IDEMIA Contribution

Consultation on the Artificial Intelligence Draft Regulation

About IDEMIA

IDEMIA, the global leader in Augmented Identity, provides a trusted environment enabling citizens and consumers alike to perform their daily critical activities (such as pay, connect and travel), in the physical as well as digital space.

Securing our identity has become mission critical in the world we live in today. By standing for Augmented Identity, an identity that ensures privacy and trust and guarantees secure, authenticated and verifiable transactions, we reinvent the way we think, produce, use and protect one of our greatest assets – our identity – whether for individuals or for objects, whenever and wherever security matters. We provide Augmented Identity for international clients from Financial, Telecom, Identity, Public Security and IoT sectors.

With €2.2bn in revenues and 15,000 employees around the world, IDEMIA serves clients in 180 countries.

For more information, visit www.idemia.com

Agenda

Introduction

As a global leader in biometrics, IDEMIA seizes the opportunity to respond to the public consultation on the draft Regulation on Artificial Intelligence (hereinafter "AI").

The highly technical nature of the concepts inherent in its field of application makes consensus difficult. But even more, and notwithstanding the impossible predictability of the risks that AI will generate in the future, the desire to regulate not AI systems globally but products and services embedding AI systems is proving to be a real challenge in terms of the articulation of standards. We endorse the need to clarify applicable rules so as to ensure legal visibility.

We would like to emphasize that IDEMIA is open to collaborate and contribute with the EU Institutions to build the most relevant AI regulation. We are fully committed to maximizing the benefits of AI while addressing its potential risks. While we acknowledge and understand the concerns raised in particular by facial recognition, **we welcome the Commission's sensible approach of not simply banning the use of remote biometric identification (hereinafter "RBI") in public spaces, but of considering the authorization of certain use cases, including those that have already proven successful.**
It is also important to stress the strong need to foster innovation in the field of AI in order to ensure the competitiveness of the European industry in a highly competitive international environment.

General remarks on the proposition will focus on the positive points that IDEMIA welcomes and the pitfalls that we wish to avoid. A detailed feedback will then be provided to address some of the crucial points that we want to emphasize.

General Comments

A. **Technology neutrality shall be a mantra**

In order to ensure fair competition and a level playing field between all market players, it is crucial to ensure technology neutrality, as one of the key principles promoted by many EU legislations, since the "Telecom packages" of 2002 and 2009, and more recently with GDPR.

Technology neutrality principle shall enable to prevent obsolescence of the rule of laws and ensure that legislation is sufficiently flexible to adapt to new technologies in a fast pace digital age. This leads us to formulate a first remark, related to the very definition of what AI is. One may regret the use of the notion of human intervention "*for a given set of human-defined objectives*", and reasonably fear that the law does not anticipate the future developments of the technology and becomes obsolete more quickly than desired.

We do believe the Regulator should let the market select the best standard (i.e., adopt a technology-neutral stance). Indeed, market standards are preferable when there are strong uncertainties about the benefits of the technology. A similar conjecture could be made for technological neutrality: it is more important when there are strong uncertainties about the development of technologies.

The draft Regulation assumed that a broad set of relevant, harmonised standards could be available 3-4 years from now, at the same time as the legislative adoption of the proposal and the transitional period envisaged before the legislation begins to apply to operators.

ISO SC37 has taken the lead through the adoption of a standard. **A European initiative for a fast-track standard to set the baseline for a further international one would have been preferable**. Choosing ISO as the preferred forum for discussing standard incorporates (among many others) US, China, Korea and Japan in a discussion about the future standard that will ultimately be the basis for regulating the technology in Europe.

B. Risk based approach needs to be improved

IDEMIA welcomes the risk-based approach chosen by the Commission. The draft Regulation distinguishes between unacceptable, high and low risk.

But the text does not define risk – a fundamental concept for conformity assessment, nor does it define the methodology to assess the risk. Instead, its provisions include the term 'risk' and the related 'harm' in various meanings. **This may cause interpretation issues within the proposed Act and across its referenced legislations as it also increases the Act's complexity and implementation cost and could result in legal uncertainty.**

Risk can be mitigated, and harm can be remedied. Therefore, the terms should be extremely precise in order to orient the mitigation and remediation processes to be put in place. In the absence of these precise definitions, risk and harm turn to absolute, leaving little space for remediation and mitigation, which is the basis of risk management.

Recommendation 1: IDEMIA would welcome a methodology to define risks and harms, jointly with the industry, that could be based on the EBIOS approach for example.

Detailed comments

A. Real-time biometric identification, a high risk AI system (article 5)

IDEMIA reckons that RBI (Remote Biometric Identification) has the potential to be intrusive as it can affect fundamental rights and freedom, **though such impact can vary considerably depending on the purpose, context and scope of the use.**

"Real-time" RBI in public spaces is prohibited in principle but the ban has three defined exceptions:

- The targeted search of a missing child
- The prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack, and
- The localisation, identification or prosecution of a perpetrator or suspect of a serious criminal offence. In this case, an authorisation granted by a judicial or independent body is required, and the use is subject to appropriate limits in time, geographic reach and the database search.

IDEMIA understands and welcomes that only real-time biometric identification is covered by the ban, the proposed regulation taking care to define only remote biometric identification and then distinguishing real-time analysis from deferred time. In other words, remote biometric identification in deferred time ("post event") is not subject to the prohibition set up in article 5, nor is biometric identification carried out by a private person on his behalf, although both systems remain high-risk (Annex III, § 1).

We believe that a general ban would not have solved the problem raised by new technology and techniques; instead, we support the draft AI Regulation approach to define clear rules to enable the use of RBI in specific use cases. In that context, consistency in the implementation by Member States should be ensured to provide legal certainty across Europe.

<u>Recommendation 2:</u> We urge the policy makers not to adopt a full ban on RBI, but rather to enable clearly identified exceptions as proposed by the draft Regulation. Specific use cases preventing dramatic events shall remain authorised, provided the appropriate safeguards are put into place. Consistency in the implementation by Member States of the legal requirements imposed for the use of real-time RBI by law enforcement agencies should also be ensured to provide legal certainty.

B. Requirements for high-risk AI Systems

The draft Regulation imposes a long list of obligations to AI products and services deemed as “high risk.” This includes requirements on testing, training, and validating algorithms, ensuring human oversight, and meeting standards of accuracy, robustness, and cybersecurity. Providers would need to prove that their AI systems comply with these requirements before placing them on the European market. The operating assumption here is that new regulation will foster trust in AI and, by extension, Europe’s competitiveness.

Most of the proposed requirements are indeed appropriate to ensure that only safe and performing AI systems are placed on the market. However, **some of the requirements necessitate further discussion to align with state-of-the-art software development practices and to ensure that no barriers are created for highly innovative software**. Some examples of these requirements are provided below.

C. *Ex ante* versus ex post conformity assessment

As all other “high risk AI system”, RBI systems must comply with stringent requirements listed in Articles 8 to 15 of the draft Regulation. While other AI systems will have to undergo a self-conformity assessment, RBI will be subject to a third-party conformity assessment, unless RBI providers demonstrate compliance with future standards that will be adopted.

In addition to *ex ante* conformity assessments, there would also be an *ex post* assessment for market surveillance and supervision of RBI systems by competent national authorities designated by the Member States.

As far as biometrics are concerned, we believe that *ex ante* evaluation is not realistic. There is no scientific consensus on that matter, nor clear guidelines or protocols. Forty years of practice in biometrics have taught us that only *ex post* conformity assessment is efficient to achieve the objectives defined by the draft Regulation**. We fear *ex ante* assessment might cause significant delays and raise the cost of AI products and services before placing them on the market.**

Quantifying *ex post* performance assessment biases remains the only way to ensure that the AI system will perform as intended and specified.

In addition, some clarifications should be provided on how these assessments interact with GDPR requirements.

<u>Recommendation 3:</u> Refrain from applying new *ex ante* conformity assessments for new AI products and services that could lead to significant delays in releasing AI products and services to the European market. The effective application of such a model and the lack of expertise in evaluating algorithms and models should also be addressed in a harmonised European approach. Instead, we suggest that policy makers consider the application of existing self-assessment tools for trustworthy AI systems such as the Data Protection Impact Assessment (DPIA) and Privacy by Design and by default under the GDPR that is well integrated into existing providers and users processes.

D. Data Governance (article 10)

A clear data governance framework is crucial. **However, the requirement to use complete and error-free data for training, validation and testing is questionable as it is neither feasible nor desirable if testing takes place under real-world conditions**. How can it be demonstrated that a dataset meets these requirements? How do you ensure that a dataset is representative when its developers do not know how, where and why the solution will be used?

Accuracy includes trueness (proximity of the measurement results to the true value) and precision (repeatability or reproducibility of the measurement). Trueness and precision represent a certain margin of error.
The draft Regulation appears to ignore *real* conditions of the use-case, which cannot be anticipated when developing a system. We are of the opinion that the only way to ensure the quality of a dataset is to test it against the relevant use case.

Recommendation 4: The requirement for complete and error-free data for training, validation and testing is unrealistic and undermines the validity of the *ex ante* approach. We would rather rely solely on an *ex post* approach in which the use of sequestered data for evaluation and benchmarking purposes, as practiced by the NIST in the United States, would be, in our opinion, the best practice.

Recommendation 5: For a better compliance, it seems that National Supervisory Authorities are best suited to be IA authorities as well. It will be easier for compliance purpose, for the IA providers and to better coordinate regulations harmonization.

E. Technical documentation (article 11) and transparency (article 13 and 52); access to data and documentation (article 64)

The technical documentation to be provided is particularly extensive. The draft Regulation would require developers of AI solution to provide access to source code and other IP information. This exposes intellectual property and trade secrets and creates security risks and could have side effect such as deterring EU companies from investing in artificial intelligence.

The draft Regulation requires transparency with regard to the level of accuracy, robustness and information on cybersecurity. We would like to express our concerns about this approach. **This approach is not technology agnostic and will not ensure a level playing field between AI solutions and solutions developed with other technologies, while the purpose of the processing will be the same.**

It also requires transparency of performance with regards to the persons or groups of persons on whom the system is intended to be used. The implementation of this requirement needs to be further clarified: the issue of defining “group of persons” is not straightforward. How to define an “ethnic group” in practice? How to define a clear protocol? Having a data base that is totally representative of the world population is illusory and misleading. **We would prefer a “black box” pre-deployment test.**

We are also concerned about the transparency related to the input data specifications, or any other relevant information in terms of the training, validation and testing datasets used, taking into account the intended purpose of the AI system.

Article 64 provides that market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming interfaces (‘API’). It also provides for the possibility for market surveillance authorities to require the source code of AI system for compliance monitoring of high risk AI system. IP protection is crucial to provide an incentive that drives investment. **This obligation is excessive as it affects trade secrets and know-how, it creates vulnerability for IT security.**

Overall, transparency and access to documentation as described by the draft Regulation is too intrusive as it requires providers of AI system to divulge their trade secrets and know-how. Providers would give access to their datasets to evaluation bodies, including through APIs, which represents a significant IT security vulnerability. This contradicts both best practices in security of R&D operations, and contractual agreements with customers when protecting sensitive technologies.
Finally, in addition to affecting intellectual property, these requirements significantly increase costs for providers and affect the competitiveness of the EU industry.

Recommendation 6: IP information of European Providers should only be shared with independent public authorities; disclosure of highly sensitive information to private third-party auditors raises IP protection concerns to the industry and could undermine the EU sovereignty.

F. Certification and test approach

Testing should be carried out on a black box mode, in the sense that a detailed knowledge of the inner workings of the product should not be required to assess whether or not the system is performing to standard.

A European NIST is the best approach in our opinion (test databases, confidential and sequestrated data).
Such a tool is definitely within Europe's grasp: Europe is fortunate to have a vibrant, state-of-the-art academic ecosystem which could form the backbone and expertise of this network. As a key industry player, IDEMIA would be happy to support the development of such a capability in the EU with our own expertise and industry experience, just as we supported the development of the NIST capability throughout 2000s and 2010s.
We think that this capability will be key in ensuring Europe's sovereignty. Europe will need to make sure that AI is tested according to its own values, following requirements derived from European use cases, and above all, using data which is relevant to use cases and the operational situation in Europe.

Recommendation 7: The evaluation of the performance of the product should be done *ex post* in a "black box mode" by a European standardisation body, as it is the only approach to ensure that the final product complies with the requirements.

CONCLUSION

Like the GDPR, this text it is far-reaching and ambitious; it has the potential to become a fundamental text and a reference for AI regulation and to be replicated outside Europe.

IDEMIA supports a clear legal framework that defines rules for both providers and users of AI system in order to create trust and transparency in the use of such a system while preserving both the European position in the AI technology landscape and the fundamental rights and freedoms of individuals.

IDEMIA, as a global leader based in Europe, is keen to work with the institutions to provide more in-depth insights to support policy making and believes that a dialogue with all stakeholders is necessary to ensure the best regulatory outcome.

RECOMMENDATIONS

Recommendation 1: IDEMIA would welcome a methodology to define risks and harms, jointly with the industry, that could be based on the EBIOS approach.

Recommendation 2: We urge the policy makers not to adopt a full ban on Remote Biometric Identification (RBI), but rather to enable clearly identified exceptions as proposed by the draft Regulation. Specific use cases preventing dramatic events shall remain authorised, provided the appropriate safeguards are put into place. Consistency in the implementation by Member States of the legal requirements imposed for the use of real-time RBI by law enforcement agencies should also be ensured to provide legal certainty.

Recommendation 3: Refrain from applying new *ex ante* conformity assessments for new AI products and services that could lead to significant delays in releasing AI products and services to the European market. The effective application of such a model and the lack of expertise in evaluating algorithms and models should also be addressed in a harmonised European approach. Instead, we suggest that policy makers consider the application of existing self-assessment tools for trustworthy AI systems such as the Data Protection Impact Assessment (DPIA) and Privacy by Design and by default under the GDPR that is well integrated into existing providers and users processes.

Recommendation 4: The requirement for complete and error-free data for training, validation and testing is unrealistic and undermines the validity of the *ex ante* approach. We would rather rely solely on an ex post approach in which the use of sequestered data for evaluation and benchmarking purposes, as practiced by the NIST in the United States, would be, in our opinion, the best practice.

Recommendation 5: For a better compliance, it seems that National Supervisory Authorities are best suited to be IA authorities as well. It will be easier for compliance purpose, for the IA providers and to better coordinate regulations harmonization

Recommendation 6: IP information of European Providers should only be shared with independent public authorities; disclosure of highly sensitive information to private third-party auditors raises IP protection concerns to the industry and could undermine the EU sovereignty.

Recommendation 7: The evaluation of the performance of the product should be done *ex post* in a “black box mode” by a European standardisation body, as it is the only approach to ensure that the final product complies with the requirements.