شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

فصلنامه تمدن حقوقی

تمدن حقوقی

دوره ۸ - شماره ۲۶ - زمستان ۱۴۰۴

Legal Civilization
Vol. 8, No. 26, Winter 2026
Pages: 445-476
Article Type: Original Research
https://www.pzhfars.ir/article_238925.html
doi: 10.22034/lc.2026.570183.1728

تمدن حقوقی
دوره ۸، شماره ۲۶، زمستان ۱۴۰۴
صفحات: ۴۷۶-۴۴۵
نوع مقاله: پژوهشی

مسئولیت مدنی ناشی از پردازش خودکار داده‌های شخصی توسط هوش مصنوعی در حقوق ایران و افغانستان (با نگاهی به اسناد بین‌المللی)

راضیه جعفرزاده
کارشناس ارشد حقوق خصوصی، دانشکده علوم انسانی، دانشگاه حکیم سبزواری، سبزوار، ایران (نویسنده مسئول)
raziye7167@gmail.com
http://orcid.org/0009-0005-5486-5573

وحید حمیدی
قاضی دادگستری افغانستان، کارشناس ارشد حقوق خصوصی، دانشگاه حکیم سبزواری، سبزوار، ایران
hamidiwahid608@gmail.com

محمدرضا رشید
کارشناسی حقوق، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد الکترونیکی، تهران، ایران
rashidmohamadreza85@gmail.com

چکیده
گسترش روزافزون هوش مصنوعی و اتکای فزاینده آن بر پردازش خودکار داده‌های شخصی، چالش‌های نوینی را در حوزه مسئولیت مدنی پدید آورده است. تصمیم‌گیری‌های الگوریتمی، به‌ویژه در فقدان نظارت انسانی مؤثر، می‌تواند منجر به نقض حریم خصوصی، ورود خسارات مادی و معنوی و تضعیف حقوق اشخاص شود؛ امری که قواعد سنتی مسئولیت مدنی را با دشواری‌های جدی در زمینه انتساب عمل زیان‌بار و اثبات رابطه سببیت مواجه ساخته است. به این ترتیب، پرسش اصلی پژوهش آن است که نظام‌های حقوقی ایران و افغانستان تا چه اندازه قادرند با تکیه بر قواعد موجود، مسئولیت مدنی ناشی از پردازش خودکار داده‌های شخصی توسط هوش مصنوعی را سامان دهند و چه الگویی برای جبران خسارت مناسب‌تر است؟ هدف پژوهش، تحلیل تطبیقی رویکرد حقوق ایران و افغانستان نسبت به مسئولیت مدنی ناشی از پردازش داده‌های شخصی و ارزیابی ظرفیت اسناد بین‌المللی در تکمیل و هدایت این نظام‌ها است. روش پژوهش توصیفی-تحلیلی با رویکرد تطبیقی و مبتنی‌بر مطالعه منابع حقوقی داخلی و اسناد بین‌المللی است. یافته‌های پژوهش نشان می‌دهند که هرچند قواعد عمومی مسئولیت مدنی در ایران و افغانستان قابلیت اعمال بر خسارات ناشی از هوش مصنوعی را دارند، اما در عمل با محدودیت‌هایی مواجه‌اند و گرایش به مسئولیت مبتنی‌بر خطر و اصل پاسخگویی می‌تواند کارآمدتر باشد. نتیجه پژوهش حاکی از آن است که همسویی با استانداردهای بین‌المللی و بازتعریف مسئولیت مدنی، نقش مؤثری در حمایت از داده‌های شخصی و جبران مؤثر خسارات خواهد داشت.

واژگان کلیدی: هوش مصنوعی، پردازش خودکار، مسئولیت مدنی، ایران و افغانستان، اسناد بین‌المللی.

دریافت مقاله: ۱۴۰۴/۱۰/۱۶ –بازنگری مقاله: ۱۴۰۴/۱۱/۱۵ –پذیرش مقاله: ۱۴۰۴/۱۲/۰۱

Civil Liability Arising from Automated Processing of Personal Data by Artificial Intelligence in Iranian and Afghan Law (with a Look at International Documents)

Raziyeh Jafarzade
Master of Science in Private Law, Faculty of Humanities, Hakim Sabzevari University, Sabzevar, Iran (Corresponding Author)

Vahid Hamidi
Judge of Justice of Afghanistan, Master of Private Law, Hakim Sabzevari University, Sabzevar, Iran

Mohammadreza Rashid
Bachelor of Laws, Faculty of Humanities, Islamic Azad University, Electronic Branch, Tehran, Iran

Abstract
The increasing expansion of artificial intelligence and its growing reliance on automated processing of personal data have created new challenges in the field of civil liability. Algorithmic decision-making, especially in the absence of effective human oversight, can lead to breaches of privacy, material and moral damages, and the weakening of individual rights; a matter that poses serious difficulties for traditional rules of civil liability in the field of attributing harmful acts and proving causation. Accordingly, the main question of the article is to what extent the legal systems of Iran and Afghanistan are able to organize the civil liability arising from the automated processing of personal data by artificial intelligence by relying on the existing rules, and what model is more appropriate for compensation. The aim of the research is a comparative analysis of the approach of Iranian and Afghan law to civil liability arising from the processing of personal data and an evaluation of the capacity of international documents to complete and guide these systems. The research method is descriptive-analytical with a comparative approach and based on the study of domestic legal sources and international documents. The research findings show that although the general rules of civil liability in Iran and Afghanistan are applicable to damages caused by artificial intelligence, in practice they face limitations, and the tendency towards risk-based liability and the principle of accountability can be more efficient. The result of the research indicates that aligning with international standards and redefining civil liability will play an effective role in protecting personal data and effectively compensating damages.

Keywords: Artificial Intelligence, Automated Processing, Civil Liability, Iranian and Afghan, International Documents.

Received: 2026/01/06 - Review: 2026/02/04 - Accepted: 2026/02/20

ارجاع:
جعفرزاده، راضیه؛ حمیدی، وحید؛ رشید، محمدرضا؛ (۱۴۰۴)، مسئولیت مدنی ناشی از پردازش خودکار داده‌های شخصی توسط هوش مصنوعی در حقوق ایران و افغانستان (با نگاهی به اسناد بین‌المللی)، تمدن حقوقی، شماره ۲۶.

مقدمه

پیشرفت شتابان فناوری هوش مصنوعی و گسترش کاربرد آن در عرصه‌های گوناگون اجتماعی، اقتصادی و اداری شیوه‌های سنتی پردازش اطلاعات را دگرگون ساخته است. امروزه بخش قابل‌توجهی از داده‌های شخصی افراد[1] به‌صورت خودکار و بدون مداخله مستقیم انسان توسط سامانه‌های هوشمند پردازش می‌شود. این تحول فناورانه، در کنار کارآمدی و سرعت بالا، مخاطرات جدی حقوقی را نیز به همراه دارد؛ چراکه تصمیم‌گیری‌های الگوریتمی می‌توانند به نقض حریم خصوصی، تبعیض، افشای غیرمجاز داده‌ها و ورود خسارات مادی و معنوی به اشخاص منجر شوند (آقایی طوق و ناصر، ۱۳۹۹، ۴۲). در چنین شرایطی، مسئله مسئولیت مدنی ناشی از پردازش خودکار داده‌های شخصی توسط هوش مصنوعی به یکی از دغدغه‌های اساسی نظام‌های حقوقی معاصر بدل شده است.

چالش اصلی در این حوزه آن است که قواعد سنتی مسئولیت مدنی که عمدتاً بر رفتار انسانی، تقصیر شخصی و رابطه مستقیم سببیت استوارند، در مواجهه با فناوری‌های خودکار و غیرشفاف کارایی لازم را ندارند. پیچیدگی الگوریتم‌ها، استقلال نسبی سامانه‌های هوشمند و تعدد کنشگران

۱- از اطلاعات هویتی و مالی گرفته تا داده‌های رفتاری و زیستی

دخیل در طراحی، توسعه و بهره‌برداری از هوش مصنوعی، انتساب عمل زیان‌بار و تعیین شخص مسئول را با دشواری مواجه می‌سازد (علی پناهی و همکاران، ۱۴۰۳، ۶). این وضعیت در نظام‌های حقوقی ایران و افغانستان[۲] اهمیت مضاعف می‌یابد و ضرورت بازاندیشی در الگوهای مسئولیت مدنی را برجسته می‌کند.

در این چهارچوب، پرسش اصلی پژوهش آن است که حقوق ایران و افغانستان تا چه اندازه توان پاسخگویی به خسارات ناشی از پردازش خودکار داده‌های شخصی توسط هوش مصنوعی را دارند و آیا قواعد موجود مسئولیت مدنی می‌توانند حمایت مؤثری از حقوق اشخاص فراهم آورند؟ همچنین، این پرسش مطرح می‌شود که اسناد و استانداردهای بین‌المللی چه نقشی در جهت‌دهی به الگوی مطلوب مسئولیت مدنی در این حوزه ایفاء می‌کنند و تا چه حد می‌توان از آن‌ها برای تکمیل نظام‌های حقوقی داخلی بهره گرفت؟

هدف پژوهش حاضر، تحلیل چهارچوب مسئولیت مدنی ناشی از پردازش خودکار داده‌های شخصی در حقوق ایران و افغانستان و ارزیابی میزان کارآمدی آن در مواجهه با چالش‌های هوش مصنوعی است. این پژوهش می‌کوشد ضمن‌شناسایی نقاط قوت و ضعف رویکردهای موجود، ظرفیت اسناد بین‌المللی را در بازتعریف مسئولیت مدنی و تضمین جبران مؤثر خسارت مورد توجه قرار دهد و الگویی هماهنگ‌تر با تحولات فناورانه پیشنهاد کند. روش پژوهش، توصیفی-تحلیلی با رویکرد تطبیقی است. در این راستا، ابتدا مفاهیم و چالش‌های ناشی از پردازش خودکار داده‌های شخصی توسط هوش مصنوعی تبیین شده، سپس قواعد مسئولیت مدنی در حقوق ایران و افغانستان مورد تحلیل قرار می‌گیرد. در ادامه، اسناد بین‌المللی مرتبط با حفاظت از داده‌های شخصی و مسئولیت‌پذیری در هوش مصنوعی بررسی و میزان تأثیرگذاری آن‌ها بر نظام‌های حقوقی داخلی ارزیابی می‌شود.

۲- که فاقد مقررات خاص و جامع در زمینه هوش مصنوعی و حفاظت از داده‌های شخصی هستند

یافته‌های پژوهش نشان می‌دهند که هرچند قواعد عمومی مسئولیت مدنی در حقوق ایران و افغانستان از انعطاف‌پذیری نسبی برخوردارند و می‌توان آن‌ها را بر برخی خسارات ناشی از پردازش خودکار داده‌ها اعمال کرد، اما در عمل با کاستی‌های جدی مواجه‌اند. دشواری اثبات تقصیر، ابهام در رابطه سببیت و فقدان سازوکارهای خاص جبران خسارت، حمایت مؤثر از اشخاص آسیب‌دیده را محدود می‌سازد. در مقابل، اسناد بین‌المللی با تأکید بر اصولی چون پاسخگویی، شفافیت و جبران مؤثر خسارت، رویکردی کارآمدتر و متناسب با ویژگی‌های هوش مصنوعی ارائه می‌دهند. جنبه نوآوری پژوهش در تحلیل تطبیقی مسئولیت مدنی ناشی از پردازش خودکار داده‌های شخصی در حقوق ایران و افغانستان و پیوند آن با استانداردهای بین‌المللی نهفته است؛ امری که در ادبیات حقوقی داخلی کمتر مورد توجه قرار گرفته است. نتیجه پژوهش حاکی از آن است که بازتعریف مسئولیت مدنی با گرایش به الگوهای مبتنی‌بر خطر و پاسخگویی، همراه با بهره‌گیری از معیارهای بین‌المللی، می‌تواند نقش مؤثری در حمایت از داده‌های شخصی و تضمین جبران خسارت در عصر هوش مصنوعی ایفاء کند.

۱- هوش مصنوعی در پردازش خودکار داده‌های شخصی

پردازش خودکار داده‌های شخصی به‌وسیله هوش مصنوعی، یکی از برجسته‌ترین نمودهای تحول دیجیتال در نظام‌های معاصر حکمرانی داده است. برخلاف پردازش سنتی که مبتنی‌بر تصمیم‌گیری مستقیم انسان بود، هوش مصنوعی با تکیه بر الگوریتم‌های یادگیری ماشین، کلان‌داده و تحلیل پیش‌بینانه، قادر است داده‌های شخصی را در مقیاسی وسیع، با سرعت بالا و حداقل مداخله انسانی تحلیل و تفسیر کند. این ویژگی، اگرچه کارآمدی و دقت تصمیم‌گیری را افزایش می‌دهد، اما هم‌زمان خطرات جدی برای حقوق بنیادین افراد، به‌ویژه حق حریم خصوصی و حق حمایت از داده‌های شخصی، ایجاد می‌کند.

پردازش خودکار داده‌های شخصی به فرایندی اطلاق می‌شود که در آن جمع‌آوری، ذخیره،

تحلیل و تصمیم‌گیری درباره داده‌ها به‌طور کامل یا غالباً توسط سامانه‌های الگوریتمی انجام می‌گیرد.[۳] ویژگی اساسی این نوع پردازش، «تصمیم‌گیری خودکار» است؛ تصمیمی که می‌تواند آثار حقوقی یا پیامدهای قابل‌توجهی برای شخص موضوع داده ایجاد کند، بدون آن‌که انسان مستقیماً در آن مداخله داشته باشد. نمونه‌های بارز آن را می‌توان در نظام‌های اعتبارسنجی مالی، تشخیص چهره، ارزیابی ریسک بیمه‌ای، استخدام هوشمند و نظارت دیجیتال مشاهده کرد.

تحلیل عملکرد این سامانه‌ها نشان می‌دهد که هوش مصنوعی نه‌تنها داده‌های آشکار، بلکه داده‌های استنباطی و پیش‌بینی‌شده را نیز تولید می‌کند. به‌عنوان مثال، الگوریتم‌ها می‌توانند از الگوهای رفتاری افراد، اطلاعاتی درباره وضعیت سلامت، گرایش‌های سیاسی یا ویژگی‌های شخصیتی آنان استخراج کنند؛ داده‌هایی که گاه حتی خود فرد نیز از وجود آن‌ها آگاه نیست (Mittelstadt et al.,2016,11). این امر دامنه داده‌های شخصی را گسترش داده و مرزهای سنتی حریم خصوصی را با چالش مواجه ساخته است. یکی از مهم‌ترین مسائل در پردازش خودکار داده‌ها، عدم شفافیت الگوریتمی است. بسیاری از سامانه‌های هوش مصنوعی، به‌ویژه مدل‌های یادگیری عمیق، به‌صورت «جعبه سیاه» عمل می‌کنند؛ بدین معنا که منطق درونی تصمیم‌گیری آن‌ها برای کاربران و حتی توسعه‌دهندگان به‌طور کامل قابل توضیح نیست. این عدم شفافیت، امکان نظارت حقوقی، اعتراض مؤثر و احقاق حق زیان‌دیدگان را محدود می‌سازد و در نتیجه، مسئولیت‌پذیری پردازش‌کنندگان داده را تضعیف می‌کند.

در واکنش به این چالش‌ها، اسناد بین‌المللی رویکردی محتاطانه و مبتنی‌بر حقوق بشر اتخاذ کرده‌اند. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا[۴] باشناسایی خطرات تصمیم‌گیری خودکار، اصولی نظیر حداقل‌گرایی داده، محدودیت هدف، شفافیت و حق مداخله انسانی را مورد تأکید قرار داده است.[۵] همچنین، اسناد سازمان همکاری و توسعه اقتصادی[۶] و توصیه‌نامه یونسکو

3- GDPR, 2016, Art. 4
4- GDPR
5- GDPR, 2016, Arts. 5 & 22

درباره اخلاق هوش مصنوعی، بر لزوم پاسخگویی، ارزیابی ریسک و حفاظت ویژه از داده‌های شخصی در سامانه‌های هوشمند تأکید می‌کنند.[۷]

در حقوق ایران و افغانستان، هرچند مقررات خاص و جامع درباره هوش مصنوعی و پردازش خودکار داده‌های شخصی وجود ندارد، اما قواعد عام حمایت از حریم خصوصی و منع اضرار به غیر، ظرفیت اعمال بر این حوزه را دارا هستند. بااین‌حال، تحلیل عملکرد هوش مصنوعی نشان می‌دهد که این قواعد، بدون بازتفسیر متناسب با ویژگی‌های فنی الگوریتم‌ها، پاسخگوی پیچیدگی‌های پردازش خودکار داده‌ها نخواهند بود. به نظر می‌رسد پردازش خودکار داده‌های شخصی توسط هوش مصنوعی، صرفاً یک تحول فنی نیست، بلکه دگرگونی عمیق در نسبت میان فرد، داده و قدرت تصمیم‌گیری ایجاد کرده است. ازاین‌رو، هرگونه تحلیل مسئولیت مدنی در این حوزه باید با درک دقیق سازوکارهای فنی هوش مصنوعی و پذیرش این واقعیت همراه باشد که خطرات ناشی از پردازش خودکار، ذاتی این فناوری‌اند. نادیده گرفتن این امر، به تداوم خلأ حمایتی و تضعیف حقوق اشخاص در برابر تصمیم‌گیری‌های الگوریتمی خواهد انجامید.

۲- انتساب مسئولیت در پردازش خودکار داده‌ها

پردازش خودکار داده‌های شخصی توسط سامانه‌های هوش مصنوعی، علاوه بر چالش‌های ماهوی مرتبط با حریم خصوصی، مسئله‌ای بنیادین در حوزه مسئولیت مدنی ایجاد می‌کند و آن تعیین معیارهای انتساب عمل زیان‌بار است. در ساختارهای سنتی مسئولیت، انتساب رفتار زیان‌بار به فاعل انسانی، مبنای اصلی تحقق مسئولیت به‌شمار می‌رفت؛ حال آن‌که در سامانه‌های هوشمند، تصمیم‌گیری‌ها حاصل تعامل پیچیده الگوریتم‌ها، داده‌ها و مداخلات غیرمستقیم انسان‌ها است. این وضعیت، مرز میان عمل انسانی و عملکرد فنی را مبهم ساخته وشناسایی شخص مسئول را با دشواری‌های نظری و عملی همراه کرده است. ازاین‌رو، تحلیل انتساب مسئولیت در پردازش خودکار داده‌ها مستلزم بررسی دقیق نقش

6- OECD
7- OECD, 2019

عامل انسانی، توسعه‌دهنده و بهره‌بردار سامانه‌های هوش مصنوعی است. این مبحث می‌کوشد با تمرکز بر معیارهای انتساب عمل زیان‌بار در سامانه‌های هوشمند، چهارچوبی منسجم برای تعیین مسئولیت و جبران خسارت در بستر پردازش خودکار داده‌های شخصی ارائه دهد.

۲-۱- معیارهای انتساب عمل زیان‌بار در سامانه‌های هوشمند

انتساب مسئولیت در سامانه‌های هوشمند، به‌ویژه آن جا که پردازش داده‌ها به‌صورت خودکار انجام می‌شود، با پیچیدگی‌های چشمگیری مواجه است. در نظام‌های مسئولیت مدنی سنتی، مسئولیت متوجه شخصی است که عمل زیان‌بار را انجام داده یا تقصیر او سبب ورود خسارت شده است. این قاعده بر مبنای وجود اراده، قصد یا بی‌احتیاطی انسانی شکل گرفته است؛ اما در سامانه‌های هوش مصنوعی که عملکردها غالباً مبتنی‌بر الگوریتم‌های یادگیری خودکار است، مفهوم «فاعل انسانی» به‌صورت مستقیم وجود ندارد، و این امر موجب پدید آمدن خلأ قابل‌توجه در انتساب مسئولیت می‌شود (باقری، ۱۴۰۴، ۵۹).

یکی از مهم‌ترین معیارهای مطرح در ادبیات حقوقی و فنی برای انتساب عمل زیان‌بار، «قواعد نقش‌محور»[8] است؛ یعنی تعیین این که کدام نقش در زنجیره خلق و به‌کارگیری سامانه‌های هوشمند مسئول قرار دارد. بر اساس دیدگاه‌های اخیر، چون سامانه‌های هوش مصنوعی فاقد شخصیت حقوقی هستند، نمی‌توان آن‌ها را به‌عنوان «فاعل مسئول» تلقی کرد و مسئولیت باید به یکی از کنشگران انسانی یا حقوقی مرتبط با طراحی، توسعه، به‌کارگیری یا نگهداری سیستم نسبت داده شود. این رویکرد در مباحث نظری مورد توجه قرار گرفته، چراکه سیستم‌های هوشمند به‌واسطه برنامه‌ریزی و پارامترسازی توسعه‌دهندگان و بهره‌برداران عمل می‌کنند و تصمیماتشان در چهارچوب دستورات و داده‌های ورودی شکل می‌گیرد (Soh,2023,597).

در مسئولیت مدنی، معمولاً دو نوع انتساب مسئولیت مورد بحث قرار می‌گیرد: «علیت حقوقی» و «نسبت نقش». علیت حقوقی عبارت است از رابطه مستقیم بین عمل زیان‌بار و خسارت وارد شده؛

8- role-based doctrines

یعنی تعیین این که کدام فعل یا ترک فعل سبب وقوع ضرر شده است. در سامانه‌های هوشمند، این رابطه می‌تواند پیچیده و غیرمستقیم باشد؛ زیرا الگوریتم‌ها ممکن است بر اساس داده‌های آموزشی ناقص، سوءگیری‌های پنهان یا خطاهای منطقی، بدون دخالت انسانی مستقیم، دست به اعمالی بزنند که منجر به خسارت شوند. چنین وضعیتی موجب می‌شود که قاعده عادی علیت، نیازمند تفسیر و توسعه برای پوشش خسارات ناشی از تصمیمات خودکار باشد (Laxmi,2025,436).

معیار دیگر، «نسبت نقش» بر سامانه‌های هوش مصنوعی است. از منظر این معیار، مسئولیت مدنی می‌تواند بر اساس میزان کنترلی که توسعه‌دهنده یا بهره‌بردار بر عملکرد سیستم دارد تعیین شود. اگرچه الگوریتم‌ها تا حدی خودمختار عمل می‌کنند، اما طراحی، پارامترسازی، داده‌های آموزشی و انتخاب اهداف توسط انسان‌ها انجام می‌شود؛ بنابراین حداقل در مرحله طراحی و توسعه، کنترل انسانی وجود دارد. به همین دلیل، برخی مراجع حقوقی و دانشگاهی پیشنهاد داده‌اند که انتساب مسئولیت باید بر مبنای درجه کنترلی باشد که کنشگرن انسانی بر عملکرد سیستم هوشمند دارند؛ بدین معنا که هر اندازه نقش و تسلط انسانی بیشتر باشد، انتساب مسئولیت به آن کنشگر تقویت شود (Laxmi,2025,439).

همچنین، در اسناد و پیشنهادهای قانونی در اتحادیه اروپا، تلاش شده است تا با تعریف «کاربر حرفه‌ای» و «اپراتور سیستم هوش مصنوعی»، مسئولیت را نه‌فقط به تولیدکننده، بلکه به بهره‌بردارانی که سامانه را در شرایط مشخص به‌کار می‌گیرند، نسبت دهند. این دیدگاه نشان‌دهنده تغییر از انتساب صرفاً مبتنی‌بر تقصیر به سمت سازوکارهای نوینی است که می‌کوشند مسئولیت را در زنجیره ارزش گسترده‌تر پخش کنند و از خلأ قضایی جلوگیری نمایند (Gredka-Ligarska,2024,17). در ادبیات علمی نیز معیارهایی چون «رویه‌های قابل پیش‌بینی و استاندارد مؤثر» مورد توجه قرار گرفته‌اند. بر اساس این معیار، توسعه‌دهندگان موظف‌اند پیش از راه‌اندازی سامانه‌های هوشمند، روش‌های معتبر و استانداردی برای آزمون، اعتبارسنجی و بهینه‌سازی عملکرد سیستم به کار برند؛ به‌گونه‌ای که خطاهای غیرقابل‌پیش‌بینی کاهش یابد و امکان بازشناسی و توضیح تصمیمات الگوریتمی فراهم شود. در صورتی که توسعه‌دهنده یا بهره‌بردار نسبت به اتخاذ این رویه‌ها کوتاهی کند، می‌توان آن را مبنای

انتساب مسئولیت دانست (Pfeiffer,2023,7).

به نظر می‌رسد انتساب مسئولیت در سامانه‌های هوشمند بدون تکیه بر معیارهای چندبعدی امکان‌پذیر نیست. معیارهایی مانند علیت حقوقی، سطح کنترل انسانی و اتخاذ رویه‌های استاندارد طراحی و آزمون سامانه‌ها، نه‌تنها می‌توانند خلأهای ناشی از فقدان شخصیت حقوقی در هوش مصنوعی را پر کنند، بلکه باعث می‌شوند مسئولیت حقوقی در نظام‌های مدنی با دقت و عدالت بیشتری تحقق یابد. در این منظر، مجموعه این معیارها باید در چهارچوب قانون‌گذاری نوین یا تفسیر تکاملی قواعد موجود گنجانده شود تا زیان‌دیدگان بتوانند در مواجهه با تصمیمات خودکار، جبران خسارت را مطالبه نمایند و نظام حقوقی نیز پاسخگوی تحولات فناوری باشد.

۲-۲- مسئولیت عامل انسانی در کنار هوش مصنوعی

یکی از مهم‌ترین چالش‌های حقوقی در عرصه مسئولیت مدنی ناشی از فناوری‌های هوش مصنوعی آن است که این سامانه‌ها فاقد اراده، قصد، یا شخصیت حقوقی هستند و در نتیجه نمی‌توان به‌طور مستقیم خود هوش مصنوعی را «فاعل مسئول» زیان‌های وارده دانست. این نکته بارها در ادبیات حقوقی مطرح شده است: هوش مصنوعی به‌عنوان ابزار یا سیستم عمل می‌کند، نه به‌عنوان شخصی که بتواند حقوق و تکالیف قانونی مستقل داشته باشد و بنابراین مسئولیت باید به شخص یا اشخاص انسانی یا حقوقی مرتبط با طراحی، توسعه، بهره‌برداری و به‌کارگیری آن نسبت داده شود (دادآفرین و اعظمی راد، ۱۴۰۴، ۲۲).

در حقوق مدرن، پیشنهاد شده است که انتساب مسئولیت باید بر مبنای معیارهای موضوعی مانند «کنترل و تسلط انسانی» بر سامانه باشد؛ یعنی هر اندازه نقش انسان در کنترل، نظارت و تصمیم‌گیری مؤثرتر باشد، مسئولیت انسانی نیز تقویت می‌شود. به‌عنوان نمونه، در تنظیمات «انسان در مدار تصمیم»[۹]، کاربر یا ناظر انسانی اطلاعات ورودی یا خروجی‌های سامانه را بررسی و اصلاح می‌کند

9- Human-in-the-Loop

(Chiodo,2025,35). چنین ساختاری ناظر بر این است که انسان می‌تواند مسئولیت عملکرد سامانه را بپذیرد، زیرا ابزار تحت تسلط فنی او قرار دارد و تصمیم نهایی تابع اراده انسانی است.

از سوی دیگر، چنانچه هوش مصنوعی در حوزه‌هایی به‌کار رود که کنترل انسانی حداقلی است و تصمیمات مهم بدون دخالت مستقیم انسان اتخاذ می‌شود، قواعد مسئولیت سنتی بر «علت‌شناسی» و «ارتباط سببیت» میان فعل انسانی و نتیجه زیان‌بار با پیچیدگی‌های بیشتری روبرو می‌گردند. به همین دلیل، حقوقدانان پیشنهاد داده‌اند که نقش انسان می‌تواند در مقام توسعه‌دهنده، بهره‌بردار یا شخص حقوقی‌ای باشد که سامانه را معرفی و در چرخه تولید تا بهره‌برداری قرار داده است؛ و در این موارد، معیار مسئولیت باید مبتنی‌بر رفتار انسانی در مراحل مختلف توسعه و به‌کارگیری سامانه باشد (قیصری اطربی و همکاران، ۱۴۰۴، ۲۳۵).

در حقوق ایران نیز این رویکرد دیده می‌شود: هوش مصنوعی در نظام حقوقی ایران فاقد شخصیت حقوقی است و نمی‌تواند خود مسئول مدنی شناخته شود، بنابراین مسئولیت زیان‌های ناشی از عملکرد آن به اشخاص مرتبط نسبت داده می‌شود، مثلاً سازنده، توسعه‌دهنده یا کاربری که از فناوری به شکلی نامناسب استفاده کرده است. این امر مطابق ماده اول قانون مسئولیت مدنی مصوب ۱۳۳۹ است که هرکس به دیگری خسارت وارد کند، ضامن است و مسئولیت ناشی از فعل زیان‌بار را بر عهده دارد؛ البته اجرای این ماده در زمینه هوش مصنوعی به تفسیرهای تکاملی از قبیل «مسئولیت مبتنی‌بر خطر» یا «مسئولیت محصول» نیاز دارد تا خلاءهای قانونی برطرف شود. در سطح بین‌المللی نیز تلاش‌ها برای تعیین نقش عامل انسانی در کنار هوش مصنوعی در قالب اسناد و پروژه‌های حقوقی ادامه دارد. از جمله در اتحادیه اروپا با طرح‌هایی مانند دستورالعمل مسئولیت مدنی هوش مصنوعی[۱۰] و مقررات هوش مصنوعی[۱۱]، سعی شده است بین توسعه‌دهندگان، بهره‌برداران و سایر اشخاص دخیل تمایز قائل شود و مسئولیت‌ها را روشن‌تر سازد تا در صورت بروز خسارت، بار اثبات و مسئولیت

10- AI Liability Directive
11- AI Act

به‌طور منطقی به سوی انسان‌ها تنظیم گردد (Noto La Diega&Bezerra,2024,19).

به نظر نگارندگان، نظام مسئولیت مدنی هنگامی می‌تواند با پیچیدگی‌های سامانه‌های هوشمند هماهنگ شود که نقش عامل انسانی در کنار هوش مصنوعی به‌صورت دقیق و چندبعدی تعریف شود. تفکیک نقش توسعه‌دهنده، بهره‌بردار و ناظر انسانی، همراه با معیارهای «کنترل مؤثر» و «توان دخالت انسانی»، می‌تواند تبعات مسئولیت را به‌نحو عادلانه‌تری انتساب دهد و از «خلاء مسئولیت» جلوگیری کند. این رویکرد نه‌تنها با اصول حقوقی موجود سازگارتر است، بلکه امکان تطبیق بهتر با استانداردهای بین‌المللی را نیز فراهم می‌سازد.

۲-۳- نقش توسعه‌دهنده و بهره‌بردار در جبران خسارت

در نظام‌های مسئولیت مدنی سنتی، تعیین مسئول جبران خسارت مبتنی‌بر عمل زیان‌بار نسبتاً روشن است: شخصی که با فعل یا ترک فعل خود سبب ورود خسارت شده، مسئول است. با ورود سامانه‌های هوش مصنوعی به عرصه تصمیم‌گیری و تعامل با داده‌ها، این «وضوح» محو شده و نقش توسعه‌دهندگان و بهره‌برداران در جبران خسارت اهمیت بسیار بیشتری یافته است. در واقع، چون هوش مصنوعی فاقد شخصیت حقوقی و اراده انسانی است، جبران خسارت باید از مسیر مسئولیت‌های انسانی و سازمانی مرتبط با طراحی، توسعه، به‌کارگیری و بهره‌برداری از این سامانه‌ها تأمین شود.

مطالعات تطبیقی بیانگر الگوی مسئولیت متداول بر «قصور» یا «بی‌احتیاطی» توسعه‌دهندگان و بهره‌برداران مبتنی است، یعنی زمانی که آنان در انتخاب، طراحی، نظارت یا استفاده از سامانه هوش مصنوعی استانداردهای لازم را رعایت نکرده‌اند، مسئول شناخته می‌شوند. بااین‌حال، به دلیل ویژگی‌های خاص هوش مصنوعی از جمله پیچیدگی، عدم شفافیت «جعبه سیاه» و استقلال نسبی سیستم‌ها، اثبات خطای انسانی یا رابطه سببیت مستقیم میان رفتار توسعه‌دهنده/بهره‌بردار و خسارت برای زیان‌دیده بسیار دشوار است و این امر منجر به بازنگری در روش‌های انتساب مسئولیت شده است (Gredka-Ligarska,2024,75).

یکی از این بازنگری‌ها، حرکت از الگوی مسئولیت صرفاً مبتنی‌بر خطا به سمت «مسئولیت مبتنی‌بر خطر» یا «مسئولیت بدون تقصیر» است. در پیشنهادهای اخیر در اتحادیه اروپا، توسعه‌دهندگان و بهره‌برداران حرفه‌ای سامانه‌های هوش مصنوعی[۱۲] می‌توانند حتی بدون اثبات تقصیر، مسئول جبران خسارت باشند، به‌ویژه زمانی که خسارت از «درگیری» سامانه هوش مصنوعی حاصل شود و نه ناشی از رفتار نامناسب منفرد انسانی. این رویکرد در پروژه‌های قانونی پیشنهادی مانند دستورالعمل مسئولیت مدنی هوش مصنوعی دیده می‌شود که تلاش دارد بار اثبات را از دوش زیان‌دیده بردارد و برعهده توسعه‌دهندگان و بهره‌برداران قرار دهد. برای توسعه‌دهنده، تعهدات در مراحل طراحی و تولید شامل اطمینان از ایمنی، تحلیل ریسک، آزمون‌های معتبر و مستندسازی دقیق است. اگر سیستم با نقص طراحی، داده‌های آموزشی نامناسب یا آزمون ناکافی عرضه شود و خسارتی ایجاد کند، توسعه‌دهنده می‌تواند مسئول شناخته شود؛ حتی در مواردی که بهره‌بردار به‌طور صحیح سیستم را به‌کار گرفته باشد. در این الگو، توسعه‌دهنده باید ثابت کند که تمام اقدامات ایمنی لازم را اتخاذ کرده است (Gredka-Ligarska,2024,81).

از سوی دیگر، بهره‌بردار[۱۳] نقش مهمی در جبران خسارت دارد، خصوصاً زمانی که وی انتخاب سیستم، نظارت بر عملکرد، یا به‌کارگیری آن در شرایط مخاطره‌آمیز را بر عهده داشته است. به‌عنوان مثال، اگر بهره‌بردار بدون درک محدودیت‌های فناوری از آن در زمینه‌هایی استفاده کند که نیاز به نظارت انسانی مؤثر دارند، می‌توان او را مسئول دانست، حتی اگر نقص به‌طور مستقیم ناشی از طراحی نباشد. این موضوع در چهارچوب‌های حقوقی چون مسئولیت تضامنی یا مسئولیت بی‌تقصیر برای بهره‌برداران حرفه‌ای نیز مورد بررسی قرار گرفته است (تخشید، ۱۴۰۰، ۲۳۶).

در حقوق بسیاری از کشورها، بهره‌برداران حرفه‌ای[۱۴] در معرض مسئولیت قهری یا مسئولیت

۱۲- به‌ویژه در موارد استفاده تجاری یا حرفه‌ای

۱۳- یعنی شخص یا حقوقی که سامانه هوش مصنوعی را در فعالیت‌های خود استفاده می‌کند

۱۴- به‌ویژه شرکت‌ها و کارفرمایانی که از هوش مصنوعی برای اهداف تجاری استفاده می‌کنند

مبتنی‌بر خطر[۱۵] هستند؛ یعنی مسئولیت مستقل از خطای انسانی، به‌واسطه بهره‌برداری از فناوری که سودآوری آن را برای خود کسب کرده‌اند. این رویکرد شبیه قوانین مسئولیت برای فعالیت‌های بالقوه خطرناک است که در آن، شخصی که سود می‌برد مسئول جبران خسارت ناشی از آن نیز هست (De Bruyne&Ooms,2025,166). در حقوق ایران نیز اگرچه هنوز چهارچوب قانونی مشخص برای هوش مصنوعی تصویب نشده، اصول کلی مسئولیت مدنی مانند مسئولیت کارفرما[۱۶] و مسئولیت تولیدکننده می‌تواند به‌عنوان مبنایی برای انتساب مسئولیت توسعه‌دهندگان و بهره‌برداران به‌کار رود؛ البته اجرای عملی آن نیازمند تفسیرهای تکاملی و گسترش مفاهیم موجود است تا بتواند پیچیدگی‌های سامانه‌های هوشمند را پوشش دهد.

به نظر نگارندگان، نقش توسعه‌دهنده و بهره‌بردار در جبران خسارت‌های ناشی از سامانه‌های هوش مصنوعی باید مبتنی‌بر تحلیل دقیق نقش‌ها و مسئولیت‌های واقعی آنان در چرخه فناوری باشد. توسعه‌دهندگان مسئول تضمین ایمنی و رعایت استانداردهای فنی و حقوقی در طراحی و عرضه محصول هستند و بهره‌برداران مسئول استفاده امن، نظارت کافی و انتخاب مناسب فناوری در محیط‌های عملیاتی. ترکیب این دو نقش در قالب نظام‌های مسئولیت مبتنی‌بر خطر می‌تواند نه‌تنها بار اثبات را از دوش زیان‌دیده بردارد، بلکه انگیزه‌ای برای تولید و استفاده ایمن‌تر فناوری‌های هوش مصنوعی فراهم آورد.

۳- رویکرد ایران و افغانستان نسبت به مسئولیت مدنی

پس از تبیین معیارهای انتساب مسئولیت و نقش کنشگران انسانی در پردازش خودکار داده‌های شخصی، بررسی نحوه مواجهه نظام‌های حقوقی داخلی با این پدیده ضرورت می‌یابد. حقوق ایران و افغانستان، هرچند از حیث مبانی فقهی و ساختار کلی مسئولیت مدنی اشتراکات قابل‌توجهی دارند، اما در مواجهه با چالش‌های ناشی از هوش مصنوعی و پردازش خودکار داده‌ها در مراحل متفاوتی قرار

15- strict liability

۱۶- ماده ۱۲ قانون مسئولیت مدنی مصوب ۱۳۳۹

گرفته‌اند. این مبحث با تمرکز بر ظرفیت قواعد مسئولیت مدنی در حقوق ایران، وضعیت حمایت حقوقی از داده‌های شخصی در افغانستان و در نهایت مقایسه کارآمدی دو نظام حقوقی، می‌کوشد میزان پاسخگویی هریک از این نظام‌ها را در جبران خسارات ناشی از پردازش خودکار داده‌های شخصی ارزیابی و نقاط قوت و ضعف آن‌ها را آشکار سازد.

۳-۱- ظرفیت قواعد مسئولیت مدنی در حقوق ایران

نظام مسئولیت مدنی در حقوق ایران بر اساس قواعد کلی جبران خسارت شکل گرفته است که منشأ آن قانون مسئولیت مدنی مصوب ۱۳۳۹ و اصول بنیادی فقهی و حقوقی است. ماده اول این قانون بیان می‌کند: «هرکس بدون مجوز قانونی عمداً یا در نتیجه بی‌احتیاطی به جان یا مال یا هر حق دیگری که قانون برای افراد ایجاد کرده لطمه‌ای وارد آورد، مسئول جبران خسارت ناشی از عمل خود است.» این اصل بر دو رکن اساسی یعنی فعل زیان بار و رابطه سببیت تکیه دارد که معمولاً نیازمند اثبات تقصیر عامل زیان‌دهنده است.

مسئولیت مدنی در حقوق ایران عمدتاً مبتنی‌بر تقصیر تعریف شده و برای اعمال انسانی طراحی شده است. هنگامی که عمل زیان‌بار توسط انسان انجام می‌شود، قواعد سنتی می‌توانند با استناد به مفاهیمی چون عدم مراقبت لازم، بی‌احتیاطی یا تخلف از قواعد ایمنی، مسئولیت عامل را احصاء کنند (کاتوزیان، ۱۴۰۳، ۴۷). بااین‌حال، در مواردی که خسارت ناشی از عمل یک سامانه هوشمند خودکار مبتنی‌بر هوش مصنوعی باشد، این الگوی سنتی با چالش‌های بنیادین مواجه است. هوش مصنوعی، برخلاف انسان، فاقد شخصیت حقوقی، اراده و قصد است و نمی‌توان به‌عنوان «فاعل» مستقل در مقام اعمال مسئولیت قرارش داد؛ لذا انتساب تقصیر به یک سیستم خودمختار از منظر حقوق ایران دشوار است.

یکی از راهکارهای حقوقی در مواجهه با این چالش‌ها استناد به قواعد مسئولیت کارفرما[۱۷] یا مسئولیت تولیدکننده است. ماده ۱۲ قانون مسئولیت مدنی مصوب ۱۳۳۹، مسئولیت کارفرما را نسبت به اعمال

۱۷- مانند ماده ۱۲ قانون مسئولیت مدنی مصوب ۱۳۳۹

کارکنان زیر نظر او می‌داند، اما مشکل اساسی در کاربرد مستقیم این ماده در مورد هوش مصنوعی آن است که این سامانه‌ها در زمره «کارکنان انسانی» قرار نمی‌گیرند و نمی‌توان آن‌ها را در قالب روابط استخدامی قرار داد. به همین دلیل‌شناسایی «کارفرما» یا شخص مسئول در کاربرد سنتی دشوار می‌شود. با این وجود برخی مبانی کلی مسئولیت مدنی، در صورت تفسیر تکاملی، ظرفیت انعطاف برای پوشش خسارات ناشی از سامانه‌های هوشمند را دارا هستند (پارسا، ۱۴۰۳، ۱۲۷). برای مثال قواعد مسئولیت مدنی ناشی از فعل غیر می‌تواند در مواردی که شخص حقیقی یا حقوقی با رفتار خود موجب ایجاد یا به‌کارگیری سامانه‌ای شده که خسارت‌بار شده است، مورد استفاده قرار گیرد. در این چهارچوب، توسعه‌دهنده، بهره‌بردار یا مالک سیستم می‌تواند به‌عنوان شخص مسئول نهایی شناخته شود، مشروط بر آن که بتوان رابطه سببیت منطقی میان اقدام یا ترک اقدام او و خسارت ایجادشده احراز کرد.

از سوی دیگر، در حقوق ایران قواعد مربوط به محصول معیوب و حمایت از مصرف‌کننده نیز می‌توانند در شرایط خاص مورد استناد قرار گیرند. قانون حمایت از حقوق مصرف‌کنندگان مصوب ۱۳۸۸ عرضه‌کنندگان کالا و خدمات را در برابر عیوب و نقص‌های محصول مسئول می‌داند. اگرچه این قانون به‌طور صریح به فناوری هوش مصنوعی اشاره نمی‌کند، اما در مواردی که محصول مبتنی‌بر هوش مصنوعی به‌گونه‌ای عرضه شود که حاوی نقص بنیادین بوده و زیان‌بار واقع شود، ممکن است این قواعد قابلیت کاربرد داشته باشند. بااین‌حال، اثبات «عیب» در سامانه‌های هوشمند پیچیده که ممکن است طی دوره بهره‌برداری و یادگیری رفتار جدیدی از خود نشان دهند، چالش‌برانگیز است و نیازمند تفسیر توسعه‌یافته حقوقی است. نکته دیگر آن است که قواعد سنتی مسئولیت مدنی در حقوق ایران ظرفیت بالقوه‌ای برای مقابله با خسارات ناشی از هوش مصنوعی دارند، اما این ظرفیت بدون تفسیر تکاملی و توسعه رویه قضایی یا تقنینی تناسب کامل با ویژگی‌های فنی سامانه‌های هوشمند پیدا نمی‌کند. به‌ویژه مفهوم «تقصیر» باید در راستای استانداردهای علمی و فنی روز و در نظر گرفتن پیچیدگی‌های الگوریتمی بازتعریف شود تا بازنمای دقیق‌تری از رفتار انسانی در چرخه طراحی، توسعه و به‌کارگیری این فناوری فراهم آید.

به نظر نگارندگان، نظام مسئولیت مدنی ایران از نظر اصولی در برابر چالش‌های ناشی از هوش مصنوعی و پردازش خودکار داده‌ها آمادگی نسبی دارد، اما فقدان قواعد اختصاصی و شفاف درباره فناوری‌های نوین موجب می‌شود که عدالت جبران خسارت در این حوزه به‌طور مؤثر تحقق نیابد. مسئولیت مدنی در مواجهه با سامانه‌های هوش مصنوعی نیازمند بازتعریف قواعد تقصیر و سببیت در پرتو دانش فنی و حقوقی نوین و همچنین قانون‌گذاری تکمیلی مشخص است تا بتواند پاسخگوی پیچیدگی‌های فناوری و نیازهای حقوقی جامعه باشد.

۳-۲- حمایت حقوقی از داده‌های شخصی در افغانستان

در افغانستان، برخلاف بسیاری از کشورها، قانون مستقل و جامع برای حفاظت از داده‌های شخصی وجود ندارد؛ یعنی هنوز چهارچوب مشخصی برای تنظیم پردازش، نگهداری و جبران خسارت ناشی از سوءاستفاده از داده‌های شخصی تصویب نشده است. این خلأ قانونی، یکی از مهم‌ترین ضعف‌های نظام حقوقی افغانستان در پاسخگویی به چالش‌های مربوط به حریم خصوصی و حفاظت از داده‌ها به شمار می‌آید (Islam,2022,45). بااین‌حال، اصل حریم خصوصی در قانون اساسی افغانستان پیش‌بینی شده است. بر اساس فصل سوم قانون اساسی، حریم خصوصی ارتباطات و مکاتبات شهروندان از هر گونه تجسس و تجاوز محفوظ است، چه به شکل نوشتاری، گفتاری یا هر وسیله دیگر. همچنین ماده چهل و یکم قانون اساسی به حفظ حقوق اشخاص در برابر مداخلات غیرقانونی در محل اقامت اشاره دارد که می‌تواند به‌صورت غیرمستقیم حمایت از داده‌های شخصی را نیز مورد پوشش قرار دهد. این اصول اساسی حقوقی، اگرچه ارزشمند هستند، اما بدون مقررات اجرایی و ضمانت اجرای مؤثر برای داده‌های شخصی در بستر دیجیتال کافی نیستند.

به جز قانون اساسی، قانون دسترسی به اطلاعات مصوب ۲۰۱۹ میلادی نیز به تعریف «اطلاعات شخصی» می‌پردازد و آن را شامل اطلاعاتی مانند نام، آدرس، سوابق سلامتی، حساب‌های بانکی، رمزهای عبور و سایر اطلاعات غیرمرتبط با وظایف رسمی می‌داند. این قانون به نحوی تلاش کرده

است تا در قالب دسترسی به اطلاعات، حداقل چهارچوبی برای تعریف داده‌های شخصی فراهم آورد؛ اما هدف اصلی آن دسترسی به اطلاعات دولتی برای تقویت شفافیت و پاسخگویی است و نه حفاظت از داده‌های شهروندان در برابر پردازش‌های خودسرانه یا سوءاستفاده‌های تجاری (Islam,2022,45).

به دلیل فقدان قانون خاص حفاظت از داده‌ها، سازمان‌های دولتی و خصوصی به‌صورت پراکنده و غیرهماهنگ اقدام به تدوین سیاست‌های حریم خصوصی برای خدمات و پلتفرم‌های خود کرده‌اند. برای مثال، برخی پورتال‌ها یا شرکت‌ها در افغانستان اسناد و سیاست‌های حفظ حریم خصوصی ارائه می‌دهند که تعهداتی مانند محدود کردن دسترسی، رمزگذاری داده‌ها یا استفاده از داده تنها برای اهداف مشخص را پیش‌بینی می‌کنند (Guntrum,2022,102). چنین سیاست‌هایی، اگرچه به‌صورت داوطلبانه و غیراجباری وضع شده‌اند، نشان‌دهنده تلاش‌های موردی برای پاسخ به نیازهای حفاظت از داده هستند، اما فاقد ضمانت‌های حقوقی و اجرایی لازم هستند. فقدان قانون جامع حفاظت از داده‌های افغانستان موجب شده است که شرکت‌ها و خدماتی که در ارتباط با کاربران افغان فعالیت می‌کنند، برای رعایت استانداردهای بین‌المللی مانند مقررات اتحادیه اروپا[۱۸] تلاش کنند؛ اما این الزام نیز زمانی برقرار می‌شود که داده‌های کاربران افغان با قوانین کشورهای دیگر تلاقی داشته باشد و نه به‌دلیل وجود نظم حقوقی داخلی افغانستان (Islam,,2022,52).

حقوقدانان و تحلیلگران حقوق بشر معتقدند که وضعیت پیچیده سیاسی و امنیتی افغانستان و بی‌ثباتی‌های مداوم، تدوین یک چهارچوب حقوقی کارآمد برای حفاظت از داده‌های شخصی را با تأخیر مواجه کرده است. درعین‌حال، فقدان مقرراتی چون قانون حمایت از داده‌های شخصی، نه‌تنها موجب خلأ قانونی در برابر سوءاستفاده‌ها می‌شود، بلکه امکان جبران خسارت قانونی برای کسانی که داده‌هایشان با نقض امنیت افشاء شده است را نیز محدود می‌سازد (Hofstetter,2024,81).

به نظر نگارندگان، با توجه به اهمیت فزاینده داده‌های شخصی در عصر دیجیتال و افزایش

18- GDPR

کاربردهای فناوری‌های نوین مانند هوش مصنوعی، وضعیت حقوقی افغانستان در زمینه حفاظت از داده‌ها ناکافی و شکننده است. وجود تنها اصول کلی در قانون اساسی و تعریف مبهم در قانون دسترسی به اطلاعات مصوب ۲۰۱۹ میلادی، بدون مقررات اجرایی و ضمانت اجرا، نمی‌تواند پاسخگوی نیازهای واقعی حفاظت از داده‌های شخصی باشد. بنابراین، تدوین قانون جامع حفاظت از داده‌های شخصی و ایجاد نهادهای نظارتی مؤثر، از الزامات ضروری برای تأمین حقوق مردم و جبران خسارات ناشی از نقض داده‌ها در افغانستان است.

۳-۳- مقایسه کارآمدی نظام‌های حقوقی

با توجه به مباحث پیشین چنین می‌توان استنباط کرد که مقایسه نظام‌های حقوقی ایران و افغانستان در زمینه حمایت از داده‌های شخصی و مسئولیت مدنی ناشی از نقض این داده‌ها، نشان‌دهنده تفاوت‌های ساختاری در میزان تکامل قانونی، تضمین اجرایی و پاسخگویی حقوقی است. این تفاوت‌ها نه‌تنها در متن قوانین، بلکه در تداوم اجرایی و ظرفیت سازوکارهای جبران خسارت نیز مشهود است.

در حقوق ایران، همان‌طور که پژوهش‌های علمی حقوقی یادآور می‌شوند، هیچ قانون جامع و مستقلی برای حفاظت از داده‌های شخصی تصویب نشده است و داده‌های شخصی عمدتاً در قالب قوانین پراکنده مانند قانون تجارت الکترونیکی مصوب ۱۳۸۲، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و سایر مقررات مرتبط با حریم خصوصی مورد حمایت نسبی قرار می‌گیرند، اما این حمایت ناقص و غیرمرتبط مستقیم است و این امر موجب ایجاد خلأ قانونی در مواجهه با نقض حریم خصوصی و مسئولیت مدنی مرتبط با آن شده است (Mohiqi,2023,10). هرچند تلاش‌هایی مانند «پیش‌نویس لایحه صیانت و حفاظت از داده‌های شخصی» نیز مطرح شده‌اند، اما تا کنون این لوایح به قانون تبدیل نشده‌اند و حمایت حقوقی از داده‌ها همچنان پراکنده و ناکافی است. علاوه بر این، قوانین موجود در ایران در موارد محدود، به تخلفات کیفری می‌پردازند[۱۹]، اما در بسیاری از موارد برای حمایت مدنی و

۱۹- مثلاً مجازات‌های مرتبط با نقض حریم خصوصی در قانون تجارت الکترونیکی مصوب ۱۳۸۲

جبران خسارت ناشی از نقض داده‌های شخصی چهارچوب مشخصی پیش‌بینی نشده است؛ یعنی اگر داده‌ها به‌واسطه الگوریتم‌های هوش مصنوعی یا پردازش خودکار افشاء یا سوءاستفاده شوند، فرد زیان‌دیده ممکن است با مشکلات جدی در مسیر دادخواهی مواجه گردد.

در مقابل، نظام حقوقی افغانستان به‌طور قابل توجهی فاقد قانون مستقل و حتی حداقلی برای حفاظت از داده‌های شخصی است. منابع بین‌المللی و تحلیل‌های حقوقی به‌روشنی بیان می‌کنند که افغانستان هیچ قانون جامع یا مشخصی برای محافظت از داده‌های شخصی ندارد و حمایت‌های موجود در قانون اساسی نیز فقط به اصولی کلی درباره حفظ حریم خصوصی اشاره می‌کند که فاقد ضمانت اجرایی عملی است. در افغانستان، تنها مقررات خفیف یا بخش‌های پراکنده مانند قانون دسترسی به اطلاعات مصوب ۲۰۱۹ میلادی وجود دارد که بیشتر به حق دسترسی عمومی به اطلاعات می‌پردازد و به‌نحوی جنبه‌های حفظ اطلاعات شخصی را نیز تعریف می‌کند، اما این قانون نیز هدف اصلی‌اش حفاظت از داده‌های شهروندان در برابر پردازش‌های خودسرانه نیست و ضمانت اجرای آن محدود است.

ایران با این که قانونی جامع ندارد، حداقل چهارچوب‌های محدود برای حمایت از حریم خصوصی دارد و دستگاه قضایی می‌تواند در موارد مشخص مسئولیت مدنی از طریق قوانین عمومی جبران خسارت را اعمال کند؛ اما فقدان نظام جامع و مشخص برای داده‌ها، باعث عدم قطعیت حقوقی و خلأ در بسیاری از دعاوی مربوط به داده‌های پردازش‌شده‌ی خودکار و هوش مصنوعی می‌شود. افغانستان حتی چهارچوب‌های نسبی محدود نیز ندارد و تقریباً هیچ سازوکار قانونی برای جبران خسارت ناشی از نقض داده‌های شخصی وجود ندارد؛ این امر باعث شده است که شهروندان افغان در صورت افشای داده‌های شخصی، تقریباً هیچ مرجع حقوقی برای پیگیری مدنی یا ادعای جبران خسارت نداشته باشند. نظام ایران از نظر اجرایی و تضمین‌پذیری حقوق شهروندی، به کمک قواعد جزایی و مدنی موجود و تلاش برای تصویب قوانین جدید، حداقلی از حمایت قانونی را ارائه می‌دهد، هرچند ناقص است. در مقابل، افغانستان در وضعیت فعلی خود فاقد پایه‌های حقوقی لازم برای حمایت از داده‌ها است و این خلاء به‌ویژه در عصر دیجیتال و گسترش هوش مصنوعی

می‌تواند پیامدهای جدی حقوقی و اجتماعی در پی داشته باشد.

در مجموع، نظام حقوقی ایران با وجود نارسایی‌ها در سطح قوانین خاص، تا حدودی در مسیر تقویت حمایت از داده‌های شخصی قرار دارد و تلاش‌هایی برای اصلاح و تکمیل قانونی در جریان است. این در حالی است که افغانستان فاقد چهارچوب قانونی مشخص و اجرایی در این حوزه است که این ضعف قانونی پایه‌ای می‌تواند مانع جدی در تحقق عدالت و جبران خسارت ناشی از نقض داده‌های شخصی در برابر پردازش خودکار داده‌ها و هوش مصنوعی ایجاد کند. در نتیجه، کارآمدی نظام ایران در این عرصه بالاتر از افغانستان ارزیابی می‌شود، اما هر دو نظام برای پاسخ به چالش‌های نوین نیازمند قوانین اختصاصی، روشن و تضمین‌پذیر در سطح ملی هستند؛ امری که با استانداردهای بین‌المللی نیز هم‌راستا می‌شود.

۴- تأثیر اسناد بین‌المللی بر مسئولیت مدنی داده‌ها

در دنیای معاصر، جریان آزاد اطلاعات و پردازش خودکار داده‌ها مرزهای ملی را درمی‌نوردد و حفاظت از داده‌های شخصی به یک دغدغه جهانی تبدیل شده است. اسناد، دستورالعمل‌ها و استانداردهای بین‌المللی، چهارچوب‌های مهمی برای تعریف حقوق شهروندان، الزامات مسئولیت مدنی و مکانیسم‌های جبران خسارت ارائه می‌دهند. این مبحث با تمرکز بر استانداردهای بین‌المللی حفاظت از داده‌های شخصی، میزان همسویی حقوق داخلی ایران و افغانستان با معیارهای جهانی و در نهایت ارائه پیشنهادهای تقنینی و تفسیری، تلاش می‌کند نقش این اسناد در شکل‌دهی و تقویت مسئولیت مدنی مرتبط با پردازش داده‌ها را بررسی کند و راهکارهای ارتقای نظام‌های حقوقی داخلی در این حوزه را شفاف سازد.

۴-۱- استانداردهای بین‌المللی حفاظت از داده‌های شخصی

حفاظت از داده‌های شخصی به‌عنوان یکی از بنیان‌های حقوق بشر و آزادی‌های فردی شناخته شده و مسیر تدوین استانداردها و چهارچوب‌های قانونی از اواخر قرن بیستم میلادی آغاز شده است. یکی از

نخستین و تأثیرگذارترین الگوهای جهانی، راهنمای اصول حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی است که توسط سازمان همکاری و توسعه اقتصادی[۲۰] در سال ۱۹۸۰ میلادی ارائه شد و تا امروز به‌عنوان مبنای بسیاری از قوانین ملی و بین‌المللی محسوب می‌شود. این اصول شامل محدودیت در جمع‌آوری داده، کفایت، هدف‌مندی، محدودیت استفاده، شفافیت، مشارکت فردی، امنیت داده و مسئولیت کنترل‌کننده داده‌ها است. این اصول در متن راهنمای اصول حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی به‌روشنی بیان شده‌اند که هدف آن ایجاد توازنی میان آزادی‌های فردی و استفاده مسئولانه از داده‌ها است.

راهنمای اصول حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی تأکید دارد که جمع‌آوری داده‌های شخصی باید محدود به مقاصد مشخص، قانونی و مشروع باشد و پیش از مرحله پردازش، هدف آن باید برای فرد موضوع داده توضیح داده شود. همچنین، داده‌های جمع‌آوری‌شده باید مرتبط، دقیق، به‌روز و نه بیشتر از حد لازم باشند تا از سوءاستفاده جلوگیری شود. استفاده از داده‌های شخصی نیز باید محدود به مقاصد اولیه شود و انتشار یا به‌کارگیری برای مقاصد دیگر مستلزم رضایت صریح فرد یا مبنای قانونی باشد.

در سطح منطقه‌ای و ملی اما کامل‌ترین چهارچوب قانونی اکنون مقررات عمومی حفاظت از داده‌ها[۲۱] در اتحادیه اروپا است که از ۲۰۱۸ میلادی لازم‌الاجرا شده و به‌عنوان یک استاندارد جهانی پذیرفته شده است. مقررات عمومی حفاظت از داده‌ها قواعدی دقیق و قابل‌اجرا درباره نحوه جمع‌آوری، پردازش، ذخیره، انتقال و حذف داده‌های شخصی وضع کرده است. این مقررات علاوه بر این که شامل همه سازمان‌هایی می‌شود که داده‌های شهروندان اتحادیه اروپا را پردازش می‌کنند، حتی زمانی که سازمان در خارج از اتحادیه مستقر است و فقط خدماتی به شهروندان ارائه می‌دهد، نیز قابل‌اعمال است.

20- OECD
21- GDPR

مقررات عمومی حفاظت از داده‌ها چند اصل کلیدی دارد که به‌صورت عمومی نیز در اسناد دیگر مورد پذیرش قرار گرفته‌اند: قانونمندی، انصاف و شفافیت: پردازش داده باید بر پایه یک مبنای قانونی روشن قرار گیرد و به‌طور شفاف به فرد موضوع داده اطلاع داده شود. محدودیت هدف: داده‌ها فقط برای اهداف مشخص، واضح و مشروع گردآوری و پردازش شوند. حداقل‌سازی داده: تنها داده‌های مورد نیاز برای انجام هدف باید پردازش شوند. دقت و به‌روزرسانی: داده‌های نادرست باید اصلاح یا حذف شوند. محدودیت نگهداری: داده‌ها نباید برای مدت طولانی‌تر از نیاز نگهداری شوند. تمامیت و محرمانگی: داده‌ها باید از دسترسی غیرمجاز، از دست رفتن یا آسیب محافظت شوند. پاسخگویی: مسئولیت رعایت این اصول بر عهده کنترل‌کننده داده‌ها است و باید قابلیت اثبات رعایت آن را داشته باشد.

علاوه بر این دو منبع اصلی، دیگر چهارچوب‌ها و راهنمایی‌های منطقه‌ای و تخصصی نیز وجود دارند که از اصول مشابه حمایت می‌کنند. به‌عنوان مثال، راهنمای چهارچوب حریم خصوصی[۲۲] که در منطقه آسیا–اقیانوسیه توسعه یافته، روی محدودیت استفاده، رضایت، انتقال امن داده‌ها و شفافیت تأکید کرده و با مقررات عمومی حفاظت از داده‌ها در اصول اساسی اشتراک دارد. همچنین، کنوانسیون ۱۰۸ شورای اروپا[۲۳] به‌عنوان نخستین معاهده چندجانبه در زمینه حفاظت از داده‌های شخصی شناخته می‌شود و چهارچوبی الزام‌آور برای کشورهای عضو تعیین می‌کند که باید تعادل میان حفظ حقوق فردی و منافع اجتماعی در پردازش داده‌ها را برقرار کنند. کنوانسیون ۱۰۸ به‌روزرسانی‌شده شامل الزامات دقیق‌تری برای انتقال داده‌های فرامرزی، تضمین حقوق سوژه داده و نظارت مؤثر است (Pauletto,2021,105433). علاوه بر این اصول عمومی، اسناد دیگری نیز به تدابیر امنیتی اختصاص دارند، از جمله اقدامات رمزگذاری، شبه‌نام‌گذاری و سازوکارهای اطلاع‌رسانی درباره نقض داده‌ها که در بسیاری از قوانین ملی نیز به‌عنوان الزامات اجرایی وارد شده‌اند. این تدابیر مبتنی‌بر اصول رایج امنیت داده است که بانک جهانی و دیگر نهادهای بین‌المللی نیز در راهنمای خود به آن‌ها اشاره کرده‌اند.

22- APEC (Asia Pacific Economic Cooperation Privacy Framework)
23- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

در مجموع، استانداردهای بین‌المللی حفاظت از داده‌های شخصی حول محور حقوق افراد، محدودیت در پردازش، شفافیت، امنیت و پاسخگویی شکل گرفته‌اند و به‌صورت گسترده در قوانین ملی و منطقه‌ای بازتاب یافته‌اند، به‌گونه‌ای که حتی در خارج از مرزهای اتحادیه اروپا نیز بسیاری از کشورها ارجاعات مستقیم یا غیرمستقیم به مقررات عمومی حفاظت از داده‌ها یا اصول راهنمای اصول حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی دارند. این استانداردها نه‌تنها به‌عنوان معیارهای فنی مطرح هستند، بلکه به‌عنوان الزامات حقوقی برای تضمین احترام به آزادی‌ها و حقوق بنیادین در عصر دیجیتال پذیرفته شده‌اند و به‌عنوان مبنای توسعه قوانین ملی در بسیاری از کشورها مورد استفاده قرار می‌گیرند.

۴-۲- همسویی حقوق داخلی با معیارهای جهانی

در بررسی همسویی نظام‌های حقوقی ایران و افغانستان با استانداردهای بین‌المللی حفاظت از داده‌های شخصی، باید سطح تطبیق قوانین داخلی با اصول پذیرفته‌شده جهانی همچون مقررات عمومی حفاظت از داده‌ها و اصول راهنمای اصول حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی را به‌طور دقیق مورد ارزیابی قرار داد. وضعیت این دو کشور در حال حاضر در نقاط مختلفی نسبت به معیارهای جهانی عقب‌تر از استانداردهای بین‌المللی قرار دارد که ناشی از خلاءهای قانونی، فقدان چهارچوب‌های اجرایی مشخص و عدم پذیرش الزامات جامع حفاظت از داده‌ها است.

در ایران، هنوز قانون مستقل، جامع و الزام‌آوری تحت عنوان «قانون حفاظت از داده‌های شخصی» به تصویب نرسیده است؛ هرچند پیش‌نویس‌هایی تحت عناوین مختلف مانند «صیانت و حفاظت از داده‌های شخصی» مورد بررسی قرار گرفته‌اند که هدف آن حمایت از حقوق افراد و حریم خصوصی است، اما تحلیل‌های نهادهای حقوقی نشان می‌دهد که این لایحه در حال حاضر فاقد تطابق کافی با تعهدات بین‌المللی و معیارهای جهانی است و در بسیاری از موارد، اصول بنیادین حفاظت از داده‌ها را که در اسناد بین‌المللی مورد تأکید قرار گرفته‌اند، به‌طور کامل رعایت نمی‌کند. به‌عنوان نمونه،

نقدهای سازمان ماده ۱۹ نشان می‌دهد که لایحه مزبور در بخش‌هایی «فاقد وضوح» است، مصادیق حقوق افراد را به‌درستی تعیین نمی‌کند و با تعهدات بین‌المللی ایران در زمینه آزادی بیان و حریم خصوصی مغایرت دارد. مطالعات تطبیقی در حقوق ایران نیز تأکید می‌کنند که با وجود وجود قوانین پراکنده در زمینه حریم خصوصی[۲۴]، نظام حقوقی ایران فاقد چهارچوبی هماهنگ و کامل مطابق اصول مقرراتی نظیر مقررات عمومی حفاظت از داده‌ها است. پژوهش‌ها نشان داده‌اند که به‌رغم وجود قواعدی مرتبط با حمایت از داده در قوانین مختلف، این قواعد نمی‌توانند به‌طور کامل حقوق موضوع داده را تضمین کنند و بسیاری از حقوقی که در اسناد بین‌المللی برای سوژه‌های داده پیش‌بینی شده، در حقوق ایران با نقصان روبرو است (لطیف زاده و همکاران، ۱۴۰۲، ۳۶۶).

برای مثال در قوانین معتبر بین‌المللی مانند مقررات عمومی حفاظت از داده‌ها، حقوقی چون حق دسترسی به داده، حق اصلاح، حق حذف[۲۵]، حق اعتراض به پردازش و الزام به ارزیابی تأثیر حفاظت از داده‌ها به‌صراحت پیش‌بینی شده‌اند، اما در حقوق ایران چنین الزامات مشخص و جامعی موجود نیست و موارد مشابه در قوانین فعلی به‌صورت پراکنده و کم‌عمق تنظیم شده‌اند. علاوه بر این، موضوعاتی چون نظارت مستقل بر اجرای قوانین، نقش کنترل‌کننده و پردازشگر داده و مسئولیت‌های دقیق آنان نیز در لایحه‌های موجود به‌روشنی تعیین نشده است؛ درحالی‌که در مقررات عمومی حفاظت از داده‌ها این موارد به‌طور دقیق تنظیم شده است (محمودی پرچینی و همکاران، ۱۴۰۳، ۲۱۶).

در افغانستان وضعیت به‌مراتب متفاوت است و هیچ قانون ملی جامع و مشخصی برای حفاظت از داده‌های شخصی وجود ندارد. تحلیل‌های تخصصی و گزارش‌های حقوقی معتبر نشان می‌دهد که نظام حقوقی افغانستان صرفاً به برخی اصول اساسی حریم خصوصی در قانون اساسی و تعدادی مقررات بخش‌محور محدود شده است و چهارچوب قوانین بخش‌محور نیز فاقد انسجام و ضمانت اجرایی قوی است (Rahimi,2024,32). در نتیجه، حتی معیارهای اولیه‌ای مانند تعریف داده‌های

۲۴- مثلاً مواد مربوط به قانون جرایم رایانه‌ای مصوب ۱۳۸۸ یا قانون تجارت الکترونیکی مصوب ۱۳۸۲

۲۵- حق فراموش‌شدن

شخصی، تعیین حقوق سوژه داده، الزامات کنترل‌کنندگان داده و امکانات قانونی برای جبران خسارت به‌صورت مشخص در حقوق افغانستان پیش‌بینی نشده‌اند؛ امری که با معیارهای بین‌المللی حفاظت از داده به‌وضوح در تضاد است.

برای مقایسه، استانداردهای بین‌المللی مانند مقررات عمومی حفاظت از داده‌ها و اصول راهنمای اصول حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی برای حمایت از داده‌ها، بر شفافیت، محدودیت در هدف و دامنه پردازش، حقوق متعدد سوژه داده و پاسخگویی کنترل‌کنندگان داده‌ها تأکید دارند. این استانداردها از جنبه‌های ضروری مانند شفافیت در پردازش، امکان اعتراض و جبران خسارت، الزامات امنیت داده و نظارت مستقل پشتیبانی می‌کنند و کشورهای دارای قوانین قوی باید آن‌ها را در چهارچوب قانونی خود بازتاب دهند.

به استنباط نگارندگان حقوق ایران در بعضی اصول کلی با استانداردهای بین‌المللی تا حدی هم‌راستا است ولی در ساختار قانونی جامع، ضمانت‌های اجرایی دقیق و تضمین حقوق سوژه‌های داده با معیارهای جهانی فاصله دارد. حقوق افغانستانبه‌طور اساسی از تدوین قوانین جامع و استانداردهای بین‌المللی عقب‌تر است و حتی اصول بنیادین حفاظت از داده‌ها را به‌صورت مشخص و قابل اجرا تنظیم نکرده است؛ بنابراین، همسویی حقوق داخلی این دو کشور با معیارهای جهانی هنوز در مرحله ابتدایی یا حداقل قرار دارد و نیازمند اصلاحات مدارک‌محور، تدوین قوانین مستقل و تبیین جزئیات حقوقی مطابق با اسناد بین‌المللی است تا بتواند در عمل حقوق افراد موضوع داده را تضمین نماید.

۴-۳- پیشنهادهای تقنینی و تفسیری برای ایران و افغانستان

از دیدگاه نگارندگان، برای ارتقای هماهنگی نظام‌های حقوقی ایران و افغانستان با معیارهای بین‌المللی حفاظت از داده‌های شخصی و بازتعریف مسئولیت مدنی در عصر هوش مصنوعی، ضروری است که اقدامات تقنینی و تفسیری مشخص و راهبردی صورت گیرد. این پیشنهادها باید هم نقص‌های موجود قوانین را پر کنند و هم با اصول جهانی همچون مقررات عمومی

حفاظت از داده‌ها و چهارچوب‌های بین‌المللی سازگار شوند.

اول- تدوین قانون جامع حفاظت از داده‌های شخصی: در ایران، به‌رغم تلاش‌هایی مانند پیش‌نویس «لایحه صیانت و حفاظت از داده‌های شخصی»، تحلیل‌های حقوقی معتبر نشان می‌دهد که این لایحه در وضعیت فعلی با معیارهای بین‌المللی فاصله دارد و فاقد بخش‌های دقیق درباره حوزه اعمال، حقوق سوژه داده و ضمانت اجرایی است. از جمله ضعف‌های آن می‌توان به فقدان تعریف روشن قلمرو کاربرد، نبود تضمین‌های معتبر برای استقلال نهاد نظارت و عدم پیش‌بینی سازوکارهای جبران خسارت اشاره کرد. تحلیلگران پیشنهاد کرده‌اند که لایحه باید از نو بازنویسی شود و اصول کامل حفاظت از داده‌های شخصی را در یک بخش مشخص و منسجم بگنجاند تا مطابق با استانداردهای مقررات عمومی حفاظت از داده‌ها و حقوق بین‌الملل حقوق بشر باشد. همچنین، باید حقوقی چون حق اصلاح، حق حذف، حق اعتراض و سازوکارهای اجرایی برای جبران خسارت و برخورداری از نهاد نظارتی مستقل پیش‌بینی شود. این گونه اصلاحات باید شامل شفافیت در قلمرو اعمال، تعیین صریح مصادیق داده‌های حساس، و تضمین سازوکارهای اجرایی مستقل باشد تا نه‌تنها با اصول بین‌المللی همسو شود، بلکه امکان تطبیق حقوقی مؤثر در کشور فراهم گردد.

دوم- تقویت ضمانت‌های اجرایی و نهاد نظارتی: یکی از چالش‌های عمده پیش‌نویس‌های فعلی در ایران، ضعف استقلال نهاد نظارتی حفاظت از داده‌ها و عدم پیش‌بینی راه‌های مؤثر برای جبران خسارت است. تجربه مقررات عمومی حفاظت از داده‌ها نشان می‌دهد که وجود اتحادیه یا کمیسیون مستقل حفاظت از داده با اختیارات اجرایی، امکان رسیدگی به تخلفات، صدور دستور توقف پردازش و اعمال جریمه، از ارکان کلیدی حفاظت داده است. بدون این ساختار، قوانین صرفاً در سطح تقنینی باقی می‌مانند و در عمل اثربخش نیستند.

سوم- ایجاد چهارچوب‌های اجرایی برای مسئولیت مدنی مرتبط با هوش مصنوعی: هم ایران و هم افغانستان باید به صراحت در قوانین خود مسئولیت مدنی پیامدهای فناوری‌های هوشمند و پردازش خودکار داده‌ها را نیز تعریف کنند. این امر می‌تواند با تدوین قواعد خاص مسئولیت مبتنی‌بر خطر

برای توسعه‌دهندگان، تولیدکنندگان و بهره‌برداران سامانه‌های هوش مصنوعی انجام شود تا اثبات تقصیر سنتی برای زیان‌دیدگان ضروری نباشد و جبران خسارت تسهیل شود. چنین رویکردی در تحلیل‌های حقوقی نوین نیز مورد توجه قرار گرفته است که می‌کوشند با درک فنی هوش مصنوعی، مسئولیت را در چهارچوب واقعیت‌های فناوری تعریف کنند.

چهارم- تدوین قانون مستقل و ظرفیت‌سازی نهادی: در افغانستان وضعیت قانونی به‌طور قابل‌توجهی ضعیف‌تر است، زیرا این کشور هنوز قانون جامع حفاظت از داده‌های شخصی ندارد و تنها آشکارسازی حقوق حریم خصوصی در قانون اساسی نیز بدون ضمانت اجرایی است. پژوهش‌های حقوقی نشان می‌دهد که فقدان چهارچوب قانون‌گذاری در این حوزه باعث شده است که حفاظت از داده‌ها در عمل ناکافی باشد و توان پاسخگویی حقوقی برای شهروندان وجود نداشته باشد. پیشنهاد می‌شود که افغانستان ابتدا با یک لایحه جامع حفاظت از داده‌های شخصی مشابه مقررات عمومی حفاظت از داده‌ها یا قوانین تدوین‌شده در دیگر کشورها شروع کند و سپس نهاد نظارتی مستقل برای اجرای آن ایجاد نماید. این قانون باید شامل تعاریف روشن داده‌های شخصی، حقوق سوژه‌های داده و مسئولیت‌های صریح پردازش‌کنندگان داده باشد و به‌ویژه در بخش‌های اجرایی شامل حسن اجرای قواعد و جبران خسارت، سازوکارهای قانونی مؤثر داشته باشد.

پنجم- ارتقای آگاهی، آموزش و همکاری منطقه‌ای: برای تضمین عملی همسویی با معیارهای جهانی، ضروری است نهادهای قانونی و قضایی در هر دو کشور برنامه‌های آموزشی و آگاهی‌بخشی برای قضات، وکلا، مقننین و مدیران فناوری برگزار کنند تا با استانداردهای جهانی آشنا شوند و بتوانند در تفسیر قوانین داخلی به آن‌ها رجوع کنند. همچنین همکاری‌های منطقه‌ای و بین‌المللی با سازمان‌هایی مانند کنفرانس تجارت و توسعه سازمان ملل متحد[۲۶] و راهنمای اصول حفاظت از حریم خصوصی و جریان‌های فرامرزی داده‌های شخصی می‌تواند به بهبود قوانین و به‌کارگیری بهترین تجربه‌ها کمک کند.

26- UNCTAD

در مجموع پیشنهادهای تقنینی و تفسیری برای ایران و افغانستان باید شامل تدوین قوانینی جامع، تقویت نهادهای نظارتی مستقل، تبیین مسئولیت مدنی مرتبط با فناوری‌های هوشمند و ظرفیت‌سازی نهادی و آموزشی باشد. این اصلاحات نه‌تنها نظام حقوقی را با استانداردهای جهانی تطبیق می‌دهد، بلکه زمینه تحقق حقوق شهروندی در عصر دیجیتال و هوش مصنوعی را نیز فراهم می‌سازد.

نتیجه

پژوهش حاضر با تمرکز بر مسئولیت مدنی ناشی از پردازش خودکار داده‌های شخصی توسط هوش مصنوعی، کوشید به این پرسش اساسی پاسخ دهد که آیا نظام‌های حقوقی ایران و افغانستان با تکیه بر قواعد موجود قادر به جبران خسارات ناشی از تصمیم‌گیری‌های الگوریتمی هستند و چه الگویی می‌تواند پاسخگوی مقتضیات این فناوری نوین باشد؟ بررسی انجام‌شده نشان می‌دهد که هرچند قواعد عمومی مسئولیت مدنی در هر دو نظام حقوقی، از حیث مبانی نظری و ساختار کلی، ظرفیت‌هایی برای حمایت از اشخاص زیان‌دیده فراهم می‌کنند، اما این ظرفیت‌ها در مواجهه با ویژگی‌های خاص پردازش خودکار داده‌ها و ماهیت پیچیده هوش مصنوعی با محدودیت‌های جدی روبرو هستند.

در حقوق ایران، امکان استناد به قواعد عام مسئولیت مدنی و اصول فقهی برای جبران خسارات ناشی از نقض حریم خصوصی و پردازش غیرمجاز داده‌های شخصی وجود دارد؛ بااین‌حال، نبود مقررات خاص در زمینه هوش مصنوعی و داده‌های شخصی، موجب ابهام در تعیین شخص مسئول و دشواری اثبات تقصیر و رابطه سببیت می‌شود. در حقوق افغانستان نیز وضعیت مشابهی مشاهده می‌گردد؛ به‌گونه‌ای که به‌رغم پذیرش کلی حمایت از حقوق اشخاص و جبران ضرر، فقدان چهارچوب‌های تقنینی منسجم در حوزه فناوری‌های نوین، کارآمدی نظام مسئولیت مدنی را در برابر خسارات ناشی از پردازش خودکار داده‌ها کاهش داده است. ازاین‌رو، پاسخ به بخش نخست پرسش پژوهش آن است که قواعد موجود، به‌تنهایی و بدون بازتفسیر یا تکمیل، توان پاسخگویی کامل به

چالش‌های مسئولیت مدنی در حوزه هوش مصنوعی را ندارند.

یکی از مهم‌ترین موانع در هر دو نظام حقوقی، تمرکز سنتی بر مسئولیت مبتنی‌بر تقصیر است؛ الگویی که در بستر سامانه‌های خودکار و غیرشفاف، عملاً اثبات آن برای زیان‌دیده دشوار یا حتی ناممکن می‌شود. در مقابل، الگوهایی چون مسئولیت مبتنی‌بر خطر یا مسئولیت تضامنی میان کنشگران دخیل در چرخه پردازش داده‌ها، ظرفیت بیشتری برای تضمین جبران خسارت دارند. این رویکردها، بدون نیاز به اثبات تقصیر فردی، بر پذیرش خطر ناشی از بهره‌برداری از فناوری‌های پیشرفته تأکید می‌کنند و با واقعیت‌های فنی هوش مصنوعی سازگارترند. بررسی اسناد بین‌المللی نشان می‌دهد که این اسناد، با تأکید بر اصولی همچون پاسخگویی، شفافیت، تناسب و جبران مؤثر خسارت، چهارچوبی پیشرو برای سامان‌دهی مسئولیت مدنی در حوزه پردازش داده‌های شخصی ارائه می‌دهند. مقررات و استانداردهای بین‌المللی، ضمن‌شناسایی مخاطرات خاص تصمیم‌گیری الگوریتمی، بر لزوم تعیین مسئول مشخص، حتی در شرایط فقدان تقصیر سنتی، تأکید دارند. این رویکرد می‌تواند خلأهای موجود در حقوق ایران و افغانستان را تا حد زیادی پوشش دهد و مسیر بازتعریف مسئولیت مدنی را هموار سازد.

حمایت مؤثر از داده‌های شخصی در عصر هوش مصنوعی، مستلزم عبور از برداشت‌های سنتی مسئولیت مدنی و حرکت به‌سوی الگوهای منعطف‌تر و کارآمدتر است. همسویی تدریجی حقوق ایران و افغانستان با استانداردهای بین‌المللی، از طریق تفسیر موسع قواعد موجود یا تدوین مقررات خاص در زمینه پردازش خودکار داده‌ها، می‌تواند ضمن تضمین حقوق اشخاص، امنیت حقوقی بهره‌برداران فناوری را نیز تأمین کند. در نهایت، پذیرش اصل پاسخگویی و اولویت جبران خسارت، به‌عنوان محور نظام مسئولیت مدنی، می‌تواند پاسخی متناسب به پرسش اصلی پژوهش و گامی مؤثر در جهت تنظیم حقوقی هوش مصنوعی در این دو نظام حقوقی باشد.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

فارسی

- آقایی طوق، مسلم و ناصر، مهدی، ۱۳۹۹، چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیاء مطالعه تطبیقی حقوق ایران و اتحادیه اروپا، **فصلنامه حقوق اداری**، شماره ۲۳.
- باقری، پرویز، ۱۴۰۴، شخصیت حقوقی و مسئولیت مدنی هوش مصنوعی؛ چالش‌ها و راهکارهای حقوقی، **فصلنامه پژوهش حقوق خصوصی**، شماره ۵۱.
- پارسا، ناهید، ۱۴۰۳، نقش و الزامات نظارت انسانی بر هوش مصنوعی در قانون اتحادیه اروپا و قوانین ایران، **دوفصلنامه تحقیق و توسعه در حقوق عمومی**، شماره ۲.
- تخشید، زهرا، ۱۴۰۰، مقدمه‌ای بر چالش‌های هوش مصنوعی در حوزه مسئولیت مدنی، **دوفصلنامه حقوق خصوصی**، شماره ۱.
- دادآفرین، کیانفر و اعظمی راد، مهشیدالملوک، ۱۴۰۴، امکان‌شناسایی شخصیت حقوقی برای ربات‌ها در چهارچوب حقوق سایبری آینده نگر، **فصلنامه حقوق سایبری**، شماره ۲.
- قیصری اطربی، زهره؛ شاکری، زهرا؛ یوسفی صادقلو، احمد، ۱۴۰۴، مسئله اعطای شخصیت حقوقی به هوش مصنوعی، **فصلنامه پژوهش تطبیقی حقوق اسلام و غرب**، شماره ۴۴.
- کاتوزیان، ناصر، ۱۴۰۳، **مسئولیت مدنی**، چاپ پنجم، تهران، انتشارات گنج دانش.
- لطیف زاده، مهدیه؛ قبولی درافشان، سیدمحمدمهدی؛ محسنی، سعید؛ عابدیف محمد، ۱۴۰۲، بررسی تطبیقی ضمانت اجرای نقض حق بر داده در حقوق اتحادیه اروپا و نظام حقوقی ایران، **فصلنامه مجلس و راهبرد**، شماره ۱۱۶.
- علی پناهی، مریم، نصیران نجف آبادی، داوود؛ شیرانی، مسعود، ۱۴۰۳، مسئولیت مدنی ناشی از استفاده هوش مصنوعی در اتحادیه اروپا، **فصلنامه مطالعات فقه اقتصادی**، شماره ۵.
- محمودی پرچینی، مرتضی؛ ریاضی، لادن؛ پورابراهیمی، علیرضا؛ موسوی، سیدعبداله امین، ۱۴۰۳، مقایسه قوانین حفاظت از داده‌های شخصی: مقررات عمومی منحصر به فرد تحت مقررات حفاظت از

داده‌های عمومی اتحادیه اروپا (GDPR) و قوانین ایالات متحده، **فصلنامه علوم خبری**، شماره ۵۲.

لاتین

- Chiodo, Maurice, et aln, 2025, Formalising Human-in-the-Loop: Computational Reductions, Failure Modes, and Legal-Moral Responsibility, arXiv preprint arXiv.10426.
- De Bruyne, Jan, and Wannes Ooms, 2025, Tort Liability and Artificial Intelligence Some Challenges and (Regulatory) Responses.
- GDPR, 2016, General Data Protection Regulation (EU) 2016/679
- Gredka-Ligarska, Iwona, 2024, Employer as an AI system operator and tortious liability for damage caused by AI systems: European and US perspectives. The Chinese Journal of Comparative Law 12.
- Guntrum, Laura Gianna, et al, 2022, Using digitally mediated methods in sensitive contexts: a threat analysis and critical reflection on data security, privacy, and ethical concerns in the case of Afghanistan. Zeitschrift für Friedens-und Konfliktforschung 11.2.
- Hofstetter, Julia-Silvana, 2024, Gendered and Postcolonial Perspectives on Data Weaponization in Armed Conflict. Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions.
- Islam, Md Toriqul, et al, 2022, Understanding GDPR: Its legal implications and relevance to South Asian privacy regimes. Islam, MT, Sahula, M., & Karim, ME (2022). Understanding GDPR: Its Legal Implications and Relevance to South Asian Privacy Regimes. UUM Journal of Legal Studies 13.1.
- Ismail, Emal, et al., 2022, Strategy, Policy, and Legal Barriers to E-Gov Implementation in Afghanistan. IEEE Access 10.
- Laxmi, Sunil Kumar, 2025, AI and Legal Liability: Who is Responsible for Decisions

Made by Algorithms?, 7 (2) IJLSI.

- Mittelstadt, Brent Daniel, et al, 2016, The ethics of algorithms: Mapping the debate. Big Data & Society 3.2.

- Mohiqi, Mohammad Mustafa, 2023, Personal Data Protection in the Iranian Legal System. J. Pol. & L. 16.

- Noto La Diega, Guido, Leonardo CT Bezerra, 2024, Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI liability directive. International Journal of Law and Information Technology 32.

- OECD, 2019, OECD Principles on Artificial Intelligence

- Pauletto, Christian, 2021, Options towards a global standard for the protection of individuals with regard to the processing of personal data. Computer Law & Security Review 40.

- Pfeiffer, Marc J, 2023, First, Do No Harm: Algorithms, AI, and Digital Product Liability. arXiv preprint arXiv.10861.

- Rahimi, Masoumeh, 2024, A comprehensive analysis of privacy and data protection in conflict-affected areas: Revising human rights and humanitarian law to address the challenges of surveillance technologies. MS thesis.

- Soh, Jerrold, 2023, Legal dispositionism and artificially-intelligent attributions. Legal Studies 43.4.

- UNESCO, 2021, Recommendation on the Ethics of Artificial Intelligence.

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.26- Winter 2026