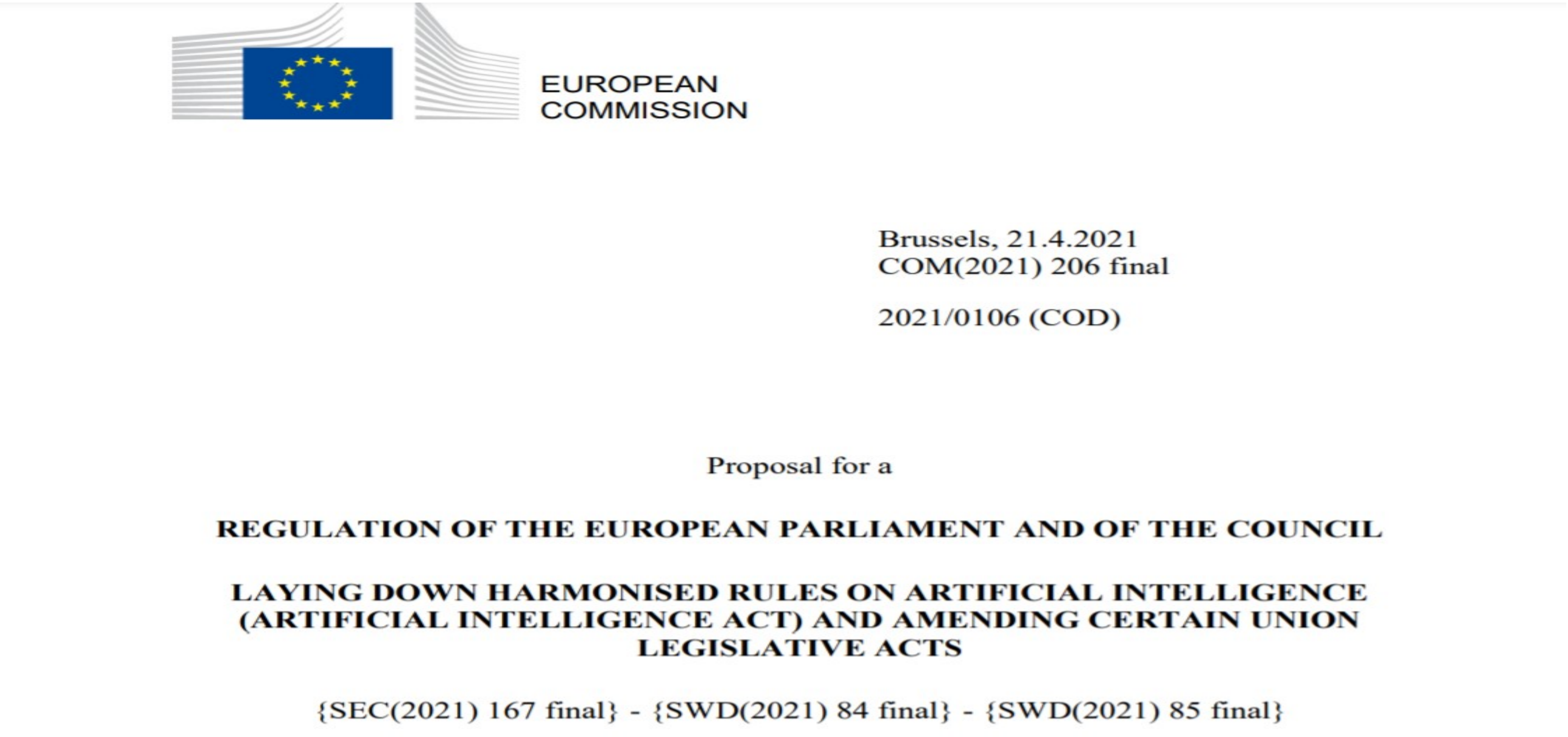
The future of AI in the EU: a preliminary analysis of the new proposal for a Regulation

Aliuska Duardo
Cátedra de Derecho y Genoma Humano. Facultad de Derecho
University of the Basque Country

he future of AI in the EU...



EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

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

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

he proposal: Rationale

ationale: protection of fundamental rights in the face of threats and risks linked to the development of A
ols/Strengthening innovation

orizontal regulatory framework – not limited to specific sectors – proportional response to risk

oncept of AI: broad definition, any software that is developed using one or more of the techniques anc
rategies listed in Annex I and that can, for a given set of objectives defined by human beings, generate
utput information such as content, predictions, recommendations or decisions that influence the
nvironments with which it interacts (Art. 3. I).

nnex I techniques and strategies: Machine learning strategies, including supervised, unsupervised anc
einforcement learning, which employ a wide variety of methods, including deep learning. Strategies basec
n logic and knowledge, especially the representation of knowledge, inductive programming (logic)
nowledge bases, inference and deduction engines, expert and (symbolic) reasoning systems. Statistica
rategies, Bayesian estimation, search methods and optimization

he proposal: Purpose

ormas armonizadas para la introducción en el mercado, la puesta en servicio y lización de sistemas de inteligencia artificial («sistemas de IA») en la n;

ohibiciones de determinadas prácticas de inteligencia artificial;

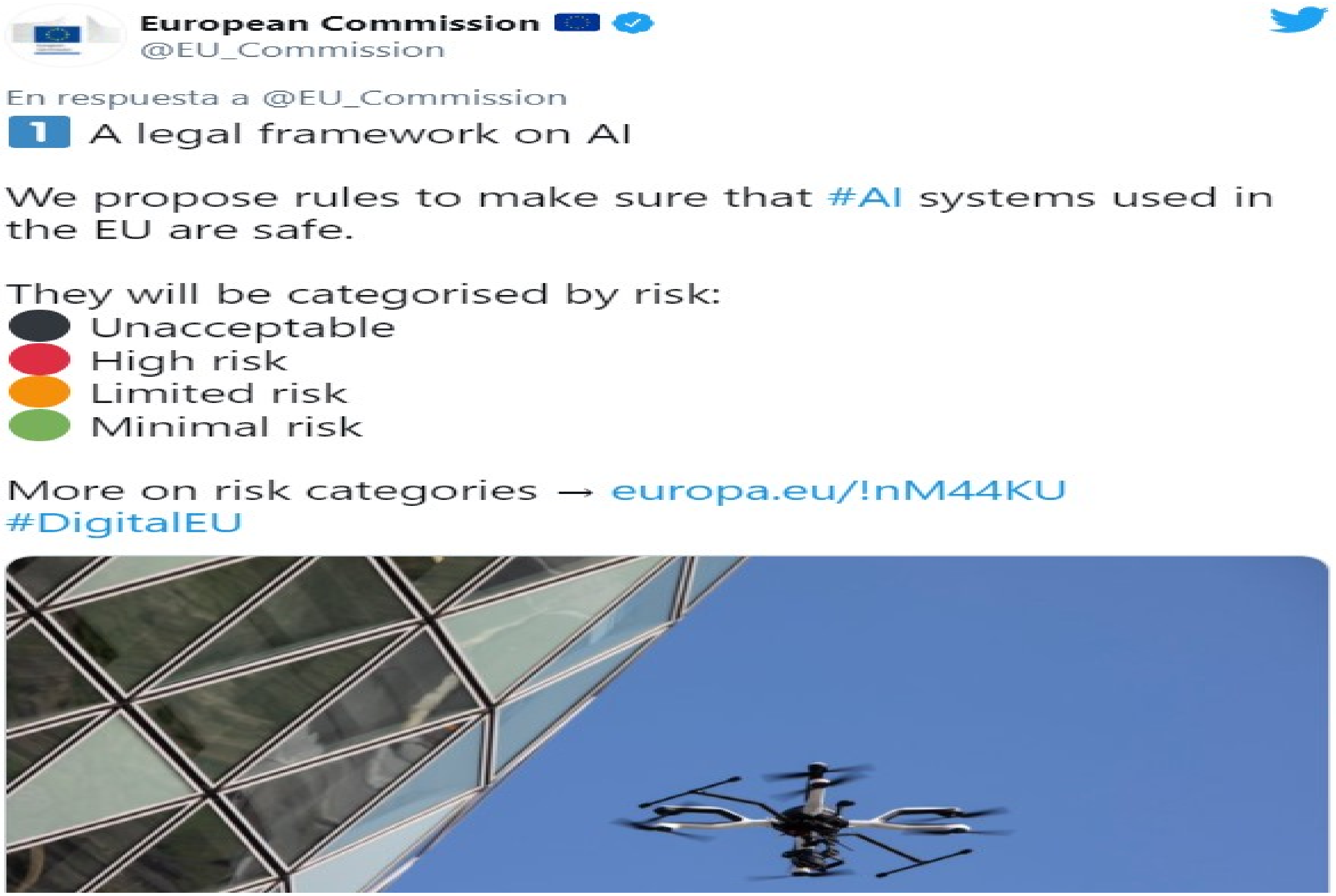
quisitos específicos para los sistemas de IA de alto riesgo y obligaciones para peradores de dichos sistemas;

ormas armonizadas de transparencia aplicables a los sistemas de IA destinados a interactuar cor onas físicas, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica omo a los sistemas de IA usados para generar o manipular imágenes, archivos de audio o vídeos;

ormas sobre el control y la vigilancia del mercado.

Risk classification

- Unacceptable Risk (Art.5)
- High risk
- Limited risk
- Minimal risk



European Commission 🇪🇺 ✓
@EU_Commission

En respuesta a @EU_Commission

1 A legal framework on AI

We propose rules to make sure that #AI systems used in the EU are safe.

They will be categorised by risk:
⚫ Unacceptable
🔴 High risk
🟠 Limited risk
🟢 Minimal risk

More on risk categories → europa.eu/!nM44KU
#DigitalEU

Jnacceptable risks

rohibited artificial intelligence practices:

a) The placing on the market, putting into service or use of an AI system that uses subliminal technique at transcend a person's consciousness to substantially alter his or her behaviour in a way that causes or is kely to cause physical or psychological harm to that person or another person.

) ... that exploits any of the vulnerabilities of a specific group of persons due to their age or physical o ental disability to substantially alter the behaviour of a person belonging to that group in a way that cause r is likely to cause physical or psychological harm to that person or another.

c) The placing on the market, putting into service or use of AI systems by or on behalf of public authoritie r the purpose of assessing or classifying the reliability of natural persons over a given period of time on th asis of their social behaviour or known or predicted personal or personal characteristics or personalit Social scoring)

) The use of "real-time" remote biometric identification systems in publicly accessible spaces for la nforcement purposes (with caveats)

Jnacceptable risks

eal-time remote biometric identification systems unacceptable risk?/high risk
rohibited "in real time" in publicly accessible spaces for law enforcement purposes

xceptions (conditional on compliance with certain requirements):
e targeted search for potential specific victims of a crime, including missing children;
) the prevention of a specific, significant and imminent threat to the life or physical safety of natura
ersons or of a terrorist attack;
i) the detection, tracing, identification or prosecution of the person who has committed or is suspected o
aving committed a serious crime

High-risk systems

assification according to its potential to harm fundamental rights taking into account the role played by AI d the specific purposes for which its use is contemplated

) the AI system is intended to be used as a safety component of one of the devices listed in Annex II, or is elf one of those devices; (conformity assessment carried out by an independent body for placing on the arket or putting into service).

systems listed in Annex II, biometric systems used in public spaces, systems used to send medical aid or efighters; used to determine access to education, employment, credit, social benefits, verification of ormation relating to criminal offenses, or limitation of a person's liberty; crime or altercation prediction stems for allocating surveillance resources; visas; and assistance to judges.

igh-risk systems: requirements

gh-risk systems permitted but subject to certain requirements and a conformity assessment to be placed the market, put into service and use

sk management system (Art.9)

ata and data governance (Art.10)

ocumentation and registration (Arts. 11 and 12)

ansparency and communication of information to users (art.13)

uman supervision (art.14)

ecision, robustness and cybersecurity (art.15)

High-risk systems: conformity assessments

onformity assessment (Art. 30 to 51)

e supplier is the one who, as a general rule, must carry out the conformity assessment under his own sponsibility,

erogation: AI systems which are intended to be used for the remote biometric identification of persons to e extent that they are not prohibited, provision should be made for a notified body to participate in the nformity assessment

High-risk systems: requirements

ations imposed on:

pliers and their authorized representatives

ufacturers of Annex II products

rters and distributors

Limited risk systems

systems intended to interact with natural persons
notion recognition system or a biometric categorization system
system that generates or manipulates image, sound or video content that significantly resembles existing
ople, objects, places or other entities or events, and that may mislead a person into thinking they are
thentic or true (ultra-counterfeiting),
ecific transparency obligations, in order to make users aware that they are interacting with a machine

Sistemas de riesgo mínimo

her uses, for video games, image applications or other AI systems that do not involve risks
xcluded
luntary codes of conduct

Governance

ach Member State should designate one or more national authorities competent to supervise
plementation and control; as well as market surveillance,
eation of a European Artificial Intelligence Committee will facilitate its implementation and promote the
eation of AI regulation.
eating a data specific to independent (non-product-integrated) high-risk AI systems
luntary codes of conduct for AI that does not involve a high risk,
ntrolled testing spaces (regulatory sandboxes) to facilitate responsible innovation.

Sanctions

sholds:

EUR thirty million or 6 % of the total annual worldwide turnover of the previous financial year, with the est amount being for infringements for non-compliance or prohibited practices in relation to data irements;

EUR 2 million or 4 % of the total annual worldwide turnover of the previous financial year for non-pliance with any other requirement or obligation of the Regulation;

EUR ten million or 2 % of the total annual worldwide turnover of the previous financial year for the ision of incorrect, incomplete or misleading information to notified bodies and national competent orities in response to a request.

Final Considerations

cts (+)

regulatory framework in this area

based rather than sectoral approach

s heavily on EU product safety regulations (Harmonize)

ine against certain practices/ prohibition of social scoring

cts (-)

y of the most harmful uses are not prohibited/high risk (EDRi))

dy charged with enforcing the RAI will have to determine when a system is manipulative or exploitative, so ffect depends on future measures.

not consider algorithms used in social media, search, online retail, app stores, mobile apps, or mobile ating systems to be high-risk

as to the information that should be disclosed to people who are affected by AI systems.

ormity assessment is a procedure, not a document, and an internal check for most high-risk AI system ders; there is no audit report for the public or regulator to review.

PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

THANK YOU

info@panelfit.com

www.panelfit.eu

@PANELFIT

PANELFIT.NEWS