PROPOSAL FOR 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 of 21 April 2021

Initial Observations

Mediaset Italia S.p.A.

5 August 2021

1. Introduction

Mediaset Italia S.p.A. (henceforth, "Mediaset") welcomes the consultation launched by the European Commission on its proposal for the EU Artificial Intelligence Act ("AI Act" or "the EU Commission's Proposal"). Mediaset is a major Italian multimedia group and the largest commercial broadcaster in the Country. Its most widely known activity is the provision of free-to-air commercial broadcasting; it also operates a series of online outlets providing coverage on news, entertainment and sports, as well as a number of radio stations, and it is a significant contributor to the production of original audio-visual content - films, TV series and entertainment shows.

In the context of the "Europe fit for the digital age" strategy, the AI proposal is another major step towards a trustworthy and safe digital environment for European citizens and businesses alike. In this paper, Mediaset outlines its views on the AI Act with a two-fold perspective: the deployment of AI in the online advertising market and the challenges and opportunities in the deployment of AI technologies for copyright protection.

Several activities resulting from the misuse of AI fall outside the scope of the EU Commission's Proposal. In order to avoid unintended effects:

1) Some services offered by social media platforms should fall, at least, into high-risk AI systems categories (or labelled as unacceptable risk), for instance: i) AI systems leading to a choice of content, namely for ad-funded

services, should be subject to additional transparency rules, in line with the provisions of the two Proposals recently tabled by the EU Commission, the Digital Service Act ("DSA") and the Digital Markets Act ("DMA"), and in compliance with competition law provisions; ii) in the high-risk AI systems it is worth including certain social media networks used by minors; iii) concerning "deep fakes", platforms should single out content that has been manipulated by an AI system, just like broadcasters do.

2) Two aspects of the use of AI with reference to the audiovisual and advertising sectors shall be addressed:
   a) As pointed out with regard to AI systems that deploy subliminal techniques beyond a person's consciousness, thus exploiting any of the vulnerabilities of a specific group of people due to their age, physical or mental disability, it is worth underlying that: (i) a subliminal technique is by its definition not detectable by the person impacted, hence informed consent is not possible, nor is it possible for an individual to prove that his/her/their behaviour was materially distorted; (ii) in the Commission's proposal it is also not clear who decides that a practice is "subliminal", "materially distorting", "likely" to cause harm; (iii) the wording of the prohibited use case with such a narrow scope to define makes it practically impossible to effectively ban any practice or protect any individual from exploitation of vulnerabilities. These minimum requirements/critical issues however fail to grasp the wider picture of the advertising market and the impact that AI tools will have on the sector.
   b) Targeted digital advertising is increasingly the business model of choice in the digital economy, with many businesses providing zero-priced services in exchange for access to consumer data to fuel the sale of targeted digital advertising. Furthermore, increased Internet coverage and mobile phone penetration has fundamentally changed the ability of advertisers to reach a broad range of consumers at almost any time of the day and in any context through digital advertising. In addition, developments in AI and machine learning, coupled with the

> storage of personal data available online, have allowed for cost-effective targeted advertising at scale. Such advertising is traded electronically in real time across a complex supply chain involving numerous actors. Competition agencies are increasingly concerned about competition in digital advertising markets, with a number of recent market studies and investigations highlighting a range of potential competition concerns. In particular, there seems to be increasing market concentration, consolidation and integration across many levels of the supply chain. As a result, several antitrust authorities are currently investigating whether some players have strengthened their dominant position with anticompetitive conducts. In this regard, suffice to mention the EU Commission's Case AT.40670 (Google – Adtech and Data-related practices), in the context of which the EU Commission is requested to assess whether Google has violated EU competition rules by favoring its own online display advertising technology services in the so called "ad tech" supply chain, to the detriment of competing providers of advertising technology services, advertisers and online publishers.

On the basis of the above, it appears that the EU Commission has decided to advance a very cautious approach, focusing exclusively on regulating high-risk AI, while leaving non-high-risk AI, such as the broad online advertising market, out of scope. Encouraging codes of conduct for non-high-risk AI seems unfit to address the issues at stake. In fact, over-reliance on codes of conduct has proved ineffective to address severe societal challenges posed by these new players in other domains.

It is also worth underlying that copyright constitutes another test to challenge the AI Act's resilience. The adaptation of the IP system to AI-generated creativity and innovation (and the challenges that it brings about) is increasingly becoming a topic of critical interest. A substantive *corpus* of literature dedicated to AI and IP is emerging[1].While existing IP regimes, including copyright law, trade secrets and

[1] See e.g. World Intellectual Property Organization, 'WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI)' WIPO/IP/AI/2/GE/20/1 REV (21.5.2020); European Parliament, 'Draft Report on Intellectual Property

patent law can protect software on which AI technology is based, the protection afforded to software does not extend to the output possibly generated by the AI. Whether this protection is available is actually still an open question, based on the construction of the present copyright framework. A distinction should also be made between computer-assisted creativity, which is copyrightable as long as the user contribution is original, and proper computer-generated creativity, where a user's interaction with a computer prompts it to generate its own expression. Additionally, there are two other fundamental questions relating to the (Machine) Learner and the (AI)Infringer. They refer to whether AI can infringe copyright through the machine learning process and training that enables the AI to generate creativity and whether AI can infringe copyright by creating an infringing output. That said, as underlined by Executive Vice-President Vestager[2], AI systems *« have to ensure an appropriate level of human oversight both in the design and implementation of the Artificial Intelligence »*.

Furthermore, following the adoption of Directive 2019/790 of 17 April 2019 on Copyright in the Digital Single Market ("DSM"), which enables more effective protection of copyrighted content online, it is likely that new AI-related technologies will be put in place to facilitate compliance with the obligations of the DSM.

Article 17 of the DSM, with its goal to close the so-called "value-gap", provides a strong incentive to apply and further develop filtering technologies. Mediaset, whose content is often distributed illegally on third-party platforms, welcomes the development of AI technologies that can make more effective the fight against the illegal distribution of copyrighted content. The EU Commission's proposal should promote the development of European AI technologies within a clear framework, in order to counter the dominance of unilaterally controlled US tools.

Rights for the Development of Artificial Intelligence Technologies' 2020/2015(INI) (24.4.2020); European Parliament, 'A Comprehensive European Industrial Policy on Artificial Intelligence and Robotics' 2018/2088(INI) (12.2.2019), paras 136-137; European Commission, 'Artificial Intelligence for Europe' COM(2018) 237 (25.4.2018), p. 14; European Parliament, 'Report with recommendations to the Commission on Civil Law Rules on Robotics' 2015/2103(INL) (27.1.2017), pp. 11, 21, 28.

[2] Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence, 21 april 2021.

2. Analysis of the Commission's proposal

2.1. Definitions

The AI Act is aimed at targeting the deployment of AI systems with a view to making such activity fully compliant with the EU fundamental values. While advancing such a value-based approach, the EU Commission's Proposal prohibits a set of practices where critical AI systems are deployed on the market, put into service or used, imposing a number of strict requirements on providers, importers, distributors and users of "high-risk" AI systems. Finally, the AI Act fosters transparency through *ad hoc* obligations on specific AI systems (which, may also be qualified as high-risk systems and/or be part of a prohibited practice).

a) *AI systems*

The AI Act generally refers to AI systems, which are defined in art 3(1) and Annex I in reference to a software (whether or not integrated or connected with hardware) that generates outputs, based on human defined objectives, developed with specified data-driven and/or code-driven techniques.

The definition clearly intends to encompass a broad scope, which is then narrowed down as the Proposal addresses high-risk AI systems (which constitutes a sub-set of AI systems).

Recital 60 recognizes the complexity of the AI value chain, made of "*relevant third parties, notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services*". The broad definition of "*AI systems*" and subsequently of a "*provider*" is likely to make it difficult to effectively determine which AI systems and which entities (providers) would be comprised in the EU Commission's Proposal. In fact, Art. 3(2) defines "*providers*" of high-risk AI systems as "*a natural or legal person, public authority, agency or other body that develops an AI system or has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark*".

b) ***AI practices***

As provided in Art. 5, four categories of AI practices are deemed to be prohibited. The scope of the definition of AI technologies is not clearly ring-fenced but is defined as the "*the placing on the market, putting into service or use of an AI system*" that affects natural persons (Art. 5(1), *sub* a, b, c) or the "use" of specific AI systems (Art. 5(1), *sub* d).

- ✓ According to a) and b), the prohibition refers to the manipulation or to the exploitation of vulnerabilities resulting in physical or psychological harm to a natural person;
- ✓ According to c), the prohibition has regard to social credit scoring by or on behalf of governments resulting in detrimental or unfavorable treatment of a natural person (together with some supplementary conditions);
- ✓ According to d), the prohibition has regard to the use of a specific technology by law enforcement with some exceptions, namely in three exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks.

c) ***Tentative Proposals and Potential Amendments***

As the first legislative proposal on AI anywhere in the world, the AI Act contains a variety of notions, which, albeit reasonable and proportionate as whole, could be better clarified.

For instance, the terms "placing/making available on the market" and "putting into service".

In the context of Article 9, it is unclear whether there is any difference between: (i) "*reasonably foreseeable*" risks, as provided for by Art 9(2), sub a) and (ii) "*risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse*", according to Art. 9(2) sub b).

Finally, in relation to Article 9, while several recitals (*e.g.*, Recitals 27, 43) indicate that the goal of the AI Act is to mitigate risks to "*health, safety and fundamental rights*", Art. 9 *per se* does not clarify the types of risks providers should consider when assessing and taking steps to mitigate risks.

While banning the use of generalized social scoring systems and the adoption of real-time biometric identification are not relevant to Mediaset's core business, we would recommend to ensure clarity about the criteria to be adopted, along with robust transparency requirements.

2.2. **High-risk AI systems**

The AI Act is intended to apply to certain AI systems, namely:

- a product, or a safety component of a product, covered by legislation in Annex II (which mainly covers health and safety threats);
- a system referred to in Annex III (which mainly covers fundamental rights threats)

Article 3(14) defines a "*safety component of a product or system*" as "*a component of a product or of a system which fulfills a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property*". In order to strengthen the definition of "*safety component*", it is of paramount importance that the assessment of a safety component refers back to EU harmonized legislation to align with any relevant essential requirements.

Furthermore, Artt. 19 and 43 require providers to subject their systems to a new conformity assessment prior to their placing on the market or putting into service and/or whenever a change occurs which may affect the compliance of the system with the EU Commission's Proposal or when the intended purpose of the system changes. Therefore, AI systems — particularly those offered as services — should be deployed on the market only once a high level of safety can be ensured.

It is worth emphasizing that the distinction between prohibited practices, high-risk systems and "*certain systems*" with extra transparency obligations does not refer

to mutually exclusive systems. A system that is not high risk may nevertheless be part of a prohibited practice, and conversely a system with extra transparency obligations may be part of a prohibited practice or qualify as a high-risk system. The above may potentially lead to limited certainty in terms of ambit and scope of application as well in terms of procedures.

a) ***Tentative Proposals and Potential Amendments***

The AI Act provides a list of requirements that AI systems labelled as high-risk must encounter.

The process to assess whether some AI systems should be considered as high risk is only broadly defined in Annex 3, which may lead to poor outcomes for product planning decisions.

The definition of a "*safety component*" set out in Art. 3(14), could possibly be strengthened as it currently encompasses general concepts which are not further specified and a wide range of notions that may be occasionally related to safety or security (*e.g.*, "*safety function*").

Similarly, Article 5(1), *sub* a) prohibits "*the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm*". In this regard, the definition used for "*manipulative, exploitative and subliminal techniques*" in relation to prohibited AI systems and for "*materially distorting*", a person's behavior could be further explained and clarified, also building on the GDPR *acquis*. In fact, the EU can foster innovative AI system which empower users in full compliance with the European fundamental rights enshrined in the Treaties.

By all means, users should always be made aware if and how their data are being processed by AI software; most importantly, as provided in the GDPR and the e-privacy regulation proposal, they must be able to refuse access to and processing of their personal data.

More in general, the list of high-risk AI systems appears largely defined in at least two respects. First, as discussed above, the definition of "*safety component of a product*" is too vague and, secondly, the list of "high-risk" systems in Annex III risks being too broad and may converge towards scope systems that are neither inherently high-risk nor involved in the decision-making function of the final system (*i.e.*, the point at which a risk of harm may materialize). This is particularly the case for component parts of larger systems and general-purpose systems that may be used in a wide range of contexts. Furthermore, although Art. 7(2) lists several criteria that the EU Commission must take into account when evaluating whether to add any new categories of AI systems to Annex III, Annex III currently could cover AI systems that would not appear to qualify as high-risk under those criteria.

2.3. **New Duties and Responsibilities for Providers of AI**

Providers of high-risk AI systems are expected to comply with a variety of transparency and reporting requirements, also by using vetted data to train and progressively adjust AI systems. Additional obligations regarding risk and quality management, data governance, accuracy, robustness and security, and human oversight are set out under the AI Act.

Some of these requirements could be further specified, such as enabling "*users to interpret the system's output and use it appropriately*" (see, in this regard, Art. 13(1)) while others require more narrowly defined form-filing activity. As provided in Art. 13(2), high-risk systems "*shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users*", including, *inter alia*, "*the identity and the contact details of the provider*" (Art. 13(3), *sub* a)), the AI high-risk systems' "*intended purpose*" (Art. 13(3), *sub* b) *lett*. (i)), "*the level of accuracy, robustness and cybersecurity* […] *against which the high-risk AI system has been tested and validated and which can be expected* […]" (Art. 13(3), *sub* b) *lett*. (ii)), and "*any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance to its intended purpose or under conditions of reasonably foreseeable misuse which may lead to risks to the health and safety or fundamental rights*" (Art. 13(3), *sub* b) *lett*. (iii)).

Data governance is a crucial aspect of any AI system, and Article 10 provides guidance in this regard.

Article 10(3) requires that "*training, validation and testing data sets shall be relevant, representative, free of errors and complete*", while Article 10(5) sheds light on the use of personal data for bias monitoring which must be "*subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued*".

Article 14(4), *sub* a) requires that individuals that exercise human oversight of AI systems "*fully understand the capacities and limitations of the high-risk AI system*".

Article 15(3) requires that high-risk AI systems be "*resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates*".

Furthermore, as to the "[t]*ransparency obligations for certain AI systems*", the EU Commission's Proposal requires AI providers to disclose the use of AI. Art. 52(1), within Title IV, asks AI providers to "*ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use*". The degree of this disclosure is targeted towards commercial applications, since the same paragraph continues by stating that "*this obligation shall not apply to AI systems authorized by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence*".

The same goes for "[u]*sers of an emotion recognition system or a biometric categorization system*" that, according to Art. 52(2), shall inform of the operation of the system the natural persons exposed.

As to the use of AI to manipulate images, audio, or video, Art. 52(3) rightly provides that users of an AI system to be informed when interacting with content generated by AI that "*appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ("deep fake")*".

a) ***Tentative Proposals and Potential Amendments***

The above-mentioned requirements – such as risk management, data governance, human oversight, robustness and accuracy – are sound and in line with the EU Commission's preliminary work.

This is the case with the requirement for datasets to be "*free of error*" and "*complete*" (Art. 10). The instructions provided for users and the human oversight requirement enabling the user to "*fully understand the capabilities*" of the systems could be better tailored to the user needs by means of specific guidelines.

In addition, the AI Act places most of the obligations to meet the requirements for high-risk AI systems on the providers of such systems. Users (*i.e.*, customers) that deploy AI systems are required to follow instructions given by the provider for the intended use.

This allocation of responsibilities is drawn from product regulation frameworks, based on the assumption that a product is sold and delivered to a customer with instructions for use. For many AI use cases, the distinction between provider and user roles is less clear than expected and it would be advisable to clarify this definition. In many scenarios, providers create applications that are generally applicable and not conceivable as high-risk. However, these same applications can be configured by users who will also control the data with which the AI system interacts. In such contexts, the provider could have little or no control over (and visibility on) the use of the AI system and there may be room to further clarify the allocation of responsibilities.

A sound example is Art. 28(1), according to which any distributor, importer, user or other third-party shall be considered a provider in case, inter alia, "[…] *(b)*

they modify the intended purpose of a high-risk AI system already placed on the market or put into service; (c) they make a substantial modification to the high-risk AI system". In this perspective, Art. 28 could be amended so to be applicable to users modifying the planned purpose of an AI system already placed on the market or put into service to create a high-risk AI system.

2.4. Governance and enforcement

The AI Act foresees a complex regulatory infrastructure to oversee and regulate AI systems - from assessment and declaration of conformity to ex-post market surveillance - in line with the New Legislative Framework. Member States have considerable leeway to set up regulatory authorities as they see fit and to take into account national administrative structures.

The AI Act provides authorities with the power to access data and documentation from providers and users of AI systems. In particular, they can compel providers of AI systems to grant access to data sets via application programming interfaces and they can request access to the source code of the AI system. It is important that, thanks to the above access, an independent expert should be enabled to fully understand and reverse engineer the material that has been made available.

***

Mediaset thanks the Commission for the opportunity to provide comments on the AI Act Proposal and would welcome the opportunity to further discuss this initial appraisal of such a timely and ambitious proposal.