



anove



Complex A.I. regulations across major global powers

Jean-Hugues Migeon



Jean-Hugues Migeon

- CTO and Founder of Anove international
- Data Protection Specialist at European Space Agency
- Former Security and Privacy Officer at ON2IT
- Former Security and Privacy Officer at NN (Listed AEX)





Agenda

Europe

Pioneering in data regulation and A.I. governance

- **Horizontal Regulation** (E.U. A.I. Act, Digital Markets Act and Digital Services Act)
- Focus on competition and interoperability
- Achieve digital sovereignty (European Chips Act)
- Ensure international companies comply with E.U. regulations

U.S.

Laissez-Faire approach to A.I. and Data regulation

- **State-Level Regulation** No comprehensive federal legislation
- Focus on innovation and industrial and private sector control
- Strong restrictions on external companies to favor national companies
- Concerned by Facial Recognition Technologies due to racial bias and concerns over accuracy

China

Centralized approach to ensure National Security

- **Centralized legislation** as early as 2017 with the National A.I. Strategy and PIPL (Chinese GDPR) in 2021
- Positioning of major tech companies as central (Baidu, Alibaba, Huawei)
- Accountability of companies on content moderation and algorithmic recommendation
- Extensive use of Facial Recognition for public surveillance



Impact of Artificial Intelligence

175 Zettabytes

Volume of data produced in the world by 2025 (33 ZB in 2018)

11-37%

Increase in labour productivity

14%

Jobs replaced by AI

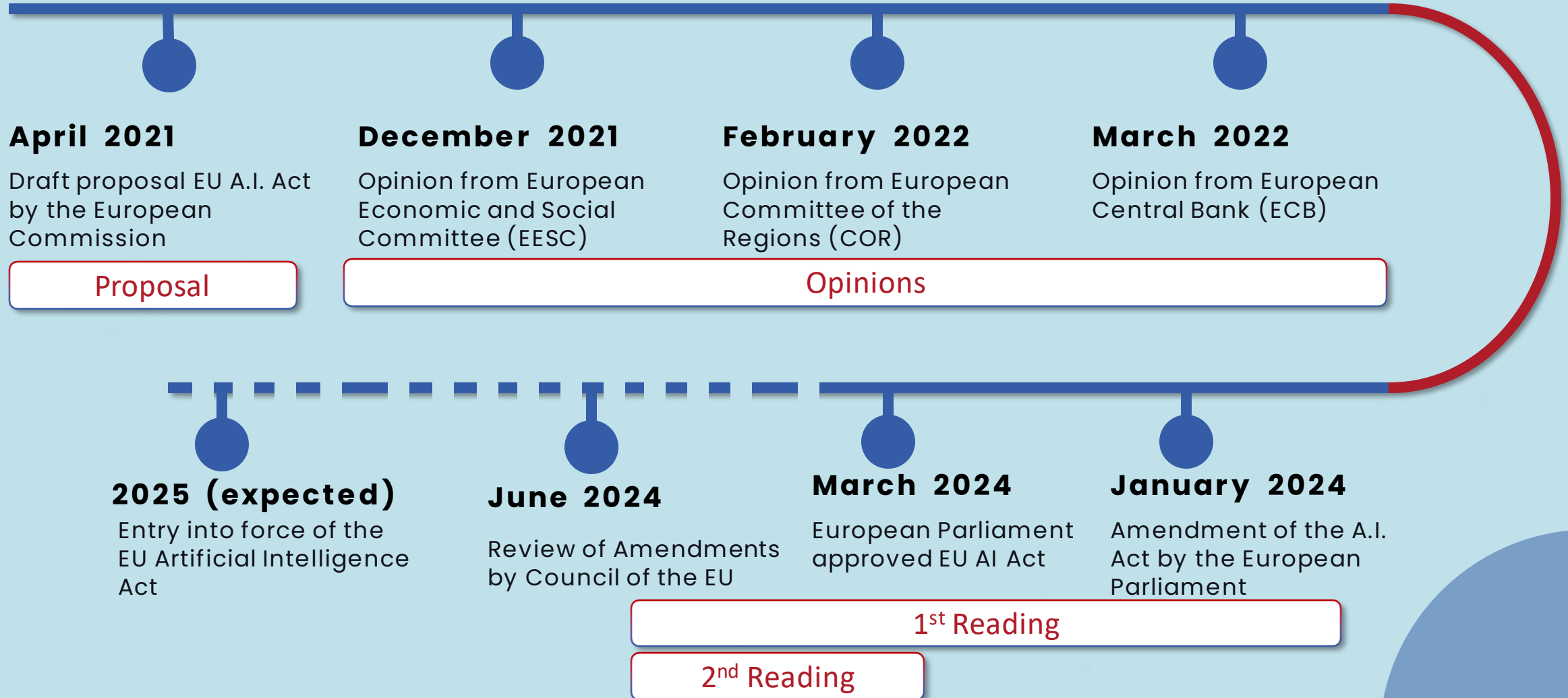
32%

Jobs facing substantial changes

01

**A.I. Legislation in
Europe**

EU AI Act : Where do we stand?





EU AI Act: 12 Key facts

1. Broad definition

4. Broad, burdensome and extensive obligations for high-risk AI systems

7. Special measures for banks, insurers, governments

10. Distinctions for General purpose AI (GPAI)

2. List of prohibited AI practices

5. Obligations throughout the value chain

8. Right to an explanation VS Trade secrets

11. Complex and layered compliance (AI Board, AI Office, national authorities)

3. High risk AI systems

6. Obligations for users of high risk AI systems

9. Lower threshold for Data Subject Rights

12. Very high fines



Digital Markets Act

Establish requirements applicable to **largest tech providers** (called « gatekeepers ») in the EU in order to reduce the bottlenecks and prevent monopolizing the digital economy

Gatekeepers must:

- Perform independent audits on user profiling methods
- Provide public description of audit and update it annually
- Provide access to Business users to their generated data
- Provide companies that advertiser independent verification of data
- Allow Business users to promote and complete contracts outside their platform

Gatekeepers must not:

- Treat their own services or products more favorably than competitors
- Prevent customers from reaching out to businesses outside their platform
- Prevent users from uninstalling pre-installed software and apps
- Track users outside their core platform for targeted advertising without effective consent

Google

Google
Google Android
Google Search
Chrome
YouTube
Google Maps
Google Play
Google Shopping

Meta

Facebook
Instagram
WhatsApp
Messenger
Meta
(advertisement)
Meta Marketplace

ByteDance

TikTok

Amazon

Amazon
Amazon Marketplace

Apple

App Store
Safari
iOS

Microsoft

LinkedIn
Windows PC OS



Digital Services Act

- Cross-sector legislation focusing on more **transparency**, **algorithmic accountability** and **content moderation**.
- Applies to hosting services, marketplaces, and online platforms offering services in the EU.

Risk assessments must be accompanied by reasonable and effective mitigation measures

Art. 34

Perform risk assessments annually or when introducing new relevant functionalities to pinpoint systemic risks.

Art. 35

Art. 37

VLOPs are required to complete and provide yearly audits conducted by independent third parties.



Other regulations and impactful entities

Existing legislation

Future legislation

Political agendas

GDPR

**Data Protection
Authorities (CNIL)**

**AI Liability
Directive**

**Product Liability
Directive**

**National strategies
(France, Germany,
Italy, Netherlands)**

02

**A.I. Regulations in the
U.S.**



AI regulation in the US

Federal level

State level

Federal level

**« SAFE »
framework**

**U.S. Blueprint
for AI Bill of
Rights**

**A.I. Executive
Order**

NIST AI RMF

**Existing
federal
agencies**

State level

**Sector specific :
Insurance**

**Sector specific :
Intellectual
property**

**Sector specific :
Privacy**

**Sector specific :
Employment**

Comprehensive state law (Automated decision-making)



AI regulation in the US

Federal level

**« SAFE »
framework**

**U.S. Blueprint
for AI Bill of
Rights**

**A.I. Executive
Order**

NIST AI RMF

**Existing
federal
agencies**



SAFE Framework

- Proposed by Senator Chuck Schumer (Democrat) in June 2023
- Mainly preparing a political agenda
- No public report of progress

Main proposals:

- Label AI products as distinct from human-originated work
- Regulation of foundation models

SCHUMER'S SAFE Innovation Framework

Since a major national workshop in 1956, artificial intelligence's (AI) potential has been clear. Today, that potential has become a reality: the AI age is here and here to stay.

The full potential of AI to benefit society is vast, and it is likely to be among the most consequential inventions in human history. Already, breakthroughs are happening all around us, from helping develop incredible new materials to synthesizing life-saving medications. But this potential for societal benefits comes with the risk of societal harms: significant job displacement, misuse by our adversaries and other bad actors, supercharged disinformation, and the amplification of bias are among the pressing concerns. For instance, while the defense and intelligence applications of AI will help tackle challenging national security threats, it may also present new risks. Concurrently, the rapid pace at which AI is advancing presents unique challenges. The 'black box' of AI systems and its ever-expanding use cases demand we invest in the research and innovation necessary to better understand how these systems work and how we can harness their potential for good. With so much potential, the U.S. must lead in innovation and write the rules of the road on AI and not let adversaries like the Chinese Communist Party craft the standards for a technology set to become as transformative as electricity.

Therefore, I am developing a policy response that invests in American ingenuity; solidifies American innovation leadership; protects and supports our workforce; enhances our national security; and ensures AI is developed and deployed in a responsible and transparent manner.

The central policy objectives of my SAFE Innovation Framework are:

1. **Security:** Safeguard our national security with AI and determine how adversaries use it, and ensure economic security for workers by mitigating and responding to job loss;
2. **Accountability:** Support the deployment of responsible systems to address concerns around misinformation and bias, support our creators by addressing copyright concerns, protect intellectual property, and address liability;
3. **Foundations:** Require that AI systems align with our democratic values at their core, protect our elections, promote AI's societal benefits while avoiding the potential harms, and stop the Chinese Government from writing the rules of the road on AI;
4. **Explain:** Determine what information the federal government needs from AI developers and deployers to be a better steward of the public good, and what information the public needs to know about an AI system, data, or content.
5. **Innovation:** Support US-led innovation in AI technologies – including innovation in security, transparency and accountability – that focuses on unlocking the immense potential of AI and maintaining U.S. leadership in the technology.

These policy objectives are at the center of my work on AI, but this is not a comprehensive list of the multitude of opportunities and challenges we face. To address the spectrum of AI topics, I have convened an all-hands-on-deck effort in the Senate, with committees developing bipartisan legislation, and a bipartisan gang of non-committee chairs working to further develop the Senate's policy response. We must approach AI with the urgency and humility it deserves.



U.S. Blueprint for an AI Bill of Rights

- Blueprint AI Bill of Rights to guide, design, deploy and develop AI systems.
- Voluntarily applied by AI providers

Safe and effective systems

Algorithmic discrimination protection

Data privacy

Notice & explanation

Human alternatives, consideration & fallback



White House AI Executive Order

- Published in November 2023
- Direct federal agencies to develop guidance on the use Artificial intelligence

Main new development:

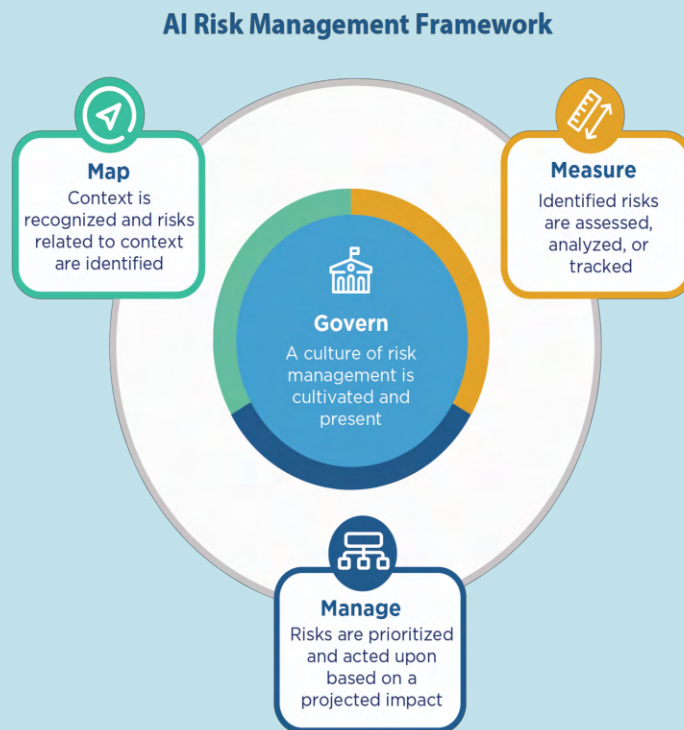
- Reporting requirements for AI companies
- New standards and labelling of AI content
- Cybersecurity program to develop AI tools





U.S. NIST AI Risk Management Framework (AI RMF)

- In line with Executive Orders 13960 (2020) and 14110 (2023)
- The AI RMF sets 72 measures to implement to address AI





Multiple supervisory authorities

Federal Trade Commission

Office of Technology (2023)
Civil Investigative Demands on AI

Joint statement of Agencies

Department of Justice (DOJ)
Federal Trade Commission (FTC)
Consumer Financial Protection Bureau (CFPB)
Equal Employment Opportunity Commission (EEOC)

Securities and Exchange Commission (SEC)

AI in Finance sector

Health and Human Services (HHS)

U.S. Department issued rule regarding AI in healthcare



AI regulation in the US (Local)

State level

**Sector specific :
Insurance**

**Sector specific :
Intellectual
property**

**Sector specific :
Privacy**

**Sector specific :
Employment**

Comprehensive state law (Automated decision-making)

03

**A.I. Regulations in
China**



China's Deep Synthesis Provisions

Came into effect in January 2023, the **regulation applies to both « deep synthesis service providers »**; companies offering AI services and those providing technical support and **« deep synthesis service users »**; organizations and people utilizing AI services to create, duplicate, publish or transfer information.

Data security & personal data protection

- Current Data protection laws apply
- Required to establish management systems for algorithm review, user, registration, and child protection among others

Transparency

- Establish guidelines, criteria and processes to recognise false or damaging information
- Form and disclose management rules, platform conventions
- Must implement real identity information authentication system

Content management & labelling

- Required to dispel fake news, keep records and report these instances to the relevant authorities.

Technical security

- Must periodically review algorithms and conduct security assessment when providing models, templates, and other tools.



AI legislation at glance : China

15/08/2023: Interim Measures for Generative Artificial Intelligence Service Management

- Generative AI must adhere to the core socialist values of China and should not endanger national security or interests or promote discrimination and other violence or misinformation
- Measures should be taken to prevent discrimination on ethnicity, belief, nationality, region, gender, age, occupation, and health resulting from generative AI
- Generative AI must respect intellectual property rights and business ethics to avoid unfair competition and the sharing of business secrets
- Generative AI must respect the rights of others and not endanger the physical or mental health of others
- Measures must be taken to improve transparency, accuracy, and reliability

10/01/2023: Deep Synthesis Provisions

The provisions apply to both « **deep synthesis service providers** » (companies that offer deep synthesis services and those that provide them with technical support) and « **deep synthesis service users** » (organizations and people that utilize deep synthesis to create, duplicate, publish or transfer information).

→ Strong emphasis on deepfake

01/11/2022: Shenzhen AI Regulation (local)

01/10/2022: Shanghai Regulations on Promoting the Development of the AI Industry (local)

01/03/2022: Internet information Service Algorithmic Recommendation Management Provisions

Providers of AI-based personalized recommendations in mobile applications must uphold user rights. In particular, providers must:

- Protect minors from harm
- Allow users to select and delete tags about their personal characteristics
- Not offer different pricing based on personal characteristics collected
- Notify users if a recommendation was made using an algorithm
- Give users the option to opt out



Conclusions



Impact

**Internal audits
(annual)**

**Publication of
audit results to
users/customers
(annual)**

**Ensure the exercise
of the Rights of
individuals**

**3rd Party audits
(annual)**

**Information about
the use of AI and
Transparency on
its impact**

**Processes for
Human
Intervention**

**Risk reports on the
use of A.I. to
Supervisory
Authorities**

**Transparency on
which Foundation
Models are used**

**A.I. Risk
Management
Framework
Requirements**



General risks (focusing on A.I.)

Loss of jobs because of higher automation

Algorithmic bias caused by bad data

Unclear legal regulation

Misalignment between the organisation's goals and AI's goals

Lack of transparency in the use of Foundation models

Program bias due to malicious (in-house) developers

Loss of control in the decision-making process

Violation of Privacy of employees (unproper data collection)

Violation of Privacy of customers (unproper data collection)

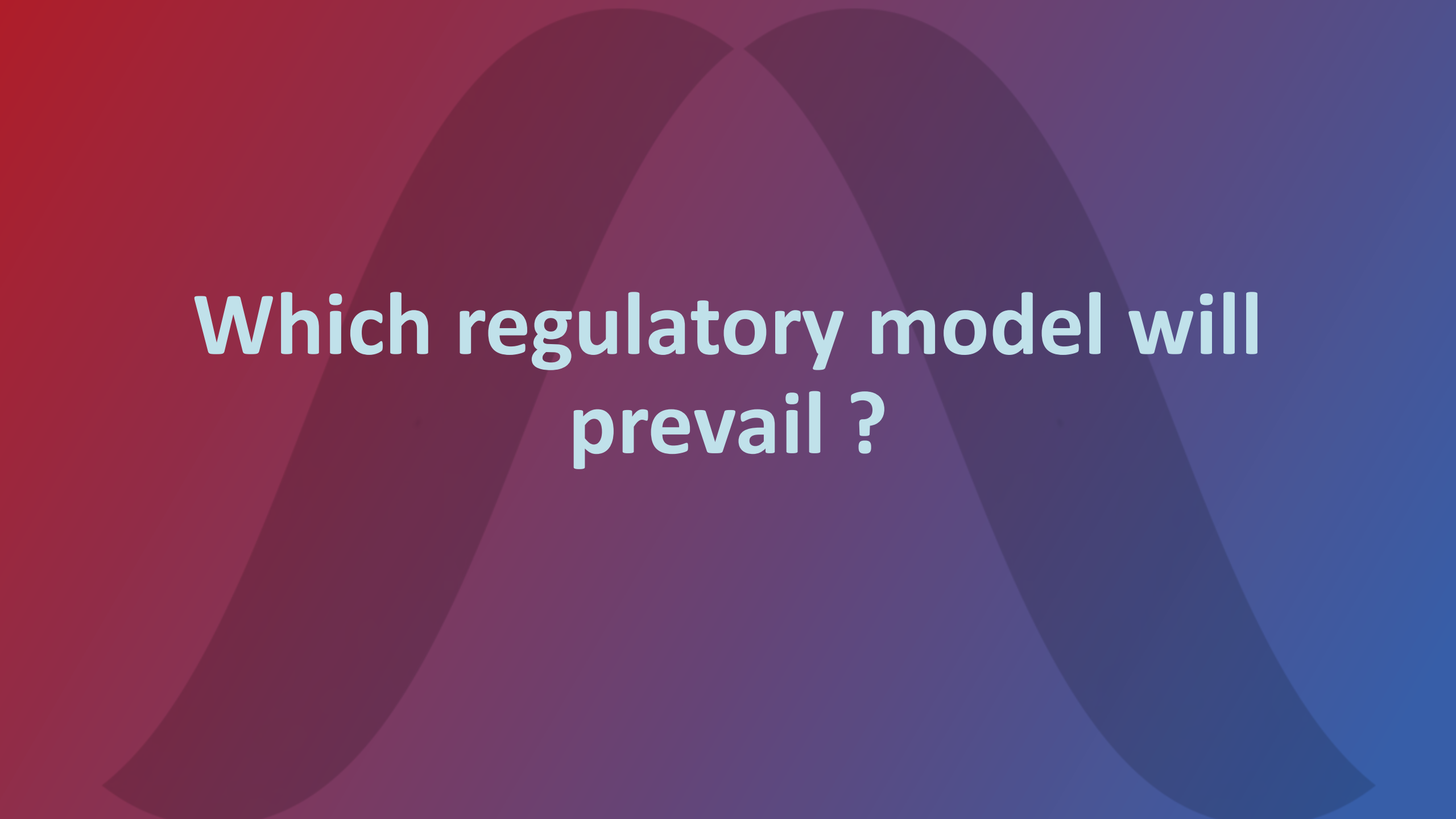
Fines for Non-compliance

External malicious actors using AI to access systems (Worm GPT, DarkBERT)

Evolved Social Engineering (Deepfakes, behavioural analytics)

Lack of transparency

Inaccuracy of data generated by AI

The background features a color gradient from dark red on the left to dark blue on the right. Two large, overlapping arches are centered horizontally. The left arch is a dark red color, and the right arch is a dark blue color. They overlap in the center, creating a purple hue.

**Which regulatory model will
prevail ?**



Questions & Answers

Thank you

For more information

Contact us:

Jean-Hugues Migeon

Jean-
Hugues.Migeon@anove.agency

Anove.ai



anove