Comparative Studies in Jurisprudence, Law, and Politics

The Traditional Model and the Risk-Based Approach to the International Responsibility of States: A Comparative Study of Artificial Intelligence Applications

1. Fatemeh Nadalizadeh: PhD Student in Public International Law, Department of Law, UAE.C., Islamic Azad University, Dubai, United Arab Emirates.
2. Atefeh Amininia*: Department of Law, CT.C., Islamic Azad University, Tehran, Iran. Email: (a.amininia@iauctb.ac.ir)
3. Seyedeh Sanaz Zabihi Shahri: Department of Law, ST.C., Islamic Azad University, Tehran, Iran.
4. Faraneh Zarafshan: Department of Computer Engineering, Ka.C., Islamic Azad University, Karaj, Iran.

ABSTRACT

States increasingly employ artificial intelligence systems in areas such as border control, natural disaster prediction, and administrative decision-making. When these systems cause harm, the question arises as to whether the traditional rules of international state responsibility remain adequate or should give way to a new model centered on risk management and prevention. This article compares these two models. The traditional model operates after harm has occurred and asks which conduct is attributable to the state and whether an international obligation has been breached. By contrast, the risk-based approach operates before harm occurs and examines what measures the state has taken to identify and mitigate risks. The study adopts a descriptive-analytical and comparative methodology and draws on the International Law Commission's 2001 Articles on Responsibility of States for Internationally Wrongful Acts, the jurisprudence of the International Court of Justice and the International Tribunal for the Law of the Sea, and technical instruments concerning risk management. The findings indicate that these two models are not competing alternatives but rather complementary approaches. Artificial intelligence exposes certain limitations of the traditional model without rendering its rules ineffective. Likewise, the risk-based approach does not replace the law of responsibility; rather, it helps determine what measures the state ought to have taken. The article concludes that the developments under consideration represent an evolution within the existing system of international responsibility rather than a transition to an entirely different legal regime.

Keywords: *international responsibility of states, artificial intelligence, risk-based approach, due diligence, prevention, risk management*

How to cite: Nadalizadeh, F., Amininia, A., Zabihi Shahri, S. S., Zarafshan, F. (2026). The Traditional Model and the Risk-Based Approach to the International Responsibility of States: A Comparative Study of Artificial Intelligence Applications. *Comparative Studies in Jurisprudence, Law, and Politics, 8*(2), 1-14.

© 2026 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 21 February 2026
Revise Date: 7 April 2026
Accept Date: 11 July 2026
Publish Date: 20 July 2026

پژوهش‌های تطبیقی فقه،
حقوق و سیاست

الگوی سنتی و رویکرد ریسک‌محور در مسئولیت بین‌المللی دولت: مطالعه تطبیقی در کاربردهای هوش مصنوعی

۱. فاطمه نادعلی‌زاده: دانشجوی دکتری حقوق بین‌الملل عمومی، گروه حقوق، واحد امارات، دانشگاه آزاد اسلامی، دبی، امارات متحده عربی.
۲. عاطفه امینی‌نیا* : گروه حقوق بین‌الملل، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران . پست الکترونیک: (a.amininia@iauctb.ac.ir)
۳. سیده ساناز ذبیحی شهری : گروه حقوق، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
٤. فرانه زرافشان : گروه مهندسی کامپیوتر، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران .

چکیده

دولت‌ها امروز در کارهایی مانند کنترل مرز، پیش‌بینی بلایای طبیعی و تصمیم‌گیری اداری از سامانه‌های هوش مصنوعی استفاده می‌کنند. وقتی این سامانه‌ها زیان می‌زنند، این پرسش پیش می‌آید که آیا قواعد سنتی مسئولیت بین‌المللی دولت هنوز کارآمدند یا باید جای خود را به الگوی تازه‌ای بدهند که بر مدیریت ریسک و پیشگیری تکیه دارد. این مقاله این دو الگو را با هم مقایسه می‌کند. الگوی سنتی پس از وقوع زیان وارد عمل می‌شود و می‌پرسد چه رفتاری به دولت منتسب است و آیا تعهدی نقض شده است. رویکرد ریسک‌محور پیش از وقوع زیان وارد عمل می‌شود و می‌پرسد دولت برای شناسایی و کاهش ریسک چه کرده است. روش مقاله توصیفی و تحلیلی و از نوع تطبیقی است و بر طرح مواد ۲۰۰۱ کمیسیون حقوق بین‌الملل، رویه دیوان بین‌المللی دادگستری و دیوان بین‌المللی حقوق دریاها و اسناد فنی مدیریت ریسک تکیه دارد. یافته‌ها نشان می‌دهد که این دو الگو رقیب هم نیستند، بلکه مکمل یکدیگرند. هوش مصنوعی محدودیت‌های الگوی سنتی را آشکار می‌کند، اما قواعد آن را از کار نمی‌اندازد. رویکرد ریسک‌محور هم جای مسئولیت را نمی‌گیرد، بلکه کمک می‌کند معلوم شود دولت چه کارهایی را باید انجام می‌داد. نتیجه آن است که با یک تحول درون نظام مسئولیت روبه‌رو هستیم، نه با گذار به نظامی دیگر.

واژگان کلیدی: *مسئولیت بین‌المللی دولت، هوش مصنوعی، رویکرد ریسک‌محور، مراقبت لازم، پیشگیری، مدیریت ریسک*

نحوه استناددهی: نادعلی زاده ، فاطمه.، امینی نیا، عاطفه.، ذبیحی شهری، سیده ساناز.، زرافشان، فرانه. (۱٤۰۵). الگوی سنتی و رویکرد ریسک‌محور در مسئولیت بین‌المللی دولت: مطالعه تطبیقی در کاربردهای هوش مصنوعی. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۸(۲)، ۱٤-۱.

© ۱٤۰۵ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۲ اسفند ۱٤۰٤
تاریخ بازنگری: ۱۸ فروردین ۱٤۰۵
تاریخ پذیرش: ۲۰ تیر ۱٤۰۵
تاریخ چاپ: ۲۹ تیر ۱٤۰۵

مقدمه

فرض کنید یک دولت برای پیش‌بینی سیل در رودخانه‌ای مرزی از یک سامانه هوش مصنوعی استفاده می‌کند. یک شب سامانه خطا می‌کند، هشدار داده نمی‌شود و سیل به روستاهای کشور همسایه آسیب می‌زند. کشور همسایه می‌خواهد بداند آیا دولت به‌کارگیرنده مسئول است. دو راه برای پاسخ دادن وجود دارد. راه اول این است که بپرسیم چه کسی چه کرد، آیا آن رفتار به دولت منتسب است و آیا تعهدی را نقض کرده است. این راه الگوی سنتی مسئولیت است. راه دوم این است که بپرسیم دولت پیش از استفاده از سامانه، ریسک آن را سنجیده بود یا نه، آن را آزموده بود یا نه، و در دوره استفاده بر کارش نظارت داشت یا نه. این راه همان چیزی است که امروز «رویکرد ریسک‌محور» نامیده می‌شود.

در نوشته‌های حقوقی درباره هوش مصنوعی، این دو راه اغلب در برابر هم قرار داده می‌شوند. گروهی می‌گویند الگوی سنتی برای هوش مصنوعی ساخته نشده است، چون سامانه‌های هوشمند خودشان یاد می‌گیرند، رفتارشان قابل پیش‌بینی نیست و چند بازیگر در ساختشان سهم دارند. این گروه پیشنهاد می‌کنند مسئولیت بر پایه ریسک بنا شود و حتی بدون اثبات تقصیر برقرار شود (Bellout, 2024). در نوشته‌های فارسی هم همین دیدگاه دیده می‌شود. به نظر سیدمرتضی حسینی، معیارهای موجود احراز مسئولیت، به‌ویژه در بخش احراز تقصیر، با کارکرد هوش مصنوعی سازگار نیست و تا زمانی که قواعد مناسب وضع نشده، تکیه بر مسئولیت مطلق مهم‌ترین رویکرد است (Seyed Morteza Hosseini, 2026). البته خود او این پیشنهاد را راهکاری موقت برای پر کردن خلأهای موجود می‌داند (Seyed Morteza Hosseini, 2026). برخی دیگر گفته‌اند عدم شفافیت عملکرد سامانه‌ها و دشواری احراز مسئولیت دولت‌ها، نظام پاسخگویی بین‌المللی را به‌شدت تضعیف می‌کند (Talaei & Jafarpour, 2025). در حوزه جنگ‌افزارها هم گفته شده است که حقوق جنگ بر جنگ‌افزارهای مبتنی بر هوش مصنوعی نظارت مؤثری ندارد و خلأ قانونی موجود به فرار از مسئولیت دولتی می‌انجامد (Lame et al., 2024).

گروه دیگر می‌گویند قواعد موجود کافی‌اند و فقط باید درست به کار روند (Kadkhodaei Elyadrani, 2024). حتی همان نویسندگانی که از خلأ مسئولیت سخن می‌گویند، می‌پذیرند که اگر استقرار سامانه‌های هوشمند به نقض تعهد بین‌المللی برسد، مسئولیت از راه نسبت دادن فعل یا ترک فعل افراد یا نهادها به دولت احراز می‌شود (Lame et al., 2024). در حقوق داخلی هم پیشنهاد شده است که به‌جای کنار گذاشتن تقصیر، بار اثبات جابه‌جا شود؛ راهی که هم مبنای تقصیر را حفظ می‌کند و هم جبران را آسان‌تر می‌سازد (Hajiesmaeili, 2024).

پرسش این مقاله این است که الگوی سنتی و رویکرد ریسک‌محور در مسئولیت بین‌المللی دولت چه شباهت‌ها و تفاوت‌هایی دارند و در برابر هوش مصنوعی چه نسبتی با هم پیدا می‌کنند. فرضیه مقاله این است که این دو الگو رقیب نیستند و رویکرد ریسک‌محور درون الگوی سنتی جای می‌گیرد؛ یعنی کمک می‌کند معلوم شود دولت چه تدابیری را باید اتخاذ می‌کرد، ولی مبنای تازه‌ای برای مسئولیت نمی‌سازد.

روش مقاله توصیفی و تحلیلی و از نوع تطبیقی است. دو الگو در شش محور مقایسه می‌شوند: زمان ورود به بحث، پرسش اصلی، جایگاه تقصیر، نقش رابطه علیت، منبع معیار و نتیجه عملی. منابع اصلی، طرح مواد ۲۰۰۱ کمیسیون حقوق بین‌الملل، رأی‌ها و نظرهای مشورتی مراجع بین‌المللی و اسناد فنی مدیریت ریسک است. در کنار این منابع، پژوهش‌های فارسی درباره مسئولیت دولت، مراقبت لازم و مسئولیت ناشی از هوش مصنوعی هم بررسی شده‌اند تا دیدگاه‌های داخلی نیز در مقایسه دیده شوند. این مقاله بخشی از رساله دکتری نویسنده نخست درباره اثر کاربرد هوش مصنوعی بر تحول نظام مسئولیت بین‌المللی است.

الگوی سنتی مسئولیت بین‌المللی دولت

ساختار الگوی سنتی

الگوی سنتی مسئولیت بین‌المللی دولت ساده است. دوپوی توضیح می‌دهد که در دیدگاه کلاسیک، تنها پیامد حقوقی فعل متخلفانه این بود که دولت مسئول باید زیان را جبران کند. میان منشأ مسئولیت و پیامد آن پیوندی ساده وجود داشت و اصولاً فقط دو دولت درگیر بودند: دولتی که رفتار کرده و دولتی که زیان دیده است (Dupuy, 1989).

طرح مواد ۲۰۰۱ کمیسیون حقوق بین‌الملل همین الگو را به شکل امروزی آن درآورده است. طبق ماده ۲، فعل متخلفانه بین‌المللی دو شرط دارد: رفتاری، چه فعل و چه ترک فعل، که به دولت منتسب باشد و رفتاری که نقض یکی از تعهدات بین‌المللی آن دولت باشد (Ziaei Bigdeli & Tarazi, 2020). اگر این دو شرط جمع شوند، دولت مسئول است و طبق ماده ۳۱ باید زیانی را که از این فعل برخاسته به‌طور کامل جبران کند (Ziaei Bigdeli & Tarazi, 2020).

ویژگی‌های الگوی سنتی

سه ویژگی این الگو برای بحث ما مهم است. ویژگی اول این است که الگوی سنتی پسینی است؛ یعنی معمولاً پس از وقوع زیان وارد بحث می‌شود. ابتدا رخدادی پیش می‌آید و سپس پرسیده می‌شود چه رفتاری پشت آن بوده است.

ویژگی دوم این است که برخلاف تصور رایج، تقصیر شرط عمومی مسئولیت در این الگو نیست. شرح ماده ۲ تصریح می‌کند که زیان و تقصیر عناصر عمومی و مستقل فعل متخلفانه نیستند و لازم بودن هر یک به محتوای تعهد اولیه بستگی دارد (Dupuy, 1989). پس این ادعا که الگوی سنتی همیشه به «تقصیر انسانی» نیاز دارد، دقیق نیست.

ویژگی سوم این است که رابطه علیت در این الگو در مرحله تعیین جبران نقش اصلی دارد، نه در مرحله احراز مسئولیت. دیوان بین‌المللی دادگستری در قضیه بوسنی نشان داد که حتی اگر نتوان «با درجه کافی از قطعیت» ثابت کرد که اجرای تعهد از زیان جلوگیری می‌کرد، مسئولیت از بین نمی‌رود؛ فقط شکل جبران از غرامت به جلب رضایت تغییر می‌کند (Ziaei Bigdeli & Tarazi, 2020).

هوش مصنوعی چه چیزی را در این الگو دشوار می‌کند؟

هوش مصنوعی سه دشواری برای این الگو پدید می‌آورد. نخست، رفتاری که زیان زده، گاهی خروجی یک سامانه است، نه تصمیم مستقیم یک انسان. باید روشن شود کدام تصمیم انسانی را باید بررسی کرد. دوم، خروجی سامانه همیشه قابل پیش‌بینی و توضیح نیست و همین اثبات را سخت می‌کند. سوم، شرکت‌های مختلفی در ساخت داده، مدل و زیرساخت سهم دارند و تشخیص سهم هر کدام آسان نیست.

نوشته‌های فارسی هم به همین سه دشواری اشاره کرده‌اند. درباره دشواری اول گفته شده است که وقتی عامل انسانی پیشنهادی از الگوریتم دریافت می‌کند، توانایی درستی برای ارزیابی پیامد آن ندارد و فقط از توصیه‌های سامانه پیروی می‌کند (Lame et al., 2024). درباره دشواری دوم، یادآوری شده است که بسیاری از سامانه‌ها ارتباط علّی میان ورودی و خروجی را توضیح نمی‌دهند و همین کمبود شفافیت، پاسخگویی و بازرسی را محدود می‌کند (Kheirandish Sorkhabadi & Ahmadi, 2024). در ادبیات مسئولیت مدنی هم آمده است که چالش پیش‌بینی‌پذیری زیان و موانع احراز رابطه سببیت، ارکان نظریه تقصیر را متزلزل می‌کند (Makki et al., 2024). درباره دشواری سوم، پیری می‌نویسد فهرست کسانی که ممکن است مسئول باشند، از برنامه‌نویسان تا رهبران سیاسی، تقریباً پایانی ندارد و همین تعیین

مسئولیت را دشوار می‌کند (Piri, 2025). ضیایی بیگدلی و ترازی برای چنین وضعیت‌هایی میان «اسباب مکمل» و «اسباب مرکب» فرق می‌گذارند و قضیه کانال کورفو را نمونه اسباب مرکب در یک زیان واحد می‌دانند (Ziaei Bigdeli & Tarazi, 2020).

اما این دشواری‌ها بیشتر به اعمال و اثبات قاعده مربوط‌اند تا به وجود قاعده. بوتین نشان می‌دهد که در کاربرد هوش مصنوعی، کانون بررسی از اپراتوری که در لحظه آخر حضور دارد به تصمیم‌گیرندگان منتقل می‌شود (Boutin, 2023) و از لحظه تولید خروجی به مراحل توسعه و تدارک سامانه (Boutin, 2023). یعنی پرسش انتساب پابرجاست، فقط نقطه‌ای که باید به آن نگاه کرد جابه‌جا شده است. تصمیم دستگاه دولتی برای خرید، آزمون و استقرار سامانه، رفتار رکن دولت است و طبق ماده ٤ طرح مواد به دولت منتسب می‌شود (Kadkhodaei Elyadrani, 2024). پیری هم بر همین اساس معتقد است دولت‌ها وظیفه دارند تعهدات بین‌المللی خود را از آغاز و در سراسر فرایند توسعه، آموزش و آزمایش هوش مصنوعی نظامی بگنجانند (Piri, 2025).

پیشگیری در الگوی سنتی چیز تازه‌ای نیست

گاهی گفته می‌شود الگوی سنتی فقط به جبران پس از زیان فکر می‌کند و از پیشگیری غافل است. این برداشت دقیق نیست. پیشگیری از دیرباز در حقوق بین‌الملل جای داشته است. دیوان داوری در قضیه کارخانه ذوب تریل نتیجه گرفت که «هیچ دولتی حق ندارد از سرزمین خود به گونه‌ای استفاده کند یا اجازه استفاده دهد» که به سرزمین دولت دیگر آسیب برسد، به این شرط که آسیب جدی باشد و با «دلیل روشن و قانع‌کننده» اثبات شود (Hosseini & Rahaei, 2024). نکته جالب این است که کارخانه تریل به یک شرکت خصوصی تعلق داشت. پس تعهد دولت از همان آغاز، فعالیت زیان‌بار اشخاص خصوصی در سرزمینش را هم در بر می‌گرفت.

دیوان بین‌المللی دادگستری هم در قضیه کانال کورفو از «تعهد هر دولت به اینکه آگاهانه اجازه ندهد قلمروش برای اعمال مغایر با حقوق دولت‌های دیگر به کار رود» سخن گفت (Hosseini & Rahaei, 2024). سال‌ها بعد، همین دیوان در قضیه کارخانه‌های خمیر کاغذ بر رود اروگوئه، ارزیابی اثرات محیط‌زیستی را پیش از اجرای فعالیتی که ریسک فرامرزی دارد، بخشی از مراقبت لازم دانست (Hosseini & Rahaei, 2024). این رأی بسیار به بحث ما نزدیک است. اگر ارزیابی پیشینی جزئی از مراقبت لازم در فعالیت‌های پرریسک است، دلیلی ندارد که سامانه‌های پرریسک هوش مصنوعی از این منطق بیرون بمانند.

رویکرد ریسک‌محور

منطق رویکرد ریسک‌محور

رویکرد ریسک‌محور از اسناد فنی و تنظیم‌گری وارد بحث مسئولیت شده است. منطق آن این است که به‌جای اینکه منتظر زیان بمانیم، پیش از آن ریسک‌ها را شناسایی کنیم، بسنجیم و برای کاهششان اقدام کنیم. سازمان همکاری و توسعه اقتصادی در چارچوب طبقه‌بندی سامانه‌های هوش مصنوعی میان سامانه «در آزمایشگاه» و سامانه «در میدان» فرق می‌گذارد و اولی را به رویکردهای پیشینی و دومی را به رویکردهای پسینی مدیریت ریسک مربوط می‌کند (Bellout, 2024).

چارچوب مدیریت ریسک هوش مصنوعی که مؤسسه ملی استاندارد و فناوری آمریکا منتشر کرده، نمونه روشنی از این رویکرد است. این چارچوب از جمله مستند کردن محدودیت‌های دانش سامانه (Bellout, 2024)، پایش کارکرد آن در دوره بهره‌برداری (Bellout, 2024) و اجرای برنامه‌های پایش پس از استقرار (Bellout, 2024) را پیش‌بینی می‌کند. همین سند یادآوری می‌کند که برخی ریسک‌ها ممکن است

مدتی پنهان بمانند و با تغییر سامانه بیشتر شوند (Bellout, 2024). پس مدیریت ریسک کاری یک‌باره نیست و باید در سراسر عمر سامانه ادامه پیدا کند.

قانون هوش مصنوعی اتحادیه اروپا این منطق را الزام‌آور کرده است. در توصیف فارسی این قانون آمده است که ارائه‌دهندگان و کاربران سامانه‌های پرریسک باید برای رویارویی با هر ریسک شناخته‌شده یا قابل پیش‌بینی، نظام مدیریت ریسک را ایجاد، پیاده‌سازی، مستند و نگهداری کنند (Kadkhodaei Elyadrani et al., 2026). کسی هم که سامانه پرریسک را مستقر می‌کند، تعهداتی مانند ارزیابی ریسک، آموزش و نگهداری گزارش‌ها بر عهده دارد (Kadkhodaei Elyadrani et al., 2026).

چرا رویکرد ریسک‌محور برای هوش مصنوعی جذاب است؟

این رویکرد برای هوش مصنوعی جذاب است، چون درست به همان دشواری‌هایی پاسخ می‌دهد که الگوی سنتی با آن‌ها روبه‌روست. اگر خروجی یک سامانه پیش‌بینی‌پذیر نیست، دست‌کم می‌توان پرسید آیا دولت این پیش‌بینی‌ناپذیری را سنجیده و برایش چاره‌ای اندیشیده بود. اگر اثبات اینکه کدام خطای فنی زیان زد سخت است، دست‌کم می‌توان دید آیا دولت سامانه را پیش از استقرار آزموده بود.

برتولینی در گزارشی برای پارلمان اروپا توضیح می‌دهد که با جا افتادن مدل ریسک‌محور، مرکز ثقل تنظیم‌گری به انطباق پیشینی منتقل شده است و جبران پس از زیان ممکن است به حاشیه برود (Bertolini, 2025). او همچنین پیشنهاد می‌کند بازیگری که بر سامانه کنترل دارد و از آن سود می‌برد، ریسک آن را بدون اثبات تقصیر بپذیرد (Bertolini, 2025). این پیشنهاد در سطح مسئولیت مدنی اروپا مطرح شده است، اما نشان می‌دهد که رویکرد ریسک‌محور گاهی به سمت مسئولیت بدون تقصیر می‌رود. در مسئولیت محض، زیان‌دیده لازم نیست تقصیر و پیوند علّی میان تقصیر و خسارت را اثبات کند و همین که زیان رخ داده باشد کافی است (Alipanahi et al., 2024).

محدودیت‌های رویکرد ریسک‌محور

رویکرد ریسک‌محور هم محدودیت دارد. نخست، خود اسناد فنی می‌گویند سنجش ریسک همیشه دقیق نیست. مؤسسه ملی استاندارد و فناوری یادآوری می‌کند که اگر نتوانیم ریسک یک سامانه را به‌درستی بسنجیم، این به معنای پایین یا بالا بودن ریسک آن سامانه نیست (Bellout, 2024). دوم، حتی قانونی که این رویکرد را به شکل الزام‌آور پذیرفته، روش روشنی برای سنجش ریسک در موقعیت‌های مشخص ارائه نمی‌کند و ریسک‌ها را بیشتر بر پایه حوزه کاربرد دسته‌بندی می‌کند (Kadkhodaei Elyadrani et al., 2026). سوم، این اسناد بیشتر غیرالزام‌آورند و به‌خودی‌خود تعهد بین‌المللی برای دولت پدید نمی‌آورند. چهارم، داشتن سازوکار مدیریت ریسک به این معنا نیست که خروجی سامانه واقعاً بازبینی می‌شود. پژوهش‌های فارسی در حوزه تنظیم‌گری هشدار داده‌اند که اعتماد بیش از حد به درستی تصمیم‌های الگوریتمی باعث می‌شود این تصمیم‌ها کمتر بازبینی و تعدیل شوند، حتی اگر داده‌های ورودی ناکافی یا نامعتبر باشند (Kheirandish Sorkhabadi & Ahmadi, 2024).

مقایسه دو الگو

مقایسه در شش محور

جدول زیر دو الگو را در شش محور کنار هم می‌گذارد.

جدول ۱. مقایسه الگوها

محور	الگوی سنتی	رویکرد ریسک‌محور
زمان ورود به بحث	پس از وقوع زیان	پیش از وقوع زیان و در سراسر عمر سامانه
پرسش اصلی	چه رفتاری به دولت منتسب است و آیا تعهدی نقض شده؟	دولت برای شناسایی و کاهش ریسک چه کرده است؟
جایگاه تقصیر	شرط عمومی نیست و به تعهد اولیه بستگی دارد	گاهی به سمت مسئولیت بدون تقصیر می‌رود
نقش رابطه علیت	در تعیین جبران نقش اصلی دارد	اهمیتش کمتر است، چون تمرکز بر تدابیر پیشگیرانه است
منبع معیار	تعهدات بین‌المللی و رویه قضایی	اسناد فنی و استانداردها، که بیشتر غیرالزام‌آورند
نتیجه عملی	جبران زیان یا جلب رضایت	آشکار شدن کوتاهی در آزمون، پایش و نظارت

شباهت‌ها

با وجود این تفاوت‌ها، دو الگو در دو نقطه به هم می‌رسند. نقطه اول این است که هر دو، سامانه هوش مصنوعی را مسئول نمی‌دانند. در الگوی سنتی، فقط رفتار منتسب به دولت مسئولیت می‌آورد. در رویکرد ریسک‌محور هم آنچه سنجیده می‌شود تدابیر سازمان یا دولتی است که سامانه را به کار برده است. بوتین هم تأکید می‌کند که رفتار متخلفانه در کاربرد هوش مصنوعی «همچنان و همیشه به انتخاب‌ها و افعال یا ترک‌فعل‌های انسانی بازگشت‌پذیر است» (Boutin, 2023).

نقطه دوم این است که هر دو به پیشگیری اهمیت می‌دهند. چنان‌که در بخش ٤–٢ آمد، الگوی سنتی از دیرباز تعهد به مراقبت لازم را می‌شناسد؛ یعنی دولت باید همه تدابیری را که در توان دارد برای پیشگیری از زیان به کار گیرد. دیوان بین‌المللی دادگستری در قضیه بوسنی آستانه نقض این تعهد را «کوتاهی بارز از اتخاذ همه تدابیر در توان دولت» دانست و تصریح کرد که مراقبت لازم ارزیابی‌ای «مشخص و موردی» لازم دارد (Hosseini & Rahaei, 2024). در ادبیات فارسی هم مراقبت لازم «مفهومی منعطف» دانسته شده که محتوای آن به اوضاع‌واحوال بستگی دارد و عواملی چون کنترل مؤثر دولت بر قلمرو، پیش‌بینی‌پذیری رویداد و اهمیت منافع مورد حمایت در سنجش آن اثر دارند (Hosseini & Rahaei, 2024). در حقوق بین‌الملل سرمایه‌گذاری هم، درباره مراقبت سرمایه‌گذار، تأکید شده است که این ضابطه به مرحله پیش از ورود محدود نمی‌شود و در تمام مدت فعالیت هم باید رعایت شود (Hosseini & Habibi Mojandeh, 2024). این همان چیزی است که رویکرد ریسک‌محور با عنوان مدیریت ریسک در سراسر عمر سامانه می‌خواهد. پس پیشگیری برای الگوی سنتی چیز تازه‌ای نیست.

تفاوت اصلی

تفاوت اصلی دو الگو در «مبنا» است. در الگوی سنتی، مبنای مسئولیت نقض یک تعهد بین‌المللی است. در برخی صورت‌بندی‌های رویکرد ریسک‌محور، مبنا خود ریسک است؛ یعنی هر کس فعالیتی پرریسک انجام دهد، باید زیان آن را بپردازد، حتی اگر کوتاهی نکرده باشد. این همان پیشنهاد مسئولیت مبتنی بر ریسک یا مسئولیت بدون تقصیر است (Bellout, 2024). اگر این صورت‌بندی پذیرفته شود، با گذار به نظامی تازه روبه‌رو هستیم، نه با تحولی درون همان نظام. این بحث فقط به حقوق بین‌الملل مربوط نیست. در مقایسه‌ای میان حقوق ایران و اتحادیه اروپا نشان داده شده است که مسئولیت کاربر هوش مصنوعی همچنان بر تقصیر استوار است، در حالی که مسئولیت سازنده در اتحادیه اروپا مطلق است و در حقوق ایران وضعیتی مبهم دارد (Hajiesmaeili, 2024).

ابعاد سیاستی انتخاب میان دو الگو

انتخاب میان این دو الگو فقط پرسشی حقوقی نیست و پیامد سیاسی هم دارد. اگر مبنای مسئولیت خود ریسک باشد، دولت‌هایی که فناوری پیشرفته را زودتر به کار می‌گیرند بار بیشتری بر دوش خواهند داشت، حتی اگر همه احتیاط‌های ممکن را رعایت کرده باشند. این امر ممکن است دولت‌ها را از پذیرش چنین قاعده‌ای دور کند، چون قواعد بین‌المللی با رضایت خود دولت‌ها شکل می‌گیرد. از سوی دیگر، اگر مدیریت ریسک فقط به داشتن گزارش‌های رسمی محدود شود، ممکن است به ابزاری برای فرار از مسئولیت تبدیل شود. دولتی که گزارش ارزیابی دارد، ممکن است ادعا کند وظیفه‌اش را انجام داده است. جای دادن رویکرد ریسک‌محور درون تعهد به مراقبت لازم، میان این دو نگرانی تعادل برقرار می‌کند. این راه با توانایی متفاوت دولت‌ها هم سازگارتر است؛ چنان‌که طرفداران ارزیابی نسبی گفته‌اند نمی‌توان توانایی دولت‌ها و ابزار و زیرساختی را که در اختیار دارند نادیده گرفت و همه را با یک معیار سنجید (Hosseini & Habibi Mojandeh, 2024). از دولت‌ها مسئولیت بدون کوتاهی خواسته نمی‌شود، اما گزارش ارزیابی هم به‌تنهایی آن‌ها را مصون نمی‌کند.

رویکرد ریسک‌محور در حقوق بین‌الملل کنونی کجا می‌نشیند؟

رویکرد ریسک‌محور سنجه مراقبت لازم است

رویه مراجع بین‌المللی نشان می‌دهد که حقوق بین‌الملل کنونی رویکرد ریسک‌محور را به‌عنوان مبنای تازه مسئولیت نپذیرفته، بلکه آن را درون تعهد به مراقبت لازم جای داده است. اتاق حل اختلافات بستر دریای دیوان بین‌المللی حقوق دریاها تصریح کرد که مراقبت لازم «مفهومی متغیر است» و تدابیری که روزی کافی بوده‌اند، ممکن است با دانش علمی یا فناورانه تازه دیگر کافی نباشند (Hosseini & Rahaei, 2024). دیوان بین‌المللی دادگستری هم در نظر مشورتی ۲۰۲۵ درباره تغییرات اقلیمی، معیار مراقبت لازم را برای پیشگیری از زیان قابل‌توجه به نظام اقلیمی «سخت‌گیرانه» دانست و یادآوری کرد که این تعهد افزون بر اتخاذ قواعد و تدابیر مناسب، سطحی از هوشیاری در اجرای آن‌ها را هم لازم دارد (Hosseini & Rahaei, 2024).

معنای این دو حکم آن است که شدت ریسک و میزان دانش درباره آن، تعیین می‌کند دولت چه تدابیری را باید اتخاذ می‌کرد. یعنی ریسک وارد بحث مسئولیت شده است، اما نه به‌عنوان مبنای جدید، بلکه به‌عنوان سنجه‌ای برای اینکه بدانیم مراقبت لازم در هر مورد چه چیزهایی را می‌خواهد.

سه نتیجه عملی

از این جایگاه سه نتیجه عملی به دست می‌آید. نتیجه اول این است که مدیریت ریسک معلوم می‌کند چه تدابیری از دولت انتظار می‌رود. اگر یک سند فنی معتبر می‌گوید سامانه باید پیش از استقرار آزموده شود و پس از آن پایش شود، این کارها جزو تدابیری است که دولت محتاط انجام می‌دهد.

نتیجه دوم این است که انجام دادن مدیریت ریسک به‌تنهایی دولت را مصون نمی‌کند. داشتن یک گزارش ارزیابی ریسک کافی نیست. آنچه سنجیده می‌شود این است که آیا دولت همه تدابیری را که در توان داشت به کار گرفت یا نه (Hosseini & Rahaei, 2024).

نتیجه سوم این است که انجام ندادن مدیریت ریسک قرینه کوتاهی است. کمیته بین‌المللی صلیب سرخ دولتی را که سامانه‌ای آزموده‌نشده یا ناکافی آزموده‌شده را به کار گیرد، مسئول می‌داند (Piri, 2025). سانحه پرواز پی‌اس۷۵۲ هم نمونه‌ای از همین منطق است. به گفته گزارش تیم بررسی کانادا، ارزیابی ریسکی که ایران در گزارش نهایی خود ارائه کرد، به اطلاعات متعارضی که نشان می‌داد سطح ریسک بسیار بالاتر

است، نپرداخته بود (Forensic & Assessment, 2021). در چنین وضعیتی، نقص ارزیابی ریسک قرینه‌ای بر کوتاهی در مراقبت لازم است.

بازگشت به مثال سیل

حالا به مثال آغاز مقاله برگردیم. در الگوی سنتی، باید پرسید آیا دولت به‌کارگیرنده تعهد به مراقبت لازم برای پیشگیری از زیان فرامرزی را نقض کرده است. رویکرد ریسک‌محور کمک می‌کند به این پرسش پاسخ دهیم. آیا دولت ریسک سامانه را در شرایط بارش شدید سنجیده بود؟ آیا سامانه را پیش از استقرار آزموده بود؟ آیا کارمند کشیک ابزار و دستورالعمل لازم برای نادیده گرفتن خروجی نادرست را داشت؟ اگر پاسخ این پرسش‌ها منفی باشد، کوتاهی دولت آشکار است و مسئولیت آن بر پایه همان الگوی سنتی برقرار می‌شود. اگر هم ثابت نشود که آزمون کافی با درجه کافی از قطعیت از سیل جلوگیری می‌کرد، مسئولیت از بین نمی‌رود؛ فقط شکل جبران تغییر می‌کند. پس دو الگو در این مثال با هم کار می‌کنند: رویکرد ریسک‌محور پرسش‌ها را مشخص می‌کند و الگوی سنتی پاسخ حقوقی را می‌دهد.

نتیجه‌گیری

این مقاله الگوی سنتی مسئولیت بین‌المللی دولت و رویکرد ریسک‌محور را در برابر کاربردهای هوش مصنوعی مقایسه کرد. یافته‌ها فرضیه مقاله را تأیید می‌کند. این دو الگو رقیب هم نیستند. الگوی سنتی پس از زیان می‌پرسد چه رفتاری به دولت منتسب است و آیا تعهدی نقض شده است. رویکرد ریسک‌محور پیش از زیان می‌پرسد دولت برای کاهش ریسک چه کرده است. در حقوق بین‌الملل کنونی، پاسخ پرسش دوم به پاسخ دادن به پرسش اول کمک می‌کند.

هوش مصنوعی محدودیت‌های الگوی سنتی را آشکار می‌کند، ولی آن را از کار نمی‌اندازد. دشواری‌هایی که این فناوری پدید می‌آورد بیشتر به اعمال و اثبات قاعده مربوط‌اند تا به نبود قاعده. رویکرد ریسک‌محور هم مبنای تازه مسئولیت نشده است، بلکه سنجه‌ای است که معیار مراقبت لازم را روشن‌تر و عینی‌تر می‌کند. به همین دلیل، آنچه رخ داده تحولی درون نظام مسئولیت است، نه گذار به نظامی دیگر. دوپوی هم در ارزیابی همین پرسش، یعنی انقلاب یا تکامل، نتیجه گرفته بود که هنوز زود است بگوییم وحدت مسئولیت بین‌المللی از میان رفته است (Dupuy, 1989).

یک پرسش باز می‌ماند. اگر روزی سامانه‌هایی به کار روند که رفتارشان ذاتاً پیش‌بینی‌ناپذیر باشد، آیا الگوی مبتنی بر نقض تعهد کافی خواهد بود؟ بوتین هم با اشاره به پیش‌بینی‌ناپذیری ذاتی برخی فناوری‌های هوش مصنوعی و ریسک خرابی آن‌ها می‌پرسد که آیا الگوی مبتنی بر سهل‌انگاری کافی است یا باید مسئولیت محض را پذیرفت (Boutin, 2023). پاسخ این پرسش به پژوهش‌های آینده نیاز دارد.

بر این پایه چند پیشنهاد مطرح می‌شود. نخست، دولت‌ها پیش از استقرار سامانه‌های هوش مصنوعی در کارهای حاکمیتی، ریسک آن‌ها را بسنجند و نتیجه را مستند کنند، زیرا همین مستندات در صورت بروز اختلاف مهم‌ترین دلیل مراقبت آن‌هاست. دوم، ارزیابی ریسک به یک بار محدود نشود و در دوره بهره‌برداری هم ادامه یابد. سوم، کارمندانی که با این سامانه‌ها کار می‌کنند، اطلاعات، آموزش و اختیار لازم برای نادیده گرفتن خروجی نادرست را داشته باشند. چهارم، در تحلیل حقوقی، اسناد فنی مدیریت ریسک به‌عنوان راهنمای سنجش مراقبت لازم به کار روند، نه به‌عنوان منبع مستقل تعهد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

Artificial intelligence is increasingly used by states in areas such as border control, disaster prediction, administrative decision-making, public regulation, and military applications. These developments have generated an important question in the law of international responsibility: whether the traditional framework of state responsibility remains capable of addressing harm caused through AI-enabled systems, or whether a new model centered on risk management, prevention, and prospective oversight is required. The traditional model generally examines responsibility after an allegedly wrongful act has occurred by asking whether particular conduct is attributable to the state and whether that conduct constitutes a breach of an international obligation. By contrast, a risk-based approach focuses on what the state did before and during the deployment of an AI system to identify, evaluate, monitor, and mitigate foreseeable risks. This contrast has led some scholars to argue that the classical model is inadequate for AI because intelligent systems may operate with a degree of autonomy, unpredictability, opacity, and technical complexity that complicates the identification of human fault and causation. Risk-based liability has accordingly been proposed as a possible response, including formulations in which liability is imposed without the traditional requirement of establishing fault (Bellout, 2024). Similar concerns have been expressed in scholarship emphasizing that conventional criteria of responsibility, particularly those associated with fault, may not fully correspond to the operational characteristics of AI systems and that stricter forms of responsibility may temporarily be required until more specific legal rules are developed (Seyed Morteza Hosseini, 2026). Other studies likewise emphasize that the opacity of algorithmic processes, the difficulty of identifying the responsible public actor, and the distributed character of technological decision-making can weaken existing mechanisms of international accountability (Talaei & Jafarpour, 2025). In the field of AI-based weapons, similar arguments have been made regarding the inadequacy of effective legal control and the risk that regulatory gaps may facilitate avoidance of state responsibility (Lame et al., 2024). Nevertheless, another body of scholarship maintains that existing principles remain legally sufficient if they are applied appropriately to the full chain of state decision-making and institutional conduct (Kadkhodaei Elyadrani, 2024). The central hypothesis of this study is therefore that the traditional model and the risk-based approach should not be understood as mutually exclusive alternatives. Rather, the risk-based approach can operate within the traditional framework by clarifying the preventive measures, oversight duties, and standards of conduct expected from states without creating an entirely new legal basis for international responsibility.

The traditional model of international state responsibility is founded on a relatively clear legal structure. Classical accounts describe responsibility as the legal consequence of an internationally wrongful act committed by a state, followed by the obligation to provide reparation for the resulting injury (Dupuy, 1989). In its modern form, this framework is organized around two basic requirements: conduct attributable to the state and the breach of an international obligation. Where these conditions are satisfied, responsibility arises and the responsible state may be required to make full reparation for the injury caused (Ziaei Bigdeli & Tarazi, 2020). An important point for the present debate is that fault is not necessarily a general and autonomous condition of international

responsibility. Whether negligence, intention, knowledge, or another subjective element must be demonstrated depends primarily on the content of the underlying primary obligation rather than on a universal requirement inherent in the law of responsibility itself. Consequently, the argument that the traditional model necessarily depends on proof of individual human fault is overstated (Dupuy, 1989). Causation also performs a more limited function than is sometimes assumed. It is especially significant in determining the scope and form of reparation, whereas responsibility may still arise even where it cannot be established with sufficient certainty that proper performance of the obligation would have entirely prevented the ultimate harm (Ziaei Bigdeli & Tarazi, 2020). These features are important for AI-related cases because they show that the traditional framework is more adaptable than a narrow fault-based interpretation suggests. AI may alter the evidentiary and factual context in which responsibility is assessed, but it does not necessarily displace the underlying legal structure. The relevant inquiry remains whether the state, through its organs or persons whose conduct is legally attributable to it, failed to comply with an international obligation. In this sense, a governmental decision to procure, authorize, test, deploy, supervise, or continue using an AI system remains attributable state conduct even if the immediate technical output is generated by a machine-learning model rather than by a human decision-maker at the final stage. The existence of technological intermediation therefore does not eliminate legal attribution; it changes the factual point at which the attribution analysis should be directed.

Artificial intelligence nevertheless creates significant difficulties for the application and proof of traditional responsibility. First, the harmful output may be generated through an automated process rather than through an identifiable final human decision, making it necessary to trace responsibility to earlier decisions concerning system design, acquisition, training, validation, deployment, or supervision. Second, many AI systems are characterized by limited explainability, making it difficult to reconstruct the causal relationship between input data, algorithmic processing, and harmful output. Third, multiple actors may participate in the construction and operation of a system, including developers, software providers, data suppliers, contractors, military or administrative officials, and political decision-makers, thereby complicating the allocation of responsibility. Scholarship on AI in public administration has emphasized that human operators may lack the expertise or practical capacity to independently evaluate algorithmic recommendations and may therefore rely heavily on machine-generated outputs (Lame et al., 2024). Other research highlights that limited transparency can restrict meaningful inspection, accountability, and review of algorithmic decision-making (Kheirandish Sorkhabadi & Ahmadi, 2024). In civil liability literature, unpredictability of harm and difficulties in establishing causation have similarly been identified as factors that destabilize conventional fault-based reasoning (Makki et al., 2024). In military applications, the potential list of responsible actors may extend from technical programmers and designers to commanders and political authorities, making the determination of legal responsibility increasingly complex (Piri, 2025). Situations involving multiple contributing causes also raise broader questions of shared responsibility and the distinction between complementary and combined causal contributions (Ziaei Bigdeli & Tarazi, 2020). Yet these problems concern the operationalization and proof of responsibility more than the absence of legal rules. In AI-related applications, the proper focus may shift from the operator who acts at the final stage to the institutional and governmental actors who made the relevant choices regarding development, procurement, deployment, and oversight (Boutin, 2023). Likewise, the temporal focus may shift from the instant at which the AI generates an output to earlier stages in the technological life cycle, including system development, preparation, testing, and integration (Boutin, 2023). Accordingly, AI

does not eliminate the attribution inquiry; it redistributes it across a wider decision-making chain. This supports the view that states must integrate their international legal obligations into the development, training, testing, and deployment of AI systems from the earliest stages and throughout their operational life (Piri, 2025).

The risk-based approach responds directly to these difficulties by shifting emphasis from retrospective reconstruction of fault to prospective identification, assessment, monitoring, and mitigation of risk. Its central logic is preventive: instead of waiting for harm to occur, the responsible public authority should identify foreseeable hazards, evaluate the probability and severity of adverse consequences, adopt proportionate safeguards, document the reasons for its decisions, and continuously monitor the system during operation. This approach is particularly attractive in the context of AI because some risks may be difficult to predict with precision, may emerge only after deployment, or may increase as systems interact with changing environments and data. Contemporary regulatory practice increasingly treats risk management as a continuing process rather than a single pre-deployment exercise. In the European context, high-risk AI systems are subject to increasingly structured obligations concerning risk assessment, documentation, oversight, monitoring, and human control (Kadkhodaei Elyadrani et al., 2026). From the perspective of civil liability, the emergence of risk-oriented regulation has shifted attention toward ex ante compliance and toward the responsibility of actors who exercise effective control over technological systems and benefit from their use (Bertolini, 2025). Some formulations move further toward forms of strict or risk-based liability in which the injured party need not prove conventional fault, especially where control over the technology and allocation of technological risk can justify placing the burden on the operator or producer (Bertolini, 2025). Comparable discussions in legal scholarship distinguish strict liability from fault-based models on the ground that the occurrence of legally relevant harm may itself activate liability without requiring proof of negligence and a causal relationship between negligence and the damage (Alipanahi et al., 2024). However, the risk-based approach also has important limitations. Risk measurement can itself be uncertain, technical standards may not provide a complete methodology for every factual context, and many risk-management instruments remain non-binding and therefore cannot automatically create international legal obligations. Moreover, the mere existence of a formal risk-assessment process does not guarantee effective human review. Excessive reliance on algorithmic outputs may discourage critical reassessment even where the data are incomplete or unreliable (Kheirandish Sorkhabadi & Ahmadi, 2024). For these reasons, risk management should not be treated as an automatic substitute for the legal analysis of responsibility. Its more convincing function is evidentiary and normative: it helps specify the conduct expected from a prudent state in technologically complex environments.

A comparison of the two models reveals both important differences and substantial areas of convergence. The traditional model is primarily retrospective and asks whether conduct attributable to the state breached an international obligation, whereas the risk-based approach is predominantly prospective and asks what the state did to identify, control, and mitigate risks before harm occurred and throughout the operation of the system. Fault is not a general requirement under the traditional framework, whereas some risk-based formulations move toward liability without fault. Causation is central to the determination of reparation in the traditional model, while its relative importance may diminish in a preventive model that focuses primarily on whether adequate safeguards were adopted. The sources of applicable standards also differ: the traditional model derives its normative basis from binding international obligations and international jurisprudence, while risk-oriented approaches frequently draw on technical standards, regulatory instruments, and professional guidance. Despite

these distinctions, the two approaches converge in two decisive respects. First, neither of them requires treating the AI system itself as the legally responsible subject. Even where an automated system produces the immediate harmful outcome, the relevant legal inquiry ultimately returns to human and institutional decisions, omissions, choices, and structures (Boutin, 2023). Second, both models recognize the importance of prevention. The obligation of due diligence has long required states to adopt appropriate preventive measures in circumstances where their conduct or activities under their jurisdiction may create risks of serious harm. Due diligence is inherently flexible and context-sensitive, and its content depends on factors such as foreseeability, the degree of control exercised by the state, the seriousness of the protected interest, the level of available knowledge, and the practical capacity of the state to act (Hosseini & Rahaei, 2024). The standard may also continue throughout the duration of an activity rather than applying only at its initial stage (Hosseini & Habibi Mojandeh, 2024). This makes due diligence the most persuasive doctrinal bridge between traditional international responsibility and contemporary risk management. Risk does not need to become an autonomous basis of international responsibility; instead, the level and nature of risk can help determine the content and intensity of the preventive measures required by due diligence. This interpretation also avoids the political and doctrinal difficulties of imposing strict international liability merely because a state has adopted an advanced but inherently risky technology. It allows international law to remain sensitive to differences in state capacity while still requiring meaningful assessment, testing, monitoring, documentation, and human supervision. In this sense, risk management can make the traditional standard of due diligence more concrete and operational without displacing the established structure of attribution and breach.

The study concludes that the development of artificial intelligence does not presently justify replacing the traditional law of international state responsibility with an entirely separate risk-based regime. The principal difficulties introduced by AI concern the identification of relevant human and institutional conduct, the evidentiary reconstruction of complex algorithmic processes, the distribution of functions among multiple public and private actors, and the determination of what preventive measures were reasonably required in a particular technological context. These problems are significant, but they do not demonstrate that the existing legal structure has become obsolete. The more persuasive interpretation is that the risk-based approach should be incorporated into the traditional model through the concept of due diligence. Risk assessment, pre-deployment testing, continuous monitoring, documentation of system limitations, post-deployment review, human oversight, and the ability to override unreliable algorithmic outputs can all serve as concrete indicators of whether a state exercised the level of care required by its applicable international obligations. Under this approach, failure to conduct meaningful risk management may constitute evidence of a lack of due diligence, while the mere existence of a formal risk-management report cannot automatically shield a state from responsibility. The result is therefore an evolutionary rather than revolutionary development in international responsibility. Artificial intelligence changes the factual and technical environment in which attribution, breach, causation, and reparation are assessed, but it does not fundamentally displace those concepts. A more integrated model preserves the normative coherence of international responsibility while allowing technical risk-management standards to clarify the practical content of preventive obligations. Future research should nevertheless continue to examine whether this model remains sufficient if AI systems become increasingly autonomous, adaptive, and inherently unpredictable, particularly where even extensive precautions cannot meaningfully reduce the possibility of serious harm. For the present, however, the strongest legal position is that risk-based governance should function as a method for specifying

and evaluating state conduct within the existing law of international responsibility rather than as an independent and competing foundation of liability.

References

Alipanahi, M., Nasiran Najafabadi, D., & Shirani, M. (2024). Civil liability arising from the use of artificial intelligence in the European Union. *Economic Jurisprudence Studies*, *6*(5), 1-18. https://doi.org/10.22034/ejs.2024.427208.1615

Bellout, S. (2024). Establishing risk-based liability for the use of artificial intelligence technologies. *Russian Law Journal*, *12*(2), 2373-2382.

Bertolini, A. (2025). *Artificial intelligence and civil liability: A European perspective*.

Boutin, B. (2023). State responsibility in relation to military applications of artificial intelligence. *Leiden Journal of International Law*, *36*(1), 133-150. https://doi.org/10.1017/S0922156522000607

Dupuy, P. M. (1989). The international law of state responsibility: Revolution or evolution? *Michigan Journal of International Law*, *11*(1), 105-128.

Forensic, E., & Assessment, T. (2021). *The downing of Ukraine International Airlines Flight 752: Factual analysis*.

Hajiesmaeili, M. (2024). Challenges of artificial intelligence civil liability in the Iranian legal system: A look at regulation in the European Union. *State and Law*, *5*(1), 81-98.

Hosseini, S. M., & Habibi Mojandeh, M. (2024). Tracing the concept and position of due diligence in international investment law. *Legal Research*, *27*(106), 97-116. https://doi.org/10.48308/jlr.2024.232359.2540

Hosseini, S. M., & Rahaei, S. (2024). The concept and nature of due diligence in international law. *Contemporary Comparative Law Studies*, *15*(35), 113-140. https://doi.org/10.22034/LAW.2024.57848.3307

Kadkhodaei Elyadrani, A., Khakzad Bojestani, A., & Majidi, A. (2026). The European Union Artificial Intelligence Act: A step towards human oversight of artificial intelligence. *Modern Technologies Law Journal*, *7*(13), 171-190. https://doi.org/10.22133/mtlj.2025.475570.1369

Kadkhodaei Elyadrani, E. (2024). *Determining the international responsibility of states in light of the development of artificial intelligence technologies* [Master's thesis in public international law, Shahid Beheshti University, Faculty of Law].

Kheirandish Sorkhabadi, M., & Ahmadi, S. M. (2024). The role of artificial intelligence in the performance of government regulatory duties: Opportunities and challenges. *Resaleh Adlieh*, *6*(10), 8-12.

Lame, E., Amininia, A., & Afshari, M. (2024). International responsibility of states for the use of artificial intelligence in weapons, emphasizing violations of the laws of war in Gaza. *Foreign Policy*, *38*(4), 205-224. https://fp.ipisjournals.ir/article_723244.html

Makki, A., Makki, Z., & Kashkoulian, E. (2024). Responsibility arising from acts of artificial intelligence in the Iranian legal system. *Jurisprudence, Law and Criminal Sciences*, *8*(32), 71-79. https://www.joce.ir/volume/80

Piri, H. (2025). International responsibility of states in relation to the use of artificial intelligence-based weapons in armed conflicts. *Modern Technologies Law Journal*, *6*(12), 169-193. https://doi.org/10.22133/mtlj.2025.449001.1353

Seyed Morteza Hosseini, R. (2026). Managing changes arising from artificial intelligence through international law: Coordinating innovation and rulemaking. *Modern Technologies Law Journal*, *7*(13), 417-437. https://doi.org/10.22133/mtlj.2025.498763.1416

Talaei, S., & Jafarpour, M. H. (2025). Artificial intelligence and cyberwarfare: Legal dimensions of state responsibility in international law. *New Jurisprudence and Law*, *6*(22), 1-13.

Ziaei Bigdeli, M. R., & Tarazi, N. (2020). Allocation of compensation in situations of shared international responsibility. *International Law Review*(63), 29-50. https://doi.org/10.22066/CILAMAG.2020.113672.1780