AI and DEMOCRACY

PROFESSOR DOCTOR RAFAEL RUBIO (Speaker)

Bruno Pica (PhD Student / Discussant)

RESUME

1. AI is radically reshaping the foundations of democracy

Artificial Intelligence is transforming key democratic concepts, including legitimacy, freedom, equality, privacy, and participation. By shifting deliberative and decision-making processes to algorithms, it compromises citizens' autonomy and the role of democratically legitimized institutions.

2. Risk of algorithmic technocracy and erosion of accountability

Overreliance on automated decision-making risks creating a form of algorithmic technocratic governance, where political decisions are made according to opaque and barely auditable criteria. This undermines democratic accountability and the principle of separation of powers.

3. Manipulation, disinformation, and fragmentation of the public sphere

AI tools are increasingly used for microtargeting, deepfakes, and disinformation campaigns, which distort public debate. This contributes to social fragmentation and ideological polarisation, weakening the common ground required for democratic deliberation.

4. Algorithmic discrimination and rising inequality

Biases in training data lead to automated and often invisible discrimination, affecting fundamental rights such as non-discrimination, equal access to services, and fair electoral processes. These systems may reinforce historical injustices and structural inequality.

5. Impact on fundamental rights and the emergence of neuro-rights

AI challenges traditional rights, such as privacy, data protection, and freedom of expression, and requires the recognition of new rights, like neuro-rights, to protect mental integrity, cognitive freedom, and protection against algorithmic manipulation.

6. The need for a new constitutional and regulatory framework

There is a growing need to "constitutionalise the algorithm", meaning to adapt democratic institutions and legal guarantees to the digital age. This entails risk-based regulation, fundamental rights impact assessments, and ethical governance of AI, both nationally and internationally.

QUESTIONS

1)You start your presentation referring to a famous sentence: *"If you are interested in democracy and its future, you had better understand computers", Ted Nelson, 1974 (Slide N. º 1).*

This aligns with a recent statement by Miguel Carvalho, President of Startup Portugal, who remarked that in the future, "people will not be replaced by computers, but by people who understand how AI works." This leads me to believe that the real threat does not lie in the technology itself, but in how it is used—or not used—by individuals and institutions. The transformative power of AI seems inevitable. It resembles a massive wave: either we are prepared to surf it, or we risk being overwhelmed—our metaphorical boat flooding and ultimately sinking.

In your view, what constitutes the greatest risk that AI poses to democratic systems: the lack of regulation, the lack of education, or digital illiteracy? Or anything else that could have more influence?

2) "*The relationship between AI and democracy must be prudent and responsible, considering the advances that can be made when it is placed at the service of the logic of political representation, where the free and sovereign will of citizens is reflected through their representatives. AI can impact the exercise of fundamental rights, such as privacy, data protection, equality, non-discrimination, effective judicial protection, and the right to vote —pillars on which democracy is built. Legal requirements for the design, development, and use of AI systems* ***must be proportionate*** *to the nature of the risks they pose to human rights, democracy, and the rule of law." (Slide N. º 13)*.

"In your opinion, how can this delicate balance be safeguarded, and which actors or institutions are best positioned to assume that responsibility?"

AI & Politic & Cyber & Technopolarity

PROFESSOR DOCTOR FILIPE DOMINGUES (Speaker)

Bruno Pica (PhD Student / Discussant)

RESUME

1. The convergence of geopolitics and cyberspace is reshaping global power dynamics

Cyberspace has become a new arena for power struggles, where state-sponsored actors, cyber mercenaries, and hacktivists operate not for profit but for geopolitical, ideological, or strategic gains. The traditional separation between political, military, and digital domains is dissolving.

2. Cybercrime is now a global parallel economy

Cybercrime has surpassed natural disasters in global economic impact and is now more profitable than the global drug trade. Despite growing investments in cybersecurity, authorities remain on the defensive. The cybercrime ecosystem thrives in complexity, speed, and legal ambiguity.

3. Cyberwarfare is cheap, versatile, and legally unregulated

Cyber operations are increasingly used for espionage, industrial sabotage, political influence, sanctions evasion, and attacks on critical infrastructure. These tactics are low-cost, anonymous, and difficult to trace, blurring the lines between warfare, sabotage, and psychological operations.

4. Europe leads in regulation, but lacks global enforceability

The EU has developed one of the most advanced digital regulatory frameworks (AI Act, Cybersecurity Act, NIS2, etc.), but no binding global framework exists. Regional conventions, such as the Budapest or Malabo Conventions, are limited in scope and enforcement.

5. Technopolarity: Big Tech rivals the power of sovereign states

We are entering a technopolar world, where power stems not from territory or military force, but from control over data, servers, and algorithms. Tech corporations wield transnational influence without democratic accountability, reshaping sovereignty in the digital era.

6. AI-powered disinformation is the main threat to democracy

Generative AI has turbocharged the production of deepfakes and persuasive disinformation, enabling foreign adversaries and domestic actors to influence elections, fragment public opinion, and undermine trust in democratic institutions at an unprecedented scale.

QUESTIONS

1) In recent years, cyberspace has become an increasingly strategic domain of competition, where geopolitical interests intersect with digital infrastructures. As state and non-state actors exploit cyber capabilities to influence political, military, and societal outcomes, the motivations behind cyber operations are shifting. No longer driven primarily by profit or criminal intent, many of today's cyber threats are rooted in power dynamics and strategic calculations. This convergence between geopolitics and cyberspace marks a profound transformation in international security, demanding new frameworks for understanding, resilience, and response, particularly in the context of the European Union's pursuit of digital sovereignty and strategic autonomy.

"How is the growing convergence between cyberspace and geopolitics transforming the motivations behind cyber threats, shifting from economic gain to strategic power, and what are the implications of this transition for national security and the European Union's strategic autonomy?"

2) The global distribution of power is no longer shaped solely by states, alliances, or conventional military capabilities. In the emerging digital order, a new form of polarity is emerging — **Technopolarity** — where global technology platforms wield disproportionate influence over public discourse, critical infrastructure, and even democratic processes. These actors, often operating beyond the reach of national jurisdictions, are reshaping the boundaries of authority and accountability. As a result, traditional state-centric models of governance are increasingly challenged, raising urgent questions about how democracies can preserve their sovereignty, uphold the rule of law, and ensure that technological development aligns with public interest and democratic values.

"To what extent does Technopolarity, the concentration of geopolitical influence in global tech platforms, challenge the traditional role of the state in regulating power, and how should democracies respond to ensure technological sovereignty and democratic resilience?"

.