LESSON 04

AI & the Law

Legal Frameworks, Copyright, and Liability in Library Contexts

90 min | All library professionals

The Legal Landscape

AI adoption in libraries raises urgent legal questions across four interconnected areas:

© Copyright

Who owns AI outputs? What are the risks of training data and AI-assisted content creation?

Data Protection

How does GDPR apply when AI processes patron data, queries, or user profiles?

EU AI Act

The world's first AI law: risk classification, deployer obligations, and enforcement.

Liability

What happens when AI produces errors? Who is responsible, the library or the vendor?

Copyright & AI

TRAINING DATA

AI models are trained on vast datasets that often include copyrighted material. Three key legal questions for libraries:

1. Do AI developers need permission to use copyrighted content for training?
2. Does training on copyrighted material constitute infringement under copyright law?
3. How do the EU, US, and UK differ on text and data mining (TDM) exceptions?

EU Copyright Directive (2019/790)

Introduced a text & data mining exception for research organisations and cultural heritage institutions. Libraries may qualify but whether it extends to commercial AI training remains contested.

Copyright & AI

WHO OWNS AI-GENERATED OUTPUTS?

Most Jurisdictions

Copyright requires human authorship. AI-generated content with no meaningful human creative input may not be copyright-protected.

Vendor Terms Vary

Terms of service differ widely outputs may belong to the user, the vendor, or fall into the public domain entirely.

Practical Implication for Libraries

Review vendor contracts carefully to understand ownership of AI-generated content especially where content will be published or shared externally (e.g., cataloguing records, finding aids, patron-facing text).

Data Protection & GDPR

Where AI systems process personal data including patron queries, borrowing records, or research profiles GDPR applies.

Lawful Basis

Libraries must identify a valid legal basis for processing personal data with AI: legitimate interests, consent, or public task.

Data Minimisation

AI tools should not collect or process more personal data than is necessary for the stated purpose.

Automated Decisions

Article 22 GDPR restricts solely automated decisions with significant effects including AI-based profiling and access systems.

DPIAs Required

Data Protection Impact Assessments are required when processing is likely to result in high-risk AI tools that profile users almost certainly qualify.

🔑 Library = data controller. AI vendor = data processor. A GDPR-compliant Data Processing Agreement (DPA) is mandatory.

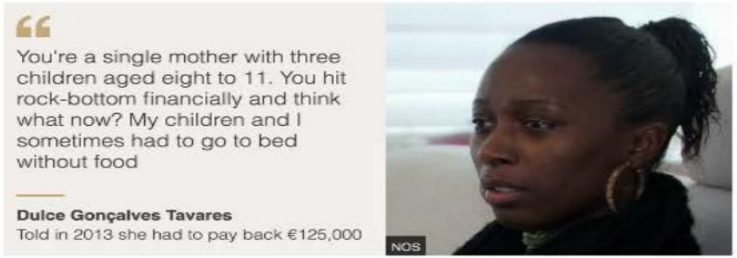
WHY THE AI ACT

The EU AI Act

BBC NEWS

Dutch Rutte government resigns over child welfare fraud scandal

Dutch PM Mark Rutte said in January 2021 the decision to resign was "unavoidable"



Last month, Prime Minister of the Netherlands Mark Rutte—along with his entire cabinet—resigned after a year and a half of investigations revealed that since 2013, 26,000 innocent families were wrongly accused of social benefits fraud partially due to a discriminatory algorithm.

The EU AI Act

Netherlands Court of Audit

Audit of 9 government algorithms finds 6 do not meet basic requirements

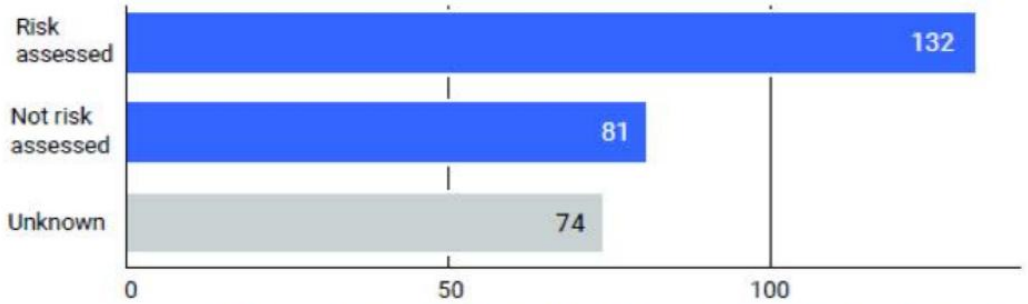
News item | 18-05-2022 | 10:45

Responsible use of algorithms by government agencies is possible but not always the case in practice. The Netherlands Court of Audit found that 3 out of 9 algorithms it audited met all the basic requirements, the other 6 did not and exposed the government to various risks: from inadequate control over the algorithm's performance and impact to bias, data leaks and unauthorised access.

The EU AI Act

Figure 14 *Risk assessment of AI systems*

Not all AI systems underwent a risk assessment



This figure presents information on only the 287 AI systems currently under development or in use.

The EU AI Act

The world's first comprehensive legal framework for artificial intelligence risk-based, binding, and in force.

UNACCEPTABLE RISK — Prohibited practices. Banned entirely.

HIGH RISK — Strict requirements, human oversight, impact assessments required.

LIMITED RISK — Transparency obligations: disclose AI use to users.

MINIMAL RISK — No specific obligations; voluntary codes encouraged.

The EU AI Act

Unacceptable risk

- Subliminal, deceptive or manipulative techniques
- Exploitation of personal vulnerabilities
- Biometric categorization systems inferring sensitive attributes
- Social scoring
- Assessing the risk of an individual committing criminal offenses
- Compiling facial recognition databases
- Inferring emotions in workplaces or educational institutions
- ‘Real-time’ remote biometric identification (RBI) in publicly accessible spaces for law enforcement

The EU AI Act

High risk

- Non-banned biometrics
- Critical infrastructure
- Education and vocational training
- Employment, workers management and access to self-employment
- Access to and enjoyment of essential public and private services
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

The EU AI Act

High risk

Providers must fulfill some requirements:

- Risk management system
- Data governance
- Technical documentation
- Record-keeping
- Instruction manual
- Allow for human oversight

The EU AI Act

Limited risk

- Mandatory transparency
- Examples: deepfakes

Minimal risk

- Unregulated
- Examples: spam filters, AI videogames

The EU AI Act – Library Use Cases

Where do library AI tools fall in the risk classification?

AI Tool / Use Case	Risk Level	Key Obligation
Social scoring / surveillance of patrons	Unacceptable	Prohibited never deploy
Patron profiling / behaviour prediction	High Risk	Human oversight + incident logging mandatory
AI chatbot for reference queries	Limited Risk	Must disclose users are interacting with AI
AI-generated content creation tools	Limited Risk	Clearly label outputs as AI-generated
AI-assisted cataloguing (staff-only tool)	Minimal Risk	No specific obligations, follow best practice

The EU AI Act – Obligations for Libraries as Deployers

Libraries that use AI tools even as end users are 'deployers' under the AI Act and carry legal obligations.

HIGH-RISK SYSTEMS

→ Conduct fundamental rights impact assessment before deployment

→ Maintain logs and ensure human oversight at all times

→ Inform individuals when subject to AI-assisted decisions

GENERAL-PURPOSE AI TOOLS (e.g. LLMs like ChatGPT, Claude, Gemini)

→ Use only within the intended purpose defined by the provider

→ Do not deploy in ways that create risks not covered in documentation

→ Request GPAI compliance documentation from vendors before signing

AI-GENERATED CONTENT AND CHATBOTS

→ Disclose to users that they are interacting with an AI system

→ Label all AI-generated outputs clearly and consistently

→ Do not use deepfakes or synthetic media without clear disclosure

Liability – When AI Gets It Wrong

AI systems can produce inaccurate, biased, or harmful outputs. In library contexts, this may include:

⚠️ Incorrect Records

Incorrect bibliographic records or citations generated by AI cataloguing tools.

🚫 Biased Outputs

Biased or discriminatory outputs in AI-powered recommendation or access systems.

🔒 Privacy Violations

Privacy violations from AI-generated content that references real individuals.

❌ Misinformation

Misinformation presented via AI-powered reference or query-answering tools.

Vendor contracts are your frontline protection. Ensure they cover: indemnification, liability caps, accuracy warranties, incident notification, and data portability on exit.

The Librarian's Legal Lens

The skills you already use for evaluating sources apply directly to AI law.

Legal Area	Key Question to Ask
Copyright	Who owns outputs from this tool, and was it trained on copyrighted material?
Data Protection	Does this tool process personal data? Is a DPIA and Data Processing Agreement required?
EU AI Act	What risk tier does this system fall into? What are our obligations as deployers?
Liability	If this AI produces an error or causes harm who bears legal responsibility?
Vendor Contract	Does the contract cover indemnification, incident notification, and data exit rights?

AI Key Vocabulary

EU AI Act

Regulation (EU) 2024/1689 — the world's first comprehensive AI law, taking a risk-based approach to regulating AI systems and their deployers.

Deployer

An organisation (like a library) that uses an AI system in its operations, distinct from the provider or developer of that system.

GPAI Model

General-Purpose AI Model — e.g. an LLM like GPT or Claude, used as the foundation of a product. Subject to specific transparency obligations.

DPIA

Data Protection Impact Assessment — a GDPR-required process before deploying AI likely to result in high risk to individuals' rights.

Text & Data Mining

A copyright exception allowing automated analysis of content — with different conditions across EU, US, and UK jurisdictions.

Indemnification

A contractual clause in which one party agrees to cover the legal liability or financial losses suffered by another party.

Activity – Compliance Challenge

- Case study 1: A library uses an AI chatbot to recommend books. It accidentally stores patrons' chat histories with personal preferences.
- Case study 2: A facial recognition system is proposed for security. Does the AI Act allow this? What safeguards are needed?
- Case study 3: A student generates an essay with ChatGPT. The library is asked to share the student's search history with the school.

In your group analyze your case involving AI, data privacy, and legal compliance to determine the best course of action under GDPR/AI Act rules.

Discussion

Q1 Does your institution have an AI procurement policy? Who reviews vendor contracts for legal compliance?

Q2 Have you used AI tools to generate content (records, summaries, descriptions)? Who owns that content?

Q3 How would you explain the EU AI Act risk classification to a colleague who has never heard of it?

Q4 What legal question about AI in your library feels most urgent right now?