Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

NOTE
ON THE RULES IN THE AI ACT ON THE USE OF "REAL TIME" REMOTE BIOMETRIC IDENTIFICATION IN PUBLICLY ACCESSIBLE PLACES BY LAW ENFORCEMENT AGENCIES

Nota Bene:

This Note is based on the unofficial 258-page consolidated text of the proposed EU Artificial Intelligence Act ("AI Act") released online on 22 January 2024 by European Parliament Senior Advisor Laura Caroli, at: https://www.linkedin.com/posts/dr-laura-caroli-0a96a8a_ai-act-consolidated-version-activity-7155181240751374336-B3Ym/

Some issues are still under consideration, but the text as discussed here appears to be the definitive one (subject to re-numbering of the articles and non-substantive editing),* due for adoption by the Council (COREPER) on 2 February 2024 (although it will only come into application later, in phases).

* In this Note, I use the numbers given to articles and paragraphs in the above text, but as noted in brackets, above, the numbering in the final text will be tidied up. I will try and amend the text to reflect the final numbers (and any possible final textual changes) in due course. When I conclude that an issue is problematic from a fundamental rights point of view, I put the relevant text in **red**.

The AI Act rules on the use of "real-time" remote biometric identification systems in publicly accessible places for the purpose of law enforcement

Civil society fought a strong campaign against allowing the use of "real time" remote biometric identification (RBI) systems in publicly accessible spaces by public and private entities, arguing that the use of such systems in such places effectively puts everyone constantly in a suspects' line-up that threatens the exercise of fundamental rights such as the right to demonstrate and express one's opinion in public, i.e., that it amounts to mass surveillance.[1] But in the end, the AI Act only contains an in-principle prohibition on the use of such systems in publicly accessible places for law enforcement purposes, subject to complex conditions and exceptions, as noted below. This in-principle prohibition-with-exceptions aside, the use of all RBI systems ("real time" or otherwise including "post" RBI, and in publicly accessible and not publicly accessible places) is classified as "high risk", subject to various conditions and restrictions, but not banned.

Before discussing the rules on the use of **"real time" RBI*** in **publicly accessible places*** for **law enforcement purposes***, it is important to first clarify the meaning given to those concepts, and related concepts, in the Act:

- A "'**real time' RBI system**" is defined as "*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*" (Article 3(37)). This is in contrast to the concept of a "'post' RBI system", not discussed here.

[1] See, e.g., "*Protect My Face: Brussels residents join the fight against biometric mass surveillance*", EDRi, 29 March 2023, available at: https://edri.org/our-work/protect-my-face-brussels-against-biometric-mass-surveillance/ But note that the links to the overall "*Reclaim My Face*" campaign in the above no longer work.

- The concept of "**publicly accessible space**" is defined as "*any publicly or privately owned physical place accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions*" (Article 3(39)). This includes, e.g., shopping centres, sport grounds and school playgrounds.
- The words "**law enforcement**" cover "*[all or any] activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*" (Article 3(41)). The term "**law enforcement authority**" covers not only typical state law enforcement bodies (police, prosecutors, etc.), but also "other bodies or entities" that are entrusted by a Member State to exercise similar functions and powers (Article 3(40)). This does not cover actions by private entities (e.g., banks) to detect and counter crimes (such as fraud) on their own behalf, but could cover the activities of private entities, including banks, that they are required to undertake to counter certain crimes (such as money laundering). **The lines are not clear.**

The AI Act allows the use of "real time" RBI in publicly accessible places for the purpose of law enforcement only in relation to a number of more specific purposes, and even then only subject to important conditions, restrictions and procedures. Thus, first of all, the use of such systems in such places for such purposes is only allowed when this is ***strictly necessary*** for one of the following purposes:

- the <u>targeted search</u> for specific victims of abduction, trafficking in human beings and sexual exploitation of human beings as well as search for missing persons;
- the <u>prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons</u> or <u>a genuine and present or genuine and foreseeable threat of a terrorist attack</u>;
- <u>the localisation or identification of a person suspected, being investigated or having been convicted of an offence</u> listed in Annex IIa* and that is punishable by a custodial sentence for a maximum of at least four years.

(Article 5(1)(d))*,**

* Annex IIa lists the following **serious criminal offences**: terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in weapons, munitions and explosives; murder; grievous bodily injury; illicit trade in human organs and tissue; illicit trafficking in nuclear or radioactive materials; kidnapping; illegal restraint and hostage-taking; crimes within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft/ships; rape; environmental crime; organised or armed robbery; sabotage; participation in a criminal organisation involved in one or more offences listed above.

** A final sentence to Article 5(1)(d) says that "*[t]his paragraph is without prejudice to the provisions in Article 9 of the GDPR for the processing of biometric data for purposes other than law enforcement.*" But this appears to be redundant since the whole of Article 5(1)(d) only applies to the use of "real time" RBI in publicly accessible places for law enforcement purposes.

Article 5(2) adds that *"[t]he use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives [set out above] shall*

only be deployed for [those purposes] ***to confirm the specifically targeted individual's identity***". In other words, "real time" RBI may be used in relation to already known victims, persons known to pose a threat, or known suspects or convicts – but it may not be used to mark ("identify") a not previously known person as such.[2]

In addition, secondly, the Act imposes a number of <u>further conditions and safeguards</u> (which themselves are subject to yet further exceptions, indicated below by "<u>BUT</u>") on the exceptionally allowed use of "real time" RBI for law enforcement purposes:

- **<u>Based on a law/more specific national legal rules?</u>:**

  The text says that Member States "may" (further) regulate the use of "real time" RBI in publicly accessible places for law enforcement purposes by <u>law</u>; and that the relevant law must then reflect the conditions noted above and below and may be stricter (but not more lax) than the AI Act (cf. Article 5(4)).*

  *NB: See also the insertion in the unofficial text of the word "concerned" in italics in the second sentence of Article 5(4): this suggests that only Member States that choose to adopt laws on the use of "real time" RBI by law enforcement need to ensure that those laws follow the rules in the Act. But **it would make more sense to require all Member States to adopt legal national rules to lay down the relevant conditions in proper detail, with reference to their own peculiar legal system.** The existence of such national rules is also assumed by the reference in Article 5(3a) to notification having to be done "in accordance with the national rules referred to in paragraph 4". (On notification, see the separate bullet-point on that issue, below).

- **<u>Subject to prior authorisation based on a reasoned request</u>:**

  Each use of "real time" RBI is subject to <u>prior authorisation</u> by a judicial or independent administrative authority, issued upon a <u>reasoned request</u> and in accordance with the above-mentioned national law –

  <u>BUT</u> in cases of "**a duly justified situation of urgency**", authorisation can be requested *ex post*; if such an *ex post* request is rejected, the RBI "*shall be stopped with immediate effect and all the data, as well as the results and outputs of this use shall be immediately discarded and deleted*".

  (Article 5(3), first sub-clause).

---

[2] Note that the term "identify" is ambiguous, and used confusingly in EU law. On the one hand, it can mean "confirming that a certain person is a specific person named (or otherwise identified) on a list or official record or document" (such as a list of missing persons, or escaped convicts). On the other hand, it is used to indicate "identification" of an individual (or an individual's actions) as matching certain pre-determined criteria (be these simple or complex), which merely indicates a certain probability (which can be quite low) that the person "may" fall into a pre-defined category. I have discussed this in relation to the use of PNR data to "identify" people who "may be" terrorists or serious criminals in the introduction to section 4.9 of my <u>Opinion on Core Issues in the PNR CJEU Case</u>, prepared at the request of the Fundamental Rights European Experts Group (FREE Group), November 2021, available at:
https://www.ianbrown.tech/wp-content/uploads/2021/12/KORFF-FREE-Paper-on-Core-Issues-in-the-PNR-Case.pdf
(With reference to an earlier, 2015, report on PNR, prepared for the Council of Europe with Marie Georges.)
Suffice it to note here that "identification" as used in the AI Act rules on "real time" RBI in publicly accessible spaces for law enforcement purposes must be limited to the first kind of "identifcation".

- **After a prior fundamental rights assessment and registration:**

  Such a request may only be issued after the law enforcement authority concerned has completed a fundamental rights impact assessment (as provided for in Article 29a) and has registered the system in the database of AI systems (that must be established in each Member State according to Article 51) –

  BUT "**in duly justified cases of urgency**, *the use of the system may be commenced without the registration, provided that the registration is completed without undue delay*".

  (Article 5(2))

  The reference to not-yet-registered systems may relate to RBI systems that are being developed and tested "in real world conditions" in "regulatory sandboxes", prior to deployment (cf. the definition of "AI regulatory sandbox" in Article 3(44bg) and Title V). If I understand this correctly, such "sandboxed" systems need not yet have undergone a fundamental rights impact assessment, and need not yet be registered in the relevant database – but may, where "appropriate", be operated in "real world conditions", which presumably means, applied to real world data in "real time". If I am correct in this, it could create a loophole in that it would allow authorisation for the use in the real world (outside of the sandboxes) and in "real time" of not yet fundamental rights assessed or registered RBI systems "in duly justified cases of urgency".

- **Conditions for authorisation:**

  The relevant court or authority may only grant the authorisation if it is:

  > satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is **necessary** for and **proportionate** to achieving one of the objectives specified in [the first three bullet-points, above], as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as geographic and personal scope.
  >
  > (Article 5(3), second sub-clause, first sentence)

  In deciding on the request, the court or administrative authority must take the following elements into account:

  > (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;
  >
  > (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.]"
  >
  > (Article 5(3), second sub-clause, second sentence, read together with Article 5(2))

  However, the Act also adds (in rather convoluted language) that:

  > It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by the judicial authority or an independent administrative

> authority whose decision is binding solely based on the output of the remote biometric identification system.
>
> (Article 5(3), second sub-clause, final sentence)

I am assuming that "adverse legal affects on a group of people" is also covered by the above; and that a decision that negatively affects the fundamental rights of people in the group – e.g., that has a chilling effect on the right to demonstrate – always by its very nature has an "adverse legal effect" on the members of that group. In other words, this *caveat* covers the very decision to authorise the use of "real time" RBI, at least in relation to the surveillance of publicly accessible places.

If I correct in the above analysis, the *caveat* appears to say that the decision of the the court or administrative authority to authorise "real time" RBI in a publicly accessible place for law enforcement purposes may not itself be based on "the output of the RBI system". But that makes no sense: prior to any authorisation, "the RBI system" in question may not be used – so how can there already be any "outputs"? Unless of course this refers to the use of such a system without (i.e., prior to) authorisation, "in duly justified cases of urgency". But that suggests that this supposedly highly exceptional unregistered use of the system may in practice be not quite that exceptional …

- Each use of "real time" RBI must also be notified to the relevant market surveillance authority and the national data protection authority (that between them must ensure compliance with the AI Act) (Article 5(3a)). The Act does not stipulate that this notification must happen at the same time as the request for authorisation (i.e., prior to any use of such RBI), or even at or shortly after any authorisation. The latter would seem to be the easiest, with the authorising authority simply copying the supervisory authorities in to the authorisation. But it would appear that in fact the notification may well take place (much?) later: the Act adds that "*[t]he notification shall as a minimum contain the information specified under paragraph 5 and shall not include sensitive operational data*" (also Article 5(3a))). The reference to "the information specified under paragraph 5" is rather obscure, since that paragraph merely refers to a "template" for the annual reporting on the use of "real time" RBI (noted in the next bullet-point) that is to be drafted by the Commission and that must "*includ[e] information on the number of the decisions taken*" by the competent authorities "*and their result*". **This** suggests that the notification too can – or perhaps even should? – include those "results", which **would mean that the notification may only happen after the specific use of the relevant "real time" RBI has finished. In other words, if this reading is correct, the national supervisory authorities can only do a retrospective check on the deployment of "real time" RBI by law enforcement agencies – but even then without being given access to "sensitive operational data". That does not appear to be a very effective form of oversight. Moreover, it would appear that these reports will not be published: in contrast to the report mentioned in the next bullet-point, Article 5(5) does not refer to publication.**
- As just noticed, the national supervisory authorities must submit to the Commission an annual report on the uses of "real time" RBI in publicly accessible places that must be based on an as yet still to be drawn up template, but that must include information on the

number of authorisations for such use issued in the year in question, and on the "results" of those deployments (Article 5(5). The Commission must then "***publish*** *annual reports on the use of [the systems] based on aggregated data in Member States based on the annual reports" submitted by the national supervisory authorities*" (Article 5(6)). The article re-emphasises that these "*shall not include sensitive operational data of the related law enforcement activities*" (*idem*).

This system of reporting only aggregate data, without even the underlying national statistics, will not ensure transparency over the real use of "real time" RBI in publicly accessible places by law enforcement agencies after the coming into application of the AI Act. Given the singular failure of the Member States and the Commission to provide proper, peer-reviewable information on other intrusive systems such as mandatory e-communication data retention and the collection, analyses and uses of PNR data, and the "results" of those other intrusive activities (and the refusal to even develop proper methodologies for the collection and reviewing of such data, or to even define how the "results" of such activities are to be assessed),[3] this gives rise to the expectation that reporting on the use of highly intrusive "real time" RBI in publicly accessible places by law enforcement, too, will be useless and amount to the misrepresentation of the real effects of those systems. This is a major defect of the rules as currently drafted.

- o – O – o -

Douwe Korff (Prof.)
Cambridge (UK), 30 January 2024

[3] See my note on The Lack of Data on the Effectiveness of Mass Surveillance, May 2023, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4437119