

Bird & Bird & Artificial Intelligence: what's next

Telecompaper 19 January 2022

About us

Feyo Sickinghe

Principal Regulatory Counsel

The Netherlands/Brussels



Shima Abbady

Associate Data Protection & IT

The Netherlands



Programme

- 1 Key Elements of the proposal and timeline**
Feyo Sickinghe, principal regulatory counsel
- 2 AI liability, interplay with GDPR and ethics and fundamental rights**
Shima Abbady – attorney-at-law and PhD researcher
- 3 Questions and Answers**

Slides contain background material for later review

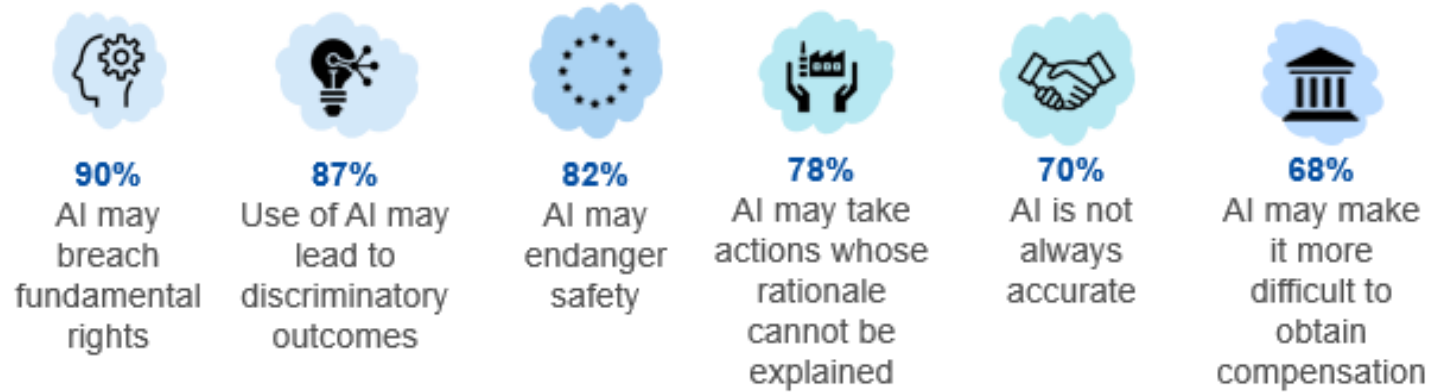


Is this a Rembrandt painting?



Public consultation on the AI White Paper

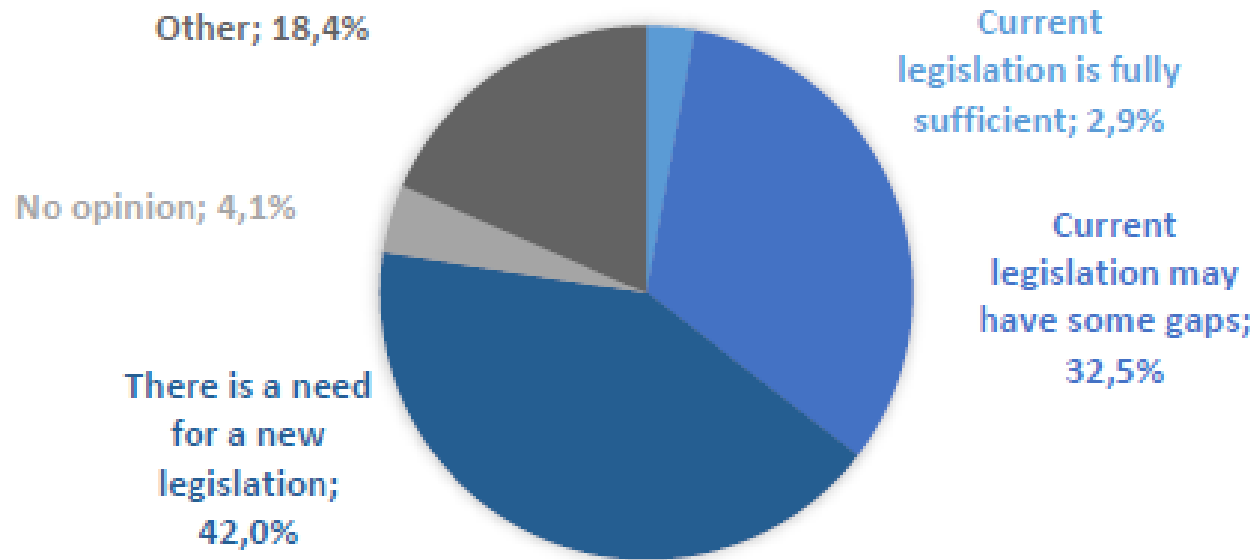
Concerns raised by respondents



Can these concerns be addressed by EU legislation?


Public consultation on the AI White Paper

Can these concerns be addressed by existing EU legislation?



France is building on Slovenian Efforts

	Council of the European Union
	Brussels, 29 November 2021 (OR. en)
<hr/> Interinstitutional File: 2021/0106(COD) <hr/>	14278/21
	LIMITE
	TELECOM 430 JAI 1288 COPEN 412 CYBER 307 DATAPROTECT 267 EJUSTICE 103 COSI 236 IXIM 262 ENFOPOL 465 FREMP 272 RELEX 1012 MI 879 COMPET 860 CODEC 1530
NOTE	
From:	Presidency
To:	Delegations
No. Cion doc.:	8115/20
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text
I. INTRODUCTION	
1.	The Commission adopted the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, AIA) on 21 April 2021.

	Council of the European Union
	Brussels, 13 January 2022 (OR. en)
<hr/> Interinstitutional File: 2021/0106(COD) <hr/>	5293/22
	LIMITE
	TELECOM 9 JAI 43 COPEN 13 CYBER 12 DATAPROTECT 5 EJUSTICE 2 COSI 11 IXIM 12 ENFOPOL 13 FREMP 8 RELEX 37 MI 26 COMPET 18 CODEC 37
NOTE	
From:	Presidency
To:	Delegations
No. Cion doc.:	8115/21
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text - Articles 8-15 and Annex IV
I. INTRODUCTION	
1.	The Commission adopted the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, AIA) on 21 April 2021.

What is an AI system

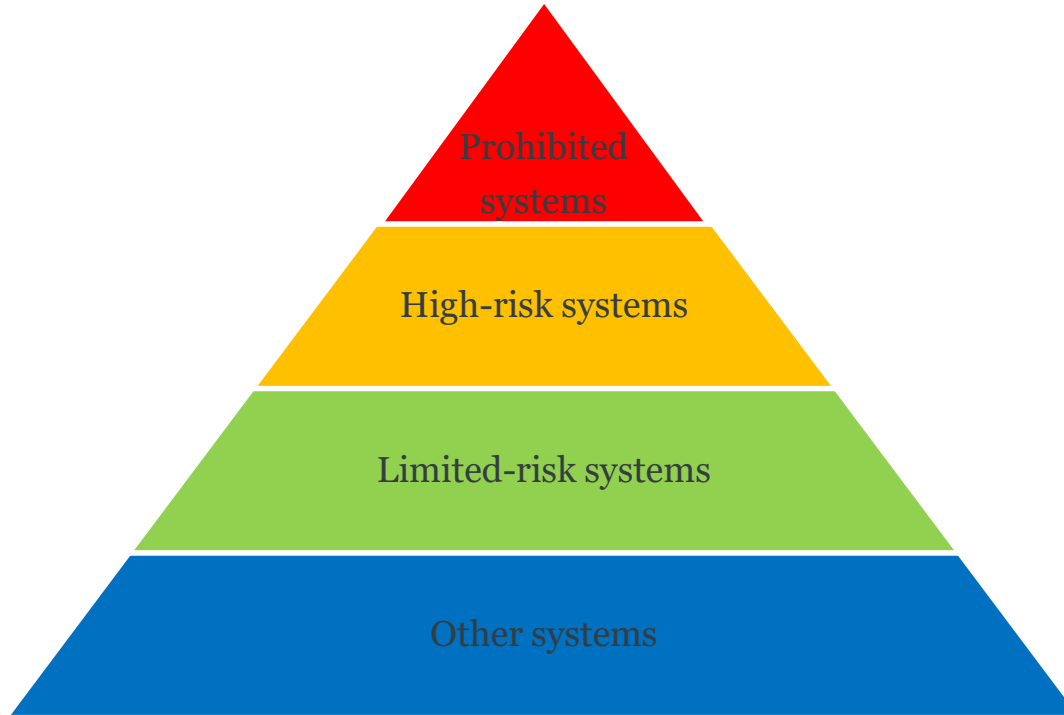
‘artificial intelligence system’ (AI system) means a system that

- (i) receives machine and/or human-based data and inputs,
- (ii) **infers how to achieve a given set of human-defined objectives using learning, reasoning or modelling** implemented with the techniques and approaches listed in Annex I, and
- (iii) generates outputs in the form of content (generative AI systems), predictions, recommendations or decisions, which influence the environments it interacts with;

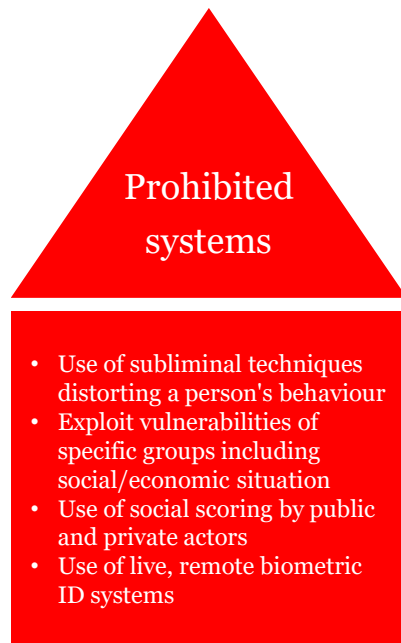
Annex I Techniques and approaches

- (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) Statistical approaches, Bayesian estimation, search and optimization methods.

Artificial Intelligence Pyramid



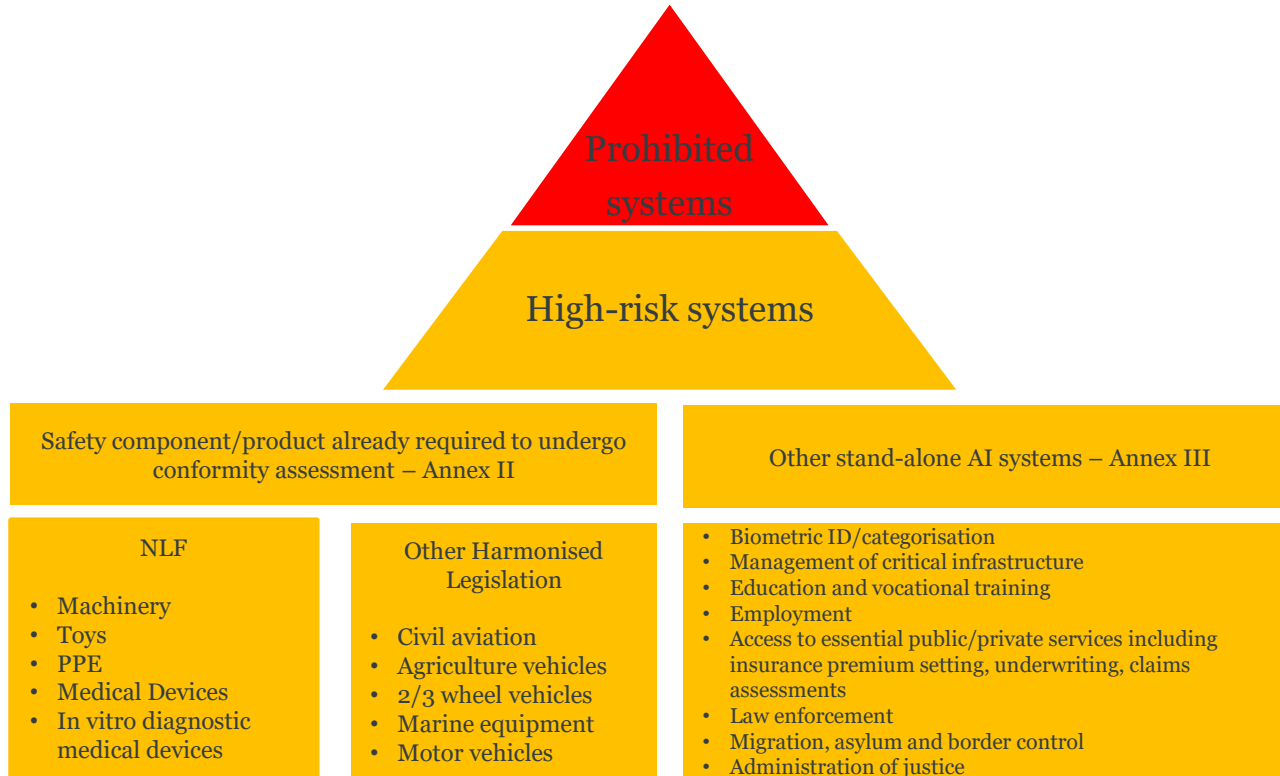
The Artificial Intelligence Pyramid



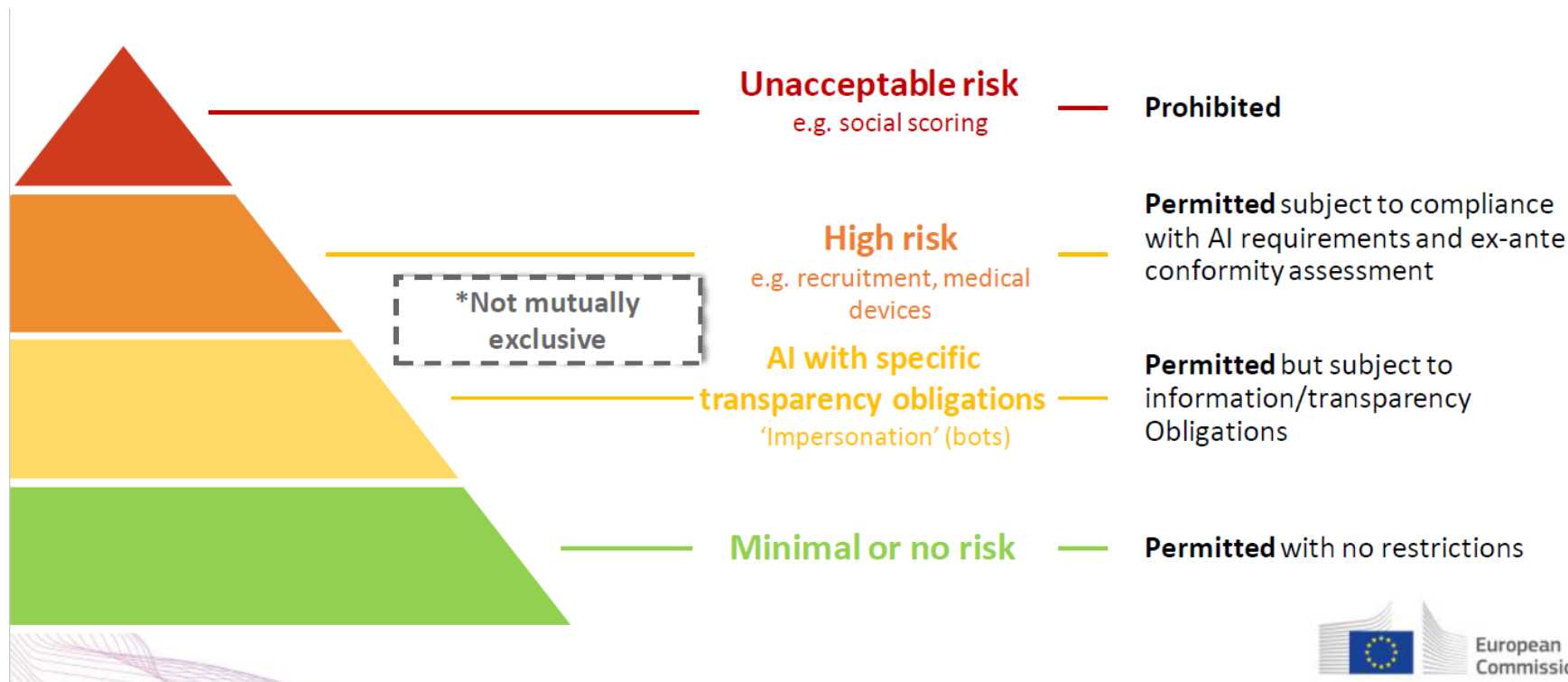
Prohibited AI systems

- **Subliminal techniques beyond a person's consciousness** to cause physical or psychological harm.
- Exploiting **vulnerabilities** of specific groups due to social or economic situation, age, physical or mental disability resulting in physical or psychological harm.
- **General purpose (social) scoring** leading to detrimental or unfavourable treatment by public and private actors
- **Real-time' remote biometric identification** for law enforcement purposes in publicly accessible spaces (not online spaces), with exceptions + authorisation (victims of crime, critical infrastructure, health, terrorist attacks, criminal offences).

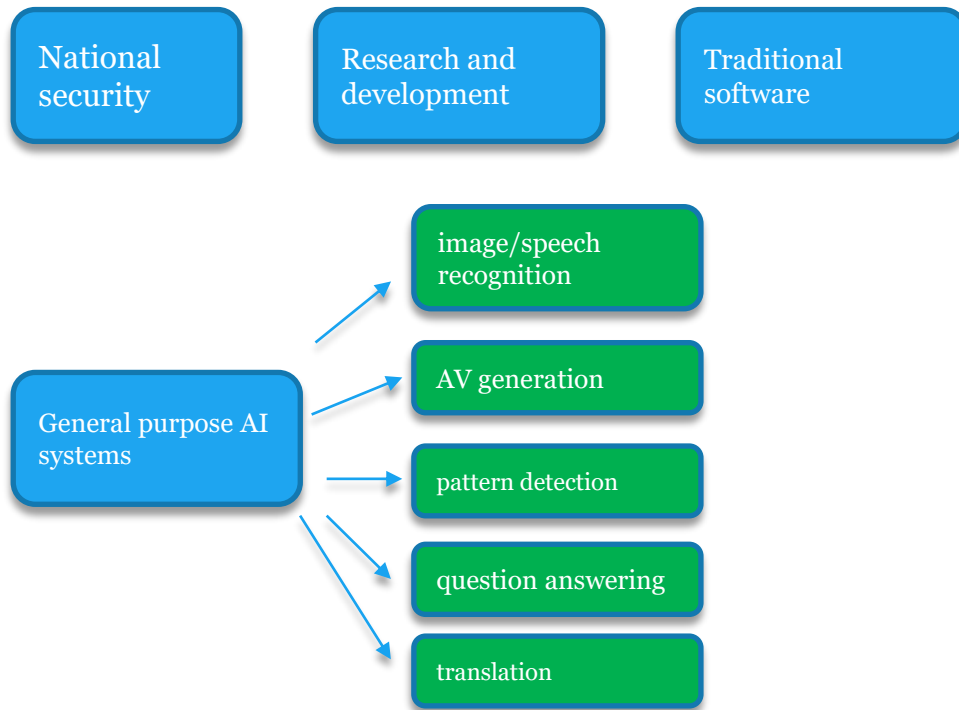
The Artificial Intelligence Pyramid



Risk-based approach (practical execution)



Out of Scope (Slovenian/French text)



Who does the regulation apply to?

Providers	Users	Providers and users
irrespective of whether established in the Union or a third country	located in the Union	located in a third country where the output of the AI system is used in the Union

High-risk AI systems

General requirements

- Establish, implement, document and maintain a **risk management system**;
- Quality and governance for **training, validation and testing data**;
- Up-to-date **technical documentation**;
- **Record-keeping and logging**;
- **Transparency** and provision of information to users;
- Ensure **human oversight** is built into system and/or implemented by users (prevent automation bias - over-relying on output)
- Ensure **accuracy, robustness and cybersecurity** of the system;
- 'conformity assessment' = the process of verifying whether the requirements relating to an AI system have been fulfilled.



What rules apply to high risk systems?

Risk management	Data governance	Technical documentation	Record-keeping	Transparency	Human oversight	Accuracy cybersecurity
<ul style="list-style-type: none"> Continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating Address foreseeable risks most likely to occur to health, safety and fundamental rights Risk minimisation Generally acknowledged state of the art including as reflected in relevant harmonised standards or common specifications Testing - prior to the placing on the market or the putting into service. Residual risk must be acceptable 	<ul style="list-style-type: none"> Data governance and management practices Examination in view of possible biases that are likely to affect health and safety of persons or lead to discrimination Training, validation and testing data sets Take into account geographical, behavioural or functional setting for intended use Data minimisation principle (GDPR) 	<ul style="list-style-type: none"> To be drawn up before that system is placed on the market or put into service Up to date Lighter SME regime 	<ul style="list-style-type: none"> Technically allow for the automatic recording of events ('logs') over the duration of the life cycle facilitation of post-market monitoring 	<ul style="list-style-type: none"> Operation to be sufficiently transparent (compliance) enabling users to understand and use the system appropriately instructions for use Additional transparency obligations apply for systems that (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content (deepfake) 	<ul style="list-style-type: none"> To be effectively overseen by natural persons Minimising the risks to health, safety or fundamental rights Understand the capacities and limitations Remain aware of the possible tendency of automatically relying or over-relying on the output (automation bias) Decision-making Interpretation Disregard, override or reverse output Intervention "stop" button Measures separately verified and confirmed by at least two natural persons 	<ul style="list-style-type: none"> Appropriate level of accuracy, robustness and cybersecurity Include measures to prevent poisoning of the training datasets Avoid input design to cause the model to make a mistake (adversarial examples) resilient as regards errors, faults or inconsistencies Technical redundancy Avoid feedback loops

Slide 17

Areas with high-risk AI systems (Annex III (art. 6))

Annex I point 8 of the RCE Directive (resilience of critical entities): Digital infrastructure

- Providers of Internet Exchange Points
- DNS service providers
- TLD name registries
- Providers of Cloud computing service
- Providers of Data centre service
- Providers of Content delivery networks
- Trust service providers
- Providers of public electronic communications networks and services

AI with specific transparency obligations

- Notify humans they are **interacting with** an AI system (e.g. chatbot) unless obvious.
- Notify humans that **emotional recognition or biometric categorisation systems** are applied.
- Label **deep fakes** (unless necessary for exercise of fundamental right/freedom or public interests).

Green category (most of AI)

- No mandatory requirements
- Commission and Artificial Intelligence Board shall encourage and facilitate drawing up **voluntary** codes of conduct

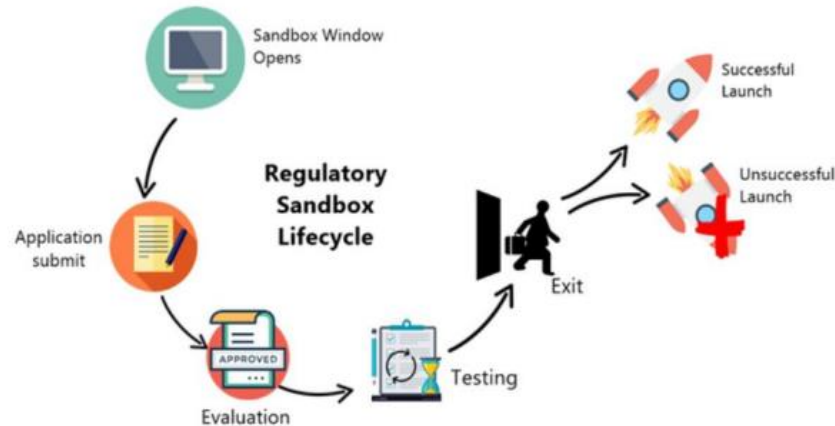


Broad space to develop artificial intelligence in all economic sectors

Regulatory sandboxes

Are not a free play ground...

- Controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market
- Under guidance of competent authority
- Participants in the AI regulatory sandbox shall remain liable
- Priority access for SMEs



Surveillance and governance

Ex ante and ex post control

(Mainly) ex-ante:

- **Notifying authorities** (assessment, designation and notification of conformity assessment bodies and for their monitoring).
- **Conformity assessment bodies** (shall submit an application for notification to the notifying authority).
- **Notified bodies** (verifying conformity high-risk AI system → issue certificates).

(Mainly) ex-post:

- **Market surveillance authorities** (national supervisory authorities carrying out activities/measures pursuant to Market Surveillance Regulation).
- **EDPS** acts as competent authority for Union institutions, agencies and bodies.
- **European Commission** (acting as Secretariat).
- **Artificial Intelligence Board** (composed of heads of national supervisory authorities).



Enforcement powers

Market surveillance authorities can:

- **Request access** to data and documentation (incl. source code) in order to **assess conformity**
- When sufficient reasons to consider that an AI system presents a **risk, evaluate the system**;
- **Require** the operator of systems which present a risk to take **all appropriate corrective actions** to bring the system into compliance/withdraw/recall;
- **Inform** the **Commission** and **other Member States** when it considers that non-compliance is not restricted to its national territory;
- **Take provisional measures** when the operator does not take adequate and timely corrective action.





(Dissuasive) penalties

Administrative fines of up to **EUR 30.000.000** or, if the offender is company, up to **6 % of its total worldwide annual turnover** for the preceding financial year, whichever is higher, if:

- a) non-compliance with regard to prohibited AI systems;
- b) non-compliance of the AI system with the requirements regarding data quality and data governance.

For violation of all other requirements: administrative fines of up to **20.000.000 EUR** or, if the offender is a company, **up to 4 %** of its total worldwide annual turnover for the preceding financial year, whichever is higher.

For the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request: administrative fines of up to **EUR 10.000.000** or, if the offender is company, up to **2 %** of its total worldwide annual turnover for the preceding financial year.

EDPS may impose administrative fines on Union institutions, agencies and bodies: **500 000/250 000 EUR**.

Emerging points of contention



- Ban on facial and emotion recognition & real-time biometric identification
- Deep fakes and enforcement: prohibit producing, offering, using and possessing deepfake technology for consumer markets
- Civil liability (European Commission consultation) & intellectual property rights
- **Extend list of high-risk uses to AI systems that pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence**
- High degree of industry selfassessment
- Quality of input data
- Multiple supervisory committees and authorities
- Regulatory sandboxes - no light touch for SMEs



Council of the
European Union

- **December 2021:** main takeaways from the first compromise text
 - Questions regarding definition of AI and scope
 - Prohibited AI practices
 - Classification and requirements for high-risk AI systems
 - Responsibilities of various actors in the AI value chain
 - Questions regarding compliance and enforcement
 - Interplay with other EU legislation



Other
EU bodies

- Critical opinions from European Data Protection Board (**EDPB**) and European Data Protection Supervisor (**EDPS**)
- Call for a **general ban on any use of AI for an automated recognition of human features in publicly accessible spaces**
- Ban recommended on **AI systems categorising individuals from biometrics into clusters**
- **ECB published an AI Opinion on 29 Dec 2021 regarding the prudential supervision of credit institutions.**
- ECB Opinion includes several **amendment proposals**

Consumer protection aspects

- Will use of biometric facial recognition in public spaces be completely banned?
 - Court orders for Clearview in France, UK, Australia
 - Human rights organization Council of Europe is calling to create the world's first legally binding treaty for artificial intelligence focused on risks relating to AI in law enforcement and public administration
- Should consumers have a complaints mechanism under the AI Act?
- Will the regulation contribute to or guard against unconscious bias?

2022 – the year of AI

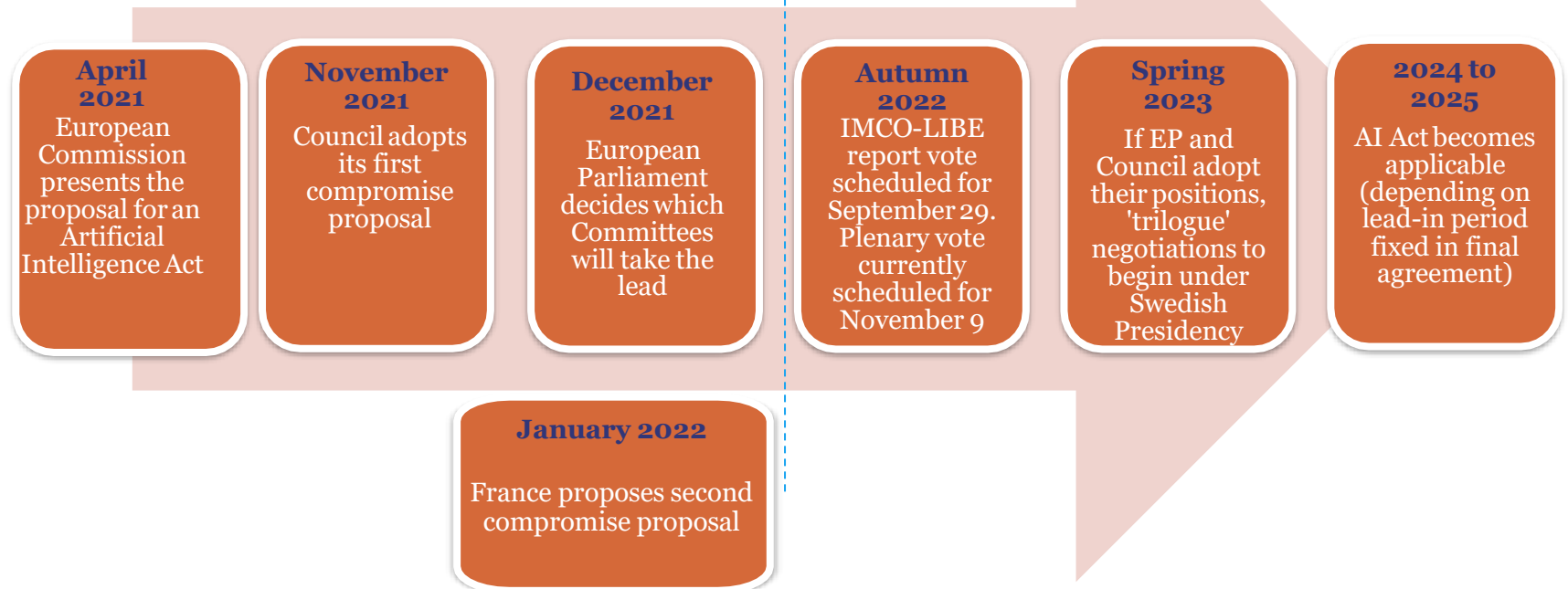
From soft law to regulation

Intelligence of Everything

Eliminate misuse

From data science to
common business tool

Prospective timeline



NL state of play

- NL in favour of Artificial Intelligence Act
- Privacy authority (AP) to become algorithm supervisor if personal data are involved
- AP also likely to be become AIA supervisory authority

AI and Data Protection/GDPR

AI Act and GDPR - purposes and background

- Intention: set the global standard!
- Stakeholders have warned the Commission to avoid duplication, conflicting obligations and overregulation
- AI Act aims to protect *inter alia* the right to data protection (Art. 8 Charter)
- AI Act is "without prejudice to and complements" the GDPR
- Overlap and similarities exist
- AI Act does not (generally) create a legal basis for processing



AI and liability –to sue or not to sue?

Existing liability framework

- Product Liability Directive 85/374/EEC & national liability regimes

Challenges:

- AI-systems may not qualify as 'products' and faults may not be 'defects'
- Unclear whether cyber vulnerabilities are covered
- Identification of procedure responsible
- Online market places fall outside scope of 'importers'
- Unclear who is liable at which stage of the life cycle
- Getting compensation is very difficult:
 - very heavy burden of proof;
 - fragmentation of liability rules;
 - only for material damage; and
 - minimum threshold for property damage of EUR 500
- NB: AIA does not create specific/extra options for redress



Timeline of developments

- November 2019: High Level Expert Group, Liability for AI and other emerging technologies
- 19 February 2020: Commission Report on Safety and liability implications of AI → >60% of respondents favoured revising Directive and/or adapting national liability rules
- October 2020: EU Parliament, Resolution on a civil liability regime (Regulation!)
- 30 June 2021: Inception impact assessment → No need for complete revision of the liability regime, but liability rules not fit for digital age



Future liability framework (Impact Assessment)

- High level of consumer/victim protection
- Modernise liability rules to take account of the characteristics and risks of new technologies
- Reduce obstacles to getting compensation for damage

Options

- Revise the Directive to extend strict liability rules to cover intangible products during entire lifecycle
- Allow for non-material damages claims
- Injured parties only have to prove that the damage emanates from the sphere of the operator/user of the AI-system
- Reduce obstacles to getting compensation: Alleviate or reverse the burden of proof, ease the conditions for making claims (time limits and EUR 500 minimum threshold for damage)
- Recommendations or legislative measures on harmonisation

Next steps

- Commission to provide feedback on public consultation (ended 10 January) Q3 2022

AI and fundamental rights

Fundamental Rights and Freedoms

(Potentially) impacted rights



- Right to liberty & security
- Right to fair trial
- Right to no punishment without law
- Right to freedom of expression
- Prohibition on discrimination
- Freedom of assembly and association
- Private life and physical and mental integrity (Privacy)
- Freedom of conscious/thought
- Social/economic rights (e.g. right to work)

Worried parties

- UNHCR: warning that right to privacy may be in danger
- Council of Europe: current human rights framework may not be sufficient and may have to be adapted or elaborated
- New digital human rights?



AI and ethics

Ethics guidelines High Level Expert Group EU



- Trustworthy AI =
 - Lawful;
 - Ethical;
 - Robust
- Key requirements for trustworthy AI: (1) *human agency and oversight*, (2) *technical robustness and safety*, (3) *privacy and data governance*, (4) *transparency*, (5) *diversity, non-discrimination and fairness*, (6) *environmental and societal well-being*, (7) *accountability*.
- Assessment List for Trustworthy AI

Other ethics guidelines

- Hot topic for EU, NGOs, governments, CoE and even private companies
- General agreement on:
 - Transparency (but how?)
 - Justice
 - Non-discrimination
 - Non-maleficence
 - Responsibility
 - Fairness
 - Privacy

However, **disagreement** between such instruments **on what should be done in practice**.

UNESCO AI Recommendation

Objectives

1. Create Universal framework of values (e.g. respect for fundamental rights, environment and diversity) and first global standard-setting instrument on the ethics of AI

2. Guide the actions of individuals, groups, communities, institutions and private sector companies

3. Protect, promote and respect human rights and fundamental freedoms

3. Foster multi-stakeholder, multidisciplinary and pluralistic dialogue and consensus building

4. Promote equitable access to developments and knowledge

Adopted by 193 countries on 25 November 2021

UNESCO AI Recommendation

Principles

- Proportionality and Do No Harm
- Safety and security
- Fairness and non-discrimination
- Sustainability
- Right to Privacy, and Data Protection
- Human oversight and determination
- Transparency and explainability; balance with privacy, safety and security
- Responsibility and accountability
- Awareness and literacy
- Multi-stakeholder and adaptive governance and collaboration

UNESCO AI Recommendation

1. Protecting data

- Individuals to have transparency, agency and control over their personal data (access and erasure)

2. Banning social scoring and mass surveillance

- Ban the use of AI systems for social scoring and mass surveillance
- AI technologies should not be given legal personality

3. Help to monitor and evaluate

- Ethical Impact Assessment: help countries and companies developing and deploying AI systems to assess the impact of those systems on individuals, on society and on the environment
- Readiness Assessment Methodology: helps Member States to assess how ready they are in terms of legal and technical infrastructure
- Independent AI Ethics Officer or some other mechanism to oversee auditing and continuous monitoring efforts

4. Protecting the environment

- Ensure that AI becomes a more prominent tool in the fight against climate change
- Asks governments to assess the direct and indirect environmental impact throughout the AI system life cycle
- Reduce the environmental impact of AI systems and data infrastructures.
- Governments to invest in green tech



***Sign up for Connected,**
our monthly round-up of
regulatory developments in
the field of technology,
communications and media*



Thank you & Bird & Bird

Feyo Sickinghe

feyo.sickinghe@twobirds.com

Shima Abbady

shima.abbady@twobirds.com

twobirds.com

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority (SRA) with SRA ID497264. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.