



Environmental Crime Prevention: Core legal foundations and AI regulation

Final PERIVALLON Meeting| 27-11-2025

Eva Korenjak Lalovic, Research Associate, Department of
Innovation and Digitalisation in Law, University of Vienna

Public



Co-funded by the
European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

73952.

Agenda

1. Introduction & Context

- the role of legal frameworks for environmental crime prevention technologies

2. Core Legal Foundations

- Human rights and privacy
- Data protection
- Intellectual property

3. AI Regulation

- AI Act

4. Q&A

1. Introduction & Context

The role of legal frameworks
for environmental crime
prevention technologies



1. Introduction & Context

- Environmental crime is increasingly sophisticated, cross-border, and data-intensive
- New technologies (AI, UAVs, satellite analytics) can dramatically enhance detection and prevention
- Legal frameworks determine what data may be used, how AI may operate, and what safeguards are required
- Compliance ensures the lawful admissibility of evidence and protects fundamental rights



2. Core Legal Foundations of PERIVALLON

- Human rights
- Data protection
- Intellectual property

2. Core Legal Foundations

1. Human Rights & Privacy

- Monitoring and surveillance → high risk of infringement
- Respect for private and family life (home, communications) → European Convention Human Rights
- Not absolute → allowing for interference, however → lawful, necessary for national security, public safety, prevention of disorder or crime etc.
- Aerial and online detection tools (legal basis, authorization, personal data)



2. Core Legal Foundations

2. Data Protection

- Derived from respect for private and family life
- Key instruments:
 - General Data Protection Regulation (GDPR) & Law Enforcement Directive (LED) → law enforcement authorities & purpose of prevention, investigation, detection etc.
- Key concepts:
 - personal (any information relating to an identified or identifiable natural person) / special categories → stricter requirements
 - Data controller (purposes & means), joint controllership, data processor (on behalf)
 - Data subject rights (information, access, objection etc.)
- Key principles:
 - Legal basis for processing (consent, necessary for the performance of a contract, public interest etc.), data minimization, purpose limitation, accuracy etc.

2. Core Legal Foundations

3. Intellectual Property

- Technologies make use of copyrighted material
 - scientific research exemption (DSM Directive)
 - web scraping generally permitted for AI training if rightholders not explicitly opted out → authorization needed
- generated material protected by copyright and related rights
 - Software, database protection
 - AI algorithms in the EU don't enjoy copyright protection (absence of the own intellectual creation)
 - needs to be properly managed (eg IPR repository)



3. AI Regulation

- AI Act

4. AI Act

- first-ever comprehensive legal framework on AI worldwide
- entry into force on August 1st 2024 , fully applicable August 1st 2026, some exceptions (high-risk from 2027)
- **nature:** binding legislative act – regulation („product safety regulation”)
- **goal:** trustworthy AI in the EU → safety, fundamental rights and human-centric AI
- **subject matter:** development & use of AI systems
- **scope:** risk-based prohibitions, requirements, obligations for providers (develops / places on the market / puts into service) and deployers

4. AI Act

Material scope of AI Act

1. It applies to.....'AI system(s)'

- a machine-based system
- varying levels of autonomy
- may exhibit adaptiveness after deployment (capacity for self-learning)
- from received input infers how to generate outputs such as predictions, recommendations, or decisions that
- influence physical or virtual environments

2. It does NOT apply to....

- sole purpose of scientific research and development, prior to their being placed on the market or put into service → however, real-world testing conditions
- purely personal non-professional activity
- free and open-source licences, unless placed on the market or put into service as high-risk AI systems

4. AI Act

Example of PERIVALLON platform → AI System

1. Machine-based

- Computational, machine-based system integrating multiple software components and data processing modules
- Relies on automated data acquisition, processing, analysis tools built on algorithmic methods

2. Autonomy

- Certain modules, eg online acquisition or risk analysis tools can perform automated processing without continuous human input

3. Generating output that influences environment

- Inferring correlations or patterns from data to produce outputs (detection of environmental crime indicators)
- Influence the environment (data-driven decision support)

AI Act

1. Unacceptable risk: clear threat to the safety, livelihoods and rights → prohibited

→ harmful AI-based manipulation and deception, emotion recognition in workplaces and education institutions, profiling, untargeted web scraping for facial recognition databases etc.

2. High-risk: can pose serious risks to health, safety or fundamental rights → strict obligations

→ Used as safety component of a product / falling under EU health and safety legislation (e.g. AI application in robot-assisted surgery)

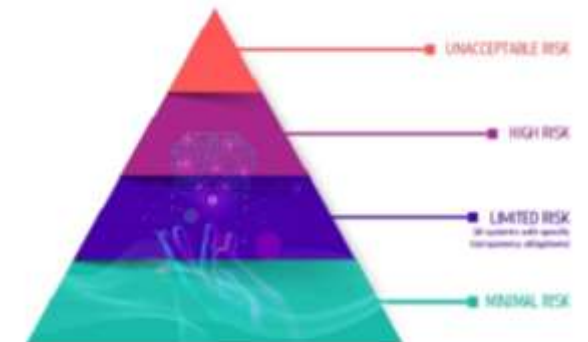
→ Deployed in 8 specific areas of Annex III (inc. law enforcement)

3. Limited-risk: transparency obligations

→ Chatbots, deep fakes

4. Minimal risk: majority of AI systems → no obligations

→ AI-enabled video games or spam filters



Source: European Commission, AI Act, A risk-based approach. URL: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

4. AI Act

- **High-risk systems in Law enforcement area:**

- to make individual risk assessments of natural persons for the purpose of assessing the risk of offending or reoffending or the risk to potential victims of criminal offenses
- as polygraphs and similar tools, or to detect the emotional state of a natural person
- to detect deep fakes
- to **predict** the occurrence or reoccurrence of an actual or potential **criminal offense based on profiling of natural persons**, or to assess personality traits, characteristics, or past criminal behaviour of natural persons or groups
- for profiling of natural persons in the context of detecting, investigating, or prosecuting criminal offenses

PERIVALLON → law enforcement, however, no individual risk assessments or profiling → focus on environmental crime indicators

AI Act – obligations for high-risk

- adequate risk assessment and mitigation systems (surveillance and privacy → anonymization, data minimisation)
 - high-quality, accurate, non-biased datasets to train the system
 - appropriate human oversight measures (accountability)
 - detailed documentation for authorities to assess its compliance (explainability)
 - clear and adequate information to the deployer
- provide trainings, documentation, information on the platform/website (transparency)

4. AI Act

Example of PERIVALLON → Proactive implementation of compliance measures, such as

- Data governance and management framework to ensure training, testing and validation data meets quality, representativeness, relevant standards
- Automatic recording of events to support traceability, accountability, auditing
- Human oversight → platform as a decision support system
- Secure data management, role-based access, encryption

Conclusion

- Legal compliance (human rights, data protection, IP) is foundational for deploying technologies in environmental crime prevention → enable not hinder innovation
- The AI Act introduces binding obligations, especially relevant for systems supporting law enforcement
- Proactive compliance with legal requirements increases
 - operational reliability and
 - strengthens admissibility of digital evidence, as well as
 - builds trust with end-users and public

PERIVALLON 

Thank you!



Logo

Eva Korenjak Lalovic |
eva.korenjak.lalovic@univie.ac.at



Co-funded by the
European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

952.