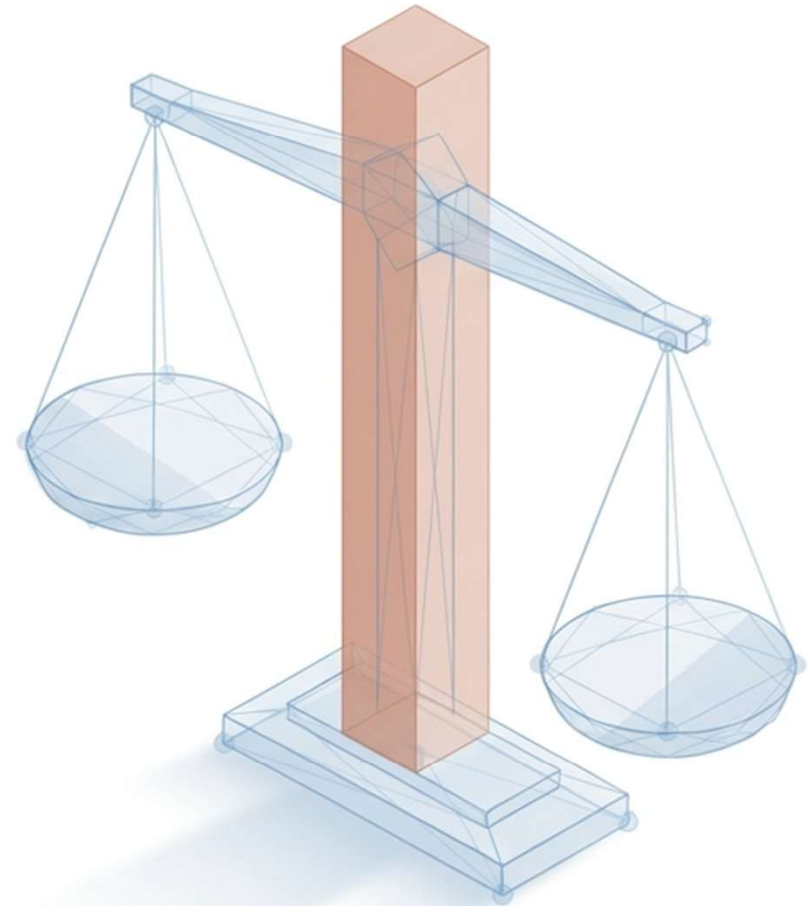


Balancing AI Security and Human Rights under the ECHR

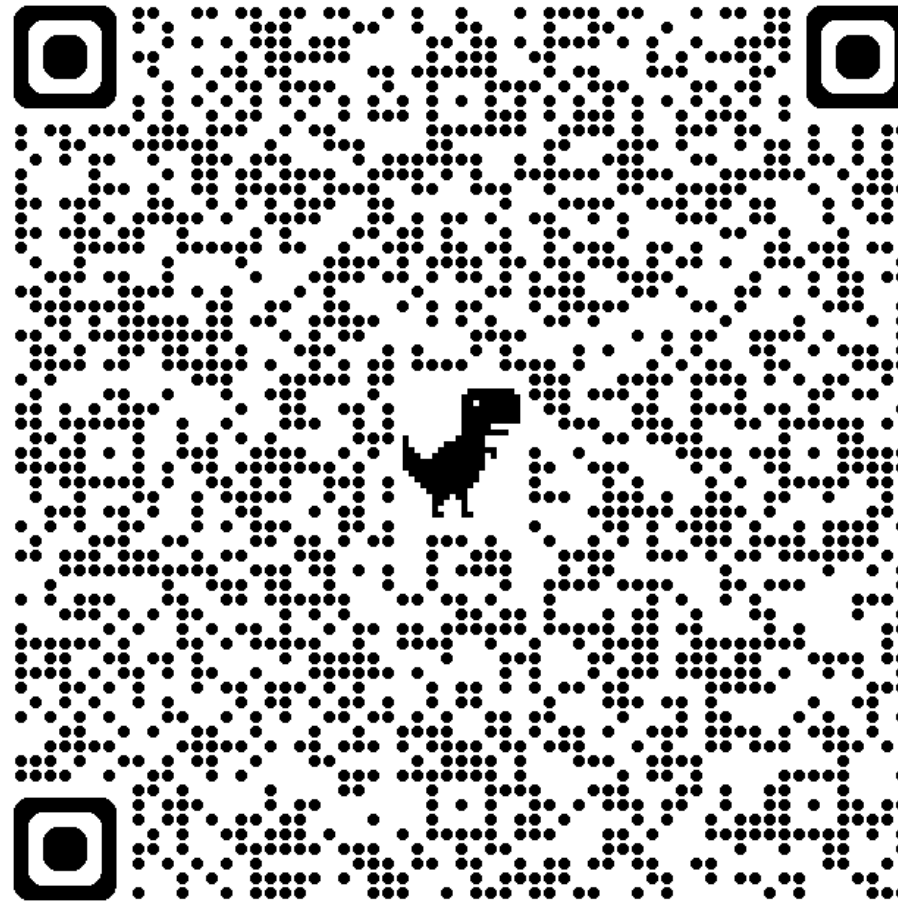
Navigating the Tension Between Technological Efficiency and Fundamental Safeguards

Digital systems monitor, predict, and decide. But when does security become overreach? Can these technologies be reconciled with the standards of the European Convention on Human Rights?

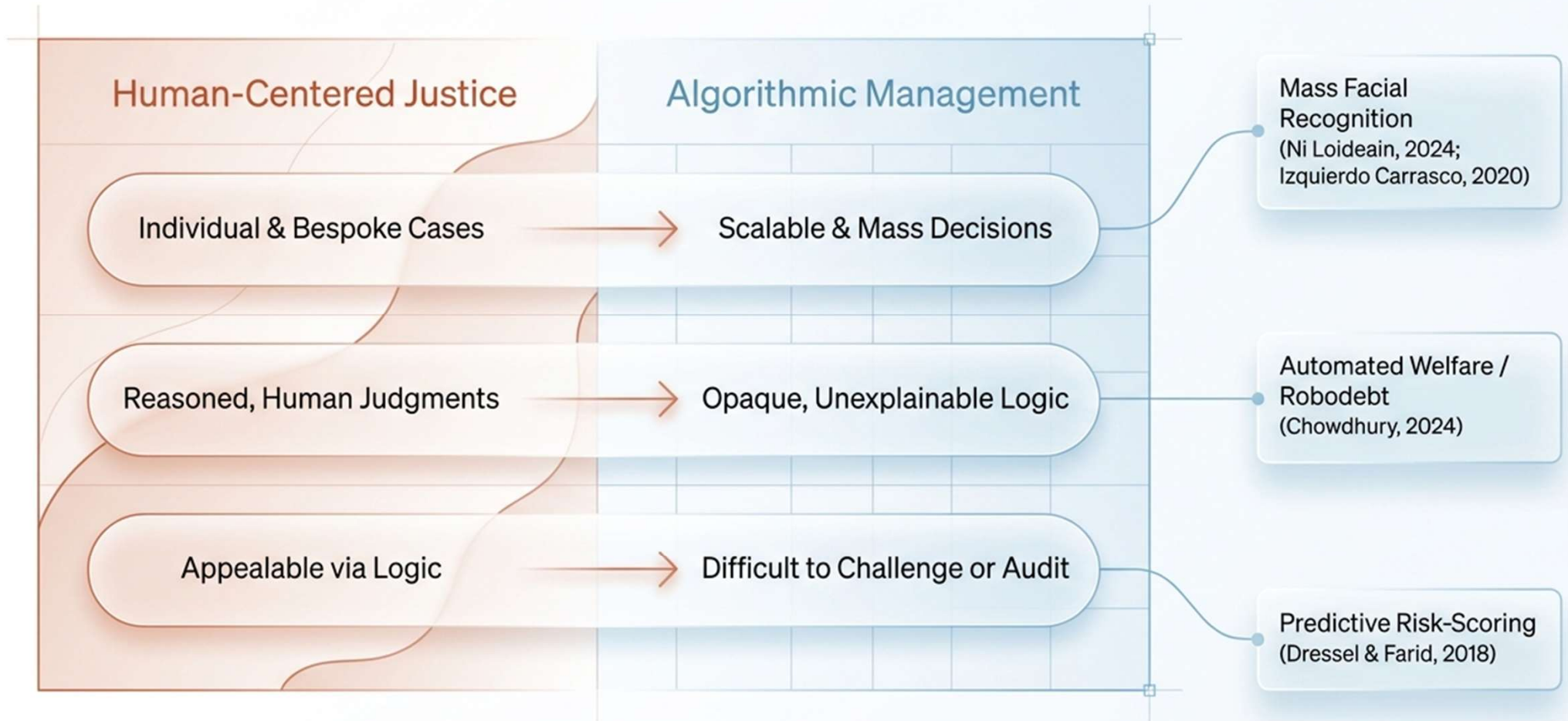
Laercio Cruvinel and Patrícia Dias



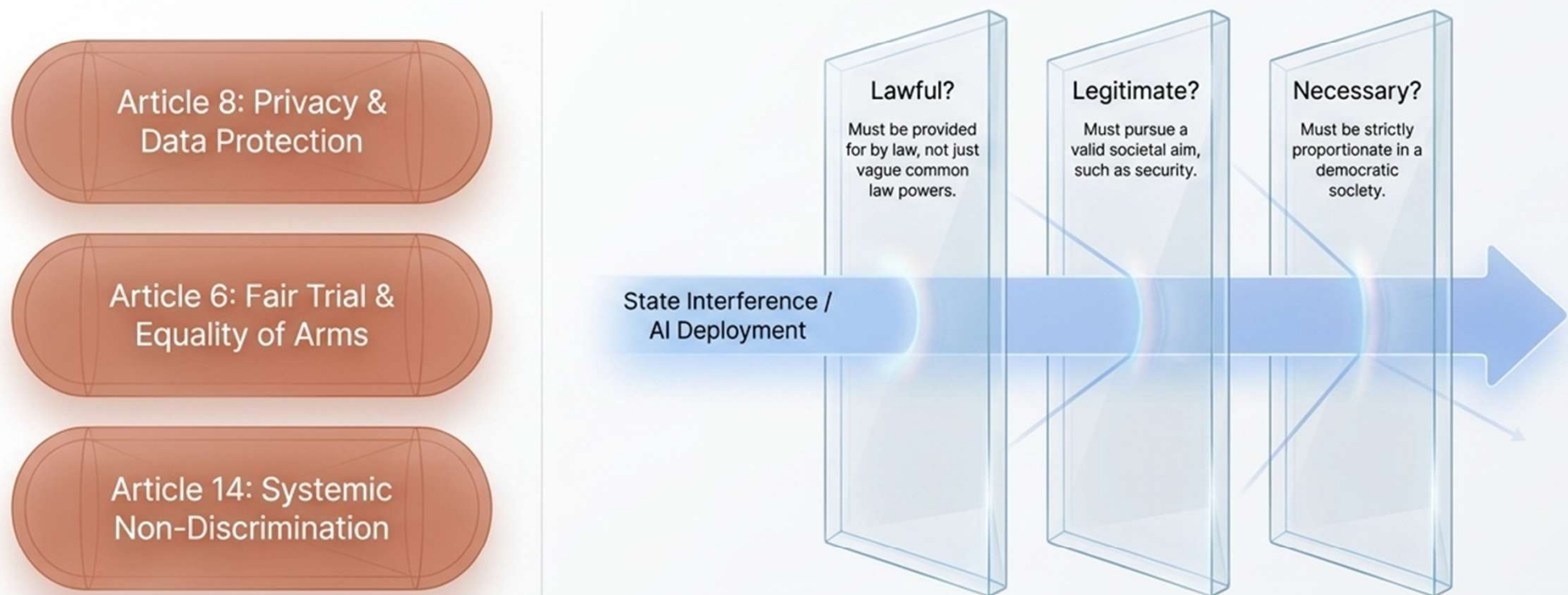
Documentation – Portuguese/English



The Shift to Algorithmic Management



The ECHR Framework and the Triple Test



The ECHR is our analytical backbone. State interference must pass a strict three-part test or be struck down.

Challenge I: Scale and the Automation of Mass Surveillance

Core Conflict: Article 8 (Privacy) vs. Mass Biometric Extraction.



Targeted
Human Suspicion

AI changes the nature of surveillance by continuously extracting unique identifiers from public spaces. The more intrusive the technology, the stricter the legal safeguards must be.

Case Spotlight

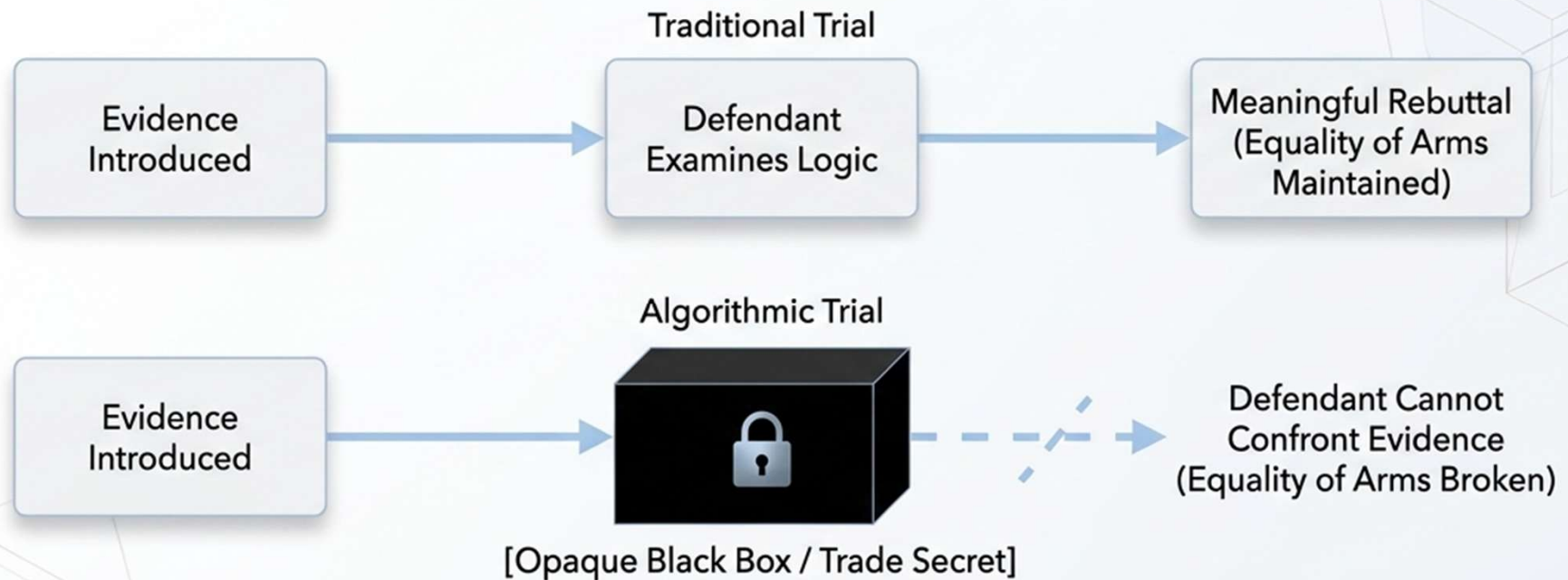
Bridges v. South Wales Police

- Finding: Live Facial Recognition ruled not in accordance with the law (Ni Loideain, 2024).
- Reason: Excessive discretion given to officers. Broad common law powers cannot justify pervasive biometric monitoring.

Continuous
Algorithmic Extraction

Challenge II: Opacity and the Breakdown of Procedural Fairness

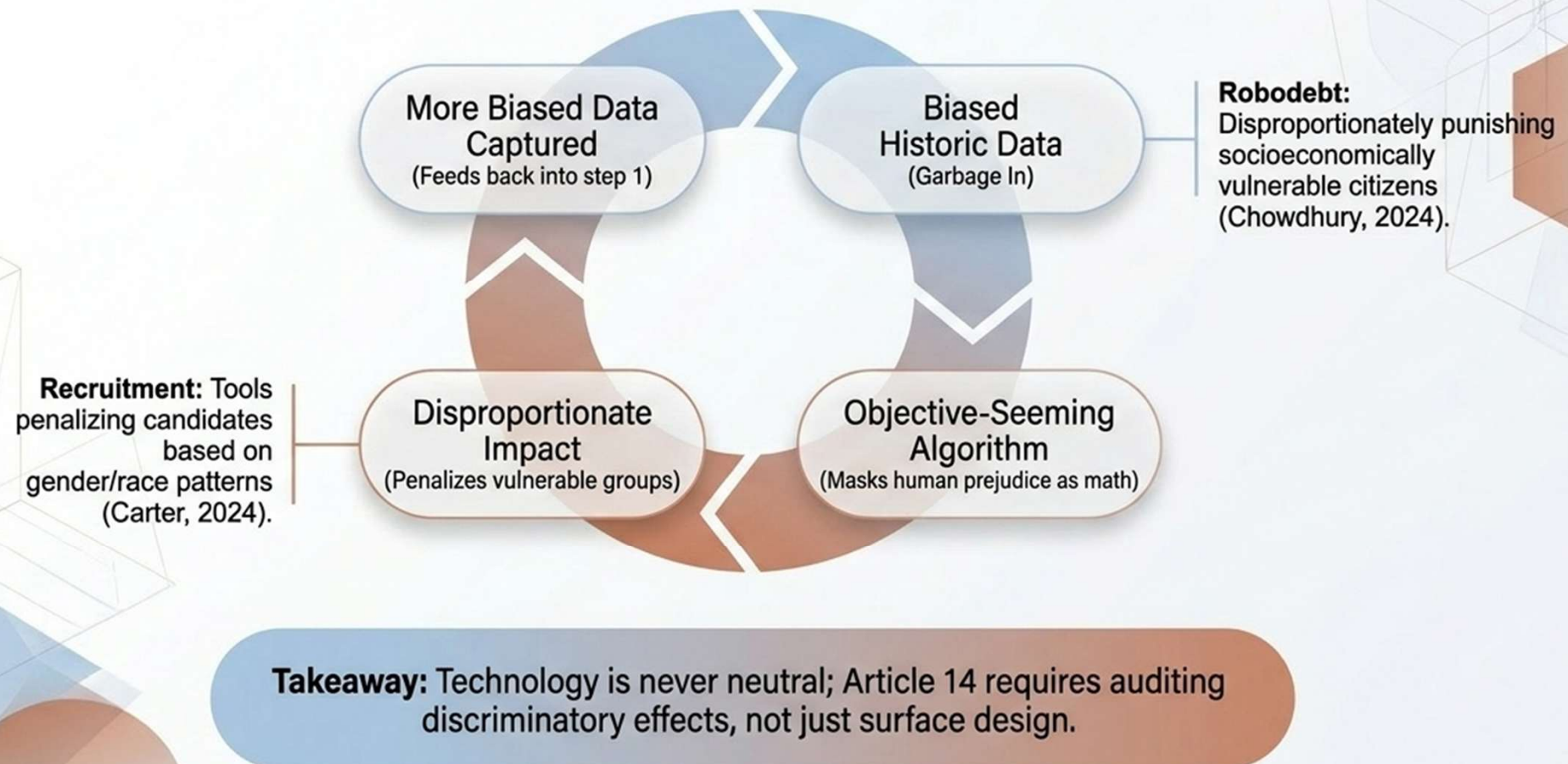
Core Conflict: Article 6 (Fair Trial) vs. Algorithmic Unexplainability



Example: COMPAS recidivism software. Logic protected as a trade secret, preventing defendants from challenging evidence they cannot understand, despite being proven no more accurate than untrained humans (Dressel & Farid, 2018; Blount, 2021).

Challenge III: The Algorithmic Feedback Loop of Discrimination

Core Conflict: Article 14 (Systemic Non-discrimination) vs. Data-Driven Prejudice



Synthesis: The Democratic Boundary of Security

The Insight:

Economic well-being and security are legitimate state aims, but they are not a blank check.

The Threat:

Highly intrusive surveillance tools initially justified for serious crimes inevitably creep into minor administrative enforcement.

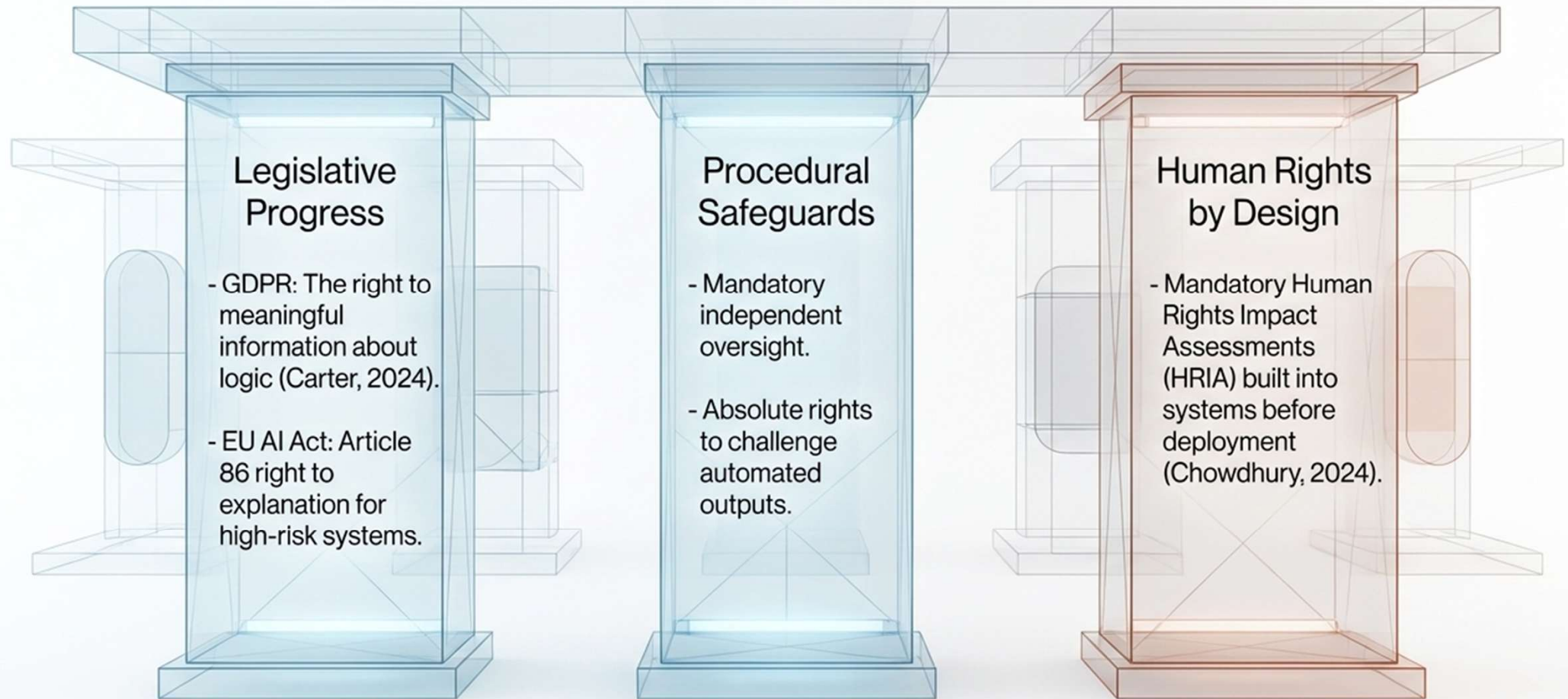
Security Demands
& Function Creep

Democratic
Accountability &
Human Rights

The Democratic Boundary:

A secure system that is legally unaccountable is not democratic. We must resist prioritizing technological efficiency over procedural rights.

Reclaiming the System: Safeguards & Legislation



Security Governed by Rights

AI tests the limits of law, but does not replace it. The ECHR remains essential and fully applicable to the digital age.

The challenge for the next generation of lawyers is not to choose between security and rights, but to ensure that the security of our future is governed by the principles of our past.

Bibliography

- Blount, K. (2021). Seeking Compatibility in Preventing Crime with Artificial Intelligence and Ensuring a Fair Trial. *Masaryk University Journal of Law and Technology*, 15(1), 25–52. <https://doi.org/10.5817/MUJLT2021-1-2>
- Carter, C. (2024). Why the algorithmic recruiter discriminates: The causal challenges of data-driven discrimination. *Maastricht Journal of European and Comparative Law*, 31(3), 333–359. <https://doi.org/10.1177/1023263X241248474>
- Chowdhury, S. (2024). Technology is never neutral: Robodebt and a human rights analysis of automated decision-making on welfare recipients. *Australian Journal of Human Rights*, 30(1), 20–40. <https://doi.org/10.1080/1323238X.2024.2409620>
- Council of Europe. (2021). *European Convention on Human Rights* [Convention]. https://www.echr.coe.int/documents/d/echr/convention_eng
- Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1), eaao5580. <https://doi.org/10.1126/sciadv.aao5580>
- Fuster, G. (2009). TEDH - Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04—Artículo 8 CEDH - Vida privada—Injerencia en una sociedad democrática—Los límites del tratamiento de datos biométricos de personas no condenadas. *Revista de Derecho Comunitario Europeo*, 13(33), 619–633.
- Izquierdo Carrasco, M. (2020). La utilización policial de los sistemas de reconocimiento facial automático. *IUS ET VERITAS*, (60), 86–103. <https://doi.org/10.18800/iusetveritas.202001.004>
- Loideain, N. N. (2024). Lawfulness and Police Use of Facial Recognition in the United Kingdom: Article 8 ECHR and Bridges v. South Wales Police. In R. Matulionyte & M. Zalnieriute (Eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (1st edn, pp. 155–172). Cambridge University Press. <https://doi.org/10.1017/9781009321211.014>

Suggested Fiction



Justicia Artificial



Mercy

Documentation – Portuguese/English

