Volume 9, No. 2 | March–April 2026

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Volume 9, No. 2 | March–April 2026

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2026 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: David Nayer
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

David Nayer, Publisher, Full Court Press at david.nayer@clio.com or at 202.999.4777

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Legal and Governance Considerations When Using Remote-Sensing Technology and Artificial Intelligence Systems in Critical Infrastructure

Arsen Kourinian*

In this article, the author explores the technical benefits of pairing remote-sensing technology with artificial intelligence (AI)–driven analytics across oil, gas, water, and electric systems; examines the evolving legal and regulatory framework governing high-risk AI in critical infrastructure; and outlines key international space law considerations for remote-sensing activities. The author concludes with key takeaways to help organizations operationalize AI governance, as the technology and regulations evolve in this area.

The convergence of space-based remote sensing and advanced artificial intelligence (AI) is reshaping how critical infrastructure operators safeguard pipelines and transmission networks. With satellites providing persistent, wide-area visibility across vast and often inaccessible corridors, and AI systems transforming raw data into actionable intelligence, operators can detect anomalies earlier, prioritize responses with greater precision, and reduce operational risk at scale.

This article explores the technical benefits of pairing remote-sensing technology with AI-driven analytics across oil, gas, water, and electric systems; examines the evolving legal and regulatory framework governing high-risk AI in critical infrastructure; and outlines key international space law considerations for remote-sensing activities. It concludes with key takeaways to help organizations operationalize AI governance, as the technology and regulations evolve in this area.

Robotics, Artificial Intelligence & Law / March–April 2026, Vol. 9, No. 2, pp. 93–103.

ISSN 2575-5633 (print) / ISSN 2575-5617 (online).

AI and Space-Based Remote Sensing Used for Monitoring Critical Infrastructure

Satellites in space and AI systems on the ground are working together to keep critical infrastructure, such as oil, gas, water, and electric transmission lines, safer and more reliable. Satellites monitor large areas quickly and repeatedly, while AI turns those pictures and signals into clear, timely insights.[1] Pipeline operators can use satellites to:

1. Detect signs of anomalies before they develop into bigger problems, such as corrosions, leaks, or interference;
2. Identify when critical components are deteriorating and need to be maintained or replaced; and
3. Take immediate action to correct issues even if the pipelines are in remote areas.[2]

By integrating AI, operators can inspect pipelines at scale and increase defect detection rates.[3]

In addition, AI and satellite imagery help restore power after natural disasters, such as hurricanes. By using real-time satellite data and AI systems, companies can provide a detailed before-and-after analysis of ravaged areas, so that crews can determine which areas have downed power lines.[4] Satellite and AI technology can also provide early detection for algae blooms, which can clog hydroelectric turbines and interfere with energy generation.[5]

In short, remote-sensing technology from outer space and AI are becoming core parts of critical infrastructure safety. By pairing wide-area visibility from space with AI analysis on the ground, operators can detect risks earlier; focus crews where they are needed most; and keep oil, gas, water, and electric networks running safely and reliably.

AI Regulations Impacting Critical Infrastructure

Legislatures have been passing regulations focused specifically on AI because of the rapid development of AI systems over the past few years and the potential risks such advanced systems present. Some of these AI regulations focus on high-risk areas, which include critical infrastructure and essential government services, such as the EU Artificial Intelligence Act (the EU AI Act), South Korea's the Basic Act on the Development of AI and Establishment of Foundation for Trust (the Basic AI Act), Colorado's Anti-Discrimination in AI Act (Colorado AI Act), and Montana's Creating the Right to Compute Act and Requiring Shutdowns of AI Controlled Critical Infrastructure (Montana AI Act). With remote-sensing technology being increasingly used with AI systems in the context of critical infrastructure and essential government services, such as oil, gas, water, and electricity, operators should consider the potential implications of these new regulations.

EU AI Act

The EU AI Act went into effect on August 1, 2024. Obligations under the law are dependent on whether the AI system's risk is prohibited, high, or minimal. As relevant here, the development and deployment of AI systems in the critical infrastructure context is considered high risk and triggers a majority of the obligations under the law. The compliance obligations for high-risk AI systems enter into force August 2, 2026.

The high-risk obligations related to critical infrastructure apply if the AI system is "intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity."[6] If an AI system is used in this context, the operator would need to assess whether it is a provider of the AI system used for critical infrastructure safety (i.e., the developer of the AI system) or deployer (i.e., the entity using the AI system). Depending on the operator's party-role, it would need to implement the following compliance obligations under the EU AI Act:

Providers	**Deployers**
Risk Management System. Establish, implement, document and maintain a risk management system throughout the AI system's life cycle.	*Input Data*. Ensure that the input data is relevant and sufficiently representative in view of the AI system's intended purpose, to the extent the input data is under the deployer's control.

Providers	**Deployers**
Data Governance and Management Practices. Apply data governance and management practices appropriate for the training, validation, and testing datasets.	*Technical and Organizational Measures*. Take appropriate technical and organizational measures to ensure that the AI system is used in accordance with the instructions for use.
Technical Documentation. Draw up technical documentation containing elements required under Annex IV of the EU AI Act.	*Data Protection Impact Assessment*. Use the instructions for use to carry out data protection impact assessment, where applicable.
Automatic Logging. Ensure that the AI system can automatically record events (logs) over its lifetime.	*Fundamental Rights Impact Assessment*. Carry out fundamental rights impact assessments where public services are involved.
Transparency and Information to Deployers. Provide instructions for use to, and ensure transparency of operation for, deployers.	*Information to Individuals*. Inform workers and workers' representatives that individuals are subject to AI system before using in the workplace. Inform individuals that they are subject to use of a stand-alone AI system where the system makes decisions or assists in making decisions relating to individuals.
Human Oversight. Ensure that the AI system can be effectively overseen by natural persons during its use.	*Human Oversight*. Assign human oversight to natural persons who have necessary competence, training, authority, and support.
Accuracy, Robustness, and Cybersecurity. Ensure an appropriate level of accuracy, robustness and cybersecurity throughout the AI system's life cycle.	*Log Keeping*. Retain automatically generated logs, to the extent they are under the deployer's control.

Providers	**Deployers**
Quality Management System. Put in place a specified quality management system for EU AI Act compliance.	*EU Database Registration*. Register the deployer and use of the AI system in the EU database, if the deployer is a public authority or an EU institution, body, office, or agency.
EU Harmonization Legislation and Accessibility Legislation. Comply with the requirements of the EU harmonization legislation and accessibility requirements legislation applicable to the AI system.	*Cooperation with Competent Authorities*. Cooperate in any action taken by authorities relating to the AI system to implement the EU AI Act.
Document Keeping. Retain relevant documentation at the disposal of competent authorities for a 10-year period.	*Monitoring*. Monitor operation of the AI system to ensure that it is following the instructions for use and inform providers where relevant.
Log Keeping. Retain automatically generated logs, to the extent they are under the provider's control.	*Duty to Inform and Suspend Use*. Where the deployer has reason to consider that the AI system presents risk to health or safety or fundamental rights, inform the provider or distributor and relevant market surveillance authority, and suspend use of the AI system.
Conformity Assessment Procedure. Carry out a conformity assessment procedure before placing the AI system on the market or putting it into service.	*Incident Reporting*. Report serious incidents first to the provider, then the importer or distributor and relevant market surveillance authorities of the incident.
EU Declaration of Conformity. Draw up and retain at the disposal of competent authorities for a 10-year period.	
CE Marking, Name, and Contact Address. Affix to the AI system, or where not possible, on its packaging or accompanying documentation.	

Providers	**Deployers**
EU Database Registration. Register the provider and AI system in the EU database before placing on the market or putting into service.	
Authorized Representative. If the provider is established in a non-EU country, appoint an EU-authorized representative before making the AI system available on the market.	
Cooperation with Competent Authorities. Upon request, provide to the competent authority all information and documentation necessary to demonstrate compliance, and automatically generated logs.	
Post-Market Monitoring System. Establish and document a post-market monitoring system in a manner proportionate to the nature of the technologies and AI system risks.	
Corrective Actions and Duty to Inform. Where the AI system on the market does not comply with the EU AI Act, take corrective actions to bring the AI system into conformity and inform relevant parties. Where the AI system on the market presents risk to health and safety or fundamental rights, inform market surveillance authorities.	
Incident Reporting. Report serious incidents to the market surveillance authorities of the EU member state where the incident occurred.	

South Korea

Similar to the EU AI Act, South Korea has also passed a comprehensive AI law, the Basic AI Act, effective January 22, 2026. Like the EU AI Act, certain AI use cases are considered high risk—referred to under the law as "high-impact AI"—if it has "the potential to significantly impact human life, safety, or fundamental rights, used in" the supply of energy and other areas that have a significant impact on the protection of human life, physical safety, and basic human rights.[7] AI business operators must comply with the following obligations when using high-impact AI:

- Notify users in advance that the product or service is AI-based;
- Implement a risk management plan;
- Provide an explanation for AI-generated outputs, including the key criteria used to derive such outputs, and an overview of the learning data used in the development and utilization of AI;
- Adopt user protection measures;
- Provide human management and supervision of the AI;
- Prepare and store documents that demonstrate measures taken to ensure AI safety and reliability;
- Conduct an AI impact assessment; and
- Appoint a domestic representative if the AI business operator does not have an address or place of business in South Korea.[8]

Colorado AI Act

The Colorado AI Act is the most comprehensive AI law in the United States, effective February 1, 2026. Like the EU AI Act, the Colorado AI Act's obligations primarily apply to high-risk AI systems and depending on whether the business is developing or deploying an AI system. Under the law, high-risk AI is a system "that, when deployed, makes, or is a substantial factor in making, a consequential decision."[9] Consequential decision means a decision that has a material legal or similarly significant effect on the provision or denial to any Colorado resident of, or the cost or terms of, among other categories, an essential government services.[10] Essential government service is not defined under the law, but if further guidance reveals critical infrastructure to be in scope, it could potentially include essential services, such as oil, gas, water, and electricity.

Under the law, developers of high-risk AI systems are obligated to:

- Provide information and documentation to deployers regarding the AI system, such as the uses and purpose, benefits, harms, limitations, summary of the training data, risk of discrimination, the evaluation steps taken, mitigation measures adopted, intended output, and how the AI system will be monitored;
- Provide a statement on their website about the types of AI systems available and how risks are managed; and
- Report within 90 days to the Colorado Attorney General and deployer if they discover that the AI system caused or is reasonably likely to cause algorithmic discrimination or receive a credible report from the deployer that algorithmic discrimination was caused.[11]

Deployers of high-risk AI systems, on the other hand, are obligated to:

- Annually prepare an AI impact assessment;
- Adopt a risk management policy (e.g., NIST AI RMF and ISO/IEC 42001);
- Annually review the AI system for algorithmic discrimination;
- Provide a notice to Colorado residents regarding the deployment, including that a high-risk AI system was deployed for a consequential decision, purpose and nature of the decision and a description of the AI system, instructions on how to access the website statement, a right to opt out and contact information;
- Provide information about any adverse decisions and how to correct any incorrect personal data used and appeal the decision;
- Provide a statement on their website about the type of AI systems deployed, how risks are managed, and nature, source, and extent of information collected and used; and

- Disclose to the Colorado Attorney General's office within 90 days if the AI system caused algorithmic discrimination.[12]

Montana AI in Critical Infrastructure Law

Montana has passed a narrow AI law that applies to deployers of critical infrastructure facilities that are controlled in whole or in part by a critical AI system.[13] Critical infrastructure facilities include petroleum, electricity, water, gas, and oil.[14] Under the law, deployers of critical infrastructure facilities are required to develop a risk management policy for the critical AI system that is reasonable and considers guidance and standards in the latest version of NIST AI RMF, ISO/IEC 4200, or another nationally or internationally recognized risk management framework for AI systems.[15]

International Space Law Considerations for Using Remote-Sensing Technology and AI for Critical Infrastructure

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, commonly known as the Outer Space Treaty of 1967 (OST) is the central legal document governing international activity in outer space.[16] The OST has been adopted by the United Nations and signed by over 100 countries, including the United States, United Kingdom, Russia, and China. It establishes the principles for using outer space in a peaceful manner. The OST does not specifically address remote-sensing technology or the use of AI systems to analyze data collected from outer space. However, OST permits the free use of outer space "without discrimination of any kind" and "access to all areas of celestial bodies."[17] The main restriction under OST is a prohibition against placing "in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction,"[18] which remote-sensing technology and AI systems for monitoring critical infrastructure would not trigger.

Along with OST, the United Nations has also adopted the Principles Relating to Remote Sensing of the Earth from Outer Space (the UN Principles).[19] A key aspect of the UN Principles is the balance between the interests of sensing states (those operating remote-sensing systems) and sensed states (those whose territory is being observed). Under the UN Principles, if a sensing state processes or analyzes information collected through remote-sensing technology, which is now being done using AI systems, it must make available this information to sensed states.[20] Further, sensing states are required to provide processed and analyzed data to sensed states as promptly as possible if they may be affected by natural disasters.[21]

Takeaways

Critical infrastructure operators should consider implementing an AI governance program if they plan on using remote-sensing technology and AI systems to monitor critical infrastructure. A harmonized AI governance program may include:

1. Forming an AI oversight team;
2. Implementing appropriate data governance;
3. Managing risks by adopting a risk management policy based on NIST AI RMF or ISO/IEC 42001 and conducting AI impact assessments;
4. Addressing legal compliance obligations arising under the AI-specific laws described above and general laws applicable to the critical infrastructure industry;
5. Applying mitigation measures to reduce risks; and
6. Demonstrating accountability through appropriate policies and procedures.[22]

By implementing a structured program, operators can help future-proof their governance structure as technology and regulations rapidly develop and make the public safer.

Notes

[*] The author, a partner in the Los Angeles office of Mayer Brown, may be contacted at akourinian@mayerbrown.com.

[1] See GIM International, "The Source of Power: How Satellite Imagery Propels the Energy Sector into the Future," https://www.gim-international

.com/case-study/the-source-of-power-how-satellite-imagery-propels-the-energy-sector-into-the-future?output=pdf.

[2] See Ground Control, "How Satellite IoT Keeps Pipeline Infrastructure Safe in Remote Environments," https://www.groundcontrol.com/blog/how-satellite-iot-keeps-pipeline-infrastructure-safe/.

[3] See Numalis, "AI for Smarter Pipeline Management in Oil and Gas Industry," https://numalis.com/ai-pipeline-management-in-oil-and-gas-industry/.

[4] See International Water Power, "Using AI and Satellite Data to Transform Disaster Response and Sustainability," https://www.waterpowermagazine.com/analysis/using-ai-and-satellite-data-to-transform-disaster-response-and-sustainability/?cf-view.

[5] See id.

[6] EU AI Act, Annex III.2.

[7] See Basic AI Act, Article 2(4)(a) & (k).

[8] Id. at Articles 31 & 34-36.

[9] Colo. Rev. Stat. Ann. § 6-1-1701(9).

[10] See id. § 6-1-1701(3).

[11] Id. at § 6-1-1702.

[12] Id. at § 6-1-1703.

[13] See Montana SB212, Section 4.

[14] See Mont. Code Ann. § 82-1-601.

[15] See Montana SB212, Section 4.

[16] See United Nations, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies" (Jan. 27, 1967), https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

[17] Id. at Article I.

[18] Id. at Article IV.

[19] See United Nations, "Principles Relating to Remote Sensing of the Earth from Outer Space" (Dec. 3, 1986), https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html#:~:text=Remote%20sensing%20activities%20shall%20be,needs%20of%20the%20developing%20countries.

[20] See id. at Principle XII.

[21] See id. at Principle XI.

[22] See A. Kourinian, "Implementing a Global Artificial Intelligence Governance Program," Bloomberg Law.