navel robotics

appliedAI institute for europe

AI Regulatory Sandbox

A regulatory tool to enable innovation in highly regulated areas?

DigiKon | 19. November 2024 | Bonn

A joint initiative

UNTERNEHMER TUM

IPAI

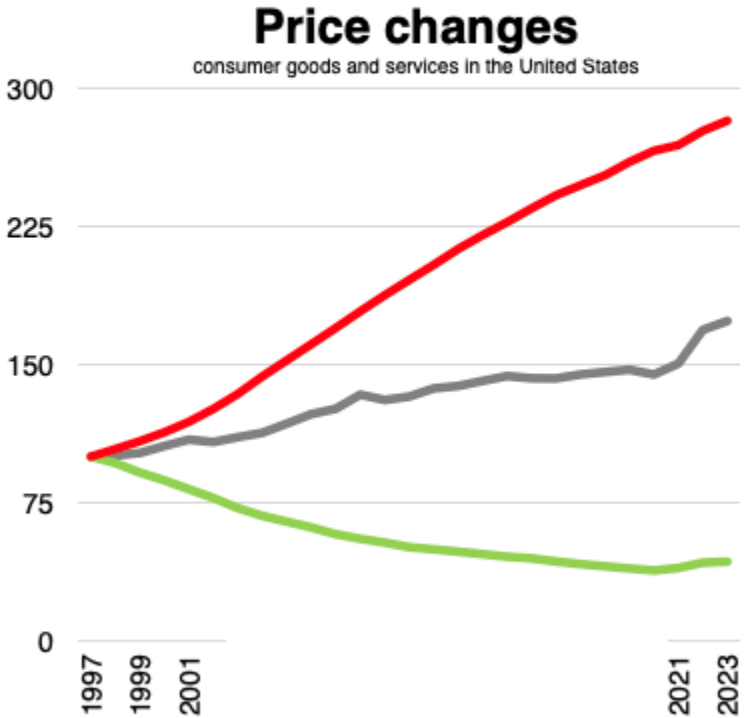
robotic beings you want to be with

for social care

Philipp Schwarz
COO

navel
robotics

Baumolscher Kosteneffekt



Soziale Dienstleistung
(Bildung, Pflege, Psychologie)

nicht automatisiert

Lifestyle
(Kleidung, Nahrung, Wohnen, Mobilität)

teilautomatisiert

Produkte
(computer, Autos, Spielzeug)

voll automatisiert

Pflegealltag

Einsamkeit
Apathie
Unruhe
...

Stress
Krankheit
Ausfälle
...


navel
robotics

Hohe Akzeptanz

Verbesserung des Wohlbefindens

Evangelische Heimstiftung
Institut für Pflege und Altern

Positiver kognitiver Effekt
(Demenz, Angstzustände,
Depression, Einsamkeit)

MHH Hannover Medical School

Langfristiges Engagement

Vorteile für Pflegekräfte

Technical University Munich

KOGNITIV
EMPATHISCHE DIALOGE

Dynamische, kontext-spezifische Prompts für **große Sprachmodelle (LLM)**

➔ soziales Verständnis

robotische Empathie

AFFEKTIV
NONVERBALE INTERAKTION

Maschinelles Sehen und Audioanalyse auf dem **Endgerät**

➔ geringe Latenz + hoher Datenschutz

How can an AI Regulatory Sandbox foster innovation?

A joint initiative

Daniel Düsentrieb is the innovative mastermind in Disney's Duckburg universe.

Claiming “U name it, I can make it,” he invented amazing things.

Painpoint in highly regulated areas | Innovators will be confronted with a Chain of Uncertainty when putting their AI System on the market

Legal Uncertainty

How to design a disruptive AI System in a compliant way?

Uncertainty about Regulatory Barrier

(i) Complex and Ambiguous Legal Language

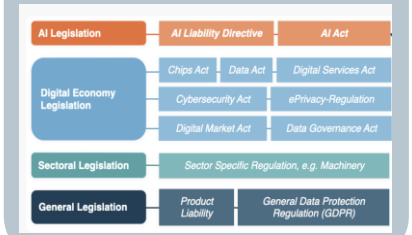
(ii) Overlapping Laws & Authorities

(iii) Emerging tech - gray areas between prohibited vs high-risk

Practical Uncertainty

How the AI Systems performs in practice aka in the “real-world”?

Regulatory Market Entry Restrictions



Supervisory Uncertainty

How will the supervisory authority react?

Pacing Problem & Regulatory Oversight

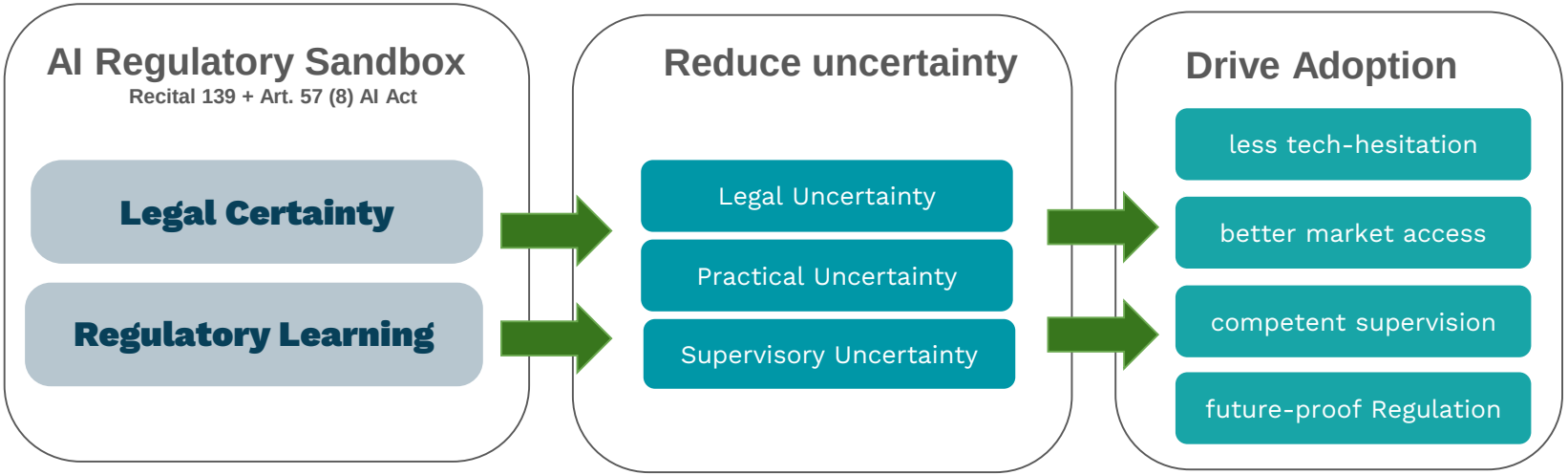
Regulation follows Tech. Most competent authorities:

(i) know less about the technology than the private sector

(ii) decide risk-averse (precautionary principle)

Why a Regulatory Sandbox for experimentation? | Regulatory Flexibility in highly regulated areas is a necessary pass-through status to enable testing under real-world conditions

Purpose of a Regulatory Sandbox | Combat “the uncertainties” and follow the explicit goal to enhance legal certainty and regulatory learning by allowing experimentation.



Take away: Outcome of an AI Regulatory Sandbox is the relief of the chain of uncertainty and thereby enabling Innovation and tech-competent supervision in a faster & safer fashion - which makes the EU market more competitive despite heavy regulation.

Practical Example for an AI Regulatory Sandbox under the AI Act.

appliedAI institute for europe

A joint initiative

UNTERNEHMER TUM

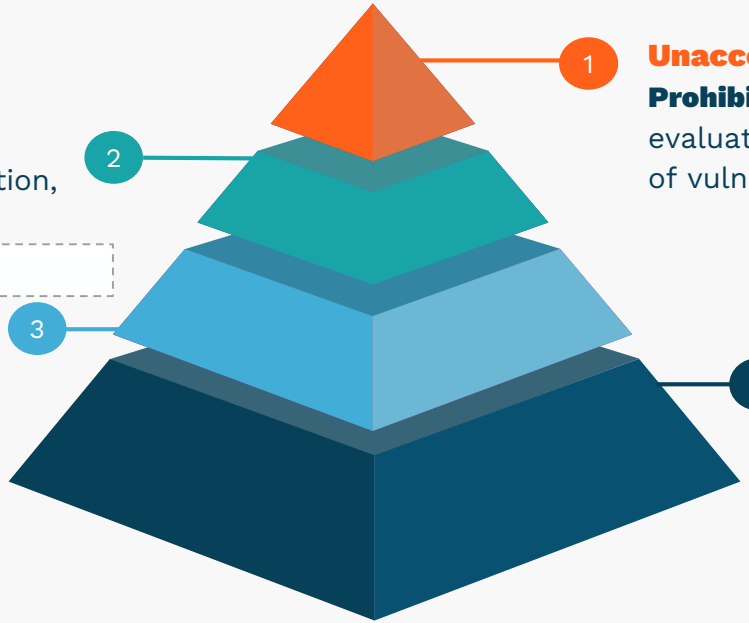
IPAI

Risk-based approach of the AI Act | Proportionality: the higher the risk of the intended use, the higher the requirements

High-Risk (Art. 6)
e.g. HR, medical devices, education, critical infrastructure

Not mutually exclusive

Limited-Risk (Art 50.)
E.g. Chatbots



Unacceptable-Risk (Art. 5)
Prohibited are, for example, social evaluation mechanisms or the exploitation of vulnerable groups

Minimal-Risk
All other AI Systems

Practical Example for an AI Regulatory Sandbox | Is the intended use of the AI System prohibited according to Article 5?

Prohibited AI System according to Article 5 (1) (f) + Recital 44?

the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

(+) Area of workplace = The elderly home where the social robot is put into service is the area of work of the caregivers.

(-) No exception applies = The intended use case is not falling under the exception of the Medical Devices or safety reasons.

Legal Disclaimer: We do not make any judgement about the classification of Navel, e.g. whether it is banned or not. Approval from navelrobotics to share provided. Any information is taken from the company's official website: https://navelrobotics.com/en/home-en-2/

Practical Example for an AI Regulatory Sandbox #1 | Is the intended use of the AI System prohibited according to Article 5?

Legal assessment addressing:

(i) Is emotion recognition within the intended use case really happening?

Recital 18: “emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. **It does not include physical states, such as pain or fatigue** … ”

“This does also not include the **mere detection of readily apparent expressions, gestures or movements** … such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person’s voice, such as a raised voice or whispering.”

Legal Disclaimer: We do not make any judgement about the classification of Navel, e.g. whether it is banned or not. Approval from navelrobotics to share provided. Any information is taken from the company's official website: https://navelrobotics.com/en/home-en-2/

Practical Example for an AI Regulatory Sandbox #2| Is the intended use of the AI System prohibited according to Article 5?

Legal assessment addressing:

(ii) Is there a concept of design to not fall into the workplace case?

What about a technical opt-out Design:

Caregivers opting out would undergo an enrollment process where their biometric data is securely registered. For example:

- Facial scan for facial recognition.
- Voice sample for voice recognition.

Result: As relief caregivers are not subject of any emotion recognition, Article 5 of emotion recognition is not applicable?

Legal Disclaimer: We do not make any judgement about the classification of Navel, e.g. whether it is banned or not. Approval from navelrobotics to share provided. Any information is taken from the company's official website: https://navelrobotics.com/en/home-en-2/

appliedAI institute for europe

There are practical challenges for effective AI Regulatory Sandboxes!

A joint initiative

UNTERNEHMER TUM | IPAI

Practical challenge#1 | The challenge of operating an effective cross-sectoral AI Regulatory Sandbox

The Situation

Establishing Authority operating the RSB has to take care off:

(i) Building up the infrastructure & governance

(ii) Gaining Technical & Legal know-how (Expert-Pools)

(iii) Handling Overlapping Laws & Competent Authorities

(iv) Ensuring Experimentation Clauses

The Challenge

Existing

“sectoral/traditional” Regulatory Sandbox
E. g. Drone Delivery, cars
> relax sectoral law

Planned

“AI Act” Regulatory Sandbox
E. g. any sector in Annex I + Annex III
> relaxing AI Act alone is insufficient

Practical challenge#1 | The challenge of operating an effective cross-sectoral AI Regulatory Sandbox

For Discussion

Which competent authority operates the AI Regulatory Sandbox?

What about a coordinating administrative body organising subject/theme batches?

How to ensure (for each AI System) the needed sector expertise in an AI Regulatory Sandbox (with limited public resources)?

Recruited external expertise in a flexible manner (individual researchers, Universities etc)

Many national/EU sector laws miss experimentation clauses to offer Regulatory Flexibility.

We need more experimentation clauses in sector law(s)

Practical challenge#2 | Open communication of the lessons learned & best practices with the entire ecosystem is crucial

Public available Exit Reports are optional in the AI Act

Article 57 (8) The exit reports of the AI RSB are not mandatory to be made publicly available - just in case the participating Innovator and the National Establishing Authority explicitly agree aka opt-in.

... which is problematic, because ...

- AI RSB is paid with **taxpayer money**, so the wider society should benefit from it
- **Regulatory Arbitrage,** as participating Innovators have priority access aka lobbying
- **Scaling effect** is missing without making such learning available to everyone
- Risk of **unfair competition**, as beneficial treatment to a limited number of Innovators

Practical challenge#2 | Recommendation: Make any exit reports publicly available (with respect to IP + trade secrets), else there will be limited scaling effects

Norway Regulatory Sandbox Datalilsynet:

"Help Many By Helping One"*

Recommendation

The implementing Act (Article 58 (1) (a)) should recommend that national AI Regulatory Sandboxes should as eligibility criteria for entrance only accept innovators, if they explicitly agree upfront that their results and experiences are shared publicly via the single information platform - and shall provide a template for such publicly available exit reports.

*Source: https://www.datatilsynet.no/en/news/aktuelle-nyheter-2022/sandbox-forever/

Practical challenge#3 | The department operating AI Regulatory Sandbox should have some risk-appetite and trial & error mindset

> By virtue of its novelty, innovation always involves the unknown and is therefore inherently risky. Experimentation in an AI Regulatory Sandbox therefore requires a considered acceptance of trial and error.

Any questions?

Feedback?