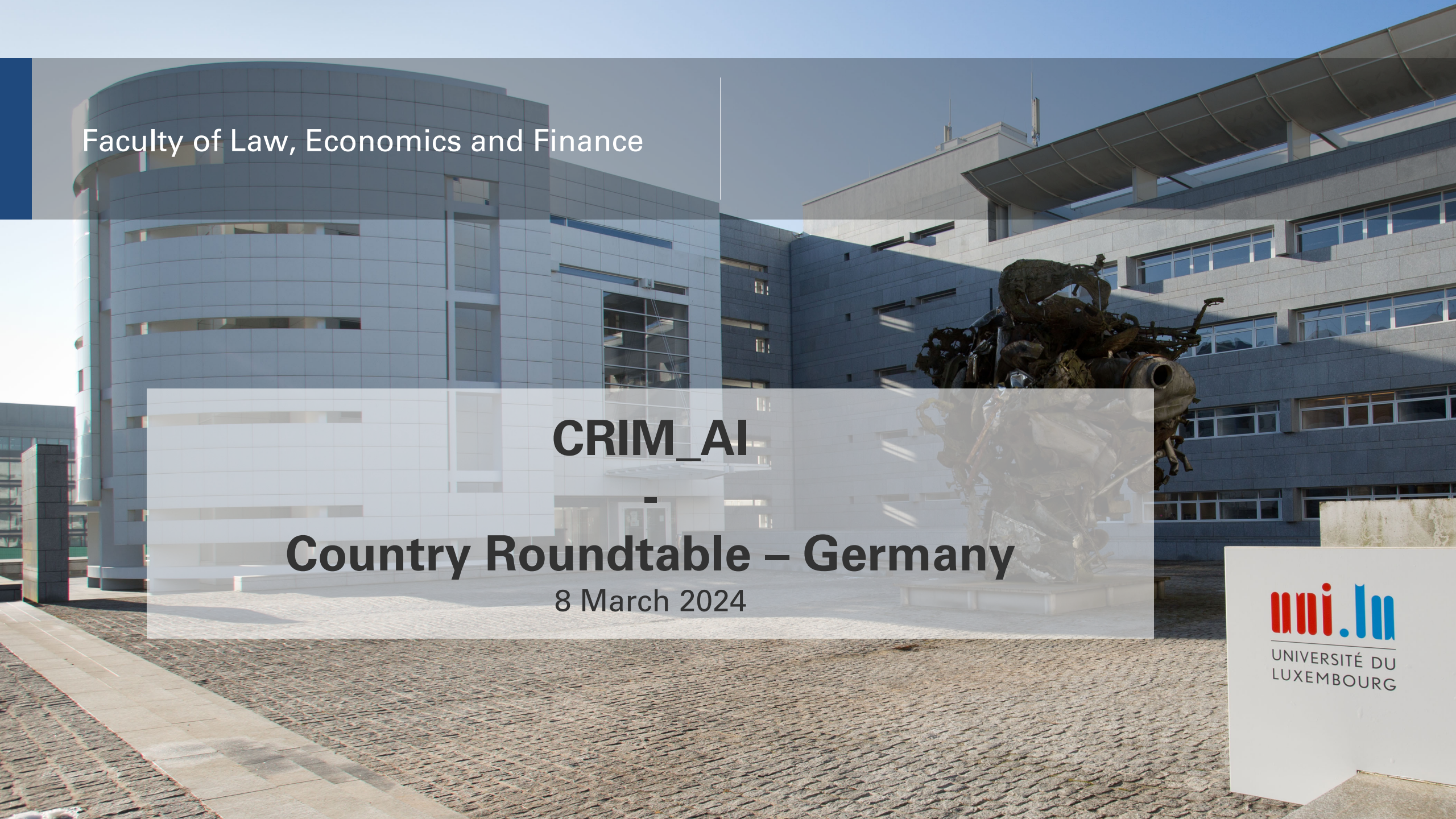

Faculty of Law, Economics and Finance
CRIM_AI
-
Country Roundtable – Germany
8 March 2024
UNIVERSITÉ DU
LUXEMBOURG

- CRIM_AI seek to address whether:

  ‘existing rules on criminal procedure, in particular evidence law and procedural guarantees, are sufficient to address the specific nature and the associated pitfalls of AI evidence?’

- CRIM_AI Methodology:
  - comparative legal research (FR, DE, UK, NL, LU, US)
  - country Roundtables

- CRIM_AI Objectives: engage with national and regional policy initiatives

CRIM_AI Project Timeline

- Date of Final Conference & Book Launch 7-8 November 2024

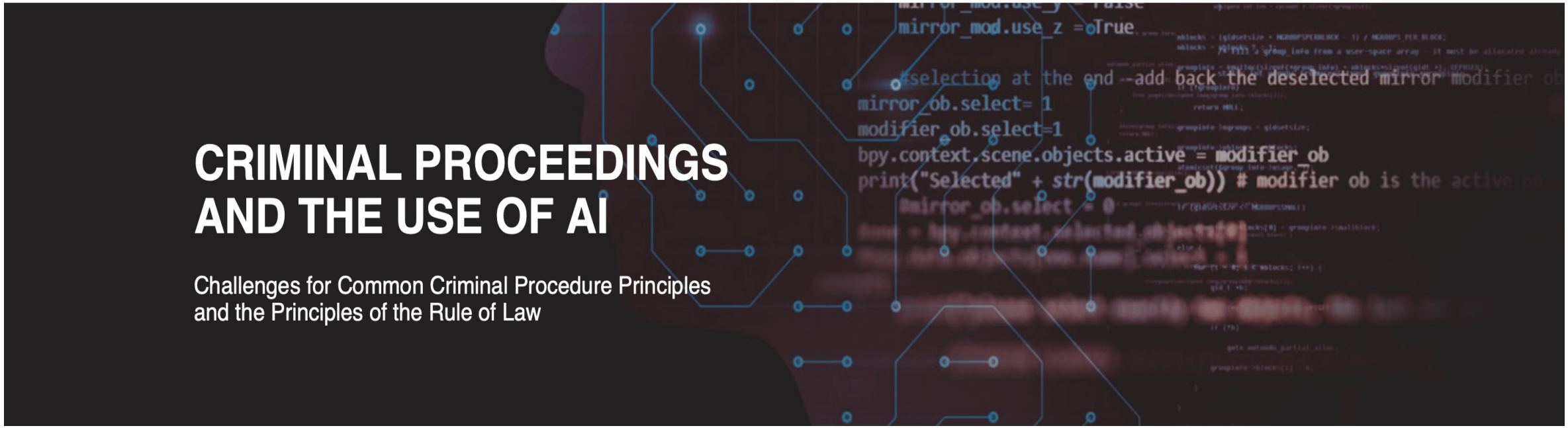
https://aiandcriminaljustice.uni.lu

FACULTY OF LAW, ECONOMICS AND FINANCE

UNIVERSITÉ DU LUXEMBOURG

CRIM/AI

HOME PROJECT NEWS TEAM RESOURCES



Scope of the project

- 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 regarding pretrial detention, sentencing, corrections, and re-entry (AI is used for risk assessment).

- AI Evidence is evidence autonomously generated by AI by using some form of machine learning.

Forensic AI

- filtering AI (e.g. Hansken);
- data mining AI;
- FRT (e.g. NeoFace Watch; Clearview)
- voiceprint;
- ANPR
- probabilistic genotyping AI e.g. TrueAllelle , STRMix)

Consumer Product AI.

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

Admissibility of AI Evidence

- AI Evidence must be reliable, valid and credible to be be admitted in trial.
- Divergent national rules on admissibility and exlcusion of evidence (controlled systems; free proof systems).
- General tendecy to admit AI Evidence without too-detailed scrutiny as to validity, reliability, or credibility. (in Europe we **lack standardized tests for admitting forensic evidence**)
- In inquisitorial systems, it is the responsibility of the trial judge or the investigating judge to establish the reliability of the evidence.
- The prosecutor is obliged to disclose both inculpatory and exculpatory evidence to the defense including if the evidence contains forensic reports.
- To challenge the admissibility the defense needs to demonstrate that the AI output is either not valid and/or not reliable and therefore needs access not only to the case file, but to the AI's source code, its original specifications, its intended purpose, and its training data set.
- New approaches in NL and DE to grant right to the AI tool, or right to the raw data.

Preliminary Comparative Observations

- legal systems face similar problems: AI evidence is becoming a sort of witness without a meaningful reliability test;
- different legal systems adopt different approaches
  - , e.g.-regulate technology?
    - Initiative for a “Justice in Forensic Algorithms Act”; ”Executive Order”
    - EU AI Act or data protection laws
  - re-interpret or modify procedural rules?
    - (a) re-interpretation of existing rules, e.g. adaption of the confrontation clause; revise admissibility of forensic evidence; … (
    - b) introduction of new rules tailored for scrutinizing AI Evidence; e.g. data access rights;
    - (c) installation of technological solutions, e.g. “explainable AI”
- legal systems reach similar results

EU AI Act – Banned applications

- biometric categorisation systems that use sensitive characteristics (e.g. political, religious, philosophical beliefs, sexual orientation, race);
- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases;
- emotion recognition in the workplace and educational institutions;
- social scoring based on social behaviour or personal characteristics;
- remote biometric identification systems (RBI) in publicly accessible spaces for law enforcement purposes, subject to prior judicial authorisation and for strictly defined lists of crime.
  - "post-remote" RBI only for the targeted search of a person convicted or suspected of having committed a serious crime.
  - real time RBI only for the purposes of
    - targeted searches of victims (abduction, trafficking, sexual exploitation),
    - prevention of a specific and present terrorist threat, or
    - the localisation or identification of a person suspected of having committed one of the specific crimes mentioned in the regulation (e.g. terrorism, trafficking, sexual exploitation, murder, kidnapping, rape, armed robbery, participation in a criminal organisation, environmental crime).

EU AI Act - Law Enforcement AI

- High risk AI systems used by LEA include
  - AI used for risk assessment of a natural person to become a victim of criminal offences
  - polygraphs
  - AI used for the evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences
  - AI used for risk assessment of a natural person of offending or reoffending not solely based on profiling
  - AI used for profiling of natural persons in the course of detection, investigation or prosecution of criminal offences
  - AI systems assisting judicial authorities in researching and interpreting facts and the law and in applying the law to a concrete set of facts

- Requirements for high-risk AI systems
  - risk management,
  - data governance rules ensuring the quality and relevance of data sets used,
  - technical documentation and record-keeping,
  - transparency and the provision of information to deployers ,
  - human oversight, and
  - robustness, accuracy and cybersecurity.

Thank you very much for your attention!