

DIGITAL TRANSFORMATION

---

# The “beauty and the Beast”: Reflection on the opportunities generated by Research, Regulation and Smart Use of AI in Criminal Justice

Pedro das Neves  
pedro.neves@prisonsystems.eu





Disney  
BEAUTY AND THE BEAST





- AI **accelerates the speed** and scale of decision-making.
  - AI may (or may not) improve the objectivity, accuracy and consistency of decision-making
  - AI systems **can be biased**.
  - **“Black box” decision-making**/Embedding decisions into code.
- Data issues** and choices are pervasive in AI systems.
- AI systems can **obscure or blur the distinction between predictions and policy**.
  - AI systems may **change the decision-maker** .
  - AI may **reduce discretion and decision-making independence**, even when there is a “human in the loop.”



## EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ)

### European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment



Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018)



## Artificial Intelligence

- European Parliament resolution of 20 January 2021 on **artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice** (2020/2013(INI))
- European Parliament resolution with recommendations to the Commission on a framework of **ethical aspects of artificial intelligence, robotics and related technologies** (2020/2012(INL) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))
- Coordinated **Plan on Artificial Intelligence 2021** Review . AI act.
- European **ethical Charter on the use of Artificial Intelligence in judicial systems and their Environment**



European Parliament

[Index](#) [Previous](#) [Next](#) [Full text](#)

Procedure : [2020/2012\(INL\)](#)

Document selected : [A9-0186/2020](#)

Texts tabled :  
[A9-0186/2020](#)

Debates :  
[PV 19/10/2020 - 15](#)  
[PV 19/10/2020 - 18](#)  
[CRE 19/10/2020 - 15](#)  
[CRE 19/10/2020 - 18](#)

## Texts adopted

Tuesday, 20 October 2020 - Brussels

[Framework of ethical aspects of artificial intelligence, robotics and related technologies](#)

- [Resolution](#)
- [Annex](#)
- [Annex](#)

Parliament resolution of 20 January 2020 on **artificial intelligence: questions of protection and application of international law as the EU is affected in the areas of military uses and of state authority in the scope of criminal justice** (INI))

Parliament resolution with recommendations to the Commission on a **framework of ethical aspects of artificial intelligence, robotics and related technologies** (INI) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))

**Plan on Artificial Intelligence 2021**  
Act.

- **European ethical Charter on the use of Artificial Intelligence in judicial systems and their Environment**





European Parliament

Parliament resolution of 20 January  
**Artificial intelligence: questions of**  
**governance and application of international**  
**law affected in the areas of**  
**freedom of state authority**  
**and fundamental justice**

Index < F

Procedure : 2020

Document selected

Texts tabled :  
A9-0186/2020

Texts adopted

Tuesday, 20 October

Framework of

- ▶ Resolutions
- ▶ Annexes
- ▶ Annexes



Brussels, 21.4.2021  
COM(2021) 205 final

ANNEX

ANNEXES

*to the*

**Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions**

**Fostering a European approach to Artificial Intelligence**

Resolution with  
Commission on a  
**Effects of artificial  
Intelligence related technologies**  
in Parliament resolution  
recommending to  
liability regime for  
2020/2014(INL))

**Artificial Intelligence 2021**

**on the use of Artificial  
Intelligence systems and their**



European Council





## Shaping Europe's digital future

[Home](#) [Policies](#) [Activities](#) [News](#) [Library](#) [Funding](#) [Calendar](#) [Consultations](#)

[Home](#) > [Library](#) > Proposal for a Regulation laying down harmonised rules on artificial intelligence

POLICY AND LEGISLATION | Publication 21 April 2021

# Proposal for a Regulation laying down harmonised rules on artificial intelligence

The Commission has proposed the first ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally.

The Proposal for a Regulation on artificial intelligence was announced by the Commission in April 2021. It aims to address risks of specific uses of AI, categorising them into 4 different levels: unacceptable risk, high risk, limited risk, and minimal risk.

In doing so, the AI Regulation will make sure that Europeans can trust the AI they are using. The Regulation is also key to building an ecosystem of excellence in AI and strengthening the EU's ability to compete globally. It goes hand in hand with the [Coordinated Plan on AI](#).

### Downloads



1. Proposal for a Regulation laying down harmonised rules on artificial intelligence (.pdf)

[Download](#) 

### See also

[View the proposal for a Regulation in all EU languages on EUR-Lex](#)

### Related topics

[eHealth, Wellbeing and Ageing](#)

[Advanced Digital Technologies](#)

[Artificial Intelligence](#)

January  
s of  
national  
e areas of  
priority

n a  
al  
ologies  
resolution  
ons to  
e for

ice 2021

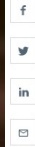
Artificial  
ir





[Back to Resource Hub](#)

[Print this page](#)



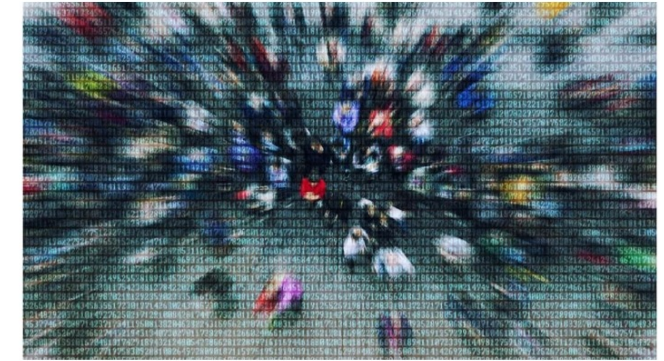
Film/Video

## End the use of AI to profile people in the EU

Published: May 19, 2022 (Last updated: May 19, 2022)

[Back to Resource Hub](#)

[Print this page](#)



News

## Fair Trials calls for ban on the use of AI to 'predict' criminal behaviour



News

## Leading European Parliament figures agree to ban predictive policing and justice AI

12 April 2022 | Article by Fair Trials

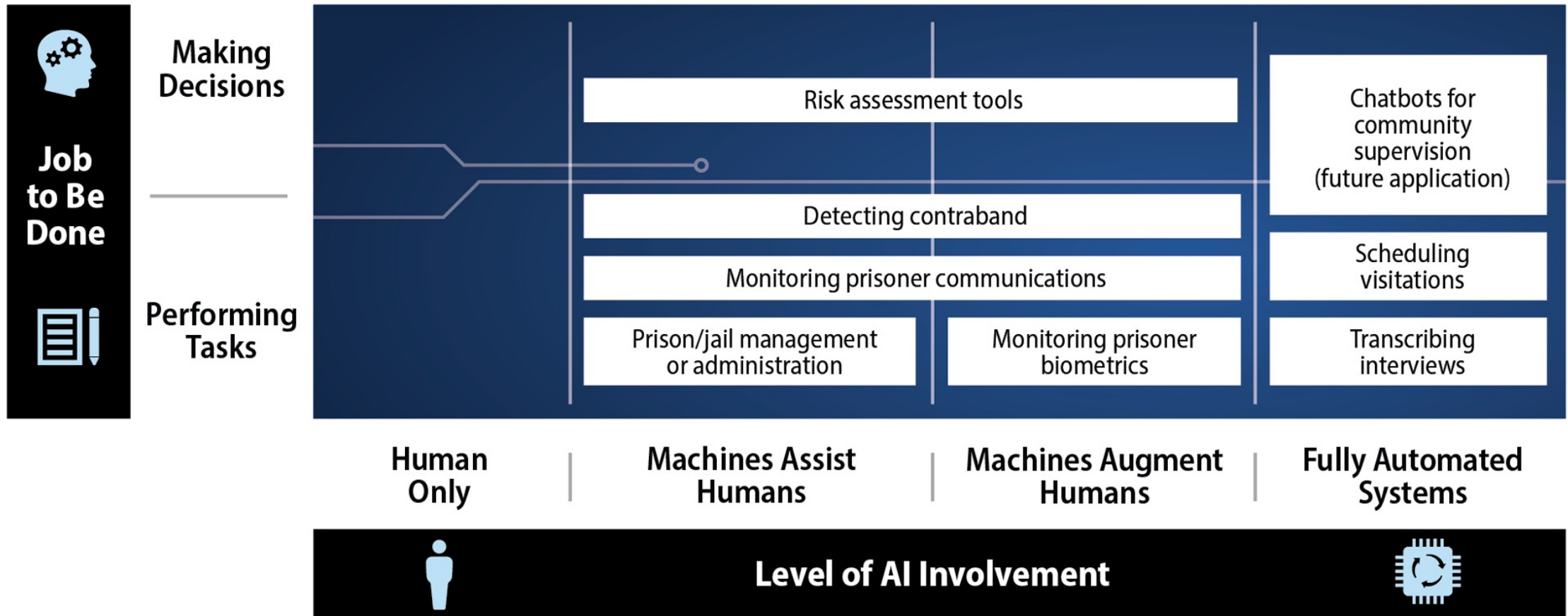
<https://www.fairtrials.org/articles/news/fair-trials-calls-ban-use-ai-predict-criminal-behaviour/>

**In the digital era if we're not moving forward, we are certainly moving backwards.**

**...and increasing the Digital Divide between jurisdictions.**



# AI in Corrections



# Decisions and tasks to be supported



## Make a Decision



## Perform a Task

### Jails

Determine whether a pretrial defendant should be detained.  
Select which rehabilitation services or type of supervision are needed for defendants.

Complete intake forms and risk/needs assessments.  
Aid in processing discharges.

### Prisons

Assign cellmates and units.  
Select appropriate services for inmates.  
Respond appropriately to behavioral issues.  
Determine whether a prisoner should be granted parole.

Detect contraband.  
Translate or transcribe calls in real-time.  
Monitor inmate communications.  
Predict inmate risk based on past records,

interactions with other inmates, and prior misbehavior.

### Community Supervision

Develop a plan to prevent recidivism and promote positive, thriving outcomes.  
Select appropriate client services and connect clients with service providers in an efficient manner.  
Provide support to community supervision officers (CSOs).

Schedule client check-ins and issue reminders.  
Test for drug use.  
Monitor location.

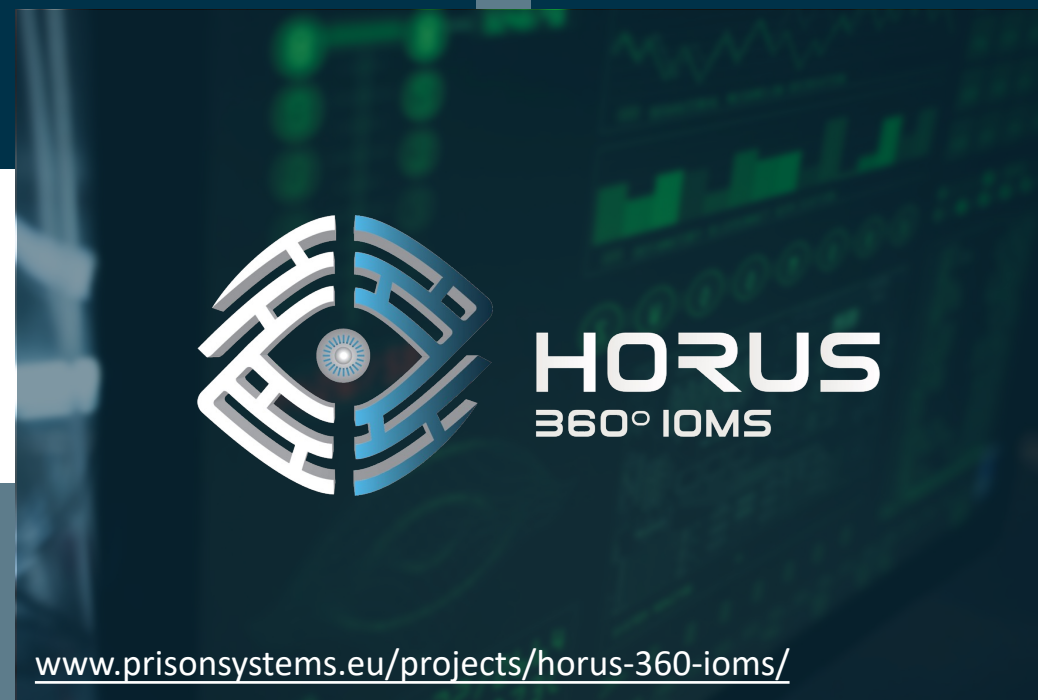
DIGITAL TRANSFORMATION

The

# HORUS 360° IOMS

Intelligent Offender Management System

R&D project



Co-financed by:



EUROPEAN UNION  
European Regional  
Development Fund

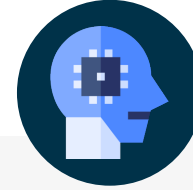
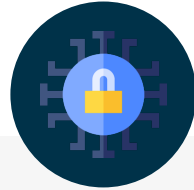




**HORUS**  
360° IOMS

## About

[www.prisonssystems.eu/projects/horus-360-ioms/](http://www.prisonssystems.eu/projects/horus-360-ioms/)



The **HORUS360** project is **researching, designing and developing** an IT solution that supports the **management of activities and information generated during the detention "life cycle", imprisonment or surveillance of persons subject to custodial and non-custodial judicial measures**, also supporting – through the use of **Artificial Intelligence and Predictive Analysis technology** - the rehabilitation process, and judicial or administrative decision-making processes.

**EU, National and private funding:**

**1,7 Million euros**

**Currently 2 Million +**



**HORUS**  
360° IOMS

[www.prisonssystems.eu/projects/horus-360-ioms/](http://www.prisonssystems.eu/projects/horus-360-ioms/)

**Design and develop an Intelligent offender Management System** that allows managing the life cycle of citizens in custody or supervised within the scope of criminal proceedings (prison and probation) and support decision making within the scope of detention, rehabilitation, therapeutic intervention, court decisions, decisions on security measures, treatment, or early release from prison.

**Research and develop an intelligent OMS** that will embody state-of-the-art technology exploring artificial intelligence, big data and predictive analytics.

**Contribute to increasing transparency and equity of decisions** affecting those citizens who are involved in the criminal justice system, as well as improving human, logistic, financial, and time resource management across criminal justice organisations.

**Close the gaps** caused by the lack of intelligent offender management solutions in criminal justice systems.





**HORUS**  
360° IOMS

# Consortium

[www.prisonssystems.eu/projects/horus-360-ioms/](http://www.prisonssystems.eu/projects/horus-360-ioms/)

## Multidisciplinary teams

### 30 professionals

Computer and data scientists, decision support systems specialists, artificial intelligence, public policy and digital governance, forensic psychology, penology, and cybersecurity, as well as world-renowned specialists in prison systems operation and digital transformation.



## Promotor and consortium leader

Corrections renowned research and advisory firm. IPS is responsible for business requirements definition, ensuring the compliance of all deliverables with Business and Partners needs.



## Partner

BSAFE LAB Law Enforcement, Justice and Public Safety University Lab. Role is the research of the artificial intelligence engine to support all decisions recommendations.



## Partner

Software engineering firm with experience in the development of IT solutions to support government and industry. iTech-ON is responsible for the development of the technical solution.



**HORUS**  
360° IOMS

# Innovation

[www.prisonssystems.eu/projects/horus-360-ioms/](http://www.prisonssystems.eu/projects/horus-360-ioms/)

1

## **Digitisation, automation and mobility**

Digitization, dematerialization and automation of critical processes.

2

## **Fully parameterisable risk and needs assessment tools**

Predictive analysis and decision support system considering risk of recurrence based on the assessment of risks, needs and responsivity (RNR) of an offender supported by scientifically validated models.

3

## **Recidivism prevention model**

Predictive analysis and decision support considering RNR information and contextual analysis.



**HORUS**  
360° IOMS

**Innovation**

[www.prisonssystems.eu/projects/horus-360-ioms/](http://www.prisonssystems.eu/projects/horus-360-ioms/)

**4**

#### **Development and integration of Predictive AI modules**

Predictive analysis and decision support system considering the risk of recurrence based on the assessment of risks and needs of an offender supported by scientifically validated models.

**5**

#### **Compliance with EU and International Directives, Framework Decisions, Standards and Recommendations in relevant areas for the use of the OMS**

Full compliance with the European regulatory and international conventions on justice and law enforcement, protection of rights, protection standards and data transfer.





**Risk and Needs Assessments  
Institutional Maturity  
Bias (human and machine)**



A strong body of evidence demonstrates three significant conclusions in offender assessment:

**Probability of future criminal behaviour can be accurately quantified.**

**Structured risk assessment methods are more accurate in predicting re-offending than unstructured “clinical” approaches.**

**Information on individual offenders’ risk level has practical utility for offender management decision-making.**



1990s: a substantial body of international research reveals that offenders could be successfully rehabilitated if particular principles were addressed when providing the services.

The “*what works*” literature comprises three central and inter-related research principles, which are:

**Risk** Offenders' relative likelihood of re-offending can be reliably predicted. Calculated risk level was taken as an indispensable factor in defining how an offender should be managed and, specifically, their appropriateness to be integrated into core rehabilitative intervention programmes.

**Need** A defined set of offender features can be relevant targets for intervention; addressing characteristics that are not included in this set is considered to be fruitless to reduce recidivism.

**Responsivity** This concept is associated with the targets and implies that offenders are capable of participating in rehabilitation programmes (and which ones) – and also that rehabilitative interventions are delivered in a way and intensity that matches the participants' capacity to learn and change.



These outcomes constitute a vital ground to the use of risk assessment since they can provide excellent support and assistance to justice and correctional services, namely:

**Guiding sentencing decisions**

**Guiding release-on-parole decisions** (both whether to release and the extent of rehabilitative involvement, monitoring, and controls necessary if released).

**Facilitating the targeting of resources** towards those most likely to re-offend and, at the same time, avoiding wastage of resources on those unlikely to re-offend.

**Enhance the validity of outcome information** involving the effectiveness of programmes, services, and interventions.





## Selecting a risk assessment tool

- Type of risk that it is wished to evaluate (e.g., general risk, risk of violence, risk of committing a sexual offence).
- Age, gender, ethnicity, mental state, and cognitive abilities of the individual.
- Performance of tools concerning the criteria outlined.

This includes validation history, empirical grounding, inter-rater reliability, and the ability to identify targets for intervention.



## **General Risk Assessment**

Tools that can be used for general application for risk

## **Violence Risk**

Instruments to predict the risk of future violence

## **Sexual Offending**

Tools to assess the likelihood of committing a sexual offence.

## **Responsivity**

Offender characteristics that affect how they respond to an intervention or treatment



**HORUS**  
360° IOMS

# Human centric approach

[www.prisonssystems.eu/projects/horus-360-ioms/](http://www.prisonssystems.eu/projects/horus-360-ioms/)



- **Assess offender** to identify the **risks**, the **needs** and the **responsiveness**
- **Identify the most suitable rehabilitation programmes**
- **Allocate inmate** to the most suitable **facility** and **programmes/activities**
- **Schedule offender** into programmes/activities
- **Support staff decision-making** (facility allocation, programmes/activities, disciplinary actions, release)
- **Learn** from successful results

In-depth scientific research (most recent metanalysis) resulted in:

### General recidivism risk

Instruments compared and analysed: **32**

Instruments selected for HORUS native integration: **7**

### Risk of violence

Instruments compared and analysed: **28**

Instruments selected for HORUS native integration: **3**

### Sexual violence risk

Instruments compared and analysed: **25**

Instruments selected for HORUS native integration: **4**

### Responsivity

Instruments compared and analysed: **38**

Instruments selected for HORUS native integration: **5**

### Mental health

Instruments selected for HORUS native integration: **3**

### Suicide risk

Instruments selected for HORUS native integration: **2**

### Radicalisation risk

Instruments selected for HORUS native integration: **3**



# How are we assessing risk and needs in Europe?

## What is the current practice?

- Is it evidence-based?
- Are risks, needs and responsivity assessment tools validated (country/specific populations)?
- How are universities involved?
- Is it consistent throughout the country?
- Is staff properly trained to perform risks and needs assessments?

## How shall we proceed to enhance current practice?





# As an organization, are we mature enough to consider AI?

## Strategy

- What are the questions we want to answer?
- Old systems may respond to old questions. New questions may require new data or new systems.
- We don't know what we (still) don't know...

## Data

- What for?
- Relevance and adequacy of data (primary and secondary data)
- Data collection process
- Do we measure enough? Data recording is expensive. We measure the indispensable.
- Mapping data (identifying variables that are relevant)
- Cleaning data (removing what is not relevant)

## IT System

- Rather old, often monolithic IT systems may respond to the questions of the past and (eventually the present)...but...

## People

- Do we have the people (number and profile) needed for the task?

## Budget

- Do we have the budget?



# Bias

How are we dealing with human bias?

Humans are substantially influenced by stereotypes about race, ethnicity, gender, age, country of origin, etc...

Bias in the sampling of observations, bias of people selected, media bias, historical-temporal bias, various types of semantic bias, technological bias, etc.

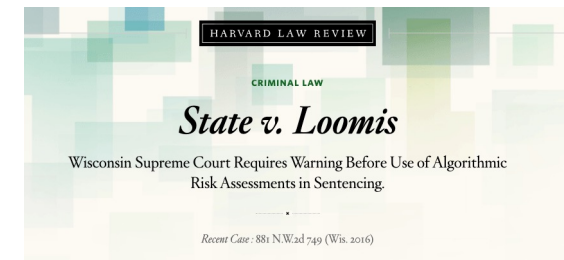
- **Major advances in techniques to minimize bias and underestimation of bias in humans**

E.g. most machine analysis in AI sample observations systematically in a manner that equilibrates different populations (placing them on an even playfield) rather than having solutions that simply reflect selection bias of the most frequent populations.

**Unfortunately, humans are ill-equipped to handle multifaceted variability.**



# Learning from the good, old, Loomis case...



Risk scores may not be used “to determine whether an offender is incarcerated” or “to determine the severity of the sentence.” **Judges using risk assessments must explain the factors other than the assessment** that support the sentence imposed.

Presentencing investigation reports that incorporate COMPAS assessments must include five written warnings for judges:

1. The “**proprietary nature of COMPAS**” prevents the disclosure of how risk scores are calculated
2. COMPAS scores are **unable to identify specific high-risk individuals** because these scores rely on group data
3. COMPAS **relies on a national data sample**, there has been “no cross-validation study for a Wisconsin population”
4. Studies “have raised questions about whether [COMPAS scores] **disproportionately classify minority offenders as having a higher risk** of recidivism”
5. COMPAS was **developed specifically** to assist the Department of Corrections in making **post-sentencing determinations.**





## Learning from the good, old, Loomis case...

There is an enormous practical burden placed on individual defendants wishing to challenge bail or sentencing decisions based in part on algorithmic risk assessment tools:

Is the **historic data used to train the tool biased, accurate, reliable and valid?**

Are **risk factors and scores weighed and calculated appropriately?**

**Which communities bear the burden of statistical errors?**

**Are the confidence estimates for predictions appropriate?**

**Are predictions validated appropriately?**

**Does the tools use factors such as education or employment as impermissible statistical proxies for race or gender?**



Key questions about AI decision-making



## Participation

- Are the public and stakeholders involved in the design, development, deployment, and oversight of the AI system? Is that participation meaningful?

## Disclosure/Notice

- What types of government AI systems must be disclosed?
- What information will be disclosed?
- Will disclosure be both substantive and accessible?
- Will persons affected by an AI system be notified of its use?

## Transparency

- Is the system sufficiently transparent to ensure the public understands its purpose, potential impact, operation, and evaluation?
- Is the system sufficiently transparent to meet or exceed legal procedural fairness standards and to ensure legal accountability?



## **Prohibitions, Risks and Harm Mitigation**

- Should the system be prohibited due to systemic risks to legal rights and vulnerable populations?
- How is an AI system's risk assessed? And by who?
- Once a system's risk is identified, how will that risk be mitigated or eliminated?

## **Explainability and Reasons**

- Can the operation and outcome of an AI system be explained to the public?
- Do AI decisions meet or exceed legal substantive fairness standards and ensure legal accountability?

## **Discrimination**

- Does the AI system discriminate against vulnerable or human rights-protected populations?
- What steps will be taken to mitigate or eliminate the risk of discrimination?
- Is there regular testing and evaluation for bias?
- Does the system meet or exceed Charter or human rights legal standards?



## Data Accuracy, Reliability, and Validity

- Is the data used to train an AI system accurate, reliable, and valid?

## Human-In-The-Loop/Discretion

- Is there a “**human-in-the-loop**” reviewing a system’s output and ensure oversight?
- Do human decision-makers have meaningful discretion to overturn or alter AI-based decisions or recommendation?
- How is automation bias addressed?

## Evaluation and Monitoring

- How will system administrators and the public know the system is effective and legal?
- Is there an evaluation plan for the entire lifecycle of the system?



## ***Avoidance of Unfair Bias***

### **European Commission's High Level Expert Group's Assessment questionnaire**

- Did you establish a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design?
- Did you consider diversity and representativeness of end-users and/or subjects in the data?
- Did you test for specific target groups or problematic use cases?
  - Did you research and use publicly available technical tools, that are state-of-the-art, to improve your understanding of the data, model and performance?
  - Did you assess and put in place processes to test and monitor for potential biases during the entire lifecycle of the AI system (e.g., biases due to possible limitations stemming from the composition of the used data sets (lack of diversity, non-representativeness))?
  - Where relevant, did you consider diversity and representativeness of end-users and or subjects in the data?
- Did you put in place educational and awareness initiatives to help AI designers and AI developers be more aware of the possible bias they can inject in designing and developing the AI system?
- Did you ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system?
  - Did you establish clear steps and ways of communicating on how and to whom such issues can be raised?
  - Did you identify the subjects that could potentially be (in)directly affected by the AI system, in addition to the (end-)users and/or subjects?
- Is your definition of fairness commonly used and implemented in any phase of the process of setting up the AI system?
  - Did you consider other definitions of fairness before choosing this one?
  - Did you consult with the impacted communities about the correct definition of fairness, i.e., representatives of elderly persons or persons with disabilities?
  - Did you ensure a quantitative analysis or metrics to measure and test the applied definition of fairness?
  - Did you establish mechanisms to ensure fairness in your AI system?



## Brookings Institution “Bias Impact Statement”

### **What will the automated decision do?**

Who is the audience for the algorithm and who will be most affected by it?

Do we have training data to make the correct predictions about the decision?

Is the training data sufficiently diverse and reliable? What is the data lifecycle of the algorithm?

Which groups are we worried about when it comes to training data errors, disparate treatment, and impact?

### **How will potential bias be detected?**

How and when will the algorithm be tested? Who will be the targets for testing?

What will be the threshold for measuring and correcting for bias in the algorithm, especially as it relates to protected groups?

### **What are the operator incentives?**

What will we gain in the development of the algorithm?

What are the potential bad outcomes and how will we know?

How open (e.g., in code or intent) will we make the design process of the algorithm to internal partners, clients, and customers?

What intervention will be taken if we predict that there might be bad outcomes associated with the development or deployment of the algorithm?

### **How are other stakeholders being engaged?**

What's the feedback loop for the algorithm for developers, internal partners and customers?

Is there a role for civil society organizations in the design of the algorithm?

### **Has diversity been considered in the design and execution?**

Will the algorithm have implications for cultural groups and play out differently in cultural contexts?

Is the design team representative enough to capture these nuances and predict the application of the algorithm within different cultural contexts? If not, what steps are being taken to make these scenarios more salient and understandable to designers?

Given the algorithm's purpose, is the training data sufficiently diverse?

Are there statutory guardrails that companies should be reviewing to ensure that the algorithm is both legal and ethical?



**How are we assessing risk and needs in Europe?**

**Machine bias is a result of human bias**

**What can the Council of Europe do to enhance current practice?**







Thank you

**Pictures:** The pictures of the “Beauty and the Beast” movie used to illustrate the metaphor in this presentation are owned by Disney Enterprises Inc.

## References:

Andrews, D., Bonta, J., & Hoge, R. (1990). *Classification for effective rehabilitation: Rediscovering psychology*. Criminal justice and behavior.

Andrews, D. A., & Bonta, J. (2010). *The Psychology of Criminal Conduct* (5th ed.). Anderson Publishing.

Busuioc, M. (2021), Accountable Artificial Intelligence: Holding Algorithms to Account. *Public Admin Rev*, 81: 825-836. <https://doi.org/10.1111/puar.13293>

Council of Europe (2018). European ethical Charter on the use of Artificial Intelligence in judicial systems and their Environment. Online: [https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment? 82\\_struts\\_action=%2Flanguage%2Fview& 82\\_languageId=fr](https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment?82_struts_action=%2Flanguage%2Fview&82_languageId=fr) FR

European Commission (2022). Independent High-Level Expert Group on Artificial Intelligence (European Commission), ALTAI - The Assessment List on Trustworthy Artificial intelligence (n.d.) [HLEG Assessment List]. Online: <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>

European Commission (2021). Coordinated Plan on Artificial Intelligence 2021 Review . AI act. Online: <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>

European Parliament (2021). Resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)). Online: [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html)

European Parliament (2020). Resolution with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)). Online: [https://www.europarl.europa.eu/doceo/document/A-9-2020-0186\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html)

European Parliament (2020). Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)). Online: [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html)

Gottfredson, S. D., & Moriarty, L. J. (2006). *Statistical Risk Assessment: Old Problems and New Applications*. *Crime & Delinquency*, 52(1), 178–200.

Hampton, A, DeFalco, Jeanine (2022). *The Frontiers of Artificial Intelligence Ethics*. Routledge. New York.

HLR (2017). *State v. Loomis Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing*. Recent Case : 881 N.W.2d 749 (Wis. 2016), Harvard Law Review MAR 10, 2017, 130 Harv. L. Rev. 1530. Online: <https://harvardlawreview.org/2017/03/state-v-loomis/>

Humerick, J. D. (2019). *Reprogramming Fairness: Affirmative Action in Algorithmic Criminal Sentencing*. HRLR Online, 4, 213.

LCO (2022). LCO final report: Accountable AI. Law Commission of Ontario, June, 2022. Online: <https://www.lco-cdo.org/en/the-lco-releases-accountable-ai-final-report/>

Monahan, J., & Skeem, J. (2016). Risk Assessment in Criminal Sentencing. *Annual Review of Clinical Psychology*, 12, 489-513.

Motiuk, L.L., & Keown, L.A. (2020). Correctional Intake Assessment and Case Planning: Application Development and Validation. *Criminal Justice and Behavior*, 48, 556 - 570.

Das Neves, P. (2020). *Horus 360° iOMS. Proposta de Candidatura. Anexo Técnico Aviso 13/SI/2020*.

Redden, J., Inkpen, C., DeMichele, M., & Criminal Justice Testing and Evaluation Consortium. (2020). *Artificial Intelligence Applications in Corrections*. U.S. Department of Justice, National Institute of Justice, Office of Justice Programs. Online: <http://cjtec.org/>

Skeem, J., & Monahan, J. (2011). *Current Directions in Violence Risk Assessment*. *Current Directions in Psychological Science*.

Turner Lee, N., Resnick, P. & Barton, G. (2019). Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms. 22 May 2019. Online: [www.brookings.edu/research/algorithmic-biasdetection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/](http://www.brookings.edu/research/algorithmic-biasdetection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/)

Yang, M., Wong, C.P., & Coid, J. (2010). *The Efficacy of Violence Prediction: A Meta-Analytic Comparison of Nine Risk Assessment Tools*. American Psychological Association.