Exercise 2 – Hi! Paris Summer School
Case Study – The Legality of Remote Biometric Systems and Video surveillance under the EU AI Act

In different parts of the world, companies have been developing biometric systems (particularly face recognition technologies) to identify and verify individuals. Such systems have been implemented by different private entities across different parts of the world to perform face recognition for security purposes, for instance, in the context of banks, casinos, private companies, shopping centers, etc. They also have been used by police departments to identify potential suspects comparing the images captured by the remote cameras in certain areas with the images contained in their internal databases.

Other companies have also been developing video surveillance systems which arguably do not analyze the biometric features of individuals, but that identify patterns of motion, movements, crowds that could indicate threats.

In the French context, the use of both face recognition systems and video surveillance have been extensively discussed with the preparations for the upcoming Olympic Games. From the one side, it has been argued that such technologies could enhance safety and undermine the threats of terrorist attacks. From the other side, it has been claimed that they could undermine fundamental rights such as data protection, non-discrimination, freedom of expression and freedom of assembly.

Let us consider whether and in what terms such technologies could be employed if the EU AI Act were to be currently applicable.

Question 1

CLASSIFICATION OF RISK. Classification of risk of the face recognition system produced – i.e., under which circumstances will it be prohibited, high-risk, low risk or no/minimal risk?

1. The class will be divided into two groups.

   a. **GROUP 1 – The use of facial recognition under the AI Act**

- Are we allowed to use real-time face recognition to identify potential persons of risk during Olympic Games under AI Act?

- If yes, under which circumstances would that be likely possible? If not, what are the likely legal arguments that could raised used against that use?

b. GROUP 2 – The 2023 French law authorizing real-time video surveillance

- Does video surveillance as planned for the Olympic Games would likely constitute a prohibited practice under the AI Act? Consider particularly the distinction between face recognition and videosurveillance. (see this article https://www.reuters.com/sports/olympics-how-france-plans-use-ai-keep-paris-2024-safe-2024-03-08/)

- Does videosurveillance constitute a high-risk practice under the AI Act?

EU AI Act (2024 – version as of May 14, 2024
https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf)

Article 5

1.The following artificial intelligence practices shall be prohibited:

(…)

(e) the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

(g) the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

(h) the use of 'real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.

2. the use of ‘real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual, and it shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used;

(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.

In addition, the use of ‘real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), of this Article shall comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with the national law authorising the use thereof, in particular as regards the temporal, geographic and personal limitations. The use of ‘real-time remote biometric identification systems in publicly accessible spaces shall be authorised only if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the EU database according to Article 49. However, in duly justified cases of urgency, the use of such systems may be commenced without the registration in the EU database, provided that such registration is completed without undue delay.

(…)

3.For the purposes of paragraph 1, first subparagraph, point (h) and paragraph 2, each use for the purposes of law enforcement of a real time remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5. However, in a duly justified situation of urgency, the use of such system may be commenced without an authorisation provided that such authorisation is requested without undue delay, at the latest within 24 hours. If such authorisation is rejected, the use shall be stopped with immediate effect and all the data, as well as the results and outputs of that use shall be immediately discarded and deleted.

The competent judicial authority or an independent administrative authority whose decision is binding shall grant the authorisation only where it is satisfied, on the basis of objective evidence or clear indications presented to it, that the use of real time remote biometric identification system concerned is necessary for, and proportionate to, achieving one of the objectives specified in paragraph 1, first subparagraph, point (h), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In deciding on the request, that authority shall take into account the elements referred to in paragraph 2. No decision that produces an adverse legal effect on a person may be taken based solely on the output of the real time remote biometric identification system.

(…)

5. A Member State may decide to provide for the possibility to fully or partially authorise the use of real time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement within the limits and under the conditions listed in paragraph 1, first subparagraph, point (h), and paragraphs 2 and 3. Member States concerned shall lay down in their national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision and reporting relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, first subparagraph, point (h), including which of the criminal offences referred to in point (h)(iii) thereof, the competent authorities may be authorised to use those systems for the purposes of law enforcement. Member States shall notify those rules to the Commission at the latest 30 days following the adoption thereof. Member States may introduce, in accordance with Union law, more restrictive laws on the use of remote biometric identification systems.

Article 6
Classification rules for high-risk AI systems

(…)

(2) In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometrics, in so far as their use is permitted under relevant Union or national law:
(a) remote biometric identification systems.

This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;
(b) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;
(c) AI systems intended to be used for emotion recognition.

2. Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.

(…)

6. Law enforcement, in so far as their use is permitted under relevant Union or national law:
(a) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences;
(b) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools;
(c) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;
(d) AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;
(e) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences.

Question 2

COMPLIANCE WITH AI ACT FOR HIGH-RISK SYSTEMS. After clarifying under which circumstances the deployment of biometric AI systems will be allowed, but still considered high-risk, what are the steps required and challenges to ensure compliance?

We have now identified which types of biometric systems would NOT be prohibited under the AI Act. Most of the allowed systems, however, would still be considered high risk and would still be subject to different compliance requirements before entering into the market.

The AI Act contains many compliance requirements applicable to high-risk systems, foremost among them the following:

a. Risk management systems (Art. 9)
b. Data protection, data quality and data governance (Art. 10)
c. Technical documentation (Art. 11)
d. Record-keeping (Art. 12)
e. Transparency and interpretability (Art. 13)
f. Human oversight (Art. 14)
g. Accuracy, robustness and cybersecurity (Art. 15)

Many of these requirements and others are specified in technical standards developed by standardization organizations.

Please:

1. Select one of the two articles highlighted above, examine it/them and seek to elaborate what types of compliance issues they would likely generate for biometric systems and why.

2. Indicate what requirements are still unclear or too vague and should be subject to further specification by the regulation/technical standards or through other instruments.

The relevant articles are contained in EU AI Act, accessible in the following link, pages 189-201: https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf.