالیتی که به‌طور خودکار توسط سیستم هوش مصنوعی پرخطر تولید می‌شوند، خواهد بود. این گزارش‌ها باید به‌موجب یک توافق قراردادی با کاربر یا به‌موجب قانون، تحت کنترل ارائه‌دهنده باشند.

(ج) در صورت درخواست مستدل در مورد هر اقدامی که آنها در رابطه با سیستم هوش مصنوعی پرخطر انجام می‌دهند، با مقامات ذی‌صلاح همکاری کنند.

ماده ۲٦: وظایف واردکنندگان

۱. قبل از عرضه یک سیستم هوش مصنوعی پرخطر در بازار، واردکنندگان چنین سیستمی باید اطمینان حاصل کنند که:

(الف) روند انطباق‌سنجی مناسب توسط ارائه‌دهنده آن سیستم هوش مصنوعی انجام شده است.

(ب) ارائه‌دهنده اسناد فنی را مطابق با پیوست ۴ تدوین کرده است.

(ج) سیستم دارای علامت انطباق الزامی و همچنین به همراه مستندات و دستورالعمل‌های استفاده الزامی است.

۲. درصورتی‌که واردکننده فکر کند یا دلیلی داشته باشد مبنی بر اینکه سیستم هوش مصنوعی پرخطر با این مقررات مطابقت ندارد، نباید آن سیستم را تا زمانی که آن سیستم هوش مصنوعی انطباق پیدا کند در بازار عرضه نماید. درصورتی‌که سیستم هوش مصنوعی پرخطر، به معنایی که در ماده ۶۵ (۱) آمده است، خطری را از خود بروز دهد، واردکننده باید ارائه‌دهنده سیستم هوش مصنوعی و مقامات نظارت بر بازار را در این زمینه مطلع کند.

۳. واردکنندگان باید در سیستم هوش مصنوعی پرخطر به نامِ نام تجاری ثبت‌شده یا علامت تجاری ثبت‌شده و آدرسی که از آن طریق بتوان با آنها تماس گرفت، اشاره کنند. در صورت عدم امکان، روی بسته‌بندی یا اسناد همراه آن ذکر کنند.

۴. واردکنندگان باید اطمینان حاصل کنند زمانی که سیستم هوش مصنوعی پرخطر تحت مسئولیت آنهاست، تا جایی که امکان دارد، شرایط نگهداری یا حمل‌ونقل، انطباق آن با الزامات مندرج در فصل ۲ از همین بخش را به خطر نمی‌اندازد.

۵. واردکنندگان باید در صورت درخواست مستدل مقامات ذی‌صلاح ملی، تمام اطلاعات و مدارک لازم را برای اثبات انطباق سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از این بخش به زبانی که به‌راحتی توسط آنها قابل‌درک باشد، ارائه کنند. این موارد شامل دسترسی به گزارش فعالیت‌هایی است که به‌طور خودکار توسط سیستم هوش مصنوعی پرخطر تولید می‌شوند. این گزارش‌ها باید به‌موجب یک توافق قراردادی با کاربر یا به‌موجب قانون، تحت کنترل ارائه‌دهنده باشند. آنها همچنین باید در مورد هر اقدامی که مقامات ذی‌صلاح ملی در رابطه با آن سیستم انجام دهند، با آنها همکاری کنند.

ماده ۲۷: وظایف توزیع‌کنندگان

۱. قبل از موجود کردن یک سیستم هوش مصنوعی پرخطر در بازار، توزیع‌کنندگان باید بررسی کنند که سیستم هوش مصنوعی پرخطر دارای علامت انطباق CE مورد نیاز است، و همچنین اینکه همراه با مستندات و دستورالعمل استفاده مورد نیاز است و در صورت امکان باید بررسی کنند که ارائه‌دهنده و واردکننده سیستم، از تعهدات مندرج در این قانون پیروی کرده‌اند.

۲. درصورتی‌که یک توزیع‌کننده فکر کند یا دلیلی داشته باشد که فکر کند یک سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از این بخش مطابقت ندارد، نباید سیستم هوش مصنوعی پرخطر را در بازار در دسترس قرار دهد تا زمانی که آن سیستم با آن الزامات مطابقت داده شود. علاوه‌بر این، درصورتی‌که سیستم هوش مصنوعی پرخطر، به معنایی که در ماده ۶۵ (۱) آمده است، خطری را از خود بروز دهد، توزیع‌کننده باید ارائه‌دهنده یا واردکننده سیستم مذکور را مطلع سازد.

۳. توزیع‌کنندگان باید در صورت امکان، زمانی که یک سیستم هوش مصنوعی پرخطر تحت مسئولیت آنهاست، اطمینان حاصل کنند که شرایط ذخیره‌سازی یا حمل‌ونقل، انطباق سیستم با الزامات مندرج در فصل ۲ از این بخش را به خطر نمی‌اندازد.

۴. توزیع‌کننده‌ای که فکر می‌کند یا دلیلی دارد که فکر کند سیستم هوش مصنوعی پرخطری که در بازار در دسترس قرار داده است با الزامات مندرج در فصل ۲ از این بخش مطابقت ندارد، باید اقدامات اصلاحی لازم را برای انطباق آن سیستم با الزامات مذکور یا پس گرفتن یا اعلام فراخوان را انجام دهد، یا باید اطمینان حاصل کند که ارائه‌دهنده، واردکننده یا هر اپراتور مربوطه‌ای، در صورت امکان، آن اقدامات اصلاحی را انجام خواهد داد.

۵. در صورت درخواست مستدل یک مقام صلاحیتدار ملی، توزیع‌کنندگان سیستم‌های هوش مصنوعی پرخطر باید تمام اطلاعات و مدارک لازم برای اثبات انطباق یک سیستم پرخطر با الزامات مندرج در فصل ۲ از همین بخش را در اختیار آن مرجع قرار دهند. توزیع‌کنندگان همچنین باید با آن مقام صلاحیتدار ملی در مورد هر اقدامی که توسط آن مقام انجام شود همکاری کنند.

ماده ۲۸: تعهدات توزیع‌کنندگان، واردکنندگان، استفاده‌کنندگان یا هر شخص ثالث دیگر

۱. هر توزیع‌کننده، واردکننده، کاربر یا شخص ثالث دیگر برای اهداف این قانون ارائه‌دهنده تلقی می‌شود و در هریک از شرایط زیر مشمول وظایف ارائه‌دهنده در ماده ۱۶ خواهد بود:

(الف) یک سیستم هوش مصنوعی پرخطر را تحت نام یا علامت تجاری خود در بازار عرضه کنند یا به خدمت بگیرند.

(ب) هدف موردنظر یک سیستم هوش مصنوعی پرخطر را که قبلاً در بازار عرضه یا در خدمت گذاشته شده، تغییر دهند.

(ج) تغییری اساسی در سیستم هوش مصنوعی پرخطر ایجاد کنند.

۲. در صورت وقوع شرایط مندرج در بند ۱، قسمت (ب) یا (ج)، ارائه‌دهنده‌ای که ابتدائاً سیستم هوش مصنوعی پرخطر را در بازار عرضه کرده یا آن را در خدمت قرار داده است، زین پس از حیث این قانون ارائه‌دهنده تلقی نمی‌شود.

ماده ۲۹: وظایف کاربران سیستم هوش مصنوعی پرخطر

۱. کاربران سیستم‌های هوش مصنوعی پرخطر باید از چنین سیستم‌هایی مطابق با دستورالعمل‌های استفاده همراه با سیستم‌ها، در راستای بندهای ۲ و ۵ استفاده کنند.

۲. وظایف مندرج در بند ۱ در تعارض با سایر تعهدات کاربر مندرج در قوانین اتحادیه یا قوانین ملی نیست. همچنین این وظایف به صلاحدید کاربر در سازماندهی منابع و فعالیت‌های خود به‌منظور اجرای اقدامات نظارتی انسانی است که توسط ارائه‌دهنده مشخص شده است.

۳. بدون لطمه به بند ۱ و تا حدی که کنترل کاربر روی داده‌های ورودی حفظ شود، کاربر باید اطمینان حاصل کند که داده‌های ورودی در راستای هدف تعریف‌شده سیستم هوش مصنوعی پرخطر است.

۴. کاربران باید بر عملکرد سیستم هوش مصنوعی پرخطر مطابق دستورالعمل‌های استفاده، نظارت کنند. هنگامی که دلایلی داشته باشند که استفاده مطابق با دستورالعمل‌های استفاده ممکن است منجر به ایجاد خطر توسط سیستم هوش مصنوعی، به معنای ماده (۱)۶۵، شود، باید به ارائه‌دهنده یا توزیع‌کننده اطلاع داده و استفاده از سیستم را تعلیق کنند. آنها همچنین باید ارائه‌دهنده یا توزیع‌کننده را در صورت شناسایی هرگونه حادثه جدی یا هرگونه اختلال در عملکرد، به معنایی که در ماده ۶۲ تعریف شده، مطلع کنند و استفاده از سیستم هوش مصنوعی را قطع نمایند. درصورتی‌که استفاده کننده نتواند به ارائه‌دهنده دسترسی پیدا کند، باید مطابق ماده ۶۲ عمل شود.

برای کاربران مؤسسات اعتباری مشمول قانون EU/۳۶/۲۰۱۳، وظایف نظارتی مندرج در بند اول با رعایت قوانین مربوط به ترتیبات، فرایندها و سازوکارهای اداری داخلی خواهد بود که در ماده ۷۴ آن قانون بدانها اشاره شده است.

۵. کاربران سیستم‌های هوش مصنوعی پرخطر باید گزارش‌های فعالیت را که به‌طور خودکار توسط سیستم هوش مصنوعی پرخطر تولید می‌شود، زمانی که این گزارش‌ها تحت کنترلشان هستند، نگه دارند. مدت زمانی نگهداری گزارش‌ها باید با هدف موردنظر سیستم هوش مصنوعی پرخطر و تعهدات قانونی قابل‌اجرا تحت قوانین اتحادیه یا قوانین ملی متناسب باشد.

کاربرانی که مؤسسات اعتباری مشمول دستورالعمل EU ۲۰۱۳/۳۶ هستند، باید گزارش‌ها را به‌عنوان بخشی از اسناد مربوط به ترتیبات، فرایندها و مکانیسم‌های اداری داخلی طبق ماده ۷۴ آن قانون نگهداری کنند.

۶. کاربران سیستم‌های هوش مصنوعی پرخطر باید از اطلاعات ارائه‌شده در ماده ۱۳ برای انجام وظایف خود در ارزیابی تأثیر حفاظت از داده، به تناسب طبق ماده ۳۵ مقررات (EU) 2016/۶۷۹ یا ماده ۲۷ دستورالعمل (EU) 2016/680، استفاده کنند.

فصل ٤: مراجع صدور مجوز و نهادهای دارای مجوز

ماده ۳۰: مراجع صدور مجوز

۱. هر کشور عضو باید یک مرجع صدور مجوز تأسیس یا تعیین کند. این مرجع، مسئول ایجاد و اجرای رویه‌های لازم برای ارزیابی، گزینش و صدور مجوز به نهادهای انطباق‌سنجی و نظارت بر آنها خواهد بود.

۲. کشورهای عضو می‌توانند یک نهاد ملی اعتباربخشی را که در مقررات (EC) شماره ۲۰۰۸/۷۶۵ ذکر شده است به‌عنوان مرجع صدور مجوز تعیین کنند.

۳. مراجع صدور مجوز باید به‌گونه‌ای ایجاد، سازماندهی و مدیریت شوند که هیچ تعارض منافعی با نهادهای انطباق‌سنجی ایجاد نشود و از واقع‌گرایی و بی‌طرفی فعالیت‌های آنها محافظت گردد.

۴. مراجع صدور مجوز باید به‌گونه‌ای سازماندهی شوند که تصمیمات مربوط به مجوز نهادهای انطباق‌سنجی، توسط اشخاص ذی‌صلاحی انجام شود که متفاوت از کسانی که ارزیابی آن نهادها را انجام داده‌اند، باشند.

۵. مراجع صدور مجوز نباید فعالیت‌ها یا خدمات مشاوره‌ای در راستای امور تجاری یا رقابتی پیشنهاد دهند یا فراهم کنند که نهادهای انطباق‌سنجی آن را انجام می‌دهند.

۶. مراجع صدور مجوز باید از محرمانگی اطلاعاتی که جمع آوری می‌نمایند، محافظت کنند.

۷. مراجع صدور مجوز باید به تعداد کافی کارمند ذی‌صلاح جهت انجام صحیح وظایف خود در اختیار داشته باشند.

۸. مراجع صدور مجوز باید اطمینان حاصل کنند که ارزیابی‌های انطباق به شیوه‌ای متناسب انجام می‌گردد و از تحمیل تکالیف غیرضروری برای ارائه‌دهندگان اجتناب می‌شود و همچنین اطمینان حاصل کنند که نهادهای دارای مجوز فعالیت‌های خود را با در نظر گرفتن میزان تعهد، بخشی که در آن فعالیت می‌کنند و ساختار و درجه پیچیدگی سیستم هوش مصنوعی موردنظر، انجام می‌دهند.

ماده ۳۱: درخواست نهادهای انطباق‌سنجی برای مجوز

۱. نهادهای انطباق‌سنجی باید درخواستی را برای مجوز به مرجع صدور مجوز کشور عضوی که در آن مستقر شده‌اند، ارسال کنند.

۲. درخواست مجوز باید همراه با شرحی از فعالیت‌های انطباق‌سنجی، جزء یا اجزاء انطباق‌سنجی و فناوری‌های هوش مصنوعی باشد که نهاد انطباق‌سنجی ادعای صلاحیت آنها را دارد. همچنین در صورت وجود، همراه یک گواهی اعتبار صادرشده توسط یک نهاد اعتباربخشی ملی باشد که گواهی می‌دهد نهاد انطباق‌سنجی الزامات مندرج در ماده ۳۳ را برآورده می‌کند. هر سند معتبر مربوط به انتصاب‌های موجودِ نهاد دارای مجوز متقاضی که در هریک از قوانین هماهنگ‌سازی دیگر اتحادیه باشد، باید اضافه گردد.

۳. در مواردی که نهاد انطباق‌سنجی مربوطه نتواند گواهی اعتبار ارائه کند، باید مدارک مستند لازم برای راستی‌آزمایی، شناسایی و نظارت منظم بر انطباق آن با الزامات مندرج در ماده ۳۳ را در اختیار مرجع صدور مجوز قرار دهد. تمامی نهادهای دارای مجوزی که توسط یکی از قوانین هماهنگ‌سازی اتحادیه تعیین شده باشند، تمام اسناد و گواهی‌های مرتبط با آن تعیین‌ها می‌تواند برای پشتیبانی از روند تعیین آنها براساس این مقررات، در جایی که مناسب باشد، استفاده گردد.

ماده ۳۲: روند صدور مجوز

۱. مراجع صدور مجوز فقط می‌توانند به مراجع انطباق‌سنجی‌ای که الزامات مندرج در ماده ۳۳ را برآورده کرده‌اند، مجوز بدهند.

۲. مراجع صدور مجوز باید با استفاده از ابزار اطلاع‌رسانی الکترونیکی که توسط کمیسیون توسعه یافته و مدیریت می‌شود، صدور مجوزها را به کمیسیون و سایر کشورهای عضو اطلاع دهند.

۳. این اطلاعیه باید شامل جزئیات کامل فعالیت‌های انطباق‌سنجی، جزء یا اجزاء انطباق‌سنجی و فناوری‌های هوش مصنوعی مربوطه باشد.

۴. مراجع صدور مجوز باید کمیسیون و سایر کشورهای عضو را از هرگونه تغییرات مربوطه بعدی در مجوزها مطلع سازند.

ماده ۳۳: نهادهای دارای مجوز

۱. نهادهای دارای مجوز باید انطباق سیستم هوش مصنوعی پرخطر را مطابق با روندهای انطباق‌سنجی مندرج در ماده ۴۳ تأیید کنند.

۲. نهادهای دارای مجوز باید الزامات سازمانی، مدیریت کیفیت و همچنین الزامات مربوط به منابع و فرایندها را که برای انجام وظایف آنها ضروری است، برآورده سازند.

۳. ساختار سازمانی، تخصیص مسئولیت‌ها، خطوط گزارش‌دهی و عملکرد نهادهای دارای مجوز باید به‌گونه‌ای باشد که نسبت به عملکرد و نتایج فعالیت‌های انطباق‌سنجی که این نهادها انجام می‌دهند، اطمینان حاصل شود.

۴. نهادهای دارای مجوز باید مستقل از ارائه‌دهندگان سیستم هوش مصنوعی پرخطری باشند که در رابطه با آن، فعالیت‌های انطباق‌سنجی را انجام می‌دهد. نهادهای دارای مجوز همچنین باید از هر اپراتور دیگری که در ارتباط با سیستم هوش مصنوعی پرخطرِ مورد ارزیابی منفعت اقتصادی دارند، و همچنین از هر رقیب ارائه‌دهنده مذکور مستقل باشند.

۵. نهادهای دارای مجوز باید به‌گونه‌ای سازماندهی و فعالیت کنند که از استقلال، واقع‌گرایی و بی‌طرفی فعالیت‌های خود محافظت نمایند. نهادهای دارای مجوز باید ساختار و روندهایی را برای حفظ بی‌طرفی و ترویج و اِعمال اصول بی‌طرفی در سراسر سازمان، پرسنل و فعالیت‌های ارزیابی خود، مستندسازی و اجرا کنند.

۶. نهادهای دارای مجوز باید روندهای مستندسازی‌شده‌ای داشته باشند که اطمینان حاصل کنند کارمندان، کمیته‌ها، شرکت‌های تابعه، پیمانکاران فرعی و هر نهاد مرتبط یا کارمندان نهادهای خارجی، محرمانه بودن اطلاعاتی را که در حین انجام فعالیت‌های انطباق‌سنجی در اختیار آنها قرار می‌گیرد، مورد توجه قرار می‌دهند؛ مگر جایی که افشای اطلاعات قانوناً لازم شمرده شده است. کارکنان نهادهای دارای مجوز موظف به رعایت رازداری حرفه‌ای در رابطه با کلیه اطلاعاتی هستند که در انجام وظایف خود براساس این مقررات به دست می‌آیند، به‌جز در رابطه با مراجع صدور مجوز کشور عضوی که فعالیت‌هایشان آنجا انجام می‌شود.

۷. نهادهای دارای مجوز باید روندهایی برای اجرای فعالیت‌هایشان داشته باشند که میزان تعهدات، بخشی که در آن فعالیت می‌کنند، ساختار آن و میزان پیچیدگی سیستم هوش مصنوعی موردنظر را لحاظ نماید.

۸. نهادهای دارای مجوز باید قرارداد بیمه مسئولیت مناسب را برای فعالیت‌های انطباق‌سنجی خود منعقد کنند، مگر اینکه مسئولیت توسط کشور عضو مربوطه مطابق با قوانین ملی بر عهده گرفته شود یا آن کشور عضو مستقیماً مسئول انطباق‌سنجی باشد.

۹. نهادهای دارای مجوز باید قادر باشند که با کمال امانت حرفه‌ای و صلاحیت لازم در زمینه‌های مشخص، همه وظایفی را که به‌موجب این آیین‌نامه برعهده آنهاست، انجام دهند خواه این وظایف توسط خود آن نهادها انجام شود یا به نمایندگی از آنها و با مسئولیت آنها انجام شود.

۱۰. نهادهای دارای مجوز باید دارای صلاحیت‌های داخلی کافی برای ارزیابی مؤثر وظایف انجام‌شده توسط طرف‌های خارجی به نیابت از آنها باشند. به این منظور، در همهٔ زمان‌ها و برای هر روش انطباق‌سنجی و هر نوع سیستم هوش مصنوعی پرخطری که در رابطه با آن تعیین شده‌اند، این نهادها باید دارای پرسنل اداری، فنی و علمی کافی باشند که دارای تجربه و دانش مربوط به فناوری‌های هوش مصنوعی مربوطه، داده‌ها و محاسبات داده‌ها و الزامات مندرج در فصل ۲ از همین بخش هستند.

۱۱. نهادهای دارای مجوز باید در فعالیت‌های مربوط به هماهنگی که در ماده ۳۸ ذکر شده است، شرکت کنند. آنها یا باید مستقیماً شرکت کنند یا در سازمان‌های استاندارد اروپایی نمایندگی داشته باشند یا اطمینان حاصل کنند که از استانداردهای مربوطه آگاه و به‌روز هستند.

۱۲. نهادهای دارای مجوز باید در صورت درخواست، تمام اسناد مربوطه، ازجمله اسناد مربوط به ارائه‌دهندگان، را در دسترس مراجع صدور مجوز — اشاره‌شده در ماده ۳۰ - قرار دهند تا آنها بتوانند فعالیت‌های ارزیابی، انتخاب، صدور مجوز، رصد و نظارت خود را انجام دهد و ارزیابی مندرج در این بخش را تسهیل کند.

ماده ۳٤: شرکت‌های تابعهٔ نهادهای دارای مجوز و برون‌سپاری توسط آن نهادها

۱. درصورتی‌که نهاد دارای مجوز وظایف خاص مرتبط با انطباق‌سنجی را برون‌سپاری کند یا به یک شرکت تابعه بسپارد، باید اطمینان حاصل کند که شرکت بیرونی یا شرکت تابعه الزامات مندرج در ماده ۳۳ را برآورده می‌کند و مراتب را به مرجع صدور مجوز، خواهد رساند.

۲. نهادهای دارای مجوز باید مسئولیت کامل وظایفی را که توسط شرکت‌های بیرونی یا شرکت‌های تابعه انجام می‌شود، زمانی که این شرکت‌ها وجود داشته باشند، بر عهده بگیرند.

۳. فعالیت‌ها را تنها با توافق ارائه‌دهنده می‌توان توسط شرکت‌های بیرونی یا تابعه انجام داد.

۴. نهادهای دارای مجوز باید اسناد مربوط به ارزیابی صلاحیت شرکت‌های بیرونی و تابعه و کارهای انجام‌شده توسط آنها را طبق این آیین‌نامه در اختیار مرجع صدور مجوز قرار دهند.

ماده ۳۵: شماره‌های شناسایی و نهادهای دارای مجوز تعیین‌شده به‌موجب این قانون

۱. کمیسیون باید یک شماره شناسایی خاص را به هریک از نهادهای دارای مجوز اختصاص دهد. حتی در مواردی که یک نهاد براساس چندین قانون اتحادیه به‌عنوان نهاد دارای مجوز تعیین شده باشد، باید یک شماره به نهاد مزبور اختصاص یابد.

۲. کمیسیون باید فهرست نهادهایی را که مطابق این قانون به آنها مجوز داده شده، شامل شماره‌های شناسایی اختصاص داده‌شده و فعالیت‌هایی که برای آنها مجوز صادر شده، در دسترس عموم قرار دهد. کمیسیون باید اطمینان حاصل کند که فهرست به‌روز نگه داشته می‌شود.

ماده ۳۶: تغییرات در مجوزها

۱. درصورتی‌که به مرجع صدور مجوز اطلاع داده شود که یک نهاد دارای مجوز الزامات مندرج در ماده ۳۳ را برآورده نمی کند یا وظایف خود را انجام نمی‌دهد، یا مرجع صدور مجوز نسبت به این امر مشکوک باشد، آن مرجع باید بدون تأخیر، موضوع را با نهایت دقت بررسی کند. در این موارد باید نهاد دارای مجوز مربوطه را از ایرادات مطرح‌شده آگاه سازد و به آن امکان دهد تا نظر خود درباره ایرادات را بیان کند. اگر مرجع صدور مجوز به این نتیجه برسد که تحقیقات نهاد دارای مجوز الزامات مندرج در ماده ۳۳ یا وظایف خود را برآورده نمی‌کند، بسته به جدیت مسئله، مجوز را محدود یا تعلیق می‌کند یا آن را پس می‌گیرد. همچنین فوراً کمیسیون و سایر کشورهای عضو را باید در این زمینه مطلع سازد.

۲. در صورت محدودیت، تعلیق یا پس گرفتن مجوز، یا زمانی که نهاد دارای مجوز فعالیت خود را متوقف کرده باشد، مرجع صدور مجوز باید اقدامات مقتضی را انجام دهد تا اطمینان حاصل شود که پرونده‌های آن نهاد دارای مجوز در اختیار نهاد دارای مجوز دیگری قرار می‌گیرد یا در صورت درخواست آنها در دسترس خواهد بود.

ماده ۳۷: اعتراض به صلاحیت نهادهای دارای مجوز

۱. کمیسیون، در صورت لزوم، تمام مواردی را که دلایلی برای تردید در صلاحیت یک نهاد دارای مجوز در پیروی از الزامات مندرج در ماده ۳۳ وجود دارد، بررسی خواهد کرد.

۲. مرجع صدور مجوز، در صورت درخواست، کلیه اطلاعات مجوز نهاد دارای مجوز مربوطه را در اختیار کمیسیون قرار خواهد داد.

۳. کمیسیون باید اطمینان حاصل کند که تمام اطلاعات محرمانه به‌دست‌آمده در جریان تحقیقات مرتبط با این ماده، محرمانه می‌ماند.

۴. درصورتی‌که برای کمیسیون اثبات شود که یک نهاد دارای مجوز الزامات مندرج در ماده ۳۳ را نداشته یا از این به بعد آنها را برآورده نمی‌کند، تصمیمی مستدل اتخاذ می‌کند و از کشور عضوی که مجوز صادر می‌کند، درخواست می‌کند اقدامات اصلاحی لازم را - ازجمله پس‌گرفتن مجوز در صورت لزوم - انجام دهد. تصمیم اجرائی مذکور باید در انطباق با روند بررسی مذکور در بند ۲ ماده ۷۴ اتخاذ گردد.

ماده ۳۸: هماهنگی نهادهای دارای مجوز

۱. کمیسیون باید اطمینان حاصل کند که با توجه به حوزه‌های تحت پوشش این قانون، هماهنگی و همکاری مناسب بین نهادهای دارای مجوز فعال در روندهای انطباق‌سنجی سیستم‌های هوش مصنوعی مطابق این قانون برقرار شده و در قالب یک گروه، به‌درستی عمل می‌کنند.

۲. کشورهای عضو باید اطمینان حاصل کنند که نهادهای دارای مجوز مربوط به آنها، مستقیماً یا از طریق نمایندگان تعیین‌شده، در امور آن گروه شرکت می‌کنند.

ماده ۳۹: نهادهای انطباق‌سنجی از کشورهای ثالث

۱. نهادهای انطباق‌سنجی که براساس قانون کشور ثالثی ایجاد شوند که اتحادیه با آن توافقنامه منعقد کرده است، جواز انجام فعالیت‌های نهادهای دارای مجوز را طبق این مقررات دارا هستند.

فصل ۵: استانداردها، انطباق‌سنجی، گواهی‌نامه‌ها و ثبت

ماده ٤٠: استانداردهای هماهنگ‌شده

سیستم‌های هوش مصنوعی پرخطری که مطابق با استانداردهای هماهنگ‌شده هستند یا مطابق با بخشی از مراجع منتشرشده در مجله رسمی اتحادیه اروپا می‌باشند، اصل آن است که با الزامات مندرج در فصل ۲ از این بخش مطابقت دارند. البته تا جایی که این استانداردها آن الزامات را پوشش می‌دهند.

ماده ٤١: مشخصات مشترک

۱. در مواردی که استانداردهای هماهنگ اشاره‌شده در ماده ۴۰ وجود نداشته باشد یا در مواردی که کمیسیون تشخیص دهد که استانداردهای هماهنگ مربوطه کافی نیستند یا نیاز به رسیدگی به نگرانی‌هایی خاص در باب ایمنی یا حق‌های بنیادین وجود دارد کمیسیون می‌تواند از طریق قوانین اجرایی، مشخصات مشترکی را در رابطه با الزامات مندرج در فصل ۲ از همین بخش اتخاذ کند. این اقدامات اجرایی باید طبق روند بررسی مذکور در ماده (۲) ۷۴ باشد.

۲. کمیسیون، هنگام تهیه مشخصات مشترک ذکرشده در بند ۱، نظر سازمان‌ها یا گروه‌های تخصصی مربوطه را که براساس قوانین بخش‌های اتحادیه تشکیل شده‌اند، جمع‌آوری خواهد کرد.

۳. سیستم‌های هوش مصنوعی پرخطر که با مشخصات مشترک ذکرشده در بند ۱ مطابقت داشته باشند، با الزامات مندرج در فصل ۲ از این بخش، تا حدی که مشخصات مشترک آن الزامات را پوشش می‌دهند، مطابقت دارند.

۴. درصورتی‌که ارائه‌دهندگان مشخصات مشترک ذکرشده در بند ۱ را رعایت نکنند، باید راه‌حل‌های فنی موجهی پیشنهاد دهند که حداقل معادل آن مشخصات باشد.

ماده ۴۲: پیش‌فرض انطباق با الزامات خاص

۱. سیستم‌های هوش مصنوعی پرخطری که بر روی داده‌های مربوط به محیط جغرافیایی، رفتاری و عملکردی خاصی که قرار است در آن استفاده شوند، آموزش دیده و آزمایش شده‌اند، با در نظر گرفتن هدف مورد نظرشان، فرض می‌شود که مطابق با الزامات مندرج در ماده ۱۰ (۴) هستند.

۲. سیستم‌های هوش مصنوعی پرخطری که گواهی انطباق آنها تحت یک طرح امنیت سایبری براساس مقررات (EU) ۲۰۱۹/۸۸۱ پارلمان اروپا و شورا[1] صادر شده که منابع آن در مجله رسمی اتحادیه منتشر شده است، باید بنابر اصل با الزامات امنیت سایبری مندرج در ماده ۱۵ این آیین نامه منطبق انگاشته شوند. البته تا جایی که گواهینامه امنیت سایبری یا بیانیه انطباق یا بخش‌هایی از آن این الزامات را پوشش می‌دهد.

ماده ۴۳: انطباق‌سنجی

۱. برای سیستم‌های هوش مصنوعی پرخطرِ فهرست‌شده در بند ۱ پیوست ۳، زمانی که برای اثبات انطباق یک سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از این بخش، ارائه‌دهنده استانداردهای هماهنگ‌شده‌ای را که در ماده ۴۰ آمده، یا مشخصات مشترک ذکرشده در ماده ۴۱ – در موارد قابل‌اجرا – را اعمال کرده است، ارائه‌دهنده باید یکی از روندهای زیر را دنبال کند:

(الف) روش انطباق‌سنجی بر اساس کنترل داخلی ذکرشده در پیوست ۶.

(ب) روش انطباق‌سنجی براساس ارزیابی سیستم مدیریت کیفیت و ارزیابی مستندات فنی، با مشارکت یک نهاد دارای مجوز، اشاره‌شده در پیوست ۷.

در مواردی که برای نشان دادن انطباق یک سیستم هوش مصنوعی پرخطر با الزامات مندرج در فصل ۲ از همین بخش، ارائه‌دهنده تنها تا حدی استانداردهای هماهنگ مندرج در ماده ۴۰ را اعمال کرده یا اصلاً این استانداردها را اعمال نکرده است، یا در مواردی که چنین استانداردهای هماهنگ‌شده‌ای وجود نداشته باشد و همچنین مشخصات مشترک ذکرشده در ماده ۴۱ در دسترس نباشد، ارائه‌دهنده باید از روش انطباق‌سنجی مندرج در پیوست ۷ پیروی کند.

برای روند انطباق‌سنجی ذکرشده در ضمیمه ۷، ارائه‌دهنده می‌تواند هریک از نهادهای دارای مجوز را انتخاب کند. با این حال، زمانی که قرار است این سیستم توسط مقامات مجری قانون، مهاجرت یا پناهندگی و همچنین مؤسسات، سازمان‌ها یا آژانس‌های اتحادیه اروپا به‌کار گرفته شود، مرجع نظارت بر بازار که در ماده ۶۳ – (۵) یا (۶)، به تناسب مورد – ذکر شده است، به‌عنوان یک نهاد دارای مجوز عمل خواهد کرد.

۲. برای سیستم‌های هوش مصنوعی پرخطر که در نکات ۲ تا ۸ پیوست ۳ بدانها اشاره شده، ارائه‌دهندگان باید از روش انطباق‌سنجی براساس کنترل داخلی که در ضمیمه ۶ بدان اشاره شده است پیروی کنند. در این روش نهاد

۱. مقررات (EU) 2019/881 مصوب ۱۷ آوریل ۲۰۱۹ توسط اتحادیه اروپا و شورا ناظر به ENISA (آژانس اتحادیه اروپا برای امنیت سایبری) و ناظر به گواهی‌نامه امنیت سایبری تکنولوژی اطلاعات و ارتباطات و نسخ مقررات (EU) 526/2013 (دستورالعمل امنیت سایبری)

دارای مجوز دخالتی ندارد. برای سیستم‌های هوش مصنوعی پرخطر اشاره‌شده در بند ۵ (ب) از پیوست ۳، که توسط مؤسسات اعتباری مشمول قانون EU/۳۶/۲۰۱۳ به بازار عرضه یا در خدمت قرار گذاشته شده‌اند، انطباق‌سنجی باید به‌عنوان بخشی از روند اشاره‌شده در مواد ۹۷ تا ۱۰۱ آن قانون انجام شود.

۳. برای سیستم‌های هوش مصنوعی پرخطر، که اقدامات قانونی فهرست‌شده در ضمیمه ۲، بخش الف، اعمال می‌شود، ارائه‌دهنده باید انطباق‌سنجی مربوطه را همان‌طور که طبق آن قوانین لازم است، دنبال کند. الزامات مندرج در فصل ۲ همین بخش، در مورد این سیستم‌های هوش مصنوعی پرخطر اعمال می‌شود و باید بخشی از آن ارزیابی باشند، نکات ۴.۳ و ۴.۴ و ۴.۵ و همچنین بند پنجم از نکته ۴.۶ پیوست ۷ نیز اعمال شود.

به‌منظور این ارزیابی، نهاد دارای مجوز که طبق آن قوانین به آنها مجوز داده شده است، می‌توانند انطباق سیستم‌های هوش مصنوعی پرخطر را با الزامات مندرج در فصل ۲ از این بخش کنترل کنند؛ مشروط بر اینکه انطباق آن نهادهای دارای مجوز با الزامات مندرج در بند (۴)، (۹) و (۱۰) ماده ۳۳ در چارچوب روند صدور مجوز تحت آن قوانین ارزیابی شده باشد.

زمانی که اقدامات قانونی فهرست‌شده در ضمیمه ۲، بخش الف، سازنده محصول را قادر می‌سازد تا از انطباق‌سنجی شخص ثالث انصراف دهد؛ مشروط بر اینکه سازنده تمام استانداردهای هماهنگ را که تمامی الزامات مربوطه را پوشش می‌دهد، اعمال کرده باشد. آن سازنده فقط زمانی می‌تواند از این گزینه استفاده کند که استانداردهای هماهنگ یا در صورت امکان، مشخصات مشترک ذکرشده در ماده ۴۱ را که الزامات مندرج در فصل ۲ از این بخش را پوشش می‌دهد، اعمال کرده باشد.

۴. سیستم‌های هوش مصنوعی پرخطر هر زمان که به‌طور اساسی اصلاح شوند، فارغ از اینکه سیستم اصلاح‌شده برای توزیع در نظر گرفته شده است یا همچنان توسط کاربر فعلی استفاده می‌شود، باید دوباره روند انطباق‌سنجی را طی کند.

برای سیستم‌های هوش مصنوعی پرخطر که پس از قرار گرفتن در بازار یا راه‌اندازی به یادگیری ادامه می‌دهند، تغییراتی در سیستم هوش مصنوعی پرخطر و عملکرد آن که در انطباق‌سنجی اولیه توسط ارائه‌دهنده از پیش تعیین شده، بخشی از اطلاعات مندرج در مستندات فنی ذکرشده در بند ۲ (و) ضمیمه ۴ است، نباید تغییر اساسی محسوب گردد.

۵. کمیسیون این اختیار را دارد که طبق ماده ۷۳ به‌منظور به‌روزرسانی پیوست‌های ۶ و ۷ در راستای معرفی عناصری از روندهای انطباق‌سنجی که با توجه به پیشرفت فنی ضروری خواهند بود، قوانین تفویضی وضع کند.

۶. کمیسیون این اختیار را دارد که قوانین تفویضی را برای اصلاح بندهای ۱ و ۲ اتخاذ کند تا سیستم‌های هوش مصنوعی پرخطر ذکرشده در نکات ۲ تا ۸ ضمیمه ۳ را مشمول روند انطباق‌سنجی مندرج در پیوست ۷ یا بخش‌هایی از آن کند. کمیسیون چنین قوانین تفویضی را با در نظر گرفتن اثربخشی روش انطباق‌سنجی براساس کنترل داخلی ذکرشده در ضمیمه ۶ در راستای پیشگیری یا به حداقل رساندن خطرات سلامت و ایمنی و حفاظت از حق‌های بنیادین ناشی از این سیستم‌ها و همچنین در دسترس بودن ظرفیت‌ها و منابع کافی در میان نهادهای دارای مجوز، وضع خواهد کرد.

ماده ٤٤: گواهی‌ها

۱. گواهی‌های صادرشده توسط نهادهای دارای مجوز مطابق ضمیمه ۷ باید به زبان رسمی اتحادیه که توسط کشور عضوی که نهاد دارای مجوز در آن تأسیس شده است یا در غیر این صورت به زبان رسمی قابل‌قبول برای نهاد دارای مجوز تنظیم گردد.

۲. گواهی‌نامه‌ها برای مدتی که در آنها ذکر شده معتبر خواهند بود. این مدت نباید از پنج سال تجاوز کند. در صورت درخواست ارائه‌دهنده، اعتبار یک گواهی می‌تواند برای دوره‌های بعدی، که نباید از پنج سال تجاوز کند، براساس ارزیابی مجدد مطابق با روش‌های انطباق‌سنجی قابل‌اجرا، تمدید شود.

۳. درصورتی‌که یک نهاد دارای مجوز تشخیص دهد که یک سیستم هوش مصنوعی الزامات مندرج در فصل ۲ از همین بخش را دیگر برآورده نمی‌کند، باید با در نظر گرفتن اصل تناسب، گواهی صادرشده را به حالت تعلیق درآورد یا پس بگیرد یا هرگونه محدودیتی بر آن اعمال کند؛ مگر اینکه انطباق با این الزامات با اقدامات اصلاحی مناسب انجام‌شده توسط ارائه‌دهنده سیستم در مهلت مناسب تعیین‌شده توسط نهاد دارای مجوز، تضمین شود. نهاد دارای مجوز باید دلایل تصمیم خود را بیان کند.

ماده ٤٥: اعتراض به تصمیمات نهاد دارای مجوز

کشورهای عضو باید اطمینان حاصل کنند که یک روند اعتراض علیه تصمیمات نهادهای دارای مجوز برای طرفینی که منافع قانونی در آن تصمیم دارند در دسترس باشد.

ماده ٤٦: وظایف اطلاع‌رسانی نهادهای دارای مجوز

۱. نهادهای دارای مجوز باید مراجع صدور مجوز را از موارد زیر آگاه سازند:

(الف) هرگونه گواهی ارزیابی مستندات فنی اتحادیه، هرگونه سند تکمیلی در کنار آن گواهی‌ها، تأییدیه‌های سیستم مدیریت کیفیت صادرشده مطابق با الزامات پیوست ۷.

(ب) هرگونه امتناع، محدودیت، تعلیق یا پس گرفتن گواهی ارزیابی مستندات فنی اتحادیه یا تأییدیه سیستم مدیریت کیفیت صادرشده مطابق با الزامات پیوست ۷.

(ج) هر شرایطی که بر دامنه یا شرایط مجوز تأثیر می‌گذارد.

(د) هرگونه درخواست اطلاعاتی که از مقامات نظارت بر بازار در مورد فعالیت‌های انطباق‌سنجی دریافت کرده‌اند.

(ه) در صورت درخواست، فعالیت‌های انطباق‌سنجی انجام‌شده در محدوده مجوز آنها و هر فعالیت دیگری که انجام شده است، ازجمله فعالیت‌های فرامرزی و قراردادهای برون‌سپاری.

۲. هریک از نهادهای دارای مجوز باید سایر نهادهای دارای مجوز را از موارد زیر آگاه سازد:

(الف) تأییدیه‌های سیستم مدیریت کیفیت که رد کرده، تعلیق یا پس گرفته، و در صورت درخواست، تأییدیه‌های سیستم کیفیتی که صادر کرده است.

(ب) گواهی‌های ارزیابی مستندات فنی اتحادیه اروپا یا اسناد تکمیلی که رد کرده، پس گرفته، تعلیق کرده یا محدود کرده، و در صورت درخواست، گواهی‌ها و/یا مکمل‌هایی که برای آنها صادر کرده است.

۳. تمامی نهادهای دارای مجوز باید اطلاعات مربوط به نتایج منفی انطباق‌سنجی و در صورت درخواست نتایج مثبت را در اختیار سایر نهادهای دارای مجوز که فعالیت‌های انطباق‌سنجی مشابهی را که فناوری‌های هوش مصنوعی مشابه را پوشش می‌دهند، قرار دهند.

ماده ٤٧: عدول از روند انطباق‌سنجی

۱. با انصراف از ماده ۴۳، هر مرجع نظارت بر بازار می‌تواند استثنائاً به دلایل امنیت عمومی یا حفاظت از جان و سلامت افراد، حفاظت از محیط‌زیست و حفاظت از دارایی‌های صنعتی و زیرساختی کلیدی اجازه عرضه در بازار یا استفاده از سیستم‌های هوش مصنوعی پرخطر را در قلمرو کشور عضو مربوطه بدهد. این مجوز باید برای مدت زمان محدودی باشد، درحالی‌که روندهای انطباق‌سنجی لازم در حال انجام باشد. پس از تکمیل آن روندها مدت زمان مذکور خاتمه می‌یابد. تکمیل این مراحل باید بدون تأخیر بی مورد انجام گردد.

۲. مجوز ذکرشده در بند ۱ تنها در صورتی صادر می‌شود که مرجع نظارت بر بازار به این نتیجه برسد که سیستم هوش مصنوعی پرخطر با الزامات فصل ۲ از همین بخش مطابقت دارد. مقام نظارت بر بازار باید کمیسیون و سایر کشورهای عضو را از هرگونه مجوز صادرشده طبق بند ۱ مطلع کند.

۳. درصورتی‌که ظرف ۱۵ روز تقویمی پس از دریافت اطلاعات ذکرشده در بند ۲، هیچ اعتراضی از سوی یک کشور عضو یا کمیسیون در رابطه با مجوز صادرشده توسط مرجع نظارت بر بازار یک کشور عضو مطابق با بند ۱ مطرح نشده باشد، آن مجوز موجه تلقی می‌گردد.

۴. درصورتی‌که ظرف ۱۵ روز تقویمی پس از دریافت اطلاعیه مذکور در بند ۲، اعتراضاتی توسط یک کشور عضو علیه مجوز صادرشده توسط مرجع نظارت بر بازار کشور عضو دیگر مطرح شود، یا در مواردی که کمیسیون این مجوز را مغایر با قوانین اتحادیه یا منطق دانستن سیستم مذکور در بند ۲ توسط کشورهای عضو را بی‌مبنا قلمداد کند، کمیسیون باید بدون تأخیر با کشور عضو مربوطه رایزنی کند. اپراتور(های) مربوطه باید مورد مشورت قرار گیرد و امکان بیان نظر خود را داشته باشد. با توجه به آن، کمیسیون تصمیم خواهد گرفت که آیا مجوز موجه است یا خیر. کمیسیون تصمیم خود را به کشور عضو مربوطه و اپراتور یا اپراتورهای مربوطه ارسال خواهد کرد.

۵. اگر مجوز ناموجه تلقی شود، این مجوز توسط مقام نظارت بر بازار کشور عضو مربوطه لغو خواهد شد.

۶. با عدول از بندهای ۱ تا ۵، برای سیستم‌های هوش مصنوعی پرخطر که به‌عنوان اجزای ایمنی دستگاه‌ها در نظر گرفته شده‌اند، یا خود دستگاه‌هایی هستند که تحت پوشش قانون (EU) ۷۴۵/۲۰۱۷ و قانون (EU) ۷۴۶/۲۰۱۷ قرار دارند، در کنار عدول از انطباق‌سنجی با الزامات مندرج در فصل ۲ از این بخش، ماده ۵۹ قانون (EU) ۷۴۵/۲۰۱۷ و ماده ۵۴ قانون (EU) ۷۴۶/۲۰۱۷ نیز اعمال می‌شود.

ماده ٤٨: اعلامیه انطباق اتحادیه اروپا

۱. ارائه‌دهنده باید اعلامیه انطباق اتحادیه اروپا را برای تمامی سیستم‌های هوش مصنوعی تنظیم کند و آن را به مدت ۱۰ سال پس از عرضه سیستم هوش مصنوعی در بازار یا به خدمت گذاشتن آن در اختیار مقامات ذی‌صلاح ملی قرار دهد. اعلامیه انطباق اتحادیه اروپا باید سیستم هوش مصنوعی را که برای آن تهیه شده است مشخص کند. یک کپی از اعلامیه انطباق اتحادیه اروپا در صورت درخواست به مقامات ذی‌صلاح ملی مربوطه داده می‌شود.

۲. اعلامیه انطباق اتحادیه اروپا باید بیان کند که سیستم هوش مصنوعی پرخطر موردنظر الزامات مندرج در فصل ۲ از همین بخش را برآورده می‌کند. اعلامیه انطباق اتحادیه اروپا باید حاوی اطلاعات مندرج در ضمیمه ۵ باشد و به زبان رسمی اتحادیه یا زبان‌های الزامی کشور(های) عضوی که سیستم هوش مصنوعی پرخطر در آنها در دسترس است، ترجمه گردد.

۳. در مواردی که سیستم‌های هوش مصنوعی پرخطر مشمول سایر قوانین هماهنگ‌سازی اتحادیه هستند که به اعلام انطباق اتحادیه اروپا نیز نیاز دارد، یک اعلامیه انطباق اتحادیه اروپا باید در رابطه با تمام قوانین اتحادیه قابل‌اعمال در سیستم هوش مصنوعی پرخطر تنظیم شود. این اعلامیه باید حاوی تمام اطلاعات مورد نیاز برای شناسایی قوانین هماهنگ‌سازی اتحادیه باشد که اعلامیه به آن مربوط می‌شود.

۴. با تنظیم اعلامیه انطباق اتحادیه اروپا، ارائه‌دهنده مسئولیت رعایت الزامات مندرج در فصل ۲ از همین بخش را بر عهده می‌گیرد. ارائه‌دهنده باید اعلامیه انطباق اتحادیه اروپا را به نحو مناسبی به‌روز نگه دارد.

۵. کمیسیون این اختیار را خواهد داشت که طبق ماده ۷۳ به‌منظور به‌روزرسانی محتوای اعلامیه انطباق اتحادیه اروپا که در ضمیمه ۵ آمده است، به‌منظور معرفی عناصری که با توجه به پیشرفت فنی ضروری خواهند بود، قوانین تفویضی را وضع نماید.

ماده ٤٩: نشان انطباق CE

۱. علامت CE باید به‌صورت قابل‌مشاهده، خوانا و غیرقابل‌حذف برای سیستم‌های هوش مصنوعی پرخطر الصاق شود. در مواردی که به‌دلیل ماهیت سیستم هوش مصنوعی پرخطر چنین امری امکان‌پذیر یا تضمینی نیست، باید با صلاحدید روی بسته‌بندی یا اسناد همراه الصاق شود.

۲. علامت CE مذکور در بند ۱ این ماده تابع اصول کلی مندرج در ماده ۳۰ مقررات (EC) شماره ۲۰۰۸/۷۶۵ خواهد بود.

۳. در مواردی که امکانش هست، بعد از علامت CE باید شماره شناسایی سازمان نهاد دارای مجوز مسئول روندهای انطباق‌سنجی مندرج در ماده ۴۳ قرار گیرد. این شماره شناسایی همچنین باید در هر مطلب تبلیغاتی نشان داده شود که سیستم هوش مصنوعی پرخطر الزامات نشان‌گذاری CE را برآورده می‌کند.

ماده ۵۰: نگهداری اسناد

ارائه‌دهنده باید برای یک دوره منتهی به ۱۰ سال پس از عرضه سیستم هوش مصنوعی در بازار یا به خدمت گذاشتن آن، موارد زیر را در اختیار مقامات ذی‌صلاح ملی قرار دهد:

(الف) مستندات فنی اشاره‌شده در ماده ۱۱؛

(ب) مستندات مربوط به سیستم مدیریت کیفیت اشاره‌شده در ماده ۱۷؛

(ج) مستندات مربوط به تغییراتی که مورد موافقت نهاد دارای مجوز بوده است، در موارد قابل‌اجرا؛

(د) تصمیمات و سایر اسناد صادرشده توسط نهاد دارای مجوز، در موارد قابل‌اجرا؛

(ه) اعلامیه انطباق اتحادیه اروپا اشاره‌شده در ماده ۴۸.

ماده ۵۱: ثبت

قبل از عرضه در بازار یا به خدمت گذاشتن یک سیستم هوش مصنوعی پرخطر که در ماده ۶ (۲) اشاره شده است، ارائه‌دهنده، یا در موارد لازم نماینده مجاز، باید آن سیستم را در پایگاه داده اتحادیه اروپا که در ماده ۶۰ ذکر شده است، ثبت کند.

بخش چهارم: وظایف مربوط به شفافیت برای سیستم‌های هوش مصنوعی خاص

ماده ۵۲: وظایف مربوط به شفافیت برای سیستم‌های هوش مصنوعی خاص

۱. عرضه‌کنندگان باید اطمینان حاصل کنند که سیستم‌های هوش مصنوعی که به قصد تعامل با اشخاص حقیقی هستند، به‌گونه‌ای طراحی شده و توسعه یافته‌اند که افراد حقیقی متوجه شوند که در حال تعامل با هوش مصنوعی هستند، مگر اینکه این امر از شرایط و بافتارِ استفاده، آشکار باشد. این وظیفه در مورد سیستم‌های هوش مصنوعی که قانوناً مجاز به کشف، پیشگیری، تحقیق و تعقیب جرایم جنایی هستند، اعمال نمی‌شود، مگر اینکه این سیستم‌ها برای گزارش جرائم جنایی در دسترس عموم باشند.

۲. کاربران یک سیستم تشخیص عواطف یا یک سیستم طبقه‌بندی بیومتریک باید افراد حقیقی را که در معرض آن قرار دارند از فعالیت سیستم مطلع سازند. این وظیفه برای سیستم‌های هوش مصنوعی که برای طبقه‌بندی بیومتریک استفاده می‌شوند و بر طبق قانون مجاز به کشف، پیشگیری و تحقیق جرایم جنایی هستند، اعمال نمی‌شود.

۳. کاربران یک سیستم هوش مصنوعی که محتوای تصویری، صوتی یا ویدیویی را تولید یا دستکاری می‌کند که شباهت زیادی به افراد، اشیاء، مکان‌ها یا سایر اشیاء یا رویدادهای موجود دارد و به اشتباه برای افراد، واقعی یا صادقانه به‌نظر می‌رسد، باید افشا کنند که محتوا به شکلی مصنوعی تولید یا دستکاری شده است.

۴. بندهای ۱، ۲ و ۳ بر الزامات و وظایف مندرج در عنوان سوم این قانون تأثیری نخواهد داشت.

بخش پنجم: اقدامات در حمایت از نوآوری

ماده ۵۳: محیط‌های آزمایشی برای تنظیم‌گری هوش مصنوعی

۱. محیط‌های آزمایشی تنظیم‌گری هوش مصنوعی که توسط یک یا چند مقام ذی‌صلاح کشور عضو یا ناظر اروپایی حفاظت از داده‌ها ایجاد شده‌اند، باید محیط کنترل‌شده‌ای فراهم کنند که توسعه، آزمایش و اعتبارسنجی سیستم‌های هوش مصنوعی نوآورانه را مبتنی بر یک برنامه مشخص برای مدت محدودی قبل از عرضه آنها در بازار یا به خدمت گذاشتن آنها تسهیل کند. این امر باید تحت نظارت و هدایت مستقیم مقامات ذی‌صلاح و با در نظر داشتن انطباق با الزامات این قانون و در صورت لزوم، سایر قوانین اتحادیه و کشورهای عضو تحت نظارت در محیط آزمایشی انجام شود.

۲. تا حدی که سیستم‌های هوش مصنوعی نوآورانه شامل پردازش داده‌های شخصی می‌شوند یا تحت صلاحیت نظارتی سایر مقامات ملی یا مقامات ذی‌صلاح ارائه‌دهنده یا حمایت‌کننده از دسترسی به داده‌ها، قرار می‌گیرند، کشورهای عضو باید اطمینان حاصل کنند که مقامات ملی حفاظت از داده‌ها و سایر مقامات ملی در مسئله فعالیت محیط آزمایشی تنظیم‌گری هوش مصنوعی وارد شوند.

۳. محیط‌های آزمایشی تنظیم‌گری هوش مصنوعی نباید بر اختیارات نظارتی و اصلاحی مقامات ذی‌صلاح تأثیر بگذارد. در صورت شناسایی هرگونه خطر قابل‌توجه برای سلامتی، ایمنی و حق‌های بنیادین در طول توسعه و آزمایش چنین سیستم‌هایی، باید فوراً اقدام به اصلاح کرد. در صورت عدم موفقیت اصلاح، باید تا زمانی که این اصلاحات صورت پذیرد، اقدام به تعلیق فرایند آزمایش و توسعه نمود.

۴. دست‌اندرکاران محیط‌های آزمایشی تنظیم‌گری هوش مصنوعی، باید تحت قوانین مربوط به مسئولیت اتحادیه و کشورهای عضو، مسئول هرگونه آسیبی باشند که به اشخاص ثالث در نتیجه آزمایش‌هایی وارد می‌شود که در محیط آزمایشی انجام می‌شود.

۵. مقامات ذی‌صلاح کشورهای عضو که محیط‌های آزمایشی تنظیم‌گری هوش مصنوعی ایجاد کرده‌اند، باید فعالیت‌های خود را هماهنگ کرده و در چارچوب هیئت هوش مصنوعی اروپا همکاری کنند. آنها باید گزارش‌های سالانه‌ای را در مورد نتایج حاصل از اجرای این طرح‌ها، ازجمله شیوه‌های مطلوب، درس‌های آموخته‌شده و توصیه‌هایی در مورد راه‌اندازی آنها و در صورت امکان، در مورد اعمال این قانون و سایر قوانین اتحادیه تحت نظارت در محیط آزمایشی به هیئت و کمیسیون ارائه دهند.

۶. نحوه و شرایط عملکرد محیط‌های آزمایشی تنظیم‌گری هوش مصنوعی، ازجمله معیارهای صلاحیت و روش درخواست، انتخاب، مشارکت و خروج از محیط آزمایشی و حقوق و وظایف شرکت‌کنندگان، در قوانین اجرایی تعیین می‌شود. این قوانین اجرایی باید طبق روند بررسی که در (۲)۷۴ بدانها اشاره شده است، اتخاذ گردند.

ماده ٥٤: پردازش بیشتر داده‌های شخصی برای توسعه سیستم‌های هوش مصنوعی خاص در راستای منافع عمومی در محیط آزمایشی تنظیم‌گری هوش مصنوعی

۱. محیط‌های آزمایشی تنظیم‌گری هوش مصنوعی، داده‌های شخصی که به‌طور قانونی برای مقاصدی جمع‌آوری شده‌اند، باید برای اهداف توسعه و آزمایش برخی از سیستم‌های هوش مصنوعی نوآورانه در محیط آزمایشی تحت شرایط زیر پردازش شوند:

(الف) سیستم‌های هوش مصنوعی نوآورانه باید برای حفاظت از منافع عمومی مهم در یک یا چند زمینه زیر توسعه داده شوند:

(۱) پیشگیری، تحقیق، کشف یا تعقیب جرایم جنایی یا اجرای مجازات‌های کیفری، ازجمله حفاظت و پیشگیری از تهدیدات امنیت عمومی، تحت کنترل و مسئولیت مقامات ذی‌صلاح. پردازش باید براساس قانون کشور عضو یا اتحادیه باشد؛

(۲) ایمنی و بهداشت عمومی، ازجمله پیشگیری، کنترل و درمان بیماری‌ها؛

(۳) سطح بالای حفاظت و بهبود کیفیت محیط زیست؛

(ب) داده‌های پردازش‌شده برای انطباق با یک یا چند مورد از الزامات ذکرشده در بخش ۳، فصل ۲ ضروری باشند؛ بدین صورت که امکان نداشته باشد که این الزامات به‌طور مؤثری با پردازش داده‌های ناشناس، مصنوعی یا سایر انواع داده‌های غیرشخصی برآورده شوند.

(ج) سازوکارهای نظارتی مؤثری جهت شناسایی خطرات مهم برای حقوق اساسی اشخاصی که اطلاعات درباره آنهاست، و همچنین سازوکار واکنش برای کاهش سریع این خطرات و در صورت لزوم توقف پردازش وجود داشته باشد.

(د) هرگونه داده شخصی که در چارچوب محیط آزمایشی پردازش می‌شود در یک محیط پردازش داده که از نظر عملکردی مجزا، ایزوله و محافظت شده است و تحت کنترل دست‌اندرکاران و صرفاً افرادی که مجاز به دسترسی به آن داده‌ها هستند، باشد.

(ه) هرگونه اطلاعات شخصی پردازش‌شده مخابره یا منتقل نشود و به انحا دیگر در دسترس طرف‌های دیگر قرار نگیرد.

(و) هرگونه پردازش داده‌های شخصی در محیط آزمایشی منجر به اقدامات یا تصمیماتی نشود که بر افرادی که داده‌ها درباره آنهاست، تأثیر بگذارد.

(ز) هرگونه داده شخصی پردازش‌شده در زمینه محیط آزمایشی پس از پایان مشارکت در محیط آزمایشی یا پایان دوره نگهداری داده‌های شخصی حذف گردد.

(ح) گزارش‌های فعالیت‌های مربوط به پردازش داده‌های شخصی در زمینه محیط آزمایشی برای مدت زمان مشارکت در محیط آزمایشی و ۱ سال پس از خاتمه آن، صرفاً به‌منظور و فقط تا زمانی که

برای انجام وظایف مسئولیت‌پذیری و مستندسازی مربوط به این ماده یا سایر قوانین اتحادیه یا کشورهای عضو ضروری باشد، نگهداری می‌شوند.

(ط) شرح کامل و دقیق فرایند و منطق پشت آموزش، آزمایش و اعتبارسنجی سیستم هوش مصنوعی همراه با نتایج آزمایش به‌عنوان بخشی از مستندات فنی در پیوست ۴ نگهداری می‌شود.

(ی) خلاصه‌ای کوتاه از پروژه هوش مصنوعی توسعه‌یافته در محیط آزمایشی، اهداف و نتایج مورد انتظار آن در وب‌سایت مقامات ذی‌صلاح منتشر می‌شود.

۲. بند ۱ در تعارض با قوانین اتحادیه یا کشورهای عضو نیست، مگر نسبت به پردازش‌هایی که برای مقاصدی غیر از مواردی که صریحاً در آن قانون ذکر شده است، انجام گردد.

ماده ۵۵: اقدامات ارائه‌دهندگان و استفاده‌کنندگان کوچک

۱. کشورهای عضو باید اقدامات زیر را انجام دهند:

(الف) ارائه‌دهندگان و شرکت‌های نوآفرین در مقیاس کوچک را، در صورت داشتن صلاحیت‌های لازم، نسبت به دسترسی به محیط‌های آزمایشی تنظیم‌گیری هوش مصنوعی در اولویت قرار دهند.

(ب) سازماندهی فعالیت‌های آگاهی‌بخش خاص در مورد اجرای این قوانین که متناسب با نیازهای ارائه‌دهندگان و کاربران در مقیاس کوچک باشد.

(ج) در شرایطی که امکانش هست، یک راه ارتباطی اختصاصی برای ارائه‌دهندگان، کاربران و سایر نوآوران در مقیاس کوچک جهت ارائه راهنمایی و پاسخ به سؤالات مربوط به اجرای این قوانین ایجاد کنند.

۲. منافع و نیازهای خاص ارائه‌دهندگان در مقیاس کوچک باید در هنگام تعیین هزینه‌های انطباق‌سنجی طبق ماده ۴۳ در نظر گرفته شود و این هزینه‌ها متناسب با مقیاس آنها و اندازه بازار آنها کاهش یابد.

بخش ششم: حاکمیت

فصل ۱: هیئت اروپایی هوش مصنوعی

ماده ٥٦: تأسیس هیئت اروپایی هوش مصنوعی

۱. هیئت اروپایی هوش مصنوعی (اختصاراً هیئت) تأسیس می‌گردد.

۲. هیئت باید در راستای موارد زیر به کمیسیون مشاوره و یاری دهد:

(الف) کمک به همکاری مؤثر مقامات ملی نظارتی و کمیسیون در رابطه با موضوعات تحت پوشش این قوانین؛

(ب) هماهنگی و کمک به راهنمایی و تحلیل کمیسیون و مقامات نظارتی ملی و سایر مقامات ذی‌صلاح در مورد مسائل نوظهور در سراسر بازار داخلی با توجه به موضوعات تحت پوشش این قوانین؛

(ج) کمک به مقامات نظارتی ملی و کمیسیون در حصول اطمینان از اجرای یکپارچه و منسجم این قوانین.

ماده ۵۷: ساختار هیئت

۱. این هیئت متشکل از مقامات نظارتی ملی است که باید توسط رئیس یا مسئول عالی‌رتبه معادل آن مقام و همچنین ناظر اروپایی حفاظت از داده‌ها نمایندگی شوند. سایر مقامات ملی را می‌توان در جلساتی که موضوعات مورد بحث مربوط به آنها می‌شود، دعوت کرد.

۲. هیئت باید آیین‌نامه داخلی خود را با اکثریت مطلق اعضای خود و با موافقت کمیسیون تصویب کند. آیین‌نامه داخلی همچنین باید شامل مسائل اجرایی مربوط به وظایف هیئت، مذکور در ماده ۵۸، باشد. هیئت می‌تواند به تناسب، کارگروه‌هایی را ذیل خود به‌منظور بررسی سؤالاتی خاص تشکیل دهد.

۳. ریاست هیئت به عهده کمیسیون خواهد بود. کمیسیون جلسات را تشکیل داده و دستور جلسه را مطابق با وظایف هیئت براساس این قوانین و همچنین آیین‌نامه داخلی تهیه می‌کند. کمیسیون باید به‌موجب این قانون، پشتیبانی اداری و تحلیلی برای فعالیت‌های هیئت فراهم کند.

۴. هیئت می‌تواند از کارشناسان و ناظران بیرونی دعوت کند در جلساتش شرکت کنند و می‌تواند با اشخاص ثالث ذی‌نفع مرتبط شود تا فعالیت‌های خود را به میزان مناسبی اطلاع‌رسانی کند. برای این منظور، کمیسیون می‌تواند ارتباط میان هیئت و سایر نهادها، دفاتر، آژانس‌ها و گروه‌های مشورتی اتحادیه را تسهیل نماید.

ماده ۵۸: وظایف هیئت

هنگام ارائه مشاوره و کمک به کمیسیون در چارچوب ماده (۲)۵۶، هیئت موظف به موارد زیر است:

(الف) گردآوری و فراهم کردن تخصص‌ها و شیوه‌های مطلوب و به اشتراک گذاشتن آنها با کشورهای عضو؛

(ب) کمک در راستای یکسان کردن روندهای اداری در کشورهای عضو، ازجمله عملکرد محیط‌های آزمایشی ذکرشده در ماده ۵۳؛

(ج) ارائه نظرها، توصیه‌ها یا مشارکت در مسائل مربوط به اجرای این قوانین با ارائه‌های مکتوب، به‌ویژه در موارد زیر:

(۱) در مورد مشخصات فنی یا استانداردهای موجود در مورد الزامات مندرج در بخش ۳، فصل ۲؛

(۲) در مورد استفاده از استانداردهای هماهنگ‌شده یا مشخصات مشترک مذکور در مواد ۴۰ و ۴۱؛

(۳) در مورد تنظیم اسناد راهنما، ازجمله دستورالعمل‌های مربوط به تعیین جریمه‌های اداری مذکور در ماده ۷۱.

فصل ۲: مراجع ذی‌صلاح ملی

ماده ۵۹: تعیین مراجع ذی‌صلاح ملی

۱. مقامات ذی‌صلاح ملی باید توسط هر کشور عضو به‌منظور اطمینان از اعمال و اجرای این قوانین ایجاد یا تعیین گردند. مقامات ذی‌صلاح ملی باید به‌گونه‌ای سازماندهی شوند که از واقع‌گرایی و بی‌طرفی فعالیت‌ها و وظایف خود حراست کنند.

۲. هر کشور عضو یک مقام نظارتی ملی را از بین مقامات ذی‌صلاح ملی تعیین خواهد کرد. مقام ناظر ملی به‌عنوان مرجع صدور مجوز و مرجع نظارت بر بازار عمل می‌کند، مگر اینکه یک کشور عضو به دلایل سازمانی و اداری بخواهد بیش از یک مرجع داشته باشد.

۳. کشورهای عضو باید کمیسیون را از تعیین یا تعیین‌های خود و در صورت امکان، از دلایل تعیین بیش از یک مرجع، مطلع کنند.

۴. کشورهای عضو باید اطمینان حاصل کنند که مقامات ذی‌صلاح ملی منابع مالی و انسانی کافی برای انجام وظایف خود براساس این مقررات را در اختیار دارند. به‌ویژه مقامات ذی‌صلاح ملی باید به تعداد کافی و به‌طور دائم پرسنلی در دسترس داشته باشند که صلاحیت‌ها و تخصص آنها شامل درکی عمیق از فناوری‌های هوش مصنوعی، داده‌ها و محاسبات داده‌ها، حقوق اساسی، خطرات بهداشتی، ایمنی و آگاهی از استانداردهای موجود و الزامات قانونی باشد.

۵. کشورهای عضو باید هر سال در مورد وضعیت منابع مالی و انسانی مقامات ذی‌صلاح ملی و همچنین ارزیابی شایستگی آنها به کمیسیون گزارش دهند. کمیسیون باید اطلاعات مذکور را برای بحث و پیشنهادهای احتمالی به هیئت ارسال کند.

۶. کمیسیون باید تبادل تجربه بین مقامات ذی‌صلاح ملی را تسهیل کند.

۷. مقامات ذی‌صلاح ملی می‌توانند در مورد اعمال این قوانین راهنمایی و مشاوره، ازجمله به ارائه‌دهندگان در مقیاس کوچک، بدهند. اگر مقامات ذی‌صلاح ملی قصد ارائه راهنمایی و مشاوره در رابطه با سیستم هوش مصنوعی در زمینه‌های تحت پوشش سایر قوانین اتحادیه را داشته باشند، در صورت اقتضا با مقامات ملی ذی‌صلاح تحت آن قانون مشورت خواهد شد. کشورهای عضو همچنین می‌توانند یک نقطه تماس مرکزی برای ارتباط با اپراتورها ایجاد کنند.

۸. مرجع ذی‌صلاح برای نظارت بر مؤسسات، آژانس‌ها و نهادهای اتحادیه که مشمول این قوانین هستند، ناظر اروپایی حفاظت از داده‌ها خواهد بود.

بخش هفتم: پایگاه داده اتحادیه اروپا برای سیستم‌های هوش مصنوعی مستقل پرخطر

ماده ٦٠: پایگاه داده اتحادیه اروپا برای سیستم‌های هوش مصنوعی مستقل پرخطر

۱. کمیسیون، با همکاری کشورهای عضو، پایگاه داده اتحادیه اروپا راه‌اندازی و نگهداری خواهد کرد که حاوی اطلاعات ذکرشده در بند ۲ در مورد سیستم‌های هوش مصنوعی پرخطر ذکرشده در ماده (۲)۶ است که مطابق با ماده ۵۱ ثبت شده‌اند.

۲. داده‌های فهرست‌شده در پیوست هشتم باید توسط ارائه‌دهندگان در پایگاه داده اتحادیه اروپا وارد شود. کمیسیون نیز باید حمایت فنی و اداری را از آنها فراهم کند.

۳. اطلاعات موجود در پایگاه داده اتحادیه اروپا باید در دسترس عموم باشد.

۴. اطلاعات شخصی تنها زمانی که برای جمع‌آوری و پردازش اطلاعات مطابق با این مقررات ضروری باشد وارد پایگاه داده اتحادیه اروپا خواهند شد. این اطلاعات باید شامل نام و مشخصات تماس اشخاص حقیقی‌ای باشد که مسئولیت ثبت سیستم را بر عهده دارند و دارای اختیار قانونی برای نمایندگی ارائه‌دهنده هستند.

۵. کمیسیون باید کنترل‌کننده پایگاه داده اتحادیه اروپا باشد. همچنین باید از پشتیبانی فنی و اداری کافی از ارائه‌دهندگان اطمینان حاصل کند.

بخش هشتم: رصد پس از فروش، اشتراک‌گذاری اطلاعات، نظارت بر بازار

فصل ۱: رصد پس از فروش

ماده ٦١: رصد پس از فروش توسط ارائه‌دهندگان و طرح نظارت پس از فروش برای سیستم‌های هوش مصنوعی پرخطر

۱. ارائه‌دهندگان باید سیستم نظارت پس از عرضه به بازار را به‌گونه‌ای ایجاد و مستند کنند که با ماهیت فناوری‌های هوش مصنوعی و خطرات سیستم هوش مصنوعی پرخطر متناسب باشد.

۲. سیستم رصد پس از فروش باید به‌طور فعال و نظام‌مندی داده‌های مرتبط ارائه‌شده توسط کاربران یا جمع‌آوری‌شده از سایر منابع در مورد عملکرد سیستم‌های هوش مصنوعی پرخطر در طول عمر آنها را جمع‌آوری، مستندسازی و تجزیه و تحلیل کند و به ارائه‌دهنده اجازه دهد تا انطباق سیستم‌های هوش مصنوعی با الزامات مندرج در بخش۳، فصل ۲ را به‌طور دائم ارزیابی کند.

۳. سیستم رصد پس از فروش باید براساس طرح نظارتی پس از فروش باشد. طرح نظارت پس از فروش باید بخشی از مستندات فنی ذکرشده در پیوست ۴ باشد. کمیسیون باید قانون اجرایی را اتخاذ کند که مقررات دقیقی برای ایجاد الگویی جهت طرح نظارت پس از بازار و فهرست عناصری که باید در این طرح گنجانده می‌شود، وضع کند. کمیسیون باید قانون اجرایی را تصویب کند که مقررات دقیقی برای ایجاد چارچوبی جهت طرح نظارت پس از فروش و فهرست عناصری که باید در این طرح گنجانده شود، مشخص کند.

۴. برای سیستم‌های هوش مصنوعی پرخطر تحت پوشش اقدامات قانونی ذکرشده در ضمیمه ۲، در مواردی که سیستم و طرح رصد پس از فروش طبق آن قانون قبلاً ایجاد شده است، عناصر شرح‌داده‌شده در بندهای ۱، ۲ و ۳ باید به تناسب در آن سیستم و طرح ادغام شوند.

زیربند اول همچنین در مورد سیستم‌های هوش مصنوعی پرخطر ذکرشده در بند ۵ (ب) ضمیمه ۳ که توسط مؤسسات اعتباری مشمول قانون EU/۳۶/۲۰۱۳ در بازار عرضه یا به خدمت گذاشته شده‌اند، اعمال می‌شود.

فصل ۲: اشتراک گذاری اطلاعات هنگام بروز حوادث و اختلالات

ماده ٦٢: گزارش حوادث خطیر و اختلالات

۱. ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر که در بازار اتحادیه عرضه شده‌اند، باید هرگونه حادثه جدی یا اختلال عملکرد در این سیستم‌ها را که خلاف وظایف مندرج در قوانین اتحادیه می‌باشند، قوانینی که جهت حمایت از حق‌های بنیادین در نظر گرفته شده‌اند، به مقامات نظارت بر بازار کشورهای عضوی که در آنجا آن حادثه یا تخلف رخ داده است، اطلاع دهند.

چنین اطلاع‌رسانی باید بلافاصله پس از اینکه ارائه‌دهنده رابطه علّی بین سیستم هوش مصنوعی و حادثه یا سوء عملکرد را تشخیص داد یا احتمال منطقی چنین رابطه‌ای را داد، صورت پذیرد، و در هر صورت حداکثر ۱۵ روز پس از اطلاع ارائه‌دهندگان از حادثه جدی یا سوء عملکرد باید انجام پذیرد.

۲. به محض دریافت اخطار مربوط به تخلف از وظایف مندرج در قانون اتحادیه که مربوط به حمایت از حق‌های بنیادین هستند، مقام نظارت بر بازار باید به مقامات عمومی ملی یا نهادهای مذکور در بند ۳ ماده ۶۴ اطلاع دهد. کمیسیون باید دستورالعملی اختصاصی جهت تسهیل انطباق با وظایف مندرج در بند ۱ ایجاد کند. این دستورالعمل حداکثر ۱۲ ماه پس از لازم‌الاجرا شدن این مقررات صادر خواهد شد.

۳. برای سیستم‌های هوش مصنوعی پرخطر اشاره‌شده در بند ۵ (ب) ضمیمه ۳ که توسط ارائه‌دهندگانی که مؤسسات اعتباری تحت مشمول قانون EU/۳۶/۲۰۱۳ هستند، در بازار عرضه یا به خدمت گذاشته می‌شوند. همچنین برای سیستم‌های هوش مصنوعی پرخطر که جزء بخش ایمنی دستگاه‌ها هستند یا خود دستگاه‌هایی هستند که تحت پوشش قانون (EU) ۷۴۵/۲۰۱۷ و قانون (EU) ۷۴۶/۲۰۱۷ قرار می‌گیرند، اطلاع‌رسانی در مورد حوادث خطیر یا سوء عملکرد باید به مواردی محدود شود که تخلف از وظایف براساس قوانین اتحادیه برای حمایت از حق‌های بنیادین محسوب می‌گردند.

فصل ۳: اجرا

ماده ۶۳: نظارت بر بازار و کنترل سیستم‌های هوش مصنوعی در بازار اتحادیه

۱. قانون (EU) ۱۰۲۰/۲۰۱۹ برای سیستم‌های هوش مصنوعی تحت پوشش این قانون اعمال می‌شود. با این حال، به‌منظور اجرای مؤثر این قانون:

(الف) هرگونه ارجاع به یک فعال اقتصادی تحت مقررات (EU) ۱۰۲۰/۲۰۱۹ باید به‌مثابه ارجاع به تمام اپراتورهای شناسایی‌شده در بخش ۳، فصل ۳ این قانون تلقی شود.

(ب) هرگونه ارجاع به محصولی تحت مقررات (EU) ۱۰۲۰/۲۰۱۹ باید به ارجاع به تمام سیستم‌های هوش مصنوعی در محدوده این مقررات تلقی گردد.

۲. مقام ناظر ملی باید نتایج فعالیت‌های مرتبط با نظارت بر بازار را به‌طور منظم به کمیسیون گزارش دهد. مقام ناظر ملی باید هرگونه اطلاعات شناسایی‌شده در جریان فعالیت‌های نظارت بر بازار را که ممکن است برای اجرای قانون اتحادیه در مورد قوانین رقابت مورد توجه باشد، بدون تأخیر به کمیسیون و مقامات رقابت ملی مربوطه منتقل کند.

۳. برای سیستم‌های هوش مصنوعی پرخطری که مربوط هستند به محصولاتی که اقدامات قانونی فهرست‌شده در ضمیمه۲ بخش الف در مورد آنها اعمال می‌شود، مرجع نظارت بر بازار برای اهداف این قانون، مقام مسئول فعالیت‌های نظارت بر بازار تعیین‌شده تحت آن اقدامات قوانین خواهد بود.

۴. برای سیستم‌های هوش مصنوعی که توسط مؤسسات مالیِ مشمولِ قوانین اتحادیه در مورد خدمات مالی، در بازار عرضه یا به خدمت گذاشته می‌شوند، مرجع نظارت بر بازار برای اهداف این قانون، مرجع مربوطه مسئول نظارت مالی آن مؤسسات تحت آن قانون خواهد بود.

۵. برای سیستم‌های هوش مصنوعی فهرست‌شده در بند ۱ (الف) که برای اهداف اجرای قانون، موارد ۶ و ۷ ضمیمه ۳ استفاده می‌شوند، کشورهای عضو باید مقامات ذی‌صلاح نظارت بر حفاظت از داده‌ها را براساس قانون (EU) ۶۸۰/۲۰۱۶، یا ۶۷۹/۲۰۱۶ یا مقامات ذی‌صلاح ملی را که بر فعالیت‌های اجرای قانون، مهاجرت یا پناهندگی با استفاده یا به خدمت گذاشتن این سیستم‌ها، نظارت می‌کنند، به‌عنوان مقامات نظارت بر بازار تعیین کرد.

۶. در مواردی که مؤسسات، آژانس‌ها و نهادهای اتحادیه در محدوده این مقررات قرار می‌گیرند، ناظر اروپایی حفاظت از داده‌ها، مرجع آنها در نظارت بر بازار خواهد بود.

۷. کشورهای عضو باید هماهنگی بین این دو مقام مسئول را تسهیل کنند: مقامات نظارت بر بازار، که براساس این مقررات تعیین شده‌اند، و سایر مقامات یا نهادهای ملی مربوطه که بر اجرای قوانین هماهنگ‌سازی اتحادیه مندرج در پیوست ۲ یا سایر قوانین اتحادیه که ممکن است به سیستم‌های هوش مصنوعی پرخطر ذکرشده در پیوست ۳ مربوط باشد، نظارت می‌کنند.

ماده ٦٤: دسترسی به اطلاعات و مستندات

۱. در راستای دسترسی به داده‌ها و اسناد در چارچوب فعالیت‌های خود، باید به مقامات نظارت بر بازار، دسترسی کامل به مجموعه داده‌های آموزشی، اعتبارسنجی و آزمایشی که توسط ارائه‌دهنده استفاده می‌شود، داده شود؛ ازجمله از طریق رابط‌های برنامه‌های کاربردی[1] یا سایر ابزارها و وسایل فنی مناسب که امکان دسترسی از راه دور را فراهم می‌کند.

۲. در صورت لزوم برای انطباق‌سنجی سیستم هوش مصنوعی پرخطر با الزامات مندرج در بخش ۳، فصل ۲ و بنا به درخواست مستدل، مقامات نظارت بر بازار باید به کد منبع سیستم هوش مصنوعی دسترسی داشته باشند.

۳. مقامات یا نهادهای عمومی ملی که بر رعایت وظایف مربوط به قانون اتحادیه در حمایت از حق‌های بنیادین در رابطه با استفاده از سیستم‌های هوش مصنوعی پرخطر ذکرشده در پیوست ۳ نظارت دارند یا آنها را اجرا می‌کنند، در مواردی که برای انجام موارد تحت امر آنها در محدوده صلاحیتشان ضروری است، نسبت به درخواست و دسترسی به هر سندی که تحت این قانون ایجاد یا نگهداری می‌شود، اختیار قانونی دارند.

۴. تا ۳ ماه پس از لازم‌الاجرا شدن این قانون، هر کشور عضو باید مقامات یا سازمان‌های عمومی اشاره‌شده در بند ۳ را شناسایی کرده و فهرستی را در وب‌سایت مرجع ملی نظارت در دسترس عموم قرار دهد. کشورهای عضو باید فهرست را به کمیسیون و سایر کشورهای عضو اطلاع دهند و فهرست را به‌روز نگه دارند.

۵. در مواردی که مستندات ذکرشده در بند ۳ برای حصول اطمینان از اینکه آیا تخلف از وظایف مندرج در قانون مربوط به حق‌های بنیادینِ اتحادیه رخ داده است، کافی نیست، مرجع عمومی یا نهادی که در بند ۳ اشاره شده است می‌تواند از مرجع نظارت بر بازار درخواست مستدلی از مرجع نظارت بر بازار جهت انجام آزمایش

1. API

سیستم هوش مصنوعی پرخطر از طریق ابزارهای فنی ارائه کند. مرجع نظارت بر بازار باید آزمایش را با مشارکت نزدیک مقام یا نهاد عمومی درخواست‌کننده در مدت زمان معقولی پس از درخواست سازماندهی کند.

۶. در مواجهه با هرگونه اطلاعات و اسنادی که توسط مقامات یا نهادهای عمومی ملی مذکور در بند ۳ به‌موجب مفاد این ماده به‌دست می‌آید، باید مطابق موازین اصول محرمانگی مندرج در ماده ۷۰ رفتار شود.

ماده ٦٥: روند مواجهه با سیستم‌های هوش مصنوعی که خطراتی در سطح ملی ایجاد می‌کنند

۱. اگر سیستم‌های هوش مصنوعی مخاطره‌آمیز، خطراتی را برای سلامتی یا ایمنی یا حمایت از حق‌های بنیادین افراد ایجاد کنند، باید به‌عنوان محصولی در نظر گرفته شوند که خطری ارائه می‌کنند که در ماده ۳، بند ۱۹ قانون (EU) ۱۰۲۰/۲۰۱۹ تعریف شده است.

۲. درصورتی‌که مرجع نظارت بر بازار یک کشور عضو دلایل کافی برای مخاطره‌آمیز بودن یک سیستم هوش مصنوعی، چنان‌که در بند ۱ اشاره شده است، داشته باشد، باید ارزیابی‌ای از سیستم هوش مصنوعی مربوطه در مورد انطباق آن با کلیه الزامات و وظایف مندرج در این قانون انجام دهد. هنگامی که خطراتی متوجه حفاظت از حق‌های بنیادین وجود داشته باشد، مقام نظارت بر بازار باید به مقامات یا نهادهای عمومی ملی مربوطه اشاره‌شده در بند ۳ ماده ۶۴ نیز اطلاع دهد. فعالان مربوطه باید در صورت لزوم با مقامات نظارت بر بازار و سایر مقامات عمومی ملی یا نهادهای مذکور در بند ۳ ماده ۶۴ همکاری کنند.

درصورتی‌که در جریان آن ارزیابی، مرجع نظارت بر بازار متوجه شود که سیستم هوش مصنوعی با الزامات و وظایف مندرج در این قانون مطابقت ندارد، بدون تأخیر باید فعال مربوطه را ملزم به انجام کلیه اقدامات اصلاحی مناسب برای مطابق کردن سیستم هوش مصنوعی نماید، که بنابر صلاحدید شامل اقداماتی همچون جمع‌آوری تمام سیستم‌های هوش مصنوعی مربوطه از بازار یا فرخوان برای پس گرفتن در یک دوره متناسب با ماهیت خطر می‌شود.

مرجع نظارت بر بازار مراتب را به اطلاع نهاد دارای مجوز خواهد رساند. ماده ۱۸ مقررات (EU) ۱۰۲۰/۲۰۱۹ در مورد اقدامات ذکرشده در زیربند دوم اعمال می‌شود.

۳. درصورتی‌که مرجع نظارت بر بازار تشخیص دهد که عدم رعایت محدود به قلمرو ملی نیست، باید کمیسیون و سایر کشورهای عضو را از نتایج ارزیابی و اقداماتی که از فعال مربوطه خواسته است، مطلع کند.

۴. فعال مربوطه باید اطمینان حاصل کند که تمام اقدامات اصلاحی مناسب در رابطه با تمام سیستم‌های هوش مصنوعی مربوطه که در بازارهای اتحادیه در دسترس قرار داده است، انجام می‌شود.

۵. درصورتی‌که فعال مربوط به یک سیستم هوش مصنوعی اقدامات اصلاحی کافی را در مدت زمان مذکور در بند ۲ انجام ندهد، مرجع نظارت بر بازار باید تمام اقدامات احتیاطی مناسب را جهت ممنوعیت یا محدودیت عرضه سیستم هوش مصنوعی در بازار ملی خود اتخاذ کند؛ بدین صورت که محصول را از بازار خارج کند یا

فراخوان پس گرفتن دهد. آن مقام باید کمیسیون و سایر کشورهای عضو را بدون تأخیر از این اقدامات مطلع سازد.

۶. اطلاعات اشاره‌شده در بند ۵ باید شامل تمام جزئیات موجود، به‌ویژه داده‌های لازم برای شناسایی سیستم هوش مصنوعی غیرمنطبق، منشأ سیستم هوش مصنوعی، ماهیت عدم انطباق ادعاشده و خطرات مربوطه باشد. همچنین باید شامل ماهیت و مدت اقدامات ملی انجام‌شده و استدلال‌های ارائه‌شده توسط فعال مربوطه نیز باشد. به‌ویژه مقامات نظارت بر بازار باید مشخص کنند که آیا عدم انطباق به دلیل یک یا چند مورد از موارد زیر است یا نه:

(الف) عدم برآوردن الزامات مندرج در بخش ۳، فصل ۲ توسط سیستم هوش مصنوعی؛

(ب) نقص در استانداردهای هماهنگ‌شده یا مشخصات مشترک ذکرشده در مواد ۴۰ و ۴۱ که فرض انطباق را محقق می‌کنند.

۷. مقامات نظارت بر بازار کشورهای عضو به غیر از مرجع نظارت بر بازار کشور عضوی که روند را آغاز می‌کند، باید بدون تأخیر کمیسیون و سایر کشورهای عضو را نسبت به این موارد آگاه بسازد: هرگونه تدابیر اتخاذشده و هرگونه اطلاعات اضافی و در اختیار آنها در رابطه با عدم انطباق سیستم هوش مصنوعی مربوطه، و در صورت عدم موافقت با اقدام ملی اعلام‌شده، اعتراضات آنها.

۸. درصورتی‌که ظرف سه ماه پس از دریافت اطلاعات مذکور در بند ۵، هیچ اعتراضی از سوی یک کشور عضو یا کمیسیون در رابطه با اقدام موقت اتخاذشده توسط یک کشور عضو مطرح نشده باشد، آن اقدام موجه تلقی خواهد شد. این امر در تعارض با حقوق دادرسی فعال مربوطه مندرج در ماده ۱۸ قانون (EU) ۱۰۲۰/۲۰۱۹ نیست.

۹. مقامات نظارت بر بازار در همه کشورهای عضو باید اطمینان حاصل کنند که اقدامات محدودکننده مناسب در رابطه با محصول مورد نظر، مانند خروج محصول از بازار آنها، بدون تأخیر انجام شود.

ماده ٦٦: روند محافظتی اتحادیه

۱. درصورتی‌که ظرف سه ماه پس از دریافت اطلاعات مذکور در بند ۵ ماده ۶۵، اعتراضاتی از سوی یک کشور عضو علیه اقدام قانونی که توسط یک کشور عضو دیگر انجام شده است، مطرح گردد، یا زمانی که کمیسیون اقدام مذکور را مغایر با قوانین اتحادیه بداند، کمیسیون باید بدون تأخیر با کشور عضو مربوطه و همچنین با فعال یا فعالین مربوطه مشورت کند و اقدام ملی مذکور را ارزیابی نماید. براساس نتایج آن ارزیابی، کمیسیون باید ظرف ۹ ماه پس از دریافت اطلاعات مذکور در بند ۵ ماده ۶۵ تصمیم بگیرد که آیا اقدام قانونی ملی موجه بوده است یا خیر و این تصمیم را به کشور عضو مربوطه اطلاع دهد.

۲. اگر اقدام ملی موجه تلقی شود، همهٔ کشورهای عضو باید اقدامات لازم را برای اطمینان از خروج سیستم هوش مصنوعی غیرمنطبق از بازارشان انجام دهند و کمیسیون را در جریان آن قرار دهند. اگر اقدام ملی غیرقابل‌توجیه تلقی شود، کشور عضو مربوطه باید اقدام قانونی مذکور را لغو کند.

۳. در مواردی که اقدام ملی موجه تلقی شود و عدم انطباق با سیستم هوش مصنوعی به نقص استانداردهای هماهنگ‌شده یا مشخصات مشترک مذکور در مواد ۴۰ و ۴۱ این قانون نسبت داده شود، کمیسیون روند مقرر در ماده ۱۱ از قانون (EU)۲۰۱۲/۱۰۲۵ را اعمال خواهد کرد.

ماده ٦٧: سیستم‌های هوش مصنوعی منطبق بر قوانین اما مخاطره‌آمیز

۱. در مواردی که پس از انجام ارزیابی براساس ماده ۶۵، مرجع نظارت بر بازار یک کشور عضو متوجه می‌شود که گرچه یک سیستم هوش مصنوعی با این قوانین مطابقت دارد، اما خطری برای سلامتی یا ایمنی افراد یا برای پیروی از وظایف مندرج در قوانین اتحادیه یا قوانین ملی حمایت از حق‌های بنیادین یا سایر جنبه‌های حفاظت از منافع عمومی ایجاد می‌کند، در این موارد باید فعال مربوطه را ملزم کند تا تمام اقدامات مناسب را انجام دهد برای حصول اطمینان از اینکه سیستم هوش مصنوعی مربوطه، هنگام عرضه به بازار یا به خدمت گذاردن، زین پس خطر مذکور را ایجاد نمی‌کند. این اقدامات شامل خارج کردن سیستم هوش مصنوعی از بازار یا فراخوانی آن در یک دوره معقول، متناسب با ماهیت خطر بنابر صلاحدید، خواهد بود.

۲. ارائه‌دهنده یا سایر فعالان مربوطه باید اطمینان حاصل کنند که اقدامات اصلاحی در رابطه با تمام سیستم‌های هوش مصنوعی مربوطه که در بازار اتحادیه عرضه کرده‌اند، در بازه زمانی تعیین‌شده توسط مقام نظارت بر بازار کشور عضو مذکور در بند ۱ انجام می‌شود.

۳. کشور عضو باید بلافاصله به کمیسیون و سایر کشورهای عضو اطلاعات را منتقل کند. این اطلاعات باید شامل تمام جزئیات موجود باشد، به‌ویژه داده‌های لازم برای شناسایی سیستم هوش مصنوعی مربوطه، منشأ و زنجیره عرضه سیستم هوش مصنوعی، ماهیت خطر و همچنین ماهیت و مدت زمان اقدامات ملی انجام‌شده.

۴. کمیسیون باید بدون تأخیر با کشورهای عضو و فعال مربوطه مشورت نماید و اقدامات ملی اتخاذشده را ارزیابی کند. براساس نتایج آن ارزیابی، کمیسیون تصمیم خواهد گرفت که آیا آن اقدام موجه بوده یا خیر و به تناسب، اقدامات مناسب را پیشنهاد خواهد کرد.

۵. کمیسیون باید تصمیم خود را برای کشورهای عضو ارسال کند.

ماده ٦٨: عدم انطباق شکلی

۱. درصورتی‌که مرجع نظارت بر بازار یک کشور عضو به یکی از یافته‌های زیر دست یابد، از ارائه‌دهنده مربوطه می‌خواهد که به عدم انطباق پایان دهد:

(الف) علامت انطباق برخلاف ماده ۴۹ الصاق شده باشد.

(ب) علامت انطباق الصاق نشده باشد.

(ج) اعلامیه انطباق اتحادیه اروپا تنظیم نشده باشد.

(د) اعلامیه انطباق اتحادیه اروپا به‌درستی تنظیم نشده باشد.

(ه) شماره شناسایی نهاد دارای مجوز، که در فرایند انطباق‌سنجی شرکت داشته و امکان الصاق داشته است، الصاق نشده باشد.

۲. در صورت تداوم عدم انطباق مندرج در بند ۱، کشور عضو مربوطه باید تمام اقدامات مناسب را برای محدود کردن یا ممنوعیت عرضهٔ سیستم هوش مصنوعی پرخطر در بازار یا اطمینان از فراخوانی یا خروج آن از بازار انجام دهد.

بخش نهم: آیین‌نامه رفتاری

ماده ٦٩: آیین‌نامه رفتاری

۱. کمیسیون و کشورهای عضو باید تدوین آیین‌نامه رفتاری را تشویق و تسهیل کنند که انطباق داوطلبانه سیستم‌های هوش مصنوعی غیرپرخطر بر الزامات مندرج در بخش ۲ عنوان ۳ را ترویج می‌کنند. انطباقی که براساس مشخصات فنی و راه‌حل‌هایی است که ابزار مناسبی برای اطمینان از انطباق با چنین الزاماتی در پرتو هدف موردنظر سیستم‌ها هستند.

۲. کمیسیون و هیئت باید تدوین آیین‌نامه رفتاری را تشویق و تسهیل کنند که انطباق داوطلبانه سیستم‌های هوش مصنوعی بر الزاماتی را ترویج دهد که مربوط به مواردی از این دست هستند: پایداری محیطی، دسترسی برای افراد دارای معلولیت، مشارکت سهامداران در طراحی و توسعه سیستم‌های هوش مصنوعی و تنوع تیم‌های توسعه براساس اهداف روشن و شاخص‌های عملکرد کلیدی برای اندازه‌گیری دستیابی به آن اهداف.

۳. تدوین آیین‌نامه رفتاری می‌تواند توسط ارائه‌دهندگان سیستم‌های هوش مصنوعی یا سازمان‌هایی که نمایندهٔ آنها هستند یا توسط هر دو و همچنین می‌تواند با مشارکت کاربران یا سهامداران ذی‌نفع و سازمان‌های نماینده آنها تهیه شود. منشورهای اخلاقی می‌توانند یک یا چند سیستم هوش مصنوعی را با در نظر گرفتن شباهت هدف آن سیستم‌ها پوشش دهند.

۴. کمیسیون و هیئت هنگام تشویق و تسهیل تهیه آیین‌نامه رفتاری، باید علایق و نیازهای خاص ارائه‌دهندگان در مقیاس کوچک و شرکت‌های نوپا را در نظر بگیرد.

بخش دهم: محرمانگی و مجازات

ماده ۷۰: محرمانگی

۱. مقامات ذی‌صلاح ملی و نهادهای دارای مجوز که در اجرای این قانون مشارکت دارند باید در انجام وظایف و فعالیت‌های خود، محرمانه بودن اطلاعات و داده‌های به‌دست‌آمده را به‌گونه‌ای لحاظ کنند که به‌ویژه از موارد زیر محافظت شود:

(الف) حقوق مالکیت معنوی و اطلاعات تجاری محرمانه یا اسرار تجاری یک شخص حقیقی یا حقوقی، ازجمله کد منبع، به‌استثنای موارد ذکرشده در ماده ۵ قانون ۹۴۳/۲۰۱۶ در مورد حفاظت از دانش فنی و اطلاعات تجاری فاش‌نشده (اسرار تجاری) علیه کسب، استفاده و درخواست افشای آنها؛

(ب) اجرای مؤثر این قانون، به‌ویژه به‌منظور بازرسی، تحقیقات یا ممیزی؛

(ج) منافع امنیت عمومی و ملی؛

(د) یکپارچگی دادرسی کیفری یا اداری.

۲. بدون خلل به بند ۱، هنگامی که سیستم‌های هوش مصنوعی پرخطر ذکرشده در نکات ۱، ۶ و ۷ ضمیمه ۳ توسط مقامات مجری قانون، مهاجرت یا پناهندگی استفاده می‌شوند، اطلاعات مبادله‌شده به‌صورت محرمانه میان خود مقامات ذی‌صلاح ملی و همچنین میان مقامات ذی‌صلاح ملی و کمیسیون، نباید زمانی که افشاگری این اطلاعات منافع عمومی و امنیت ملی را به خطر می‌اندازد بدون مشورت قبلی مرجع ذی‌صلاح ملی مبدأ و کاربر فاش شود.

هنگامی که مقامات مجری قانون، مهاجرت یا پناهندگی، خود ارائه‌دهندگان سیستم‌های هوش مصنوعی پرخطر ذکرشده در نکات ۱، ۶ و ۷ ضمیمه ۳ باشند، اسناد فنی ذکرشده در پیوست ۴ در محل اقامت آن مقامات باقی می‌ماند. این مقامات باید اطمینان حاصل کنند که مقامات نظارت بر بازار در صورت امکان و درخواست، فوراً به اسناد دسترسی داشته باشند یا یک نسخه از آن را دریافت کنند. فقط کارکنان مرجع نظارت بر بازار که دارای سطح مناسبی از مجوز امنیتی هستند، مجاز به دسترسی به آن اسناد یا کپی آن خواهند بود.

۳. بندهای ۱ و ۲ بر حقوق و وظایف کمیسیون، کشورهای عضو و نهادهای دارای مجوز در رابطه با مبادله اطلاعات و انتشار هشدارها و همچنین وظایف طرف‌های ذی‌نفع برای ارائه اطلاعات براساس قوانین جزایی کشورهای عضو تأثیری نخواهد داشت.

۴. کمیسیون و کشورهای عضو می‌توانند در صورت لزوم، اطلاعات محرمانه را با مقامات نظارتی کشورهای ثالثی مبادله کنند که با آنها قراردادهای محرمانه دوجانبه یا چندجانبه - که ضامن سطحی کافی از محرمانگی است - منعقد کرده‌اند.

ماده ۷۱: مجازات‌ها

۱. در راستای پیروی از مقررات این قانون، کشورهای عضو باید قوانینی مربوط به مجازات‌ها وضع نمایند؛ ازجمله جریمه‌های اداری که قابل‌اعمال در موارد نقض این قانون باشند و همچنین باید تمام اقدامات لازم را برای اطمینان از اجرای صحیح و مؤثر آن قوانین انجام دهند. مجازات‌های پیش‌بینی‌شده باید مؤثر، متناسب و بازدارنده باشد. آنها خصوصاً باید منافع ارائه‌دهندگان در مقیاس کوچک و شرکت‌های نوپا و توانایی اقتصادی آنها را در نظر بگیرند.

۲. کشورهای عضو باید قوانین و اقدامات مذکور و همچنین هرگونه اصلاحیه بعدی را که بر آنها تأثیر می‌گذارد، بدون تأخیر به کمیسیون اطلاع دهند.

۳. تخلفات زیر مشمول جریمه‌های اداری تا سقف ۳۰ میلیون یورو یا درصورتی‌که متخلف شرکت باشد تا ۶ درصد از کل گردش مالی سالانه جهانی آن برای سال مالی قبل، هر کدام که بیشتر باشد، خواهد بود:

(الف) عدم رعایت موارد ممنوعیت استفاده از هوش مصنوعی مذکور در ماده ۵؛

(ب) عدم رعایت الزامات مندرج در ماده ۱۰.

۴. عدم انطباق سیستم هوش مصنوعی با هریک از الزامات یا وظایف مندرج در این قانون، به غیر از موارد مندرج در مواد ۵ و ۱۰، مشمول جریمه اداری تا سقف ۲۰ میلیون یورو خواهد بود یا اگر متخلف یک شرکت باشد، تا ۴ درصد از کل گردش مالی سالانه جهانی آن برای سال مالی قبل، هر کدام که بیشتر باشد.

۵. ارائه اطلاعات نادرست، ناقص یا گمراه‌کننده در پاسخ به درخواست‌های نهادهای دارای مجوز و مراجع ذی‌صلاح ملی، مشمول جریمه‌های اداری تا سقف ۱۰ میلیون یورو خواهد بود، یا اگر متخلف یک شرکت باشد، تا ۴ درصد از کل گردش مالی سالانه جهانی آن برای سال مالی قبل، هر کدام که بیشتر باشد.

۶. هنگام تصمیم‌گیری در مورد میزان جریمه اداری در هر مورد، تمام شرایط مربوط به وضعیت خاص باید در نظر گرفته شود و به موارد زیر توجه شود:

(الف) ماهیت، شدت و مدت تخلف و پیامدهای آن؛

(ب) اینکه آیا جریمه‌های اداری قبلاً توسط سایر مقامات نظارت بر بازار برای همان فعال و برای همان تخلف اعمال شده است یا خیر؛

(ج) اندازه و سهم بازار فعال مرتکب تخلف.

۷. هر کشور عضو قوانینی را در مورد اینکه آیا جریمه‌های اداری بر مقامات و نهادهای دولتی مستقر در آن کشور عضو اعمال شود یا نه، و میزان این جریمه چقدر باشد، وضع خواهد نمود.

۸. بسته به نظام حقوقی کشورهای عضو، قواعد مربوط به جریمه‌های اداری می‌تواند به‌گونه‌ای اعمال شود که جریمه‌ها توسط دادگاه‌های ملی صلاحیتدار سایر نهادهای قابل‌اعمال در آن کشورهای عضو اعمال گردد. اعمال چنین قوانینی در کشورهای عضو باید آثار یکسانی داشته باشد.

ماده ۷۲: جریمه‌های اداری مؤسسات، سازمان‌ها و نهادهای اتحادیه

۱. ناظر اروپایی حفاظت از داده‌ها می‌تواند جریمه‌های اداری را برای مؤسسات، سازمان‌ها و نهادهای اتحادیه که مشمول این قوانین هستند، اعمال کند. هنگام تصمیم‌گیری برای اعمال جریمه اداری و تصمیم‌گیری در مورد میزان آن، تمام شرایط مربوط به وضعیت خاص هر مورد باید در نظر گرفته شود و به موارد زیر نیز توجه گردد:

(الف) ماهیت، شدت و مدت تخلف و پیامدهای آن؛

(ب) همکاری با ناظر اروپایی حفاظت از داده‌ها به‌منظور رفع تخلف و کاهش آثار نامطلوب احتمالی آن، ازجمله انطباق با اقداماتی که قبلاً توسط ناظر اروپایی حفاظت از داده‌ها علیه مؤسسه یا سازمان یا نهاد اتحادیه مربوطه در رابطه با موضوعی مشابه اعمال گردیده است؛

(ج) هرگونه تخلف قبلی مشابه توسط مؤسسه، سازمان یا نهاد اتحادیه.

۲. تخلفات زیر مشمول جریمه اداری تا سقف ۵۰۰،۰۰۰ یورو خواهند بود:

(الف) عدم رعایت فعالیت‌های ممنوع هوش مصنوعی مذکور در ماده ۵؛

(ب) عدم انطباق سیستم هوش مصنوعی با الزامات مندرج در ماده ۱۰.

۳. عدم انطباق هر سیستم هوش مصنوعی که تحت شمول الزامات یا وظایف این قانون است، به غیر از موارد مندرج در مواد ۵ و ۱۰، مشمول جریمه اداری تا سقف ۲۵۰،۰۰۰ یورو خواهد بود.

۴. ناظر اروپایی حفاظت از داده‌ها باید قبل از اتخاذ تصمیمات براساس این ماده، به مؤسسه، سازمان یا نهاد اتحادیه که موضوع رسیدگی‌های ناظر است، این فرصت را بدهد که دفاعش در مورد تخلف احتمالی استماع شود. ناظر اروپایی حفاظت از داده‌ها باید تصمیمات خود را فقط براساس عناصر و شرایطی مبتنی کند که طرف‌های ذی‌نفع قادر به اظهارنظر در مورد آنها باشند. شاکیان، در صورت وجود، باید از نزدیک با روند رسیدگی در ارتباط باشند.

۵. حقوق ذی‌نفعان در دفاع از خود باید در جریان رسیدگی کاملاً رعایت گردد. آنها حق دسترسی به پرونده ناظر اروپایی حفاظت از داده‌ها را دارند، مشروط به وجود منافع مشروع افراد یا شرکت‌ها یا تهعد به حفاظت از داده‌های شخصی یا اسرار تجاری‌شان.

بخش یازدهم: تفویض اختیارات و روند کمیته

ماده ۷۳: تفویض اختیارات

۱. اختیار تصویب قوانین تفویض‌شده با رعایت شرایط مندرج در این ماده به کمیسیون واگذار می‌شود.

۲. اختیارات مذکور در ماده ۴، بند ۱ ماده ۷، بند ۳ ماده ۱۱، بند ۵ و ۶ ماده ۴۳ و بند ۵ ماده ۴۸ از زمان [لازم‌الاجرا شدن قانون] برای مدت نامتعینی به کمیسیون واگذار می‌شود.

۳. تفویض اختیارات ذکرشده در ماده ۴، بند ۱ ماده ۷، بند ۳ ماده ۱۱، بند ۵ و ۶ ماده ۴۳ و بند ۵ ماده ۴۸ می‌تواند در هر زمان توسط پارلمان اروپا یا شورا لغو شود. شورا در تصمیم ابطال تفویض اختیارات، به حوزه‌ای از اختیارات که در آن تصمیم مشخص شده، پایان می‌دهد. این ابطال یک روز پس از انتشار آن در مجله رسمی اتحادیه اروپا یا در تاریخ دیگری که در آن تصمیم مشخص شده است، لازم‌الاجرا خواهد بود. این تصمیم بر اعتبار هیچ‌یک از قوانین تفویضی مصوب که قبلاً لازم‌الاجرا بوده‌اند، تأثیر نخواهد گذاشت.

۴. کمیسیون به محض تصویب یک قانون تفویضی، آن را به‌طور هم‌زمان به پارلمان اروپا و شورا اطلاع خواهد داد.

۵. هر قانون تفویضی که براساس ماده ۴، بند ۱ ماده ۷، بند ۳ ماده ۱۱، بند ۵ و ۶ ماده ۴۳ و بند ۵ ماده ۴۸ مصوب شده باشد تنها در صورتی لازم‌الاجرا می‌شود که هیچ اعتراضی از سوی پارلمان اروپا یا شورا ظرف مدت سه ماه پس از ابلاغ آن قانون به پارلمان اروپا و شورا ابراز نشده باشد یا اینکه قبل از انقضای آن دوره، پارلمان اروپا و شورا هر دو به کمیسیون اطلاع داده باشند که مخالفت نخواهند کرد. این مدت به درخواست پارلمان اروپا یا شورا می‌تواند به مدت سه ماه تمدید شود.

ماده ٧٤: روند کمیته

۱. باید یک کمیته به کمیسیون کمک کند. این کمیته باید کمیته‌ای مطابق با معنای قانون (EU) شماره ۲۰۱۱/۱۸۲ باشد.

۲. در مواردی که به این بند اشاره می‌شود، ماده ۵ مقررات (EU) ۲۰۱۱/۱۸۲ اعمال می‌شود.

بخش دوازدهم: مواد پایانی

ماده ۷۵: اصلاحیه قانون (EC) ۲۰۰۸/۳۰۰

در ماده ۴ (۳) مقررات (EC) ۲۰۱۱/۳۰۰ ، زیربند زیر اضافه می‌شود:

هنگام اتخاذ تدابیر دقیق مربوط به مشخصات فنی و روندها برای تأیید و استفاده از تجهیزات امنیتی مربوط به سیستم‌های هوش مصنوعی به معنای قانون (EU) YYY/XX [درباره هوش مصنوعی] پارلمان اروپا و شورا، الزامات مندرج در فصل ۲، بخش سوم آن قانون باید در نظر گرفته شود.

ماده ۷۶: اصلاحیه قانون (EU) ۲۰۱۳/۱۶۷

در ماده ۱۷ (۵) مقررات (EU) ۲۰۱۳/۱۶۷ ، بند زیر اضافه می‌شود:

هنگام تصویب قوانین تفویضی طبق بند اول در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای مقررات (EU) YYY/XX [درباره هوش مصنوعی] پارلمان اروپا و شورا هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

ماده ۷۷: اصلاحیه قانون (EU) ۲۰۱۳/۱۶۸

در بند ۵ ماده ۲۲ مقررات (EU) ۲۰۱۳/۱۶۸ ، بند زیر اضافه می‌شود:

هنگام تصویب قوانین تفویضی طبق بند اول در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانون (EU) YYY/XX [در مورد هوش مصنوعی] پارلمان اروپا و شورا هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

ماده ۷۸: اصلاحیه دستورالعمل EU/۹۰/۲۰۱٤

در ماده ۸ دستورالعمل EU/۹۰/۲۰۱۴ بند زیر اضافه می‌شود:

۴. برای سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای مقررات (EU) YYY/XX [درباره هوش مصنوعی] پارلمان اروپا و شورا هستند، کمیسیون باید هنگام انجام فعالیت‌های خود طبق بند ۱ و هنگام اتخاذ مشخصات فنی و استانداردهای آزمایش مطابق با بندهای ۲ و ۳، الزامات مندرج در بخش ۳، فصل ۲ آن قوانین را در نظر بگیرد.

ماده ۷۹: اصلاحیه دستورالعمل (EU) ۷۹۷/۲۰۱٦

در ماده ۵ دستورالعمل (EU) ۷۹۷/۲۰۱۶ بند زیر اضافه می‌شود:

۱۲. هنگام تصویب قوانین تفویضی طبق بند ۱ و اجرای اقدامات مطابق بند ۱۱ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای مقررات YYY/XX (EU) [در مورد هوش مصنوعی] پارلمان اروپا و شورا هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

ماده ۸۰: اصلاحیه قانون (EU) ۸۵۸/۲۰۱۸

در ماده ۵ قانون (EU) ۸۵۸/۲۰۱۸ بند زیر اضافه می‌شود:

۴. هنگام تصویب قوانین تفویضی طبق بند ۳ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانون YYY/XX (EU) [درباره هوش مصنوعی] پارلمان اروپا و شورا هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

ماده ۸۱: اصلاحیه قانون (EU) ۱۱۳۹/۲۰۱۸

قانون (EU) ۱۱۳۹/۲۰۱۸ به شرح زیر اصلاح می‌شود:

(۱) در ماده ۱۷ بند زیر اضافه می‌شود:

۳. بدون خلل به بند ۲، هنگام تصویب قوانین اجرایی مطابق بند ۱ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانون YYY/XX (EU) [درباره هوش مصنوعی] پارلمان اروپا و شورا هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

(۲) در ماده ۱۹ بند زیر اضافه می‌شود:

۴. هنگام تصویب قوانین تفویضی طبق بندهای ۱ و ۲ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانونYYY/XX (EU) [درباره هوش مصنوعی] هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

(۳) در ماده ۴۳ بند زیر اضافه می‌شود:

۴. هنگام تصویب قوانین تفویضی طبق بندهای ۱ و ۲ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانونYYY/XX (EU) [درباره هوش مصنوعی] هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

(۴) در ماده ۴۷ بند زیر اضافه می‌شود:

۳. هنگام تصویب قوانین تفویضی طبق بندهای ۱ و ۲ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانونYYY/XX (EU) [درباره هوش مصنوعی] هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

(۵) در ماده ۵۷ بند زیر اضافه می‌شود:

هنگام تصویب قوانین اجرایی در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانون (EU) YYY/XX [درباره هوش مصنوعی] هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

(۶) در ماده ۵۸ بند زیر اضافه می‌شود:

۳. هنگام تصویب قوانین تفویضی طبق بندهای ۱ و ۲ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانون (EU) YYY/XX [درباره هوش مصنوعی] هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

ماده ۸۲: اصلاحیه قانون (EU) ۲۱٤٤/۲۰۱۹

در ماده ۱۱ قانون (EU) ۲۱۴۴/۲۰۱۹ بند زیر اضافه می‌شود:

(۳) هنگام تصویب قوانین اجرایی مطابق بند ۱ در مورد سیستم‌های هوش مصنوعی که اجزای ایمنی به معنای قانون (EU) YYY/XX [درباره هوش مصنوعی] پارلمان اروپا و شورا هستند، الزامات مندرج در بخش ۳، فصل ۲ آن قانون باید در نظر گرفته شود.

ماده ۸۳: سیستم‌های هوش مصنوعی که قبلا در بازار عرضه یا به خدمت گذارده شده اند

۱. این قانون در مورد سیستم‌های هوش مصنوعی که جزئی از سیستم‌های فناوری اطلاعات در مقیاس بزرگ هستند که توسط قوانین فهرست‌شده در ضمیمه ۹ ایجاد شده‌اند و قبل از [۱۲ ماه پس از تاریخ اجرای این قانون مذکور در بند ۲ ماده ۸۵] در بازار عرضه شده یا به خدمت گذاشته شده‌اند، اعمال نمی‌گردد، مگر اینکه جایگزین یا اصلاح آن اقدامات قانونی منجر به تغییر قابل‌توجهی در طراحی یا هدف موردنظر سیستم هوش مصنوعی یا سیستم‌های هوش مصنوعی مربوطه شود.

الزامات مندرج در این قانون، در صورت امکان، در ارزیابی هر سیستم فناوری اطلاعات در مقیاس بزرگ که به‌وسیله قوانین مندرج در پیوست ۹ ایجاد شده‌اند، در نظر گرفته می‌شوند تا طبق قوانین مربوطه رفتار گردد.

۳. این مقررات در مورد سیستم‌های هوش مصنوعی پرخطر، به غیر از سیستم‌هایی که در بند ۱ ذکر شده‌اند، که قبل از [تاریخ اعمال قانون مذکور در بند ۲ ماده ۸۵] در بازار عرضه شده یا به خدمت گذاشته شده‌اند، تنها در صورتی اعمال می‌شود که از آن تاریخ، آن سیستم‌ها در معرض تغییرات قابل‌توجهی در طراحی یا هدف موردنظر خود قرار گرفته باشند.

ماده ۸٤: ارزیابی و بازبینی

۱. کمیسیون نیاز به اصلاح فهرست پیوست ۳ را سالی یک بار پس از لازم‌الاجرا شدن این قانون ارزیابی خواهد کرد.

۲. تا سه سال پس از تاریخ اجرای این قانون، مذکور در بند ۲ ماده ۸۵ و پس از آن هر چهار سال یک‌بار، کمیسیون گزارشی درباره ارزیابی و بررسی این قانون به پارلمان اروپا و شورا ارائه خواهد کرد. گزارش‌ها باید به اطلاع عموم برسد.

۳. گزارش‌های مذکور در بند ۲ باید به موارد زیر توجه ویژه‌ای داشته باشد:

(الف) وضعیت منابع مالی و انسانی مقامات ذی‌صلاح ملی به‌منظور انجام مؤثر وظایف محوله به‌موجب این قانون؛

(ب) وضعیت مجازات‌ها و به‌ویژه جریمه‌های اداری که در بند ۱ ماده ۷۱ ذکر شده که توسط کشورهای عضو برای نقض مفاد این قانون اعمال گردیده است.

۴. تا سه سال پس از تاریخ اجرای این قانون، مذکور در بند ۲ ماده ۸۵ و پس از آن هر چهار سال یک‌بار، کمیسیون باید تأثیر و اثربخشی آیین‌نامه رفتاری را برای تقویت اعمال الزامات مندرج در بخش ۳، فصل ۲ و احتمالاً سایر الزامات اضافی برای سیستم‌های هوش مصنوعی به غیر از سیستم‌های هوش مصنوعی پرخطر ارزیابی کند.

۵. برای اهداف بندهای ۱ تا ۴، هیئت، کشورهای عضو و مقامات ذی‌صلاح ملی باید اطلاعات درخواستی کمیسیون را در اختیارش قرار دهند.

۶. در انجام ارزیابی‌ها و بازبینی ذکرشده در بندهای ۱ تا ۴، کمیسیون مواضع و یافته‌های هیئت، پارلمان اروپا، شورا و سایر نهادها یا منابع مربوطه را در نظر می‌گیرد.

۷. کمیسیون در صورت لزوم، پیشنهادهای مناسبی برای اصلاح این قانون، به‌ویژه با در نظر گرفتن پیشرفت‌های فناوری و در پرتو وضعیت پیشرفت در جامعه اطلاعاتی ارائه خواهد کرد.

ماده ۸۵: لازم‌الاجرا شدن و کاربرد

۱. این قانون در بیستمین روز پس از انتشار در مجله رسمی اتحادیه اروپا لازم‌الاجرا می‌شود.

۲. این قانون از ۲۴ ماه پس از لازم‌الاجرا شدنش اعمال می‌شود.

۳. با تقیید بند ۲:

(الف) بخش ۳، فصل ۴ و بخش ۶ از سه ماه پس از لازم‌الاجرا شدن این قانون اعمال می‌شود.

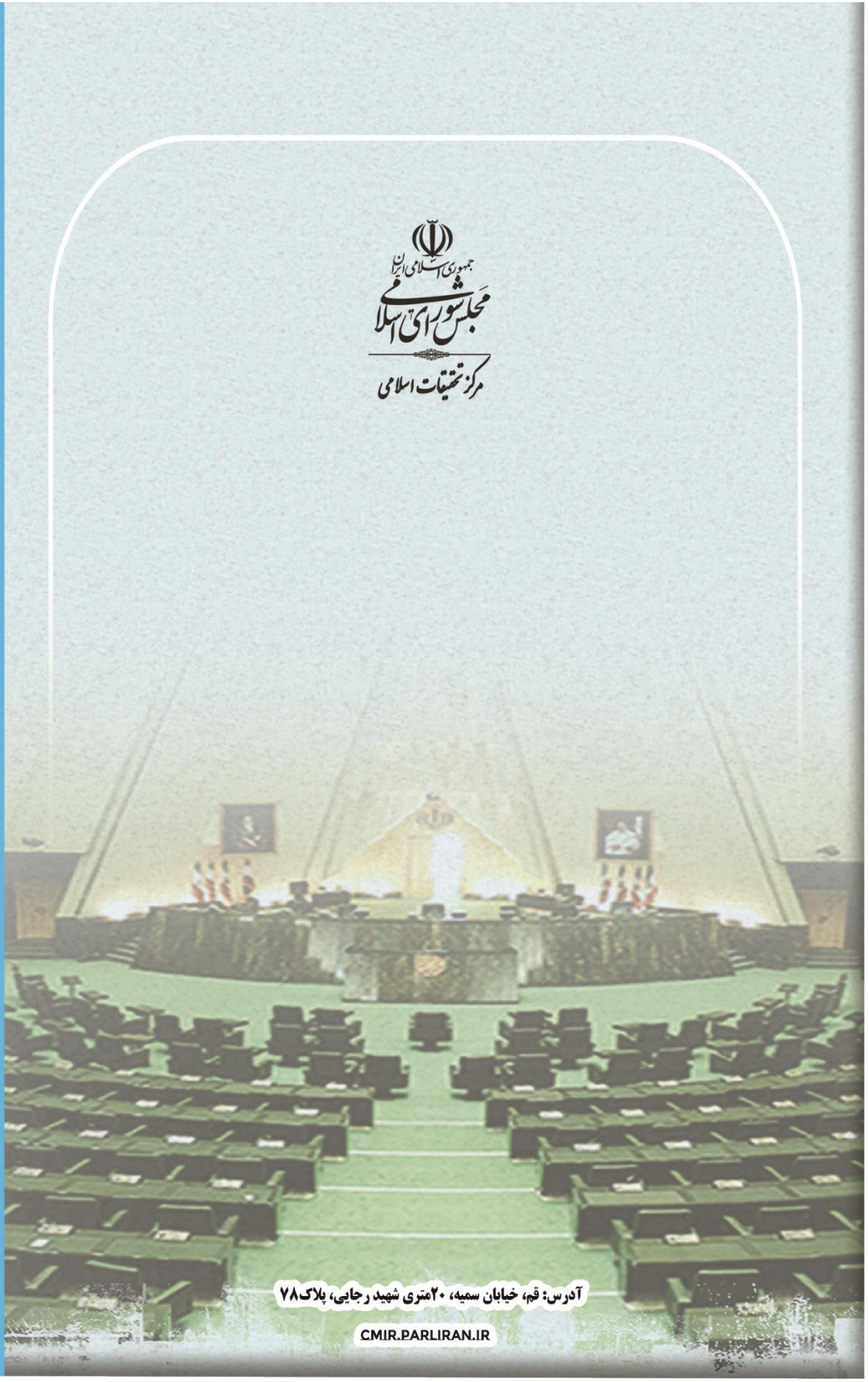
(ب) ماده ۷۱ از دوازده ماه پس از لازم‌الاجرا شدن این قانون اعمال می‌شود.

این قانون در تمامیت خود الزامی بوده و مستقیماً در تمامی کشورهای عضو قابل‌اجراست.

نگاشته شده در بروکسل.

۰۲/-/۵۸-۶۱۲

جمهوری اسلامی ایران
مجلس شورای اسلامی
مرکز تحقیقات اسلامی



آدرس: قم، خیابان سمیه، ۲۰متری شهید رجایی، پلاک۷۸
CMIR.PARLIRAN.IR