

# FACTSHEET NO. 3

## PEACEFUL ASSEMBLIES AND FACIAL RECOGNITION TECHNOLOGY: INTERNATIONAL STANDARDS



European Center for  
Not-for-Profit Law

 #right2freeassembly

### 01. What is Facial Recognition Technology (aka FRT) and how does it work?

Simply put, facial recognition is the process of using biometrics – i.e., measurements of an individual's unique biological (in this case, facial) features – to compare images in order to make one or more of the following decisions:

**1. Verification (one-to-one):** comparing a face to another specific image to determine if the individual shown in the two images is the same person. This process can be carried out, for example, for purposes of authentication and/or authorisation to ensure that the individual is indeed who they claim they are: e.g., when you use your FaceID to unlock your iPhone or scan your passports at Automated Border Controls at airport gates, a live image is taken on the spot, the FRT compares it with the biometric features (aka biometric template) stored in the iPhone or in the passport and if the probability of the two images being of the person is above a certain statistical threshold, the identity is verified and access granted.

**2. Identification (one-to-many):** comparing a face to a pre-existing set of faces/biometric templates to find out if the face corresponds to one or more faces/images already stored in centralised databases or watchlists: e.g., when the police check if the person in the image matches one image of suspects, criminals or persons of interest; or when a shopping mall security guard checks an individual's face from a CCTV camera against a list of persons previously banned for shoplifting.

### 3. Classification (matching general characteristics):

analysing facial features of one or more individuals to categorise their expressions (smile, laugh, frown, etc.) and/or features (skin colour, texture, skull structure, eye colours, etc.) in order to match them with characteristics such as emotions (anger, joy, fear, sadness, etc.) or sex, age and ethnic background. This type of FRT is already used, e.g., by some advertisers to test customers' responses to products but it could also be used to identify potentially dangerous people in certain contexts (such as public protests) before they act violently.

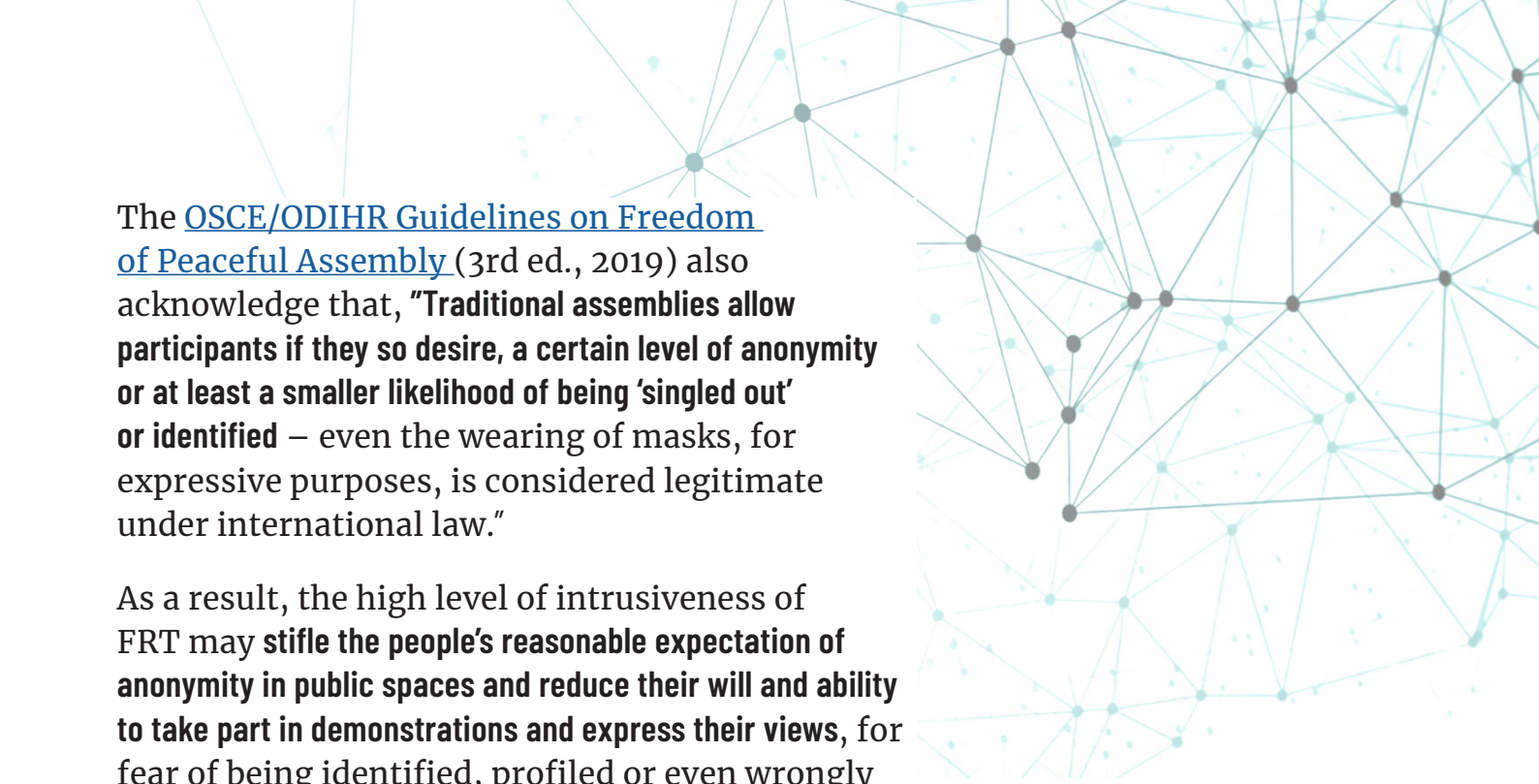
## 02. What kind of technology does FRT rely on nowadays?

To different extents and with different complexity levels, all these types of FRT today rely on statistical analysis and algorithm-based systems (aka, machine learning or artificial intelligence/AI) that learn how to identify consistent patterns in biometric templates after being trained on existing datasets of images.

FRT can take the form of live FRT – that is, when the images of an individual are taken from videos (e.g., CCTV cameras in publicly accessible spaces) in real time to be compared, matched or classified in near-real time. Therefore, live FRT can also be defined as a specific form of video surveillance of people in public or publicly accessible spaces, including at peaceful assemblies.

The use of FRT in publicly accessible spaces constitutes an interference with several fundamental rights of individuals, including their rights to privacy and to take part in a peaceful assembly. As the UN Human Rights Committee (HRC) [General Comment \(GC\) No. 37 on Article 21 \(Right of Peaceful Assembly\)](#) of the International Covenant on Civil and Political Rights (ICCPR) clarifies, **"the mere fact that a particular assembly takes place in public does not mean that participants' privacy can be violated"** (para 62).

## 03. How can FRT affect my right to take part in a peaceful assembly?



The [OSCE/ODIHR Guidelines on Freedom of Peaceful Assembly](#) (3rd ed., 2019) also acknowledge that, “**Traditional assemblies allow participants if they so desire, a certain level of anonymity or at least a smaller likelihood of being ‘singled out’ or identified** – even the wearing of masks, for expressive purposes, is considered legitimate under international law.”

As a result, the high level of intrusiveness of FRT may **stifle the people’s reasonable expectation of anonymity in public spaces and reduce their will and ability to take part in demonstrations and express their views**, for fear of being identified, profiled or even wrongly persecuted.

## 04. What risks are commonly associated with FRT?

As the [Fundamental Human Rights Agency of the EU](#) (FRA) warns, “**an algorithm never returns a definitive result, but only probabilities**”: this means that when a large number of peoples’ images are checked in mass (in real time or not), even if the risk of a false positive (i.e., a person wrongly identified as someone in a watchlist of suspects or persons of interest) was reduced to 1%, a significant number of people would still likely to be wrongly identified (e.g., 1000 people out of 100,000 demonstrators in a public assembly).

The risk of wrong identification is further compounded by the risk of **bias and discrimination**. FRT can have higher error rates depending on the quality of the image and the environment in which it is extracted, but also depending on the age, gender, skin colour, etc. of the individuals. Even the dataset of images against which the FRT systems are trained may amplify existing social bias against people of colour, minorities, women and other vulnerable groups, perpetuating discriminations against them.

Last but not least, **FRT can be done openly but also covertly**. People whose images are taken and processed may not know this is happening or may not be in a position to avoid this from happening, so their right to challenge such use and possible abuse is also compromised.

In her [2020 Report on the impact of new technologies on human rights in the context of peaceful protests and assemblies](#), the UN High Commissioner For Human Rights acknowledges the “considerable adverse effects” of the use of FRT and states that “Authorities should generally refrain from recording assembly participants”, with the only exceptions of situations in which “there are concrete indications that serious criminal offences are actually taking place

or that there is cause to suspect imminent and serious criminal behaviour, such as violence or the use of firearms.” In other words: **the use of FRT in the context of assemblies should be the exception, not the rule**, and such exception should always meet the three-part-test of being established by law, necessary for a legitimate cause and proportionate. Authorities should also put in place **a regulatory framework effectively protecting personal data, including facial images and data processed and establishing times for data retention, deletion, right of access, right to rectification of false matches and oversight mechanisms.**

The UN’s standards are also reflected in the [OSCE/ODIHR Guidelines on Freedom of Peaceful Assembly](#), which similarly state that, “**The use of image recording for the purpose of identification (including facial recognition software) should be confined to those circumstances where criminal offences are actually taking place, or where there is a reasonable suspicion of imminent criminal behaviour**” (para 172).

The [Council of Europe Guidelines on Facial Recognition](#) (2021) equally indicate that States should adopt **a robust legal framework applicable to the different cases of FRT use and data processing** that should include:

1. the **specific use and intended purpose**;
2. **minimum reliability and accuracy levels of the algorithms** used;
3. **retention duration of images** captured;
4. **minimisation of data** processed;
5. possibility of **auditing** the system;
6. **traceability** criteria of the whole process;
7. **all other safeguards** (including right to information, right of access, right to obtain knowledge of underlying reasoning, right to object and right to rectification) and where these are restricted, how such restrictions comply with the three-part test (legality, necessity and proportionality) and do not impair the essence of the rights.

## 05. What do the international human rights standards protecting assemblies say about FRT?



Sweden  
Sverige



Text by the European Center for Not-for-Profit Law Stichting (ECNL) as part of the ‘Monitoring the Right to Free Assembly’ regional project. The project is made possible by the International Center for Not-for-Profit Law (ICNL) through

the Civic Space Initiative, financed by the Government of Sweden. The Government of Sweden does not necessarily share the opinions here within expressed. The author bears the sole responsibility for the content.

However, the Guidelines also recommend that, **“The use of live facial recognition technologies in uncontrolled environments, in light of its intrusiveness on the right to privacy and the dignity of individuals, coupled with the risk of an adverse impact on other human rights and fundamental freedoms, should be subject to a democratic debate and the possibility of a moratorium pending a full analysis.”**

In the context of the EU countries in particular, the [FRA](#) has reiterated the need to apply the three-part test to the use of FRT and data processing as per Article 52(1) of the [Charter of Fundamental Rights](#) of the EU (CFR), since **the mere existence of an objective of general interest – such as crime prevention or public security – “is not, it itself, sufficient to justify an interference”** with the fundamental rights of the people, including Article 12(1) of the CFR, which protects freedom of assembly and association.

Finally, in a [Joint Opinion](#) released on the EU proposal to regulate AI, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) – respectively the EU body in charge of the application of the EU General Data Protection Regulation (GDPR) and the EU independent data protection authority – call for **a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces – including FRT - in any context.** The EDPB and EDPS argue that this stricter approach is necessary because, **“The use of AI systems might present serious proportionality problems, since it might involve the processing of data of an indiscriminate and disproportionate number of data subjects for the identification of only a few individuals.”** According to EDPS and EDPB, remote biometric identification – including FRT – of individuals in publicly accessible spaces also presents still unsolved problems of **lack of transparency on how these systems work and process data.** As a result, they have an **“irreversible, severe effect on the populations’ (reasonable) expectation of being anonymous in public spaces, resulting in a direct negative effect on the exercise of freedom of expression, of assembly, of association as well as freedom of movement.”**