Faculty of Law, Economics and Finance

CRIM_AI
-
Country Roundtable – The Netherlands

2-3 October 2023

Tour de Table - Introducing the Project Team

FACULTY OF LAW, ECONOMICS AND FINANCE

UNIVERSITÉ DU LUXEMBOURG

Interdisciplinary Group of Experts

- Sabine Gless
- John Vervaele
- Paul De Hert
- Christoph Sorge
- Cornelia Kutterer
- Martin Sacleux
- *(Andre Klip)*
- *(Iain Walden)*

Country Rapporteurs

- DE: Dominik Browoski
- NL: Rick Robroek &
  (Pieter Liefrink)
- UK: Valsamis Mitsilegas &
  Clementine Salvi &
  Rudi Fortson
- US: Brandon Garett
- LU: Theo Antunes
- FR: Juliette Lelieur

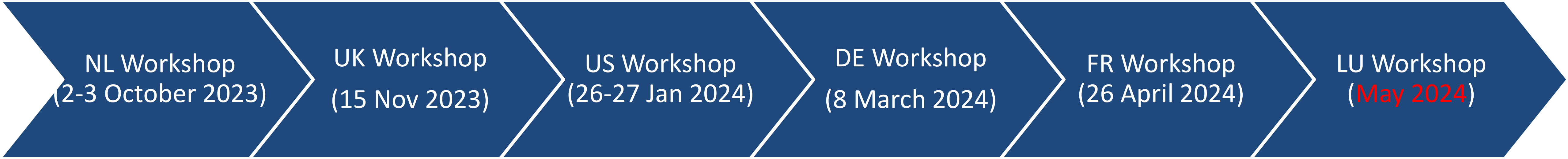
Luxembourg Team

- Katalin Ligeti (PI)
- Charlotte Quaisser (RA UL)
- *(Pia Levicnik (PhD))*

Other Participants

- Juraj Seifert (VUB/UL)
- Lea Bachmann (PhD Uni Basel)
- *Kelly Blount (PhD UL)*
- *Georgia Theodorakakou (PhD UL)*

CRIM_AI Project Timeline



NL Workshop (2-3 October 2023)

UK Workshop (15 Nov 2023)

US Workshop (26-27 Jan 2024)

DE Workshop (8 March 2024)

FR Workshop (26 April 2024)

LU Workshop (May 2024)

- AIDP Congress 25-28 June 2024
- Date of Final Conference & Book Launch 7-8 November 2024

Program and Objectives of the Country Roundtable

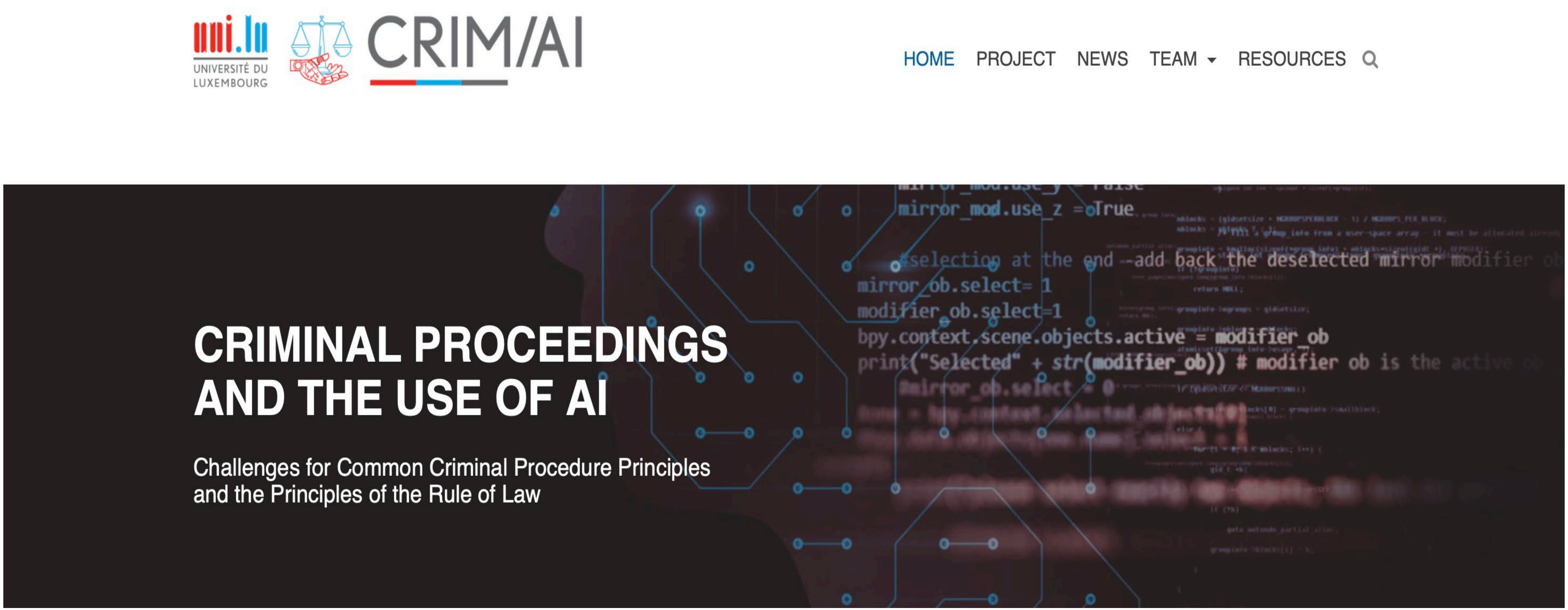
1. Brief Summery of the project objectives and methodology

2. Presentations on the Dutch Legal Framework and Practice

Introduction to the CRIM_AI Project

https://aiandcriminaljustice.uni.lu

FACULTY OF LAW, ECONOMICS AND FINANCE



CRIMINAL PROCEEDINGS AND THE USE OF AI

Challenges for Common Criminal Procedure Principles and the Principles of the Rule of Law

- Focus of CRIM_AI is **AI Evidence**, i.e. AI directed towards providing evidence against criminal defendants
  - no attention to AI informed predictive policing (helps to prioritize deployment of police, but it is not introduced in court as evidence of guilt)
  - no attention to AI informed judicial decision on regarding pretrial detention, sentencing, corrections, and re-entry (AI is used for risk assessment).

- Types of AI Evidence studied by the project are

Forensic AI Evidence

- filtering AI (e.g. Threat to Life; Hansken);
- data mining AI;
- FRT (e.g. CATCH)
- ANPR
- probabilistic genotyping AI e.g. TrueAllelle , STRMix)

Consumer Product AI.

- Google Earth
- Find My iPhone
- Alexa
- Etc.

1. Main points of the national policy discussion

2. Legal definition and legal framework for AI Evidence

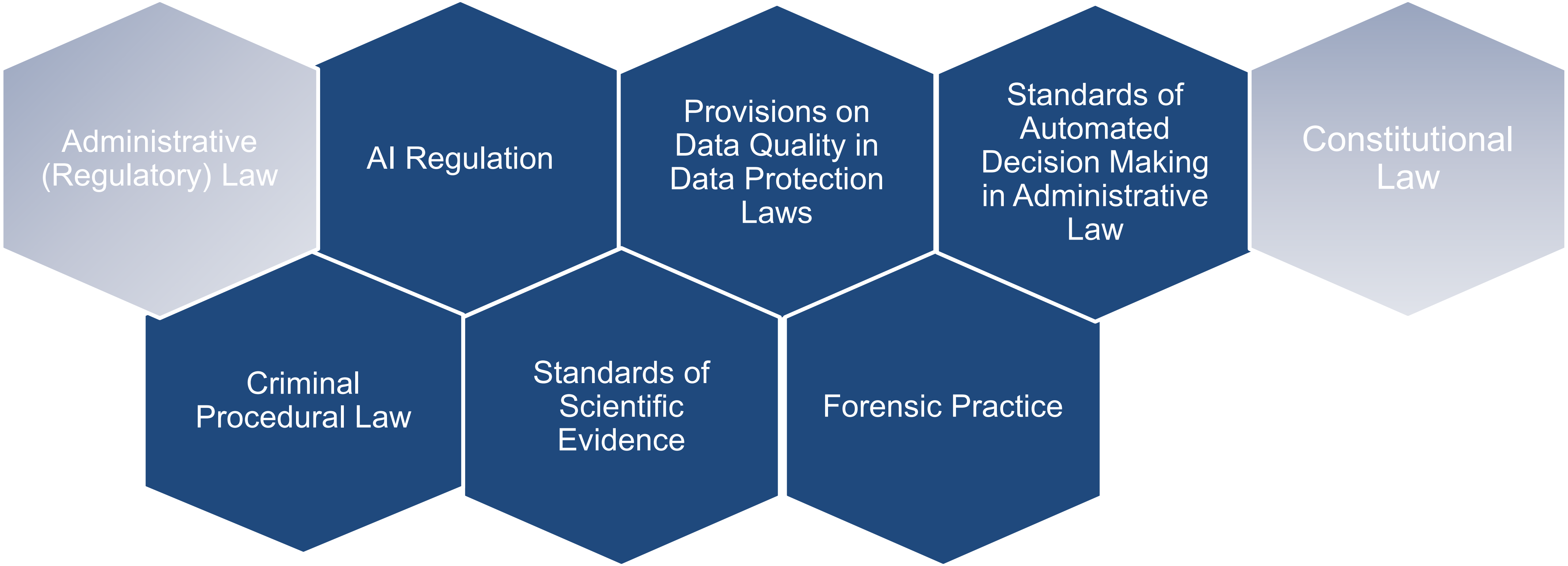
    - Existing categories of evidence and AI Evidence
    - Rules of scientific evidence and criminal forensics
    - Admissibility of AI Evidence
    - Right of the defence and AI Evidence
    - Requirements of AI Developers

Legal Framework for the Design and Deployment of AI in Criminal Proceedings

- Convergence towards global standards (EU – CoE – OECD)?
  - soft law or hard law?
  - EU internal market (risk-based) approach
  - regulation for public sector only, or also for private sector?
  - curbing innovation, maintaining efficiency?
  - exceptions for national defence? national security? law enforcement?
  - prohibited technologies (FRT?, predicitive policing?, ethnic profiling?)

- From general regulatory framework to criminal justice
  - human oversight
  - trustworthiness (linked to the debate on transparency *v* accountability and the need for AI registers)
  - discrimination bias and profiling (see decision of the *Gerechtshof Den Haag* of 14 February 2023 on enthic profiling).

Legal Frameworks Applicable to AI Evidence



Administrative (Regulatory) Law

AI Regulation

Provisions on Data Quality in Data Protection Laws

Standards of Automated Decision Making in Administrative Law

Constitutional Law

Criminal Procedural Law

Standards of Scientific Evidence

Forensic Practice

No specific legal framework for AI Evidence, but a patchwork of frameworks that reveal **tensions** between different bodies of law (see e.g. the proposed reform of the NL Code of Criminal Procedure)

Applying exisiting categories of evidence to AI Evidence

- AI Evidence is not considered as a special form of evidence (neither is computer evidence).
- AI Evidence can be introduced via
  - witness testimony;
  - expert testimony;
  - documentary evidence
  - inspection report (?)
  - measurement of raw data (?).
- Divergent national rules on admissibility and exlcusion of evidence.

Admissibility of AI Evidence

- Evidentiary AI must be reliable, valid and credible to be be admitted in trial.
- General tendecy to admit Evidentiary AI without too-detailed scrutiny as to validity, reliability, or credibility (assumptions in national practice that computers – and hence AI –, is reliable).
- Litigation in the reporting countries tends to apply the rules of scientific evidence to Evidentiary AI.
- Are exisiting rules sufficient for the judge to assess the admissibility of evidence?
    - How do violations of privacy and data protection affect the lawfulness of the evidence?
    - How to test the authenticity and integrity to AI Evidence especially in case of black box AI?

Defence rights and AI Evidence

- No duty to inform in advance the defence of the use of AI Evidence.
- Whether the court orders the disclosure of the AI Evidence’s specifications, source code, and training data relevant to the reliability and admissibility of the AI Evidence very much depends on the case.
- How can the defence scrutinise and critically assess (incriminating) AI Evidence (black box AI) ?
- Defence might not have the financial means to challenge it.
- Do we need new defence rights such as access to the dataset or access to the AI tool?

- When assessing the fairness of the proceedings as a whole, ECtHR reviews the domestic courts’ evaluation of evidence to determine whether the domestic courts’ assessment of the weight of the evidence could be considered unacceptable or arbitrary.
- National judges will have to
  - take into account the unforeseeability of ML and clarify how they reached their verdict based on what
  - be sensitive to automation bias and its abuse by the prosecution, criminal investigators may tend to place greater weight on automated assessments over other sources of advice or evidence, even though AI-powered tools replicate (and may even exacerbate) pre-existing human biases.

AI Developers

- We see both public and private development of Evidentiary AI
  - so far states shy away from imposing obligations on AI Developers;
  - few voluntary initiatives of private sector to disclose how their AI works.

- Areas of tension
  - claims of proprietary or trade secrets protection by AI Developers;
  - right to information and the needs and efficiency of law enforcement.

- Approaches to address the tensions
  - National approaches
    - IT if automated decision affects individuals all information has to be given to the court)
    - NL Algorithm Register
    - US Justice in Forensic Algorithms Act
  - EU approach
    - Draft EU AI Act stipulates transparency obligations (need to be detailed at national level for AI Evidence).
    - Data protection law
      - Article 15(1)(h) GDPR right to “meaningful information about the logic involved as well as the significance and envisaged consequences of automated processing operations for the data subject”
      - Recital 63 GDPR “that right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property”
      - Opinion of Advocate General Pikamäe in SCHUFA Holding (C-634/21).

Conclusion

Thank you very much for your attention!