



# BEJ

مجله اخلاق زیستی

دوره دهم، شماره سی و پنجم، ۱۳۹۹

Journal Homepage: <http://journals.sbm.ac.ir/be>



مقاله پژوهشی

## چالش‌های اخلاقی و حقوقی آیین‌نامه اتحادیه اروپا در سازوکارهای هوش مصنوعی در حوزه سلامت

حسین صادقی\*<sup>۱</sup>، مهدی ناصر<sup>۲</sup>

۱. استادیار حقوق، گروه کسب و کار، دانشکده کارآفرینی، دانشگاه تهران، تهران، ایران.

۲. دانشجوی دکتری حقوق خصوصی، دانشگاه علوم قضایی، تهران، ایران.

### چکیده

**زمینه و هدف:** اگرچه کاربرد هوش مصنوعی در حوزه‌های مختلف، از جمله سلامت منجر به تحولات عظیمی شده است، اما کاربرد آن با چالش‌هایی همراه است که استفاده از آن را نیازمند سیاستگذاری‌های تقنینی و اجرایی می‌کند. هدف از پژوهش حاضر تبیین چالش‌های اخلاقی و حقوقی بر اساس آیین‌نامه اتحادیه اروپا در سازوکارهای هوش مصنوعی در حوزه سلامت است.

**مواد و روش‌ها:** پژوهش کیفی حاضر به تبیین چالش‌های حقوقی و اخلاقی عملکرد هوش مصنوعی در حوزه سلامت بر اساس تحلیل آیین‌نامه عمومی حفاظت از داده‌های خصوصی اتحادیه اروپا می‌پردازد.

**یافته‌ها:** مهم‌ترین چالش‌های موجود در سازوکار عملکرد هوش مصنوعی از نظر اخلاقی عبارت از نابرابری، تبعیض نژادی، عدم دقت در پردازش داده‌ها و ... و از نظر حقوقی عبارت از عدم مراقبت کافی در حفاظت از اطلاعات خصوصی اشخاص، عدم رعایت حریم خصوصی، و مسؤولیت‌پذیری و سازوکار شناسایی و تقسیم مسؤولیت در موارد وقوع خسارات ناشی از عملکرد ابزار می‌باشند. در این مقاله تلاش شده هر یک از این موارد بررسی و راهکارهای مقتضی ارائه گردد.

**ملاحظات اخلاقی:** در تألیف مقاله حاضر تمامی اصول اخلاقی اعم از امانتداری، صداقت و اصالت متن رعایت گردیده است.

**نتیجه‌گیری:** علی‌رغم وجود چالش‌های بیان شده در این پژوهش، ظرفیت‌های حقوقی مناسب در نظام حقوقی ایران برای رفع برخی دغدغه‌های مطرح شده وجود دارد، اما در جهت حصول وضعیت مناسب‌تر به ویژه اعمال استانداردهایی که در مقررات اتحادیه اروپا اتخاذ شده است، ضرورت دارد که برای استفاده از فناوری هوش مصنوعی به ویژه در حوزه سلامت، سیاستگذاری تقنینی از جمله تصویب قوانین کارآمد و اجرایی در خصوص کیفیت اعطای مجوز به سازمان‌های تولیدکننده این ابزارها، چگونگی جبران خسارات وارده توسط تولیدکنندگان و احقاق حقوق متضررین، آگاهی‌بخشی به مردم، کیفیت عرضه این ابزارها در بازار و شفافیت در نظام حقوقی ایران، صورت پذیرد.

### اطلاعات مقاله

تاریخ دریافت: ۹۸/۰۸/۰۶

تاریخ پذیرش: ۹۹/۰۳/۲۰

تاریخ انتشار: ۱۴۰۰/۰۱/۲۸

### واژگان کلیدی:

هوش مصنوعی

چالش‌ها و راه حل‌ها

حفظ کرامت انسانی

حریم خصوصی

حفظ اطلاعات شخصی

مسؤولیت

\* نویسنده مسؤول: حسین صادقی

آدرس پستی: ایران، تهران، دانشگاه تهران،

دانشکده کارآفرینی، گروه کسب و کار.

تلفن: ۰۹۱۲ ۳۹۳ ۰۳۳۶

نمابر:

پست الکترونیک:

hosadeghi@ut.ac.ir

## ۱. مقدمه

هوش مصنوعی تأثیرگذارترین فناوری قرن بیست و یکم تلقی می‌گردد. در سال‌های اخیر سرمایه‌گذاری‌های میلیاردی در راستای توسعه این فناوری به حوزه سلامت صورت گرفته است (۱). از این رو شرکت‌های جهان در راستای شناسایی علائم بیماری‌ها و درمان سریع امراض، مبادرت به بهره‌برداری از انواع هوش مصنوعی نموده‌اند. به عنوان مثال تولید برنامه GP at Hand توسط شرکت Babylon Health این امکان را به پزشکان داده است تا با نصب دستگاه برخوردار از این نرم‌افزار به پوست بدن انسان، نسبت به شناسایی علائم بیماری‌های مختلف اقدام نمایند (۲). علاوه بر آن طراحی برنامه Deep Learning Algorithm توسط شرکت گوگل امکان بررسی شبکه چشم و شناسایی بیماری‌های شبکه را فراهم کرده است (۳). نهایتاً پیاده‌سازی پروتکل‌های Image Related Technologies در ابزارهای اینترنت اشیا امکان انجام وظایف کارکنان بیمارستان، کاهش هزینه‌ها و افزایش بازده کارکنان را فراهم آورده است (۴). ابزارهای اینترنت اشیا ابزارهایی هستند که در آن‌ها با نصب سنسورها و محرک‌های متعدد و تعبیه دستورالعمل به پردازنده آن‌ها این ابزارها قادر به انجام وظایف از پیش تعیین شده یا اعمالی از قبیل شبیه‌سازی عملکرد انسان و... می‌شوند.

اصطلاح هوش مصنوعی در ابتدا توسط جان مک کارتی با عنوان «علم و مهندسی ساخت ماشین‌های هوشمند» مطرح شد (۵). در تعریفی که در بند یازدهم از مذاکرات اتحادیه اروپا در موضوع هوش مصنوعی (۲۰) در سال ۲۰۱۸ صورت گرفته است، از هوش مصنوعی به «سیستم‌هایی تعبیر شده است که با تجزیه و تحلیل محیط پیرامون خود، با برخورداری از درجه‌ای از استقلال در راستای دستیابی به اهداف تعیین شده برای خود، نسبت به تصمیم‌گیری و عمل اقدام می‌کنند.» پیشرفته‌ترین نوع این سیستم‌ها، سیستم‌های خبره می‌باشند که از قابلیت یادگیری و تجزیه و تحلیل بالایی برخوردار هستند.

تمامی انواع هوش مصنوعی از پروتکل‌هایی بهره‌مند می‌باشند که در راستای تعیین خط مشی عملکرد سیستم و چگونگی انجام وظایف تعیین شده برای آن‌ها در پردازنده آن‌ها تعبیه می‌گردند (۶). پروتکل‌های تعبیه شده از الگوریتم‌های «یادگیرنده» و «طبقه‌بندی‌کننده» برخوردارند که چگونگی جمع‌آوری اطلاعات از محیط پیرامون، پردازش اطلاعات و طبقه‌بندی آن‌ها را به سیستم نشان می‌دهد (۷). تصمیم‌گیری هوش مصنوعی برای انجام چگونگی وظایف نیز به شکلی است که این سیستم با پردازش اطلاعات به دست آمده، مبادرت به سنجش چگونگی تصمیم‌گیری از زوایای مختلف می‌نماید. علاوه بر آن هوش مصنوعی همانند دیگر ابزارهای اینترنت اشیا، دارای طراحی می‌باشد که اصطلاحاً کنترل‌کننده نامیده می‌شوند. کنترل‌کنندگان این ابزارها وظیفه نظارت بر عملکرد ابزار و بهبود کارایی آن‌ها را بر عهده دارند. گاه ابزار مذکور برای انجام وظایف محوله نیازمند ارسال داده‌های خام به کنترل‌کننده خود هستند. کنترل‌کنندگان این ابزارها نیز برای انجام فرایند پردازش، مبادرت به ارسال داده‌های خام به شرکت‌های پردازنده اطلاعات می‌نمایند. این شرکت‌ها با پردازش داده و ارسال نسخه پردازش شده به کنترل‌کننده، در فرایند عملکرد هوش مصنوعی ایفای نقش می‌کنند.

از آنجا که با توسعه فناوری، همواره ابزارهای جدید برای کاهش و بهبود عملکرد انسان در انجام وظایف به کار گرفته می‌شوند، توسعه آن‌ها به اقصی نقاط جهان، زمینه به کارگیری آن‌ها در کشورهای در حال توسعه و رو به توسعه مانند ایران را نیز فراهم آورده است؛ اما مسأله مهم، ضرورت تبیین چالش‌های مرتبط با این فرایند در کشورهای توسعه‌یافته می‌باشد تا سیاست‌گذاری‌های تقنینی و اجرایی مناسبی در کشورهای پذیرنده صورت پذیرد. هدف از پژوهش حاضر تبیین چالش‌های اخلاقی و حقوقی کاربرد هوش مصنوعی در حوزه سلامت است.

## ۲. ملاحظات اخلاقی

در این اثر تمامی اصول اخلاقی انجام یک پژوهش اعم از امانتداری و رعایت اصالت مقاله مد نظر نویسندگان قرار گرفته است.

## ۳. مواد و روش‌ها

پژوهش کیفی حاضر به تبیین چالش‌های حقوقی و اخلاقی عملکرد هوش مصنوعی در حوزه سلامت براساس تحلیل آیین‌نامه عمومی حفاظت از داده‌های خصوصی اتحادیه اروپا می‌پردازد. الزامات پارلمان اروپا و شورای ۲۷ آوریل ۲۰۱۶ در مورد حفاظت از اشخاص حقیقی در خصوص پردازش اطلاعات شخصی و انتقال حریم خصوصی داده‌ها منتج به تصویب آیین‌نامه‌ای با مقررات فوق‌الذکر گردید. این مقررات که از ۲۵ ماه می سال ۲۰۱۸ لازم‌الاجرا گردید، در ۱۱ فصل و ۹۹ ماده به الزامات، حقوق و تکالیف و دیگر احکام مرتبط با سازوکار حفاظت از اطلاعات خصوصی اروپاییان پرداخته است. آیین‌نامه مذکور با بیان کلیات و اصول حاکم بر پردازش اطلاعات در فصل اول و دوم، در فصل سوم و پنجم به تبیین حقوق دارندگان اطلاعات در سازوکار پردازش داده‌های خصوصی آن‌ها پرداخته است. مقررات مذکور در فصل چهارم، هشتم، نهم و دهم نیز به تشریح مقررات حاکم بر کنترل کنندگان و پردازندگان اطلاعات، وظایف قانونی آن‌ها و سازوکار جبران خسارات وارده ناشی از نقض مفاد مقررات این آیین‌نامه اقدام نموده است.

## ۴. یافته‌ها

ضرورت حفظ کرامت انسان همواره مورد تأکید نظام‌های اخلاقی و حقوقی قرار گرفته است. در ماده ۱ منشور حقوق اساسی اتحادیه اروپا نیز بر ضرورت این مهم به عنوان یکی از اصول اخلاقی و مبانی بنیادین این نظام تصریح شده است. وجود این اصل مهم دربردارنده نتایجی از جمله انصاف و برقراری عدالت در جامعه و شفافیت در عملکرد می‌باشد (۱۴).

دو مقوله فوق چالش‌های اساسی می‌باشند که هوش مصنوعی در جمع‌آوری و پردازش اطلاعات با آن مواجه می‌باشد. چالش‌های مذکور در دو بعد در سازوکار عملکرد هوش مصنوعی بروز می‌نمایند. بعد اول در تصمیم‌گیری این ابزار در مواجهه با شرایط به وجودآمده می‌باشد که مواردی از قبیل تبعیض نژادی را می‌توان نمونه‌ای از چالش‌های اخلاقی مذکور قلمداد کرد؛ بعد دوم نیز در مقرراتی جلوه می‌نماید که وظیفه جهت‌دهی بر سازوکار عملکرد هوش مصنوعی را دارا می‌باشند. از جمله این مقررات آیین‌نامه عمومی حفاظت از داده‌های خصوصی (General Data Protection Regulations) اشخاص می‌باشد که با تصویب آن در سال ۲۰۱۶، مقرراتی در جهت چگونگی جمع‌آوری و پردازش داده‌های خصوصی اشخاص پیش‌بینی شده است (۲۱).

مهم‌ترین ایراداتی که بر مقررات مذکور وارد می‌باشد، کلی‌گویی و عدم پیش‌بینی سازوکار اساسی در ایجاد شفافیت در سازوکار عملکرد اشخاص و ابزارهای مرتبط با حوزه پردازش داده‌های خصوصی اشخاص می‌باشد. ماده ۴ از مقررات مذکور در جهت حفظ کرامت و شأن انسان، به صورت کلی مسأله ضرورت پردازش داده‌های خصوصی جهت خدمت به بشریت را مورد تصریح قرار داده است (۱۵). این در حالی است که در این مقررات نه به صورت جزئی بر شرایط و مصادیقی که پردازندگان اطلاعات در راستای احترام به استقلال فردی باید مورد رعایت قرار دهند، تأکید شده است و نه با ارائه تعاریفی شفاف، خصوصیات عملی که انجام آن به منزله خدمت به شخص می‌باشد، تبیین گردیده است. از طرف دیگر بند اول از بخش اول از ماده مرقوم بر ضرورت وجود شفافیت در عملکرد نهادهای مرتبط با سازوکار عملکرد هوش مصنوعی اشاره نموده است. در ماده ۱۲ از مقررات مذکور نیز در جهت تحقق این امر تنها بر ضرورت آگاهی‌بخشی به دارنده اطلاعات در زمینه پردازش داده‌های وی تأکید شده است. این در حالی است که سازوکار ایجاد شفافیت در عملکرد و کیفیت آگاهی بخشی به عنوان دو عنصر اساسی در زمینه ایجاد شفافیت فاقد

برای سیستم به شکلی باشد که در پردازش داده‌ها زمینه تبعیض برخورد میان اقشار یا نژادهای مختلف جامعه را ایجاد نماید (۹). این چالش در به کارگیری هوش مصنوعی در سیستم قضایی بیشتر جلوه می‌کند. امروزه در دادگاه‌های آمریکا هوش مصنوعی در پیش‌بینی ارتکاب جرائم مجدد توسط محکومان به کار می‌رود. این در حالی است که گزارشات حاکی از آن است که پیش‌بینی‌های سیستم بیان‌شده در مواجهه با پرونده‌هایی که متهمان آن‌ها سیاه‌پوست می‌باشند، در مواجهه با سفیدپوستان دارای اختلافات فاحشی است که حاکی از عدم تناسب چگونگی پردازش داده‌های ورودی توسط سیستم می‌باشد (۱۰). علاوه بر آن مسأله یادگیری این ماشین‌ها نیز چالش دیگری است که در این خصوص مطرح می‌گردد. سیستم‌های بیان‌شده به صورت استقرایی قادر به یادگیری هستند. چگونگی یادگیری این سیستم‌ها نیز بستگی مستقیم به الگوریتم‌هایی دارد که خط مشی دریافت اطلاعات را از محیط پیرامون تعیین می‌کنند. در صورتی که این خط مشی به شکلی باشد که در طول زمان به صورت جهت‌دار چگونگی دریافت اطلاعات را بر سامانه تحمیل نماید، می‌تواند تأثیرگذاری فراوانی بر عدم صحت تصمیمات این سیستم بر جای گذارد (۱۱).

در نظام حقوقی اتحادیه اروپا در مقررات متعددی بر جلوگیری از هرگونه تبعیض و برابری تمامی اقشار جامعه، زن و مرد، کودک و بزرگسال، سیاه و سفید و... تصریح شده است. مطابق با ماده ۲ دستورالعمل برابری نژادی، تبعیض نژادی به دو گروه تبعیض مستقیم و غیر مستقیم تقسیم می‌گردد. مطابق با بند b ماده مرقوم، تبعیض مستقیم به تبعیضی گفته می‌شود که منحصراً بر روی فرد خاصی صورت گرفته و قومیت یا جنسیت یا نژاد آن شخص ارتباطی با وقوع تبعیض علیه وی ندارد، در حالی که تبعیض غیر مستقیم ارتباط مستقیم با ویژگی‌های قومیتی یا جنسیتی افراد دارد. از آنجا که سازوکار تصمیم‌گیری و عملکرد هوش مصنوعی مطابق با خط مشی است که در پروتکل طراحی شده برای آن پیش‌بینی می‌گردد؛

هرگونه مقرر در این آیین‌نامه می‌باشد، ضمن این‌که از ضروریات ایجاد این مهم، کیفیت نظارت بر عملکرد نهادهای پردازشگر اطلاعات می‌باشد. مفاد مواد ۲۳ و ۴۵ آیین‌نامه مرقوم تنها بر تأکید سیاستگذاران اتحادیه در دریافت تضمین مالی در جبران خسارات وارده ناشی از پردازش داده‌های خصوصی و صلاحیت مراجع قضایی داخلی کشورها بر صدور رأی در این زمینه اشاره دارد، در حالی که پیشگیری از سوءاستفاده از اطلاعات و نظارت همه‌جانبه در فرایند پردازش، امری مهم بوده که از نظر سیاستگذاران اتحادیه مغفول مانده است. به عبارت دیگر نقص در وجود مقرر خاص در پیش‌بینی جزئیات نظارت بر فرایند پردازش داده واجد این ایراد می‌باشد که نظارت یک کشور در این نظام بر عملکرد یک نهاد آیا به صورت سمعی و بصری صورت گرفته یا با پیش‌بینی مراجع صلاحیت‌دار و معرفی اشخاص ناظر در محل پردازش داده باید صورت پذیرد. تعیین معیارهای ایجاد نظارت بر عملکرد نهادهای مرتبط با جمع‌آوری و پردازش داده‌های اشخاص و شاخصه‌های چگونگی نظارت بر عملکرد آن نهادها در تطابق با این مقررات از جمله چالش‌هایی است که دلالت بر نقص مقررات مصوب ۲۰۱۶ در رعایت اصول اخلاقی بیان شده در این گفتار دارد.

**۴-۱. چالش‌های اخلاقی:** چالش‌های اخلاقی پیرامون عملکرد هوش مصنوعی در حوزه سلامت در موضوعات نابرابری و تبعیض و عدم دقت و احتمال ضرر به شرح ذیل خلاصه می‌شوند:

۴-۱-۱. نابرابری و تبعیض: نحوه دریافت اطلاعات از محیط پیرامون هوش مصنوعی بستگی به کیفیت پروتکل طراحی شده و الگوریتم‌های داده‌شده به آن دارد، در صورتی که متغیرهایی مانند سن، نژاد، جنسیت و... برای یک سیستم تعریف نشود، سیستم در پردازش اطلاعات مربوط به آن‌ها واکنشی نشان نخواهد داد. عدم واکنش سیستم در پردازش اطلاعات می‌تواند در تصمیم‌گیری‌های این ابزار تأثیرگذار باشد (۸). از طرف دیگر حتی امکان دارد نوع الگوریتم طراحی شده

عملکرد آن همواره بر اساس ویژگی‌های خلقی گروهی خاص صورت می‌گیرد که می‌تواند با تبعیض غیر مستقیم در ارتباط باشد. به عنوان مثال تفاوت تصمیم‌گیری میان قابلیت انجام عمل مجرمانه در خصوص سیاه‌پوستان و سفیدپوستان مسأله‌ای نیست که مربوط به شخص خاص یا ویژگی‌های خاصی در یک شخص معین باشد. سیاهی و سفیدی خصوصیتی است که مربوط به نژاد و قومیت اشخاص بوده و در زیرمجموعه تبعیض غیر مستقیم نژادی قرار می‌گیرد (۱۶). برای تشخیص این‌که عملکرد هوش مصنوعی در مواجهه با موضوعات نژادپرستانه تلقی گردد یا خیر، متخصصان در اتحادیه اروپا مبادرت به پیش‌بینی معیارهایی در جهت بررسی تصمیم اتخاذشده توسط هوش مصنوعی نموده‌اند. این معیارها به سه گروه «هدف مشروع، مناسب بودن و ضرورت» تقسیم می‌شوند (۱۷).

مشروعیت هدف عملکرد ابزار در حوزه سلامت به شکلی است که تصمیم‌گیری نهایی ابزار منتج به هدف مشروعی باشد که از قابلیت ارائه خدمات به انسان برخوردار باشد. بنابراین در صورتی که هوش مصنوعی در زمینه شناسایی تومورهای سینه یا انواع دیگر سرطان یا شناسایی بیماری‌های مختلف به کارگرفته شود، این امر به منزله یک هدف مشروع در حوزه سلامت قلمداد می‌گردد.

مناسب بودن که به تأثیرگذاری عملکرد ابزار مرتبط است در صورتی است که عملکرد ابزار در مواجهه با کیس‌های مختلف دارای تأثیرگذاری یکسان باشد. از این رو در صورتی که دو کیس دارای علائم برابر، مورد بررسی توسط هوش مصنوعی واقع و تصمیم‌گیری این ابزار در مورد هر کدام از آن‌ها دارای اختلاف باشد، به گونه‌ای که باید در حالت عادی تصمیم‌گیری مشابه در خصوص هر دو مورد اتخاذ می‌گردید، می‌توان به عدم تأثیرگذاری این ابزار در بخش مورد نظر حکم نمود.

ضرورت که از آن به تصمیم‌گیری‌های لحظه‌ای یک ابزار اطلاق می‌گردد، به این معناست که در مواردی ممکن است ابزار نیاز به تصمیم‌گیری‌های لحظه‌ای داشته باشد که باید در مواجهه

با موارد مختلف، رفتارهای همسان از خود نشان دهد. در صورتی که رفتار ابزار در مواجهه با موردهای مختلف دارای علائم و شرایط یکسان، مشابه نباشد، می‌توان به تبعیض‌آمیز بودن رفتار مذکور حکم نمود. به عنوان مثال ممکن است در هنگام جراحی یا برش بافتی خاص، خونریزی لحظه‌ای در بدن بیمار رخ دهد. در این صورت اگر تصمیم‌گیری لحظه‌ای در خصوص افراد چاق و لاغر یا زن و مرد یا سیاه و سفید به طور مشابه نباشد، تبعیض‌آمیز بودن رفتار وی مشخص می‌گردد. این معیار در آراییی از دادگاه‌های اتحادیه اروپا مانند پرونده Chief Constable of West Yorkshire

Homer علیه Police در سال ۲۰۱۲ نیز مورد تأکید قرار گرفته است.

۴-۱-۲. عدم دقت و احتمال ضرر: پردازش داده‌های دریافتی و تصمیم‌گیری سیستم همواره به معنای تصمیم‌گیری صحیح نمی‌باشد، چراکه در هر حال امکان خطا و اشتباه در عملکرد این سامانه‌ها نیز وجود دارد. وجود چنین اشتباهاتی ممکن است در مواردی خسارات جبران‌ناپذیری را ایجاد نماید. به عنوان مثال این سیستم‌ها در تصمیم‌گیری در خصوص نوع بیماری افراد مبتلا گاهی دچار اشتباه شده و در مواردی که بیماری‌ها دارای علائم مشابه بودند، با تشخیص اشتباه بیماری، موجبات تضرر بیمار را فراهم نمودند. یا در مواردی نیز با تشخیص درست بیماری، نسبت به تجویز نسخه غیر صحیح برای درمان آن اقدام نمودند. به عنوان مثال در مواردی مشاهده گردید که هوش مصنوعی در تشخیص بیماری آسم، نسبت به ترخیص بیماران از بیمارستان بدون توجه به سابقه بستری آن‌ها اقدام نمود (۱۲). علاوه بر آن انواع هوش مصنوعی از قابلیت تقلید و یادگیری برخوردار هستند، حتی نوع پیشرفته این ابزارها که سیستم‌های خبره نام دارند، قابلیت درک احساسات انسان را داشته و مطابق با روحیات و خلقیات وی مبادرت به تصمیم‌گیری می‌نمایند، اما چگونگی عملکرد این سیستم‌ها نیز مجدداً مرتبط با پروتکلی است که به پردازنده آن داده می‌شود. اگر افرادی که نسبت به طراحی پروتکل‌ها و الگوریتم‌هایی که خط مشی عملکرد این ابزار را

تعیین می‌کنند، صلاحیت ورود به این حوزه را نداشته باشند، مشکلات بیان شده بیش از پیش بروز خواهد نمود (۱۳).

**۴-۲. چالش‌های حقوقی:** چالش‌های حقوقی پیرامون عملکرد هوش مصنوعی در حوزه سلامت در موضوعات نقض حریم خصوصی و محرمانگی، خسارت و مسؤلیت جبران آن و مسؤلیت‌پذیری نهادی به شرح ذیل خلاصه می‌شوند:

۴-۲-۱. نقض حریم خصوصی و محرمانگی: پردازش داده‌های اشخاص، ارتباط تنگاتنگ با حفظ حریم خصوصی اشخاص دارد. به همین جهت است که مواد ۶ و ۱۲ آیین‌نامه بر ضرورت آگاهی‌بخشی به دارنده اطلاعات در خصوص کمیت و کیفیت اطلاعات مورد پردازش وی اشاره دارد، اما مسأله آگاهی دارنده اطلاعات از داده‌های پردازش شده یکی از چالش‌هایی است که بررسی ابعاد مختلف آن حاکی از نقض مقررات مصوب ۲۰۱۶ دارد. بند اول از ماده ۲۰ این مقررات بر ضرورت ارائه اطلاعات پردازش شده به دارنده اشاره دارد، اما سؤال پیش رو این است که دارنده اطلاعات آیا امکان بازخوانی و تحلیل داده‌های پردازش شده را خواهد داشت؟ آیا نهاد حکومتی در زمینه ارائه آموزش‌های لازم در این زمینه وجود داشته و چه آموزش‌هایی به آحاد جامعه در این زمینه باید ارائه گردد؟ نقش حکومت در فرایند نظارت بر دریافت و ارائه اطلاعات پردازش شده از سوی کنترل‌کننده به دارنده چه بوده و آیا این اطلاعات باید توسط حکومت نیز مورد بازبینی واقع شوند؟

مسأله دیگر در زمینه آگاهی‌بخشی به دارنده اطلاعات که ارتباط تنگاتنگ با حریم خصوصی وی دارد، وجود رضایت وی در پردازش داده‌های شخصی می‌باشد. بند اول از ماده ۶ آیین‌نامه مصوب ۲۰۱۶ بر ضرورت کسب رضایت موردی دارنده در پردازش داده‌های خصوصی وی اشاره دارد. مطابق با مفاد این مقرر، نهادهای کنترل‌کننده در جمع‌آوری و انتقال اطلاعات شخصی اشخاص، باید رضایت آن‌ها را در خصوص کمیت و کیفیت داده‌های مورد پردازش کسب نمایند. اما سؤال مهم این است که آیا آحاد یک جامعه آگاهی‌چندانی از فرایند پردازش اطلاعات خود و ضرورت یا عدم ضرورت

پردازش داده‌های مذکور برخوردار می‌باشند؟ آیا محول‌نمودن وظیفه آگاهی‌بخشی به یک کنترل‌کننده هوش مصنوعی که خود ذی‌نفع عدم آگاهی هرچه بیشتر دارنده در فرایند پردازش می‌باشد، می‌تواند اهداف ناشی از تصویب مقررات ۲۰۱۶ را تأمین نماید؟ چالش مذکور زمانی جلوه بیشتر می‌یابد که کنترل‌کننده هوش مصنوعی، جهت پردازش داده نیاز به ارسال اطلاعات جمع‌آوری شده به یک شرکت فراملی پردازنده یا دارای تابعیت کشوری ثالث داشته باشد. در این خصوص مسأله ضرورت پردازش داده جهت انجام وظایف از پیش تعیین‌شده ابزار از یک طرف و از طرف دیگر ضرورت حفظ امنیت داده‌های مورد پردازش مسائلی است که محول نمودن تعیین تکلیف این امر بر تصمیم یک دارنده صرف، می‌تواند در مواردی خطرات جبران‌ناپذیری را فراهم آورد، چراکه هرگونه سوءاستفاده از داده‌های شخصی اشخاص از جمله اطلاعات زیستی آن‌ها می‌تواند زمینه ایجاد سلاح‌های زیستی و یا تولید ویروس‌های آزمایشگاهی و به خطراتدان امنیت ملی یک کشور را فراهم آورد.

مشکل دیگر مفاد بند سوم از ماده ۲۰ این مقررات می‌باشد. این بند تبادل و پردازش اطلاعات اشخاص در راستای حفظ منافع عمومی را بدون کسب رضایت دارنده میسر نموده است. عدم پیش‌بینی ابعاد دقیق عبارت «منافع عمومی» می‌تواند زمینه نقض شدید حریم خصوصی افراد را دربرداشته باشد، چراکه یک کنترل‌کننده یا پردازنده امکان تفسیر هر یک از اعمال خود در جهت حفظ منافع عمومی را برخوردار بوده و معیار و شرایطی برای این موضوع در مقررات مرقوم پیش‌بینی نشده است. سوءاستفاده از مقرر بیان شده نه تنها می‌تواند زمینه نقض وظایف مرتبط با آگاهی‌بخشی به دارنده و کسب رضایت او را فراهم آورد، بلکه زمینه سوءاستفاده و پردازش پنهانی اطلاعات وی را نیز می‌تواند دربرداشته باشد، به خصوص این‌که در این مقررات وظیفه‌ای نیز برای دولت متبوع دارنده در جهت کیفیت نظارت بر اجرای مقررات این بند پیش‌بینی نشده است.

سؤال پیش رو این است که آیا در زمینه سلامت کسب اجازه موردی بیمار توسط عامل انسانی ممکن است؟ به نظر نگارندگان در صورتی که دسترسی به اطلاعات شخصی اشخاص لازمه امر طبابت باشد، نیازی به کسب اجازه موردی وجود ندارد، چراکه حضور بیمار نزد پزشک به منزله ارائه اذن ضمنی برای انجام طبابت می‌باشد، اما در مواردی لازم است تا پزشک برای اطمینان از نظر خود در موضوع مطروحه، نیاز به اطلاعاتی داشته باشد که ارتباط مستقیم با بیماری بیمار ندارد. در این صورت به نظر می‌رسد کسب رضایت وی جزء ملزومات باشد. این راه حل در زمینه عملکرد هوش مصنوعی نیز قابلیت ارائه دارد. چالش دیگر مسأله آگاهی از نوع اطلاعات مورد پردازش است. مطابق با مفاد ماده ۱۲ آیین‌نامه بیان شده، در راستای ایجاد شفافیت در عملکرد این ابزارها، افراد باید از قابلیت مشاهده اطلاعات مورد پردازش آگاهی داشته باشند. سؤال پیش رو این است که آیا در موارد مرتبط با حوزه سلامت نیز چنین سازوکاری قابلیت اجرایی خواهد داشت؟ آیا در مواردی که بیمار نیاز به طبابت اورژانسی داشته باشد، نیاز به وجود چنین شفافیتی وجود دارد؟ اگر خیر آیا بیمار محق بر مشاهده اعمال صورت‌گرفته بر اطلاعات به دست‌آمده از وی خواهد بود؟

به نظر نگارندگان، حوزه سلامت به جهت اهمیتی که دارد نباید با شرایطی که دیگر حوزه‌ها در ذیل مقررات آیین‌نامه مذکور قرار می‌گیرند، مورد تفسیر واقع گردد. از این رو اگر قرار بر این باشد که هر اطلاعاتی که در حوزه درمان به آن دسترسی پیدا می‌گردد و مورد تجزیه و تحلیل واقع می‌شود، با تمام جزئیات به بیمار بیان گردد، اولاً زمینه سوءاستفاده برخی از بیماران فراهم می‌شود تا در زمانی که نتیجه‌ای از تلاش‌های پزشکی در امر طبابت حاصل نگردد، با دست‌آویز قراردادن مقررات آیین‌نامه مرقوم مبادرت به طرح دعاوی واهی علیه اطبا نمایند؛ ثانیاً اهمیت رشته طبابت به قدری است که در مواردی مصلحت در مخفی‌نمودن برخی اطلاعات از بیماران می‌باشد تا در زمینه درمان آن‌ها از نظر روحی دچار اختلال

۴-۲-۲. خسارت و مسؤولیت جبران آن: راه حلی که در راستای حل معضلات بیان‌شده می‌توان بیان داشت، ضبط اطلاعات و بررسی آن‌ها به وسیله انسان می‌باشد تا در صورت وقوع خطا در عملکرد هوش مصنوعی، قابلیت پیشگیری از آن وجود داشته باشد (۱۸)، اما این امر به منزله در اختیارگرفتن اطلاعات شخصی اشخاص توسط انسان می‌باشد که با مقررات حفاظت از اطلاعات افراد در اتحادیه اروپا واجد تعارض است. مطابق با ماده ۶ آیین‌نامه مصوب ۲۰۱۶ دسترسی به اطلاعات شخصی اروپاییان باید با رضایت موردی آن‌ها باشد. در صورتی که چنین عملکردی از سوی نهاد عامل صورت نگرفته باشد، در صورت وقوع هرگونه خسارت، نهاد عامل مسؤول جبران خسارات وارده است. مطابق با بند اول از ماده ۴ آیین‌نامه، اطلاعات شخصی افراد به هرگونه اطلاعاتی بیان می‌گردد که عرفاً از قابلیت اشتراک به عموم جامعه برخوردار نباشد. مطابق با بند یازدهم از ماده مرقوم، و مواد ۶ و ۱۲ آیین‌نامه، کسب رضایت افراد در دسترسی و پردازش اطلاعات وی باید به صورت خاص و بدون ابهام توسط عامل صورت پذیرد. از این رو در صورتی که فرد به هر شکل در خصوص اطلاعات به دست آمده توسط وی آگاهی و رضایت نداشته باشد، مسؤولیت‌های مندرج در آیین‌نامه مرقوم شامل حال وی می‌گردد.

این موضوع در نظام حقوقی ایران نیز موکداً در مواد ۵۹ و ۵۸ قانون تجارت الکترونیکی مورد تصریح قرار گرفته است. مواد مرقوم ذخیره، پردازش و توزیع داده‌های شخصی اشخاص را تنها در محدوده رضایت وی، اهداف مشخص، به صورت کاملاً شفاف، به اندازه متناسب تعیین نموده و به مالکان اطلاعات این امکان را داده است تا در هر زمان امکان دسترسی به اطلاعات مذکور و حذف آن‌ها از فرایند پردازش یا ذخیره و تبادل را داشته باشند. بدیهی است با عنایت به مقررات عام مسؤولیت مدنی، توجهاً به آرمه‌بودن مقررات موضوع مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی، نقض هر یک از شرایط مواد مرقوم، می‌تواند منجر به مسؤولیت مدنی ناقضان نیز می‌گردد.

می‌باشد، اما در هر حال در صورتی که خسارتی بر بیمار وارد آید، می‌توان بر اساس قواعد عام مسؤلیت مدنی یا کیفری وی را مسؤؤل جبران خسارات وارده نمود.

۴-۲-۳. مسؤولیت‌پذیری نهادی: چالش حقوقی دیگر در سازوکار عملکرد هوش مصنوعی مسؤولیت‌پذیری نهادهای فعال در این فرایند در جبران خسارات وارده می‌باشد. آیین‌نامه مصوب ۲۰۱۶ در این زمینه واجد مقرراتی است. مواد ۴۵ و ۲۴ از مقررات مذکور ارائه تضامین مالی برای جبران خسارات ناشی از نقض قواعد امنیتی و ارائه گزارش سازوکار پردازش اطلاعات از سوی کنترل‌کننده به کشور متبوع دارنده اطلاعات را پیش‌بینی نموده است. علاوه بر آن، پروتکل الحاقی به ماده ۴۵ مقررات مرقوم واجد شرایطی برای کشورهای غیر اروپایی میزبان اطلاعات خصوصی اروپاییان از جمله شرط «کفایت» می‌باشد. مطابق با بخش اول از بند دوم پروتکل مزبور، کشورهای میزبان اطلاعات خصوصی اروپاییان که خارج از اتحادیه اروپا می‌باشند، در دریافت این اطلاعات باید واجد سطح امنیتی لازم برای حفظ امنیت داده‌های مذکور و شفافیت کافی برای امکان نظارت بر عملکرد نهادهای فعال در صلاحیت سرزمینی خود باشند. این امر در صورتی محقق خواهد شد که معاهدات یا دیگر مقررات مصوب اتحادیه اروپا از جمله مفاد دستورالعمل حمایت از حقوق جمعی مصرف‌کنندگان مصوب ۲۰۱۸ (۲۲) این اتحادیه در پیش مسؤولیت تضامنی دولت در موارد نقض قواعد امنیتی پردازش داده‌های خصوصی توسط شرکت‌های تبعه این کشور، مورد پذیرش کشور ثالث قرار گیرد.

علاوه بر آن چالش دیگر ضرورت سیاستگذاری تقنینی در پیاده‌سازی این سازوکار در نظام داخلی کشورهای عضو اتحادیه است. به عبارتی در صورتی که کشوری از مقررات مواد ۲۴ و ۴۵ آیین‌نامه پیروی ننماید، ضمانت اجرای این امر در چه می‌باشد؟ آیا امکان محکوم‌نمودن دولت مذکور در دادگاه‌های اتحادیه اروپا با سازوکاری معین وجود دارد؟ در این خصوص به نظر نگارندگان با اخذ وحدت ملاک از ماده ۱۶

نشوند، لذا در پاسخ به سؤالات مطرح‌شده در فوق، احوط برخورداری از دیدگاهی معتدل می‌باشد که در عین حال که بیماران محق بر مشاهده کم و کیف اطلاعات به دست آمده و مورد تجزیه و تحلیل قرار گرفته خود می‌باشند، در مواردی نیز به جهت مصالحی، چنین حقی از آنان سلب گردد؛ البته ایراد آیین‌نامه مذکور این است که این حق را به صورت مطلق بیان نموده است که در این حالت امکان ارائه تفاسیر متعدد وجود دارد.

نکته دیگر مفاد ماده ۲۹ اعلامیه مرکز نظارت بر داده پیام‌های اتحادیه اروپا مصوب ۲۰۱۰ با الحاقات و اصلاحات ۲۰۱۵ می‌باشد که جمع‌آوری اطلاعات شخصی افراد و پردازش آن‌ها را در فرایندی «معنی‌دار و تأثیرگذار» قرار داده است. سؤال پیش رو این است مرجع تشخیص تأثیرگذار بودن یا نبودن اطلاعات به دست‌آمده از افراد کجا بوده و چه معیارهایی در این زمینه وجود دارد؟ آیا در حوزه سلامت امکان جمع‌آوری اطلاعات بدون تأثیر وجود دارد؟ در صورتی که اطلاعات به دست‌آمده ارتباطی با حوزه عملکرد عامل نداشته باشد، آیا ضمانت اجرایی در این خصوص متصور است؟ برای پاسخ به سؤالات فوق می‌توان بیان داشت که منظور از تصویب چنین مقرره‌ای، جهت‌بخشی بر چگونگی عملکرد عامل می‌باشد. از این رو در صورتی که در راستای اعمال عامل خسارتی وارد گردد و با نظر کارشناس رسمی اطلاعات به دست‌آمده ارتباط و تأثیری بر حوزه عملکرد وی نداشته باشد، این عمل به عنوان تقصیر وی تلقی و او را ملزم به جبران خسارت خواهد نمود.

ضمن این‌که ممکن است اعمال وی واجد مسؤولیت کیفری نیز باشد. در کنار این موارد در حوزه سلامت، تشخیص بی‌ارتباط بودن اطلاعات و نوع طبابت کمی مشکل است، چراکه ممکن است پزشک برای اطمینان از نظر پزشکی خود، مبادرت به کسب اطلاعات غیر مرتبط با عمل مورد درمان نماید. این امر نمی‌تواند به منزله تقصیر وی تلقی گردد. از این رو در حوزه سلامت اصلح در تعدیل مقررات این ماده به موارد متیقن و احتراز از پیش‌بینی مسؤولیت‌های مدنی برای پزشکان

کشورها جزء دیگر مشکلات اجرایی پیش روی اتحادیه خواهد بود.

**۳-۴. نظام حقوقی ایران:** موضوعات قابل بحث در سازوکار عملکرد هوش مصنوعی در حوزه سلامت در ارتباط با نظام حقوقی ایران در محوریت مسؤلیت ناشی از تبادل داده و نقش نظارت دولت و چگونگی شناسایی و تقسیم مسؤلیت واردکنندگان خسارت به شرح ذیل شناسایی می‌شوند:

۳-۴-۱. مسؤلیت ناشی از تبادل داده و نقش نظارت دولت: در نظام حقوقی ایران، سازوکاری مبنی بر تبادل اطلاعات خصوصی میان شرکت‌های تابعه و دیگر شرکت‌های فراملی یا موجود در کشوری دیگر وجود ندارد. پیاده‌سازی فناوری هوش مصنوعی در بخش‌های مختلف حوزه سلامت در نظام حقوقی ایران، ضرورت چنین تبادلاتی را خصوصاً در مواردی که پردازندگان این اطلاعات به صورت انحصاری تنها در چند کشور خاص وجود داشته باشند، به وجود خواهد آورد. از این حیث مقوله‌های مورد بحث در پیاده‌سازی فناوری مذکور، چگونگی اعطای مجوز فعالیت به شرکت‌های کنترل‌کننده و پردازنده اطلاعات، نحوه وقوع فرایند ارسال و تبادل اطلاعات ایرانیان به کشورهای خارجی و ضمانت اجرای نقض مقررات امنیتی تعیین‌شده از سوی دولت ایران می‌باشد. در این زمینه نکته قابل توجه عدم قابلیت قیاس قدرت حاکمیتی اتحادیه اروپا که متشکل از چندین کشور بوده و از ابزارهای اعمال فشاری از جمله تحریم‌های اقتصادی در واردنمودن فشار بر ناقض مقررات یا دولت متبوع آن، با کشور ایران می‌باشد. از این رو برای انجام فعالیت کنترل‌کنندگان و پردازندگان اطلاعات در کشور ایران اولاً دریافت تضمین‌های مالی کافی از آن سازمان؛ ثانیاً انعقاد قراردادهای متقابل میان کشور متبوع سازمان و کشور ایران برای پیش‌بینی مسؤلیت بین‌المللی آن کشور الزامی می‌باشد. از سوی دیگر تا زمانی که شعبه‌ای از یک شرکت کنترل‌کننده در کشور ایران دایر نبوده و امکان صدور و اجرای حکم بر علیه این سازمان وجود نداشته باشد، هرگونه فعالیت این سازمان‌ها در خارج از مرزهای ایران واجد

دستورالعمل ۲۰۱۸ که در راستای مقررات ماده ۸۰ آیین‌نامه ۲۰۱۶ در حوزه اقامه دعاوی جمعی برای جبران خسارات ناشی از نقض قواعد امنیتی تصویب شده است، امکان پیش‌بینی مسؤلیت تضامنی دولت‌های عضو اتحادیه و سازمان‌های فعال در محدوده صلاحیت سرزمینی آن‌ها در جبران خسارات وارده ناشی از نقض قواعد تعیین‌شده در مقررات مذکور موجود است، چراکه عدم اجرای مقررات اولیه مواد ۴۶ و ۴۵ از حیث قواعد عام حقوقی به منزله تقصیری تلقی می‌گردد که خسارات وارده را منتسب دولت متبوع سازمان واردکننده زیان می‌گرداند. از طرف دیگر مبنای تصویب مقررات ماده ۱۶ حمایت از حقوق دارندگان اطلاعات است و تسری این مقررات به موارد مشابهی که ضرورت حفاظت از حقوق دارندگان اطلاعات در اتحادیه اروپا احساس می‌گردد خالی از هرگونه ایراد خواهد بود.

مضاف بر آنچه بیان شد، در خصوص مفاد پروتکل الحاقی ماده ۴۵ نیز می‌توان بیان داشت، وجود چنین سازوکاری اگرچه در جهت حفظ امنیت اطلاعات اروپاییان می‌تواند مفید باشد، اما برای کشورهای خارج از اتحادیه اروپا واجد چالش‌هایی است. اولاً حاکمیت و استقلال هیچ کشوری نخواهد پذیرفت که الزامات امنیتی کشور یا اتحادیه دیگری در نظام قانونگذاری داخلی آن کشور وارد گردد، ضمن این‌که سؤال پیش رو این است که معیار تعیین سطح امنیتی لازم که در بند دوم از پروتکل الحاقی مورد تصریح قرار گرفته است چه می‌باشد؟ به جهت آنکه در هر حال امکان تفاسیر متعدد از کیفیت تعیین امنیت لازم برای حفاظت از داده‌ها وجود دارد، به نظر نمی‌رسد معیار مشخصی نیز پیش روی اتحادیه اروپا در همکاری مبادلاتی با کشورهای دیگر جهان وجود داشته باشد. ثمره این امر ایجاد رویکردهای متعدد در مواجهه با این حکم خواهد بود؛ از طرف دیگر، برخی از کشورهای در حال توسعه مانند ایران، حتی فاقد قوانین اولیه در زمینه حفاظت از داده‌های الکترونیکی مورد تبادل در مبادلات فرامرزی می‌باشند که پذیرش شرایط اتحادیه اروپا در نظام داخلی این

ایراد است. علاوه بر آن دولت نیازمند اخذ تضمین‌های کافی مبنی بر ضمانت صحت فرایند پردازش داده توسط شرکت‌های پردازشگری که در خارج از مرزهای ایران مبادرت به پردازش داده می‌نمایند، از سوی کنترل‌کننده می‌باشد.

سازوکارهای بیان‌شده نیازمند تصویب مقررات قانونی خواهد بود، چراکه اولاً حقوق ایران، مسؤولیت ناشی از فعل غیر را تنها در موارد استثنایی پذیرفته و اصل و قاعده‌ای خلاف در این خصوص وجود ندارد، لذا اجرایی‌نمودن پیشنهاد بیان‌شده نیازمند تصویب قانونی مستقل در این باب است؛ از طرف دیگر در حقوق ایران، مستفاد از مواد ۱، ۲ و ۳ قانون مسؤولیت مدنی، مطابق با صحیح‌ترین نظر از میان نظرات موجود، دولت در صورتی ملزم به جبران خسارات ناشی از اعمال اتباع خود می‌باشد که این عمل قابلیت انتساب به وی را نیز داشته باشد (۱۹)، ضمن این‌که حتی بر فرض انتساب عمل بر دولت، مبنای ارائه‌شده در ماده ۵۲۶ قانون مجازات اسلامی، تنها محکومیت دولت بر اساس میزان تقصیر وی را لازم شمرده و در صورتی که تعیین میزان مسؤولیت وی از سوی دادگاه ایرانی امکان‌پذیر نباشد، صدور حکم بر مسؤولیت مساوی تمامی مسببین ضرورت خواهد یافت؛ اما مشکل موجود این است که اگر دولت به هر دلیل مسؤولیت جبران تمامی خسارات وارده به اتباع ایرانی یا دولت ایران را عهده‌دار نشود ممکن است از یک طرف امکان دسترسی به عامل دیگر زیان فراهم نبوده و از طرف دیگر حتی بر فرض دسترسی، توانایی جبران خسارت وارده را نداشته باشد.

۲-۳-۴. چگونگی شناسایی و تقسیم مسؤولیت واردکنندگان خسارت: هوش مصنوعی ابزاری است مرکب که اشخاص متعدد در فرایند تولید آن مشارکت دارند. سؤال موجود این است که در صورتی که از عملکرد این ابزار خسارتی وارد آید، آیا می‌توان تمامی اشخاص سازنده آن را به عنوان مسؤول جبران خسارت تلقی نمود یا باید اشخاص خاصی مسؤول جبران باشند؟ از آنجا که عملکرد هوش مصنوعی همواره به عنوان کلی واحد در نظر گرفته شده و تمامی اجزای آن با

مشارکت یکدیگر در انجام وظایف محوله اقدام می‌کنند، مسأله شناسایی مسؤول اصلی در بروز خسارت بیش از پیش مشکل می‌گردد. از یک طرف اطلاق عنوان مسؤولیت بر شخصی که هیچ دخالتی در بروز آن نداشته و در انجام وظیفه خود دچار هیچ تقصیری نشده است، امری خلاف عدالت بوده و از طرف دیگر عدم جبران خسارات وارده به افراد می‌تواند وجهه نظام حقوقی را خدشه‌دار نماید. همچنین مسأله عملکرد مستقل هوش مصنوعی دیگر مشکلی است که انتساب مسؤولیت به شخصی دیگر را با چالش مواجه می‌کند. سؤال مهم این است که آیا طراحان این ابزار همیشه در معرض مسؤول تلقی شدن برای جبران خسارات وارده می‌باشند؟ آیا عنصر زمان در تعیین مسؤولیت آن نقش دارد؟ به عنوان مثال ابزاری که سال‌ها پس از تولید منجر به ایجاد خسارت می‌گردد آیا می‌تواند سازنده خود را مسؤول جبران خسارات گرداند؟

یکی از ارکان برای تحقق مسؤولیت اشخاص، «غفلت» آن‌ها از انجام وظایف مقرر (مستفاد از تبصره ماده ۱۴۵ قانون مجازات اسلامی) می‌باشد. در صورتی که شخصی وظیفه مراقبت یا پشتیبانی از ساخته خود را داشته باشد، بالطبع در صورتی که خسارت از اعمال ابزار ساخته‌شده به دست وی وارد آید، مسؤول جبران خسارات وارده می‌گردد. از این رو مسأله انتساب مسؤولیت به اشخاص در برابر ابزارهای ساخته‌شده به وسیله آن‌ها در موارد وجود وظیفه قانونی یا قراردادی آن‌ها بر نظارت بر عملکرد آن ابزار محقق است. این قاعده فارغ از عنصر زمان بوده و ارتباطی به مدت زمان تولید آن ابزار توسط تولیدکننده ندارد. از طرف دیگر پزشکان در صورتی مسؤول جبران خسارات وارده می‌باشند که خارج از عرف پزشکی مبادرت به طبابت نموده و تصمیم‌گیری‌های آن‌ها ناشی از غفلت در انجام وظایف باشد، لذا در صورتی که پزشکی مطابق با روش معمول پزشکی، مبادرت به طبابت نماید و اتفاقاً از این راه خسارتی به بیمار وارد آید، وی مسؤول جبران خسارات نخواهد بود.

مسئولیتی نداشته و جبران خسارت متوجه وی نخواهد بود، اما در صورتی که وی مسؤول پشتیبانی فنی باشد، جبران خسارات به نسبت میان مسؤولان تقسیم می‌گردد، اما در خصوص اشخاصی که مبادرت به طراحی پروتکل‌های عملکرد هوش مصنوعی می‌نمایند یا نسبت به طراحی نرم‌افزارهایی که برای بهبود عملکرد این ابزار اقدام می‌کنند، شناسایی مسؤولیت برای آنان منصرف از مسؤولیت تولیدکنندگان ابزار می‌باشد، چه این‌که در آرایه از دادگاه عالی عدالت اتحادیه اروپا (از جمله *Centre hospitalier universitaire de Besancon v Dutruieux*), 21 December (2010, CJEU, 10.5.2001, Case 203/99 (*Veedfald v Arhus Amtskommune*), 10 May 2001 و تصریح بخش «الف» از بند دوم از ماده اول دستورالعمل دستگاه‌های پزشکی مصوب ۱۹۹۳ با اصلاحات سال ۲۰۱۷ اتحادیه اروپا، نرم‌افزار طراحی‌شده برای ابزارهای الکترونیکی به منزله «خدمت» در نظر گرفته شده است نه یک «محصول». از این رو جز در مواردی که نرم‌افزار واجد عیب باشد، امکان تسری مسؤولیت به طراح آن ممکن نخواهد بود، البته از آنجا که در ابتدای تولید ابزار، نرم‌افزارهای طراحی‌شده به وسیله تولیدکننده ابزار مورد بررسی دقیق واقع می‌شوند، عملاً تسری مسؤولیت جبران خسارت به سازنده نرم‌افزار امری دشوار خواهد بود.

##### ۵. بحث

پایاده‌سازی و بکارگیری هر ابزار هوشمندی در نظام اجتماعی یک کشور نیازمند سیاستگذاری تقنینی و اجرایی سیاستگذاران می‌باشد. هوش مصنوعی به عنوان فناوری نوظهور قرن بیست و یکم از نقش مؤثری در توسعه کشورها برخوردار است. اگرچه در این پژوهش سعی بر بیان مهم‌ترین چالش‌های اخلاقی عملکرد این فناوری در حوزه سلامت شده است، اما این سازوکار دارای چالش‌های دیگری نیز در سایر حوزه‌های مرتبط با حقوق خواهد بود که ضرورت توجه هرچه بیشتر سیاستگذاران را ایجاب می‌نماید.

سازوکار تعیین مسؤولیت بر عملکرد هوش مصنوعی نیز در مواردی که در جایگاه یک پزشک مبادرت به تصمیم‌گیری می‌نماید، مطابق با قواعدی خواهد بود که در تعیین مسؤولیت پزشکان به کار گرفته می‌شود. از این رو در صورتی که عملکرد و تصمیم‌گیری هوش مصنوعی بر مبنای عرف و عادت باشد که پزشکان بر مبنای آن مبادرت به تصمیم‌گیری می‌نمایند، خسارات وارده قابلیت مطالبه از سوی بیمار را نخواهد داشت. از آنجا که علم پزشکی علم به روز بوده و ریسک‌پذیری آن موجب می‌گردد تا پزشکان در موارد انجام امر طبابت در صورت لزوم مبادرت به بکارگیری روش‌های نو در طبابت نمایند، در صورتی که پزشکی در پیاده‌سازی روشی نو مطابق با مبنای علم پزشکی مرتکب غفلت نشده باشد، مسؤول تلقی نمودن وی نیز واجد اشکال خواهد بود. این قاعده با توجه به آنچه که فوقاً بیان گردید، در خصوص هوش مصنوعی که در جایگاه یک پزشک مبادرت به تصمیم‌گیری می‌نماید نیز جاری خواهد بود (۱۷).

از سوی دیگر استفاده از ابزارهایی مانند هوش مصنوعی در درمان بیماری‌های خطرناک که نیاز به توجه بیشتر پزشک معالج دارد نیز به منزله غفلت پزشک از انجام وظایف قانونی است. از این رو در صورتی که خسارتی از عملکرد ابزار ناشی گردد، پزشک مسؤول جبران خسارات وارده خواهد بود. به عنوان مثال در مواردی مانند بیماری ذات‌الریه که نیاز به مراقبت‌های ویژه توسط پزشک دارد، در صورتی که این وظیفه به یک ابزار سپرده شود، پزشک مسؤولیت مطلق در برابر خسارات ناشی از عملکرد ابزار خواهد داشت (۱۷)، اما سؤال پیش رو این است که در صورتی که خسارت ناشی از عملکرد ابزار به جهت نقص فنی صورت گرفته باشد، مسؤول جبران چه کسی خواهد بود؟ آیا مسؤول، سازنده ابزار است یا پزشک مسؤول جبران خسارت خواهد بود؟ همانطور که بیان گردید، مسؤولیت سازنده ابزار در صورتی قابل تصور است که وی وظیفه پشتیبانی از کارایی فنی ابزار را در زمان حاضر داشته باشد. از این رو اگر وی چنین وظیفه‌ای نداشته باشد،

- شفافیت در عملکرد نهادهای متولی تولید ابزارهای مذکور و چگونگی اجرای بهتر اهداف تعیین شده در جهت حفاظت از اطلاعات شخصی کاربران.

#### ۷. تقدیر و تشکر

نگارندگان از مرکز تحقیقات اخلاق و حقوق پزشکی دانشگاه شهید بهشتی و اعضای محترم هیأت تحریریه فصلنامه ارزشمند اخلاق زیستی و سایر دست‌اندرکاران این نشریه وزین، کمال تشکر و قدردانی را دارند.

#### ۸. سهم نویسندگان

کلیه مراحل تألیف پژوهش حاضر اعم از تألیف، اصلاح، ویرایش و مطالعه و استفاده از منابع به کار گرفته شده در پژوهش، توسط نگارندگان، دکتر حسین صادقی و مهدی ناصر انجام شده است.

#### ۹. تضاد منافع

نگارندگان هیچ‌گونه تعارض منافی را گزارش نکرده‌اند.

#### ۶. نتیجه‌گیری

به کارگیری هوش مصنوعی در حوزه سلامت، علی‌رغم برخورداری از فواید فراوان، با چالش‌هایی همراه است. این چالش‌ها در محدوده کیفیت پردازش داده‌های ورودی، نحوه پردازش، دقت در انجام فرایند مذکور توسط هوش مصنوعی و احتمال ضرر، با مسائل مرتبط با احترام به استقلال فردی و حفاظت از حریم خصوصی، چالش‌های حقوقی مرتبط با حفظ محرمانگی و حریم خصوصی، کیفیت تصمیم‌گیری و مکانیسم عملکرد این ابزار و چگونگی تقسیم مسؤلیت میان عوامل انسانی دخیل در سازوکار عملکرد هوش مصنوعی همراه است. توسعه سریع ابزارهای مختلف مبتنی بر فناوری‌های نوظهور، ضرورت سیاست‌گذاری‌های تقنینی و اجرایی صحیح در کشورهای در حال توسعه جهت به کارگیری آن‌ها را ایجاب می‌نماید. به منظور پیاده‌سازی هرچه بهتر این فناوری در نظام حقوقی ایران و پیشگیری از چالش‌های پیشگفت، سیاست‌گذاری تقنینی در زمینه‌های زیر توصیه می‌گردد:

- چگونگی اعطای مجوز به سازمان‌های تولیدکننده ابزارهای هوش مصنوعی در حوزه سلامت.

- پیش‌بینی مسؤلیت تولیدکنندگان این ابزارها، چگونگی جبران خسارات وارده و دیگر ابعاد حقوقی راجع به مسؤلیت‌های قراردادی یا غیر قراردادی که ممکن است در تفسیر قواعد عمومی مندرج در قانون مدنی ایران با اختلاف نظرانی همراه باشد.

- چگونگی توزیع ابزارهای تولیدشده توسط تولیدکنندگان خارجی در بازارهای داخلی جهت حفظ رقابت میان تولیدکنندگان داخلی و خارجی.

- پیش‌بینی مقرراتی در خصوص کیفیت حفاظت از اطلاعات شخصی کاربران این ابزارها از طریق بهره‌مندی از تجربیات نظام حقوقی اتحادیه اروپا در تصویب آیین‌نامه ۲۰۱۶.

## References

1. Darzi A, Quilter-Pinner H, Kibasi T. Institute for Public Policy Research (IPPR), Better health and care for all: A 10-point plan for the 2020s The Lord Darzi Review of Health and Care. New York: Briefing; 2018. Available at: <https://www.ippr.org/research/publications/better-health-and-care-for-all>. Accessed October 3, 2019.
2. NHS, GP at Hand. Available at: <https://www.gpathand.nhs.uk>. Accessed October 1, 2019.
3. Varun G, Peng L, Coram M. Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs. *Jama Review* 2016; 316(22): 1-9.
4. Moorfields Eye Hospital NHS Foundation Trust, Moorfields announces research partnership. Available at: <https://www.moorfields.nhs.uk/news/moorfields-announces-research-partnership>. Accessed October 2, 2019.
5. McCarthy J. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. *AI Magazine* 2006; 27(4): 1-15.
6. Robin KH. What an Algorithm Is. *Phil & Technol* 2016; 29(1): 35-59.
7. Burrell J. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. *Big Data & Society* 2016; 3(1): 1-12.
8. Caliskan A, Bryson JJ, Narayanan A. Semantics Derived Automatically from Language Corpora Contain Human-like Biases. *Artificial Intelligence Studies* 2017; 356(6334): 183-186.
9. Romei A, Ruggieri S. A Multidisciplinary Survey on Discrimination Analysis. *The Knowledge Engineering Review* 2017; 29(5): 1-54.
10. Angwin J. Machine Bias. Portland: Wall Street; 2016. Available at: <https://www.propublica.org/article/machinebias-risk-assessments-in-criminal-sentencing>. Accessed October 1, 2019.
11. Tutt A. An FDA for Algorithms. *Admin L Rev* 2017; 83(69): 1-29.
12. Crawford K, Calo R. There is a Blind Spot in AI Research. *Europe PMC* 2016; 538(7625): 311-313.
13. Hart R. If you're not a White Male. Artificial Intelligence's Use in Healthcare could be Dangerous. Massachusetts: Harvard Medical School; 2019. Available at: <https://www.qz.com/1023448/if-youre-not-a-white-male-artificial-intelligences-use-in-health-care-could-be-dangerous/>. Accessed October 2, 2019.
14. Arman A, Varvaei A, Jafari MJ. Ethical Dimensions of Public Information Protection Regulations and Its Impact on Iranian Laws and Citizenship Rights in Cyberspace. *Bioethics Journal* 2018; 8(30): 119-136.
15. Clifford D, Ausloos J. Data Protection and the Role of Fairness. London: Oxford University Press; 2017.
16. Hacker P. Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law. McLean: Alion; 2018. Available at: [https://www.academia.edu/36494567/Teaching\\_Fairness\\_to\\_Artificial\\_Intelligence\\_Existing\\_and\\_Novel\\_Strategies\\_against\\_Algorithmic\\_Discrimination\\_under\\_EU\\_Law\\_Common\\_Market\\_Law\\_Review\\_forthcoming](https://www.academia.edu/36494567/Teaching_Fairness_to_Artificial_Intelligence_Existing_and_Novel_Strategies_against_Algorithmic_Discrimination_under_EU_Law_Common_Market_Law_Review_forthcoming). Accessed September 23, 2019.
17. Schonberger D. Artificial intelligence in healthcare: A critical analysis of the legal and ethical implications. *International Journal of Law and Information Technology* 2019; 2(27): 91-121.
18. Laurie G, Harmon S, Porter G. Mason and McCall Smith's Law and Medical Ethics. 10th ed. Oxford: Oxford University Press; 2016.
19. Rahpik S. Civil Liability Rights and Compensation. 1st ed. Tehran: Khorsandi Publication; 2016.
20. EC Communication Artificial Intelligence for Europe. Available at: <https://www.ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>. Accessed May 7, 2020.
21. General Data Protection Regulation. Available at: <https://www.gdpr-info.eu/>. Accessed May 7, 2020.
22. EU Consumer Rights Directive. Available at: [https://www.ec.europa.eu/info/law/law-topic/consumer-law/consumer-contract-law/consumer-rights-directive\\_en](https://www.ec.europa.eu/info/law/law-topic/consumer-law/consumer-contract-law/consumer-rights-directive_en). Accessed May 7, 2020.



# BEJ

Bioethics Journal

2020; 10(35): e17

Journal Homepage: <http://journals.sbmu.ac.ir/en-be>



## ORIGINAL RESEARCH

# Legal-Ethical Challenges of the EU regulation on Artificial Intelligence Performance in Health Domian

Hossein Sadeghi<sup>1\*</sup> , Mahdi Naser<sup>2</sup>

1. Ph.D. in Private Law, Assistant Professor of Business Department, Faculty of Entrepreneurship University of Tehran, Tehran, Iran.

2. Ph.D. Student in Private Law, Judicial Sciences and Administrative Services University, Tehran, Iran.

### ARTICLE INFORMATION

#### Article history:

**Received:** 28 October 2019

**Accepted:** 09 June 2020

**Published online:** 17 April 2021

#### Keywords:

Artificial Intelligence  
Challenges and Solutions  
Preserving Human Dignity  
Protecting Privacy  
Personal Data Protection  
Responsibility

\* Corresponding Author: Hossein Sadeghi

Address: Faculty of Entrepreneurship University of Tehran, Tehran, Iran.

Postal Box: 1417935840

Tel: 09123930336

Email: [hosadeghi@ut.ac.ir](mailto:hosadeghi@ut.ac.ir)

### ABSTRACT

**Background and Aim:** Artificial intelligence is a tool that has led to enormous changes in different fields such as health. But despite the many uses of this tool, there are also challenges in its operation that require legislative and executive policymaking to address them. The purpose of this study is to explain the ethical and legal challenges under the EU regulations in artificial intelligence performance in the field of health.

**Materials and Methods:** The present qualitative research explains the legal-ethical challenges of artificial intelligence performance in the field of health based on the analysis of the EU General Data Protection Regulation.

**Findings:** The most important challenges in the mechanism of performance of artificial intelligence from the ethical point of view are inequality, racial discrimination, Lack of accuracy in data processing, etc as legally include insufficient care in the protection of personal information, Lack of privacy, and liability and the mechanism of identification and division of responsibility in cases of damage caused by the operation of the tool. In this article, an attempt has been made to review each of these cases and provide appropriate solutions.

**Ethical Considerations:** In compiling this article, all moral principles including fidelity, honesty and originality of the text have been observed.

**Conclusion:** Despite the challenges expressed in this study, there is adequate capacity in the Iranian legal system to address some of the concerns raised, but in order to achieve a better situation, especially the apply of standards adopted in EU regulations, it is necessary to use artificial intelligence technology especially in the field of health, by legislative policy, including the adoption of efficient and executive laws on the quality of licensing organizations that produce these tools, how to compensate the damages caused by manufacturers and the rights of aggrieved party, public awareness, quality of these tools and transparency In the Iranian legal system.

© Copyright (2018) Medical Ethics and Law Research Center, Shahid Beheshti University of Medical Sciences, Tehran, Iran.

Cite this article as:

Sadeghi H, Naser M. Legal-Ethical Challenges of the EU regulation on Artificial Intelligence Performance in Health Domian. *Bioethics Journal* 2020; 10(35): e17.