May 27th, 2021

AI-REGULATION.COM

Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021

By Theodore Christakis, Mathias Becuywe and AI-Regulation Team

To cite this article:

T. Christakis, M. Becuywe & AI-Regulation Team, Facial Recognition in the Draft European AI Regulation: Final Report on the High-Level Workshop Held on April 26, 2021, AI-Regulation.com, May 27th, 2021, https://ai-regulation.com/facial-recognition-in-the-draft-european-ai-regulation-final-report-on-the-high-level-workshop-held-on-april-26-2021/

AI-Regulation.com

CHAIR LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

The following is the Final Report on the high-level workshop on facial recognition organised on April 26, 2021 by the Chair on the Legal and Regulatory Implications of Artificial Intelligence (MIAI@Grenoble Alpes) in association with Microsoft. A shorter version of this Report was published in the European Law Blog, while useful related materials, charts and tables have been posted here.

Introduction

The draft Artificial Intelligence (AI) Regulation proposed by the European Commission on April 21 was eagerly anticipated. Its provisions on facial recognition to an even greater degree, given the heated debate going on in the background between those who support a general ban of this technology in public spaces and those who consider that it has "a lot to offer as a tool for enhancing public security" *provided that rigorous red lines, safeguards and standards are introduced.* NGOs (such as those who support the "Reclaim Your Face" campaign) and political groups (such as the Greens) have been calling for a total ban of "biometric mass surveillance systems in public spaces". Contrary to these calls, in their submissions to the public consultation on the White paper, some countries (e.g. France, Finland, the Czech republic and Denmark) have claimed that the use of facial recognition in public spaces is justified for important public security reasons provided that strict legal conditions and safeguards are met (see the Impact Assessment Study, at 18). The results of the public consultation on the White Paper on AI have been mixed on the issue of the ban, but an overwhelming majority of respondents are clearly calling for new rules to be applied in this field.[i]

Whilst the idea of a *complete* ban has been rejected, something that has already led the European Data Protection Supervisor (EDPS)[ii] and NGOs[iii] to react, the Commission's draft regulation attempts to deliver on the idea of introducing new rules for what it calls "remote biometric identification" (RBI) systems, which include both facial recognition but also other systems for processing biometric data for identification purposes such as gait or voice recognition.

In order to gain a better understanding of what is proposed by the Commission and to discuss the basic features of this proposed set of rules, the Chair on the Legal and Regulatory Implications of Artificial Intelligence (MIAI@Grenoble Alpes), in association with Microsoft, organised a preliminary high level discussion on this topic on April 26, 2021. The workshop, which was held under Chatham House rules, included representatives of three different directorates-general of the European Commission (DG-Connect, DG-Just and DG-Home), the UK Surveillance Camera Commissioner, members of the EU Agency for Fundamental Rights (FRA) and Data Protection Authorities (CNIL), members of Europol and police departments in Europe, members of the European and the French Parliaments, representatives of civil society and business organisations and several academics. A list of attendees can be found at the end of this Report.

Part I of this Report discusses the presentation that we gave at the beginning of the workshop, which was based on a chart that we produced to enable an understanding of the facial recognition related provisions of the draft AI Regulation "at a glance".

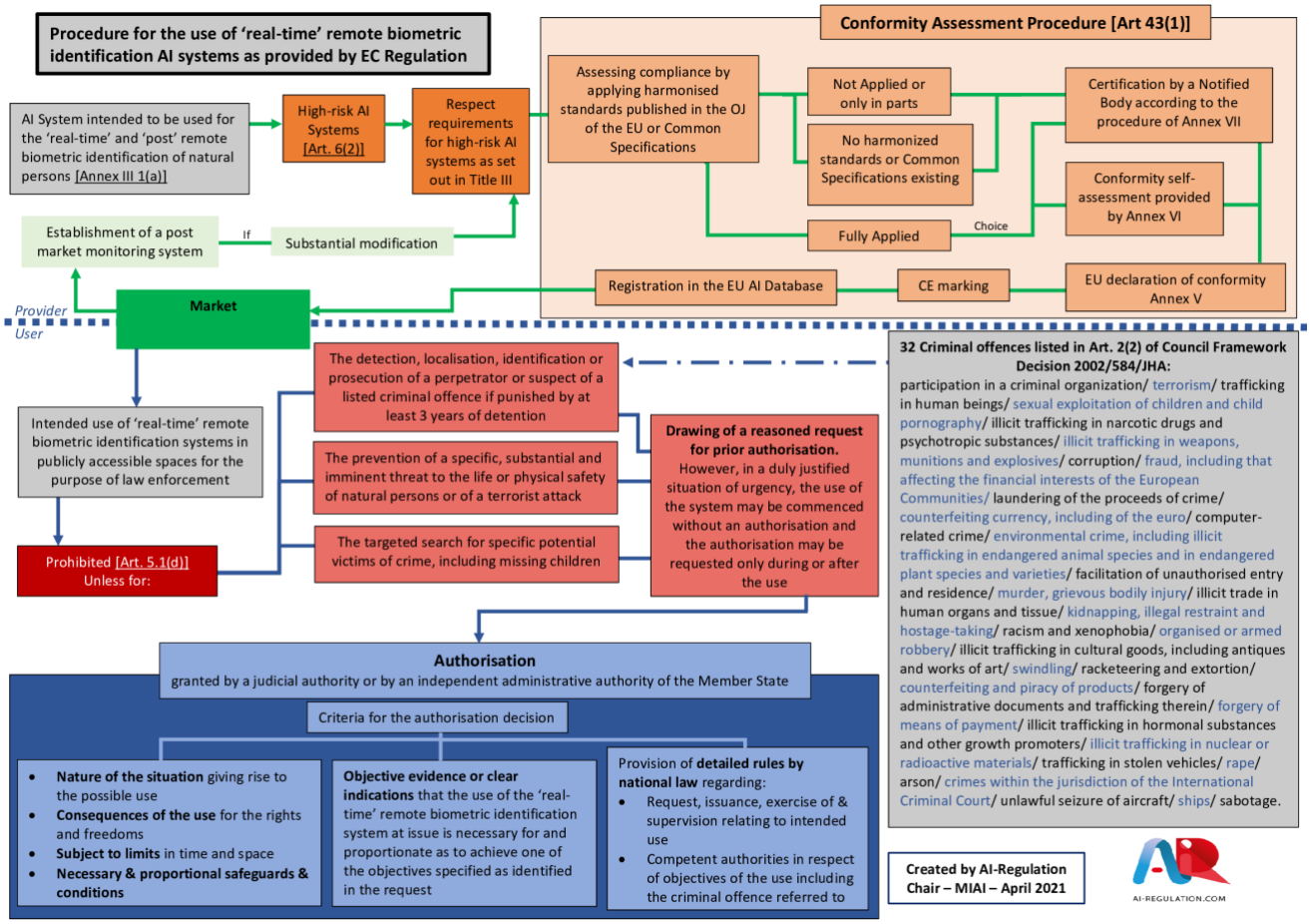
Part II of the Report presents the major points raised in the discussions that took place during the workshop on the rules and definitions proposed in the draft to regulate the use of RBI in publicly accessible spaces for the purpose of law enforcement.

Part III of the Report presents highlights of the discussions on the important novelties introduced in the draft in relation to the "pre-market" requirements that RBI systems must meet, which include a conformity assessment.

Part I.

RBI Rules, At A Glance (Chart and Analysis)

In order to present the Commission's proposal in a structured and more accessible way, we have produced the following table giving a visual overview of the basic RBI rules and mechanisms in the draft AI Regulation (more useful materials can be found here).



The chart is divided into two parts (indicated by the blue dotted line) to represent the distinction made by the draft Regulation between obligations for **"providers"** of RBI systems (i.e., any natural or legal person who develops an RBI system in order to place it on the market and make it available for use); and **"users"** (i.e., any person or authority that deploys or uses an RBI system which is already available on the market).

(1) The Upper Section: Important Pre-Market Requirements for RBI Developers and Providers

When one focuses on the **upper section**, it is immediately apparent that the draft Regulation proposes some remarkable **novelties** in relation to the obligations and pre-market requirements for providers that develop RBI systems.

Firstly, these new obligations concern **all** RBI systems, not only "real-time" RBI systems[iv], the regulation of the use of which by law enforcement authorities (LEAs) is shown in the lower section of the table. This is very important because it means that these pre-market obligations will also cover "post" RBI systems[v], used for instance by LEAs to aid in the identification of a person who has committed a crime, using photos or video stills. Such identification/forensic methods are already used for instance in France in accordance with Article R 40-26 (3) of the French Code of Criminal Procedure. In 2019, a person who was identified, using such a system, after committing a burglary in Lyon, tried, unsuccessfully, to challenge the use and reliability of such post-RBI systems (the Court followed the prosecutor who explained that the facial recognition system was just one of several tools used by LEAs during the investigation). The Commission suggests that henceforth the development of post-RBI systems should be subject to exactly the same kind of strong pre-market requirements as those that concern "real-time" RBI.

Secondly, these RBI systems, in common with all other "high-risk AI systems" (that the Commission lists in Article 6 and Annex III of the Regulation), will be subject to a series of strict requirements and obligations (Articles 8-15) before they can be put on the market. These include:

- Adequate **risk assessment** and **mitigation** systems;
- High quality of the datasets feeding the system, to **minimise risks and discriminatory outcomes**;
- Logging of activity to ensure traceability of results;
- Detailed documentation which provides all the necessary information about the system and its purpose so that authorities can assess whether it complies with requirements;
- Information that can clearly and adequately be read by the user;
- Appropriate human **oversight** measures to minimise risk;
- High level of **robustness**, security and **accuracy**.

Thirdly, RBI systems will be subject to **stricter conformity assessment procedures than those of all other high-risk AI systems** in order to ensure that they meet these requirements. Whereas with other high-risk AI systems, the conformity assessment could be conducted by the system provider based on an ex ante assessment and by means of **internal** checks, RBI will have to undergo an ex ante **third-party conformity assessment**, because of the particularly high risks that fundamental rights might be breached. The only exception to this would be if RBI providers fully comply with the harmonised standards that are to be adopted by the EU standardisation organisations in this field. If this were the case, RBI systems providers could replace the third-party conformity assessment with an ex ante internal conformity assessment (Article 43(1)). In addition to ex ante conformity assessments, there would also be an ex post

system for market surveillance and supervision of RBI systems by competent national authorities designated by the Member States.

During the April 26 workshop, several very interesting issues were discussed by the participants in relation to the obligations of providers under the draft Regulation, the requirements set for RBI systems and the way the conformity assessment should be conducted. These issues are presented below in Part III of this Report.

(2) The Lower Section: Constraints for LEA Users of "Real-Time" RBI in Public Spaces

The lower section of the table focuses on the RBI related provisions in the draft Regulation which concern **the use** of such RBI systems. Once an RBI system has obtained certification, it can be put on the market and be used by public or private actors in accordance with existing, binding EU Law, in particular the GDPR and the LED. However, the draft Regulation intends to introduce new rules and constraints which concern a specific way in which RBI systems are used, namely employing **"real-time"** RBI in **publicly accessible spaces** for the purpose of **law enforcement** (terms defined in Article 3 and also reproduced in our materials accompanying this blog). The draft Regulation announces that using RBI in such a way is to be **prohibited**, unless it meets the criteria for three **exceptions** which appear in pink in our table (and in Article 5(1)(d)). One of these exceptions allows for the use of RBI for the "detection, localisation, identification or prosecution of a perpetrator or suspect" who commits one of the 32 categories of criminal offences listed in the Framework Decision on the European Arrest Warrant (in our table, in grey, on the right) on the condition that such offences are punishable in the Member State concerned by a custodial sentence of at least three years.

When one compares these proposals with Article 10 of the LED, which already prohibits processing of biometric data by LEAs unless where "strictly necessary", subject to "appropriate safeguards" and "where authorized by Union or Member State Law", one may wonder whether they add anything new to the existent legal framework. The answer is, clearly, yes, and this for two main reasons.

Firstly, the draft Regulation intends to **entirely prohibit certain ways in which RBI is used** in publicly accessible spaces for the purpose of law enforcement, such as when the police use facial recognition to identify persons participating in a public protest or persons who have committed offences other than the 32 that appear in our table – although one could argue that this had already been somewhat addressed by the "strict necessity" requirement of Article 10 of the LED.

Secondly, and most importantly, the draft AI Regulation aims to introduce an **authorisation procedure** that does not yet exist in law. Article 5(3) provides that such real-time uses of RBI by LEAs in publicly accessible spaces shall require prior authorisation "granted by a judicial authority or by an independent administrative authority of the Member State" (most probably the relevant Data Protection Authority). LEAs that intend to use the Article 5(1)(d) exceptions will thus need to submit a "reasoned request" based on a Data Protection Impact Assessment (DPIA) which determines whether all the conditions and constraints of the new instrument and the existing data protection legislation, as well as national law, are met.

Having presented our table and the basic structure of the RBI-related provisions of the draft AI regulation, let's now look at some important issues concerning, firstly, the use of RBI systems and, secondly, the pre-market obligations of service providers.

Part II. Use of RBI and Facial Recognition: "Nationalising" the "ban" debate – and other interesting issues

Here are some of the highlights of the issues discussed and clarifications given during the April 26 workshop mentioned above.

(1) What Happens When Facial Recognition is Used in *Other* ways? The Draft AI Regulation as *Lex Specialis*

The participants of the 26 April workshop agreed that the prohibition in Article 5(1)(d) of the draft AI Regulation **does not cover a series of other ways in which RBI and facial recognition is used**. In particular the draft does not intend to prohibit:

a) Real-time use of RBI in publicly accessibly spaces **by public authorities** for **purposes other than "law enforcement"** (as defined in Article 3(41)). This means, for instance, that local governments are not prohibited under the draft Regulation from using such systems in order to control access to a venue for purposes other than law enforcement (for instance in order to facilitate and accelerate access by people).

b) Real-time use of RBI in publicly accessible spaces **by private actors**, such as private security companies (unless they are entrusted by the State to exercise public powers for law enforcement purposes). This means that retailers, transport companies or stadiums are not prohibited *under the draft Regulation* from using real-time RBI for any purpose, including scanning shoppers entering supermarkets to reduce shoplifting and abuse of staff, or preventing fans that have been banned from entering a stadium.

c) **"Post" RBI**, including when it is used by LEAs for the purpose of helping identify, using a photo or video-still, a person who has committed a crime.

d) Use of real-time RBI by all actors (including LEAs) **in non-publicly accessible spaces**, as defined in Article 3(39) and Recital 9.

e) Any use of facial recognition technologies that does not equate to "RBI" in terms of the meaning given in Article 3(36) and recital 8. This covers, for instance, the use of facial recognition for **authentication purposes** in security access protocols, where the system is able to determine a one to one match in order to confirm that a person is who they claim to be (example: comparing a passport photo to a passenger or a badge to a person who tries to enter a building).

The fact that all these uses of facial recognition are not *prohibited* by the draft AI Regulation, and *are not subject either to "authorisation"* under Article 5(3), does not mean, however, that this Regulation does not cover them, nor that these uses are not otherwise regulated by EU law (*infra*).

On the one hand, it must be emphasised, once again, that the draft Regulation contains an important number of novelties vis-à-vis **all** RBI systems, whether real-time or ex-post, and whether used by public authorities or private actors, in publicly accessible spaces or not. These

novelties concern all the **pre-market requirements** and demanding **conformity assessment** procedures explained in Part 1 above. These should ensure, for instance, that the RBI systems that are put on the market cater for strict conditions around accuracy, risk management, robustness and cybersecurity, etc. They should also help develop systems that do not contain bias based on ethnic, racial, gender, and other human characteristics. This means that in all the scenarios mentioned in (a), (b), (c) and (d) above, only systems that are in principle certified by third bodies to meet these requirements could be used.

On the other hand, it must be stressed that all the uses of RBI and facial recognition mentioned above are **already regulated by existing law**, namely the GDPR and, when relevant, the LED. Article 9 of the GDPR prohibits, in principle, the processing of biometric data and provides for certain strict exceptions, subject to a series of conditions and safeguards, including the principles of necessity and proportionality. Data protection authorities (DPA) and courts around Europe have already taken the opportunity to declare that the use of facial recognition systems in some cases is illegal because using it in certain ways cannot meet the GDPR requirements. A good example is the February 27, 2020 decision of a French Court, which considered that the "experimental" use of facial recognition in two high schools in the South of France to grant or refuse access to students, did not meet the "consent" requirements of Article 9(2)(a) of the GDPR and did not meet the "less intrusive means" requirement from the "strict" proportionality test under the GDPR either.

The participants of the 26 April workshop stressed that the prohibition regarding LEAs that appears in Article 5(1)(d) of the draft AI Regulation is intended to apply as ***lex specialis*** with respect to the rules on the processing of biometric data contained in Article 10 of the LED. The Commission therefore decided to focus on the most problematic and dangerous uses of RBI in terms of human rights, namely real-time use by public authorities, in publicly accessible spaces, for law enforcement purposes. While Article 10 of the LED already poses serious obstacles with regard to the processing of biometric data by LEAs (stating that it "shall be allowed only where strictly necessary" and subject to conditions and appropriate safeguards), the Commission sought to go further down this road by regulating such use and the processing of biometric data involved in an exhaustive manner, while also imposing the fundamental condition of prior authorisation by a Court or a DPA when LEAs intend to use real-time RBI. But in any case, for all conceivable uses of facial recognition by public or private actors, existing data protection law still applies.

(2) To Ban or Not to Ban? That is NOT a Question for the EU, But for Member States

An issue that was discussed extensively during the 26 April workshop was why the Commission did not accept the invitation of some stakeholders to ban the use of RBI by LEAs altogether in publicly accessible spaces. Several responses were given to this by participants. These responses focused on the fact that law enforcement authorities in several EU States consider that the use of RBI could be a useful tool for enhancing public security in certain circumstances and if subject to appropriate red lines and safeguards. While EU Member States conferred competences to the EU in relation to data protection and respect of fundamental rights, they did not concede powers relating to the maintenance of national security and public order. National security (including the fight against terrorism) remains a competence of the Member States. Identity checks and police controls are also an exclusive competence of the Member States. The fight against crime and preservation of public order are also mainly competences

of the Member States, despite the emergence of EU criminal law, which boosts cooperation between LEAs and deals with certain practical problems at an EU level.

Against this background, it was probably difficult for the Commission to consider the use of RBI systems by LEAs *exclusively* through the data protection prism[vi] and to ignore that its proposals will directly affect how the police acts on Member State territories, an issue that remains a prerogative of Member States.

The Commission is therefore attempting, to a certain degree, **to "nationalise" the debate** around the opportunity of banning the use of RBI by LEAs in publicly accessible spaces. Its draft proposals set strong pre-market requirements and conformity assessments for the development of RBI software. They also impose a general ban on the use of real-time RBI for law enforcement purposes which can only be overturned if Member States adopt clear and precise rules of national law in order to authorise such use under one or more of the three possible exceptions. If they do so, they will need to respect both the conditions that already exist under Article 10 of the LED and the additional requirements and safeguards introduced by Article 5 of the draft Regulation, including the need for express and specific authorisation by a judicial authority or by an independent administrative authority (most probably a DPA). As Recital 22 explains:

> "Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation".

Each State will therefore be able to engage debate on these issues and decide whether it wishes to enact some of the exceptions provided in Article 5. Some EU Member States might refrain from doing so, in which case they will remain under the ban. Others might decide to enact "rules of national law" in order to authorise some uses by LEAs, in which case they will only be able to use software that has been "certified" as meeting the draft Regulation's requirement and they will also have to respect the strict additional conditions set by the future AI Regulation (once, of course, it enters into force).

(3) The Meaning of "National Law" in the Draft AI Regulation

The previous discussion brings us to another important issue that needs to be clarified. During the April 26 discussions, some participants stressed that the use of RBI by LEAs in publicly accessible spaces is *already* prohibited in principle by existing EU Law, so the "ban" in Article 5(1)(d) does not seem, as such, to constitute that surprising a novelty – although the additional conditions and requirements brought in by the draft Regulation certainly do.

Indeed, Articles 8 and 10 of the LED in principle prohibit processing of biometric data by LEAs unless such processing is "strictly necessary" and is **"authorised by Union or Member State law"**.

The draft Regulation clearly explains in Recital 23 that it "is not intended to provide the legal basis for the processing of personal data" under Articles 8 and 10 of the LED. This means that Member States that wish to use the exceptions provided by Article 5(1)(d) of the draft Regulation will not be able to rely on the "authorised by Union law" clause. They will only be able to use such exceptions if they adopt clear and "detailed rules of national law" (Recital 22).

This, in turn, raises the question of what the draft Regulation means when it refers to "rules of national law". Does this necessarily mean legislative measures adopted by national parliaments? Or could it mean simple non-statutory, regulatory measures adopted by competent bodies (for instance the Prime Minister or the Ministers of the Interior, Home or Justice) in EU Member States?

It is striking that the draft Regulation does not explain this issue and does not define what is meant by "rules of national law". This is clearly an oversight. However, as was stressed during the April 26 workshop, the LED fully applies and its Recital 33 (drafted in the same way as recital 41 of the GDPR) gives a clear answer to this question. According to Recital 33:

> "Where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned..."

Recital 33 of the LED also explains that such a legal basis in relation to a Member State "should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights" and moves on to highlight a series of specific requirements. The draft AI Regulation introduces additional requirements that "national laws" should enact, which concern both the prior authorisation mechanism and the specific limitations (including temporal and geographical) that the "reasoned request" by LEAs should take into consideration in order to obtain such authorisation.

(4) Assuring Consistency and Coherence in Europe

Based on the draft AI Regulation each country is entitled to create its own legal framework around the use of RBI by LEAs and each national DPA will need to assess whether to authorise such use, in response to a "reasoned request" by the country's LEAs. As mentioned during the April 26 workshop, this risks a certain fragmentation of position on the use of facial recognition in Europe including fragmentation on issues such as how necessity and proportionality should be assessed. Participants therefore raised the issue of how to achieve consistency and coherence with regard to Europe in terms of how to interpret the legal requirements imposed by the draft regulation for the use of RBI by LEAs.

This problem was addressed in a very interesting way in a previous leaked draft of the AI regulation, obtained by POLITICO (paywalled) on April 13, 2021. Article 43 of this leaked draft provided that "before giving or refusing authorisation, the authorising authority shall publish a summary of the planned use of the remote biometric identification system in publicly accessible spaces for at least 15 working days for public comments" and shall also "inform the European Data Protection Board and the European Artificial Intelligence Board of its draft decision". According to the same leaked draft article: "The European Data Protection Board and the European Artificial Intelligence Board shall ensure consistency of decisions under paragraph 3 and for that purpose adopt recommendations. [OR can object the draft decision within 10 working days.]".

The text in brackets therefore shows that the Commission initially intended that the EDPB and European AI Board would play an important role, which would include, eventually, the option to object to a national DPA's decision to authorise use of RBI by LEAs. This option was however discarded entirely in the final draft, together with all the other procedural requirements which were initially considered in the earlier version.

Those who participated in the April 26 workshop noted that, since November 2020, there have been dozens of changes to the draft AI Regulation and dozens of different drafts, as well as very intense discussions, and nobody knows why this particular version was leaked. In any case the procedural requirements that appeared in the leaked version were considered too burdensome and complicated. The risk that there would be inconsistency in the application of the RBI-related provisions of the draft AI regulation was deemed to be limited, due to a number of reasons, including the fact that European DPAs meet for discussions around EDPB matters frequently, and work very closely at a technical and legal level to ensure that regulations are applied consistently throughout Europe, which should ensure a "dialogue" between data protection authorities on the use of RBI in different countries. Participants also noted that the draft AI regulation creates additional tasks for DPAs, which will in turn require that national authorities be given additional resources.

Part III. An Important Novelty:
Pre-Market Requirements for RBI Systems and Providers

The last part of the discussion at the 26 April workshop focused on the evaluation of systems, and the conformity assessment procedure provided for in the Regulation. Here are some key takeaways.

(1) Is there a Need for a Centralised Conformity Assessment at EU Level?

Some participants mentioned the risk of fragmentation due to the fact that, under the draft regulation, certification of RBI systems must be conducted at the national level. They said that the industry/developers would very probably prefer to be certified purely at the European level, using a centralised assessment and evaluation body. This would permit the establishment of clear, centralised criteria for conformity assessment, which are not dependent on geography but on specific use cases. For example, some have highlighted the need to have a European body that has access to enough operational data for an operational assessment of algorithm performance to be conducted.

Two responses were given that addressed these concerns.

Firstly, it was emphasised that the conformity assessment procedures in the draft AI regulation were very much influenced by existing EU product safety legislation, including the 2001 General Product Safety Directive.

Therefore, in order to maintain the logic and consistency of existing product safety legislation, the conformity assessments for high-risk AI systems that are safety components of products

will follow a system in the draft regulation that already has third party conformity assessment procedures in place under the relevant sectoral product safety legislation. Similarly, conformity assessments for RBI systems introduced by the draft AI regulation should also be conducted by nationally designated bodies.

Secondly, participants stressed that several mechanisms contained in the draft regulation will prevent fragmentation between states, and will support harmonisation. Participants remarked, in particular, that the work on standardisation at European level, combined with the creation of the European AI database and the coordination bodies, including the creation of the European Artificial Intelligence Board, will ensure a harmonised, holistic life cycle approach. As mentioned in the Impact Study (at p.57), the assumption of the Commission is that a broad set of relevant, harmonised standards could be available 3-4 years from now, which would coincide with the time needed for the legislative adoption of the proposal and the transitional period envisaged before the legislation begins to apply to operators.

(2) Quality of Data Sets and Other Issues for Conformity Assessments

Some participants welcomed the importance given to data sets in the proposed Regulation, in particular the emphasis on data quality as a means of avoiding bias. However, whilst others agreed that imposing data requirements is a good thing, they raised several questions on this issue.

One speaker questioned the very notion of unbiased data, indicating that he was not sure whether it was possible to trust that any data set, no matter how well it is cleaned up and analysed, can be 100% error free. The issue of the amount of data available was also raised by a stakeholder who emphasised the need to ensure that the data set that is being used for evaluation is actually big enough to yield tangible results. Comparing the European situation with US evaluation capabilities developed by NIST, the panelist attributed the disparities not to a difference in scientific talent but to a difference in the amount of data available.

Noting that US scientists have a significant amount of sequestered data, which they can use as the basis for their evaluation, participants expressed regret that this aspect was lacking at the European level, particularly where European capabilities in this domain are concerned. Finally, one participant pointed out that keeping data sets with a view to handing them over to supervisory authorities could pose other risks, particularly in terms of storage.

In addition to the issue of data sets, participants discussed how to measure the accuracy of facial recognition systems, stressing the need to test beyond the level of a conformity assessment, so that a proper assessment can be made as to whether the system design is fair.

One participant insisted that the issues of transparency and explainability are systematically linked to the ways in which the risks that emerge from the deployment of facial recognition are mitigated, in particular where non-discrimination, access to remedy and issues around effective administration are concerned. To this end, it was argued that providers (the private sector) should provide all relevant information to the public administration authority planning to use the technology.

Another participant emphasized that the issue of demonstrating fairness and how a system works where it is to be bought by a public body should be an integral part of the procurement process rather than just a requirement for the developer/seller to explain.

The consideration of technical factors, as well as legal factors, in a risk analysis of the proposed Regulation, was welcomed by several participants. It was also noted that engineers and researchers from private companies face great difficulty when it comes to implementing certain legal requirements vis-à-vis facial recognition systems. Noting the differences in language between the legal and engineering fields, one speaker highlighted the fact that the latter would have to analyse the text thoroughly, not to shirk responsibility, but to really ensure that the regulation works in the way that it is intended to.

A particular emphasis was put on the need to take into account the *real* conditions that typically transpire when these systems are deployed, to measure their accuracy. Testing and evaluation of how the algorithm behaves in a situation that is as similar as possible to the *actual* use case is important.

For instance, an RBI system will perform differently *inside* a train station than it will *outside* the same station, due to the different light available.

(3) Testing

The aforementioned observation led to an interesting discussion about how testing in 'real' conditions (as opposed to laboratory trials) could be conducted under the provisions of the draft regulation. Several options were discussed, including the use of consent (as provided by Article 9(2)(a) of the GDPR and used, for instance, during the 2019 Nice Carnival) and the "sandboxes" system proposed in the draft regulation (Articles 53 and 54).

First and foremost, it was highlighted that **testing the technical aspects of a system is possible using consent as a legal basis** (as provided by Article 9(2)(a) of the GDPR), in the same way that testing was carried out for instance, during the 2019 Nice Carnival. This option is not challenged by the Regulation.

However, as other participants noted, the purpose of testing may go beyond technical considerations, particularly in the case of law enforcement officers' testing of the system's effectiveness for broader activities, to determine possible operational use. For this type of testing, consent cannot constitute the legal basis, since for a stakeholder, this can be likened to active deployment, which implies that there are non-participants or people not on the watch list whose rights might be affected. A panelist highlighted that it was precisely such a lack of legal basis that had prompted the German police to stop testing of this nature at the Banhhof Südkrauz station in Berlin.

The draft AI Regulation seeks to propose a legal basis for the testing of systems by introducing **sandboxes** (Article 53 and 54). Firstly, it was made clear that these sandboxes form part of the pre-market framework, as indicated in Recital 72 of the Regulation, and aim to ensure compliance with the requirements laid down in the Regulation. These sandboxes therefore allow the developer of a system to test and develop it using data that had previously been lawfully collected for another purpose (Article 54(1)). Since the law enforcement framework in which 'real-time' RBI systems are used is a special sector because of the risks to fundamental rights, the possibility of using these sandboxes needs to be explicitly provided for in national law.

In view of the concern expressed by one participant about the idea that because you're just testing a technology, you might not really have to meet all the requirements, it was highlighted that the proposed Regulation intends to set **a strict framework** for these

Sandboxes. Article 54.1 (d) therefore necessitates the establishment of mechanisms to monitor the occurrence of risks during these tests in order to take appropriate corrective action or, failing that, to stop the test. It was also mentioned that national data protection authorities must be involved from the outset in the implementation of these Sandboxes, and that the competent authorities have the power to stop them in the event of non-compliance with the requirements or the appearance of significant risks (Article 53 (2) and (3)). In any case, it was highlighted that due to the particular nature of the data involved in the Sandboxes, which is intended to test 'real-time' RBIs, the prior establishment of a **Data Protection Impact Assessment**[vii] would be required.

Furthermore, one participant noted the importance of the relationship between the system and the natural person using it. Therefore, it has been said that the best way to ensure accuracy is not by solely using the system but by combining the insight of a trained expert with the information that an AI facial recognition system can provide. It was therefore recommended that the training of the people that oversee the system (i.e. the operators) should be given special attention. Recalling that not all algorithms are configured equally, a participant encouraged the authorities to take this into account in their choice of system according to how they intend to deploy it.

(4) RBI Systems Already Available On the Market

Another issue raised during the April 26 discussions was the relationship between the conformity assessment requirements and the facial recognition systems that are already on the market and/or have been put into service. An example given was the use of post-RBI for forensic purposes in certain countries: should the systems that are already in use then be subject to the conformity assessment procedures of the draft AI Regulation once it enters into force?

Clearly the answer is no. Article 83 of the draft Regulation addresses this issue by stating that: "This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before *[12 months after the date of application of this Regulation referred to in Article 85(2)]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned".

As stressed during the April 26 workshop the rationale behind this provision was that the draft Regulation should not have a retroactive effect. Therefore only the products which are already on the market but undergo a substantial modification will fall under the new requirements and conformity assessment procedures.

This, in turn, led to a discussion about how to ensure ex-post monitoring.

(5) Ex-post monitoring and a Life-Cycle Approach

During the April 26 workshop several participants stressed the need for oversight of "certified" RBI systems throughout their entire lifecycle. It was noted, for instance, that while accuracy can improve over time, regular reevaluation is needed. One participant argued accordingly that using a technology which is not transparent, and which cannot be evaluated, should not

be acceptable. Furthermore, it was pointed out that we should not hesitate to stop certain systems if they don't perform as they are intended to.

The response given to these concerns was that, in addition to ex-ante conformity assessments, the draft Regulation provides for an ex-post system for market surveillance and supervision by national competent authorities designated by Member States. Indeed, enforcement bodies (in particular DPAs) can go back to the provider at any point and request information about the training required for a specific RBI system, and whether it functions properly. The EU-wide database created by the draft Regulation will be accessible to everyone, which means that there will be quite a bit of control that can be exercised in terms of whether things are going well or not. These factors, combined with progressive standardisation, should ensure a holistic life-cycle approach and should provide safeguards that go beyond the initial pre-market requirements and procedures.

Conclusion

All participants in the April 26 workshop acknowledged that the process of adoption of the draft AI regulation will be long. As a first step, the European Data Protection Board and the EDPS have been asked to provide a joint opinion on the draft Commission's proposals in the next eight weeks, a period during which the draft is also open to public consultation. It will be interesting to see, in the next step, to what extent the Council of the EU and the European Parliament (several Committees of which had been competing to instruct the AI legislative proposal[viii]) will be able to find common ground on the issues of RBI and facial recognition. As shown by the initial reactions to the draft AI proposal, these issues will be crucial in the discussions about the draft AI regulation. The debate has just begun and it is essential to have a good understanding of what is proposed by the Commission...

LIST OF PARTICIPANTS

The following persons participated in the April 26 workshop[ix]:

1. **Antoine-Alexandre Andre,** European Commission
2. **Mathias Becuywe,** University Grenoble-Alpes
3. **Stephanie Beltran Gautron**, Grenoble-Alpes Data Institute
4. **Vincent Bouatou,** IDEMIA
5. **Claude Castelluccia,** INRIA
6. **Fabio Chiusi,** Algorithm Watch
7. **Theodore Christakis**, University Grenoble-Alpes
8. **Damianos Chronakis,** Europol
9. **Alexandru Circiumaru,** Microsoft
10. **Maeva El Bouchikhi,** University Grenoble-Alpes
11. **Zsuzsanna Felkai Janssen,** European Commission
12. **Peter Fussey**, University of Essex
13. **Mona Giacometti,** UCLouvain
14. **Cornelia Kutterer**, Microsoft
15. **Gwendal Le Grand,** CNIL
16. **Wim Liekens**, Belgian Federal Police
17. **Jean-Michel Mis**, Member of French Parliament
18. **Olivier Micol,** European Commission
19. **Evdoxia Nerantzi,** Microsoft
20. **Michal Nespor**, FRA
21. **Irina Orssich,** European Commission
22. **Marion Oswald**, University of Northumbria
23. **David Reichel**, FRA
24. **Gilles Robine,** European Commission
25. **Ilona Ruys**, Belgian Federal Police
26. **Fraser Sampson**, Surveillance Camera Commissioner
27. **Frank Torres,** Microsoft
28. **Anaïs Trotry**, University Grenoble Alpes
29. **Petar Vitanov**, European Parliament
30. **Paul Wouters,** Belgian Federal Police

[i] In the public consultation on the White Paper on AI, 28% of respondents supported a general ban of this technology in public spaces, while another 29.2% stated that a specific EU guideline or legislation should be adopted before such systems may be used in public spaces. 15% agreed with allowing remote biometric identification systems in public spaces only in certain cases and under certain conditions and another 4.5% asked for further requirements (on top of the 6 requirements for high-risk applications proposed in the white paper) to regulate such conditions. Only 6.2% of respondents did not think that any further guidelines or regulations are needed. See here, at 11.

[ii] The European Data Protection Supervisor (EDPS), for instance, said he "regrets to see that our earlier calls for a moratorium on the use of remote biometric identification systems - including facial recognition - in publicly accessible spaces have not been addressed by the Commission"

[iii] NGOs such as EDRi called on European legislators to "reject the idea that some forms of remote biometric identification are permissible" and to "instead implement a full prohibition on all forms of biometric mass surveillance practices in publicly accessible spaces by all public authorities and private actors".

[iv] According to Article 3 (37) of the draft Regulation, **"'real-time' remote biometric identification system'** means "a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention".

[v] According to Article 3 (38) of the draft Regulation, **"'post' remote biometric identification system'** means "a remote biometric identification system other than a 'real-time' remote biometric identification system".

[vi] The Commission clearly considered RBI from the point of view of data protection though and this is why it explained (both in the Explanatory Memorandum p.6 and in Recital 23) that "it is appropriate to base this regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU". (p.6)

[vii] In this field, two INRIA researchers affiliated with the Chair, Claude Casteluccia and Daniel le Métayer, have published a methodology for Data Protection Impact Assessment. This methodology, which is the only one proposed so far, can be found here.

[viii] After the workshop it was reported that the European Parliament's internal market committee (IMCO) had finally been appointed to lead the Parliament's work on the draft AI Regulation. Other committees will be able to present their opinions, but IMCO will be the leading committee.

[ix] Please note that other persons (such as representatives of NGOs involved with the Reclaim Your Face campaign) had also been invited to participate but had in the end been unable to do so.

This work has been partially supported by MIAI @ Grenoble Alpes, (ANR-19-P3IA-0003)