Biometric Mass Surveillance:
What is it, and why does it need to be banned?

According to the General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive (LED), **biometric data are an especially sensitive type of personal data**. The process of biometrics refers to turning our bodies and our behaviours into data through specific technical processing for the purpose of uniquely identifiying us.

Mass surveillance relates to actions which rely on watching the public indiscriminately. This means that such actions lack reasonable suspicion, and do not give people sufficient possibilities to know what is happening, to give genuine consent, or to have a truly free choice to opt in or out. The Council of Europe defines it as any monitoring that is not performed in a "targeted" way against a specific individual, and the EU Fundamental Rights Agency explains that untargeted surveillance is that which is done "without prior suspicion".[1] Privacy International adds that mass surveillance "uses systems or technologies that collect, analyse, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing."[2]

When systems or technologies are used to process anyone's biometric data in public spaces such as parks, squares or online public spaces (or in publicly-accessible spaces such as arenas and train stations) **this can be considered biometric mass surveillance**. This is because performing untargeted biometric recognition in public spaces relies on (1) the indiscriminate or arbitrarily-targeted collection, processing or storage of sensitive biometric data, (2) which is undertaken on a large scale, (3) without the control or knowledge of the random passersby that are an inherent feature of public spaces. This is different from targeted or personal uses such as unlocking one's personal phone, as this use does not infringe on people's ability to enjoy their rights in public spaces.

Biometric mass surveillance technologies work by collecting or analysing the biometric data of everyone that enters those spaces, even if their data is later discarded. This creates a genuine perception of being watched all the time, which can create what is known as a **"chilling effect"**; disincentivise people from participating in public life; and unduly restrict many of our fundamental rights and freedoms.[3] Such uses in public spaces may also be combined with mass-scale citizen scoring, profiling, and/or "affect" (emotion) recognition, all of which can unduly restrict people's fundamental rights and freedoms.

1 https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e; https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_en.pdf
2 https://privacyinternational.org/learn/mass-surveillance
3 https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

EDRi calls for a European prohibition on uses which constitute mass surveillance, regardless of whether they are deployed by public or private actors. Real examples of uses in the EU include the following:

- In 2019, a so-called "innovative" biometric surveillance system was deployed in the **Italian** municipality of Como. It was used to widely monitor public spaces in order to detect "loitering", and included the green spaces where hundreds of migrants had previously been stranded after being turned away at the Swiss-Italian border.[4] This constitutes biometric mass surveillance.

- European police forces have started to use biometric technologies against protesters. In 2020 in **Slovenia**, the police's widespread use of facial recognition has been coupled with surveillance of online and social media profiles, and this has been used to surveil and target anyone attending a legitimate protest.[5] This constitutes biometric mass surveillance.

- In 2019, the **Belgian** police unlawfully deployed real-time, automated facial recognition cameras at Brussels airport. These cameras surveilled all visitors to the aiport to see if they were a match with profiles on a watch-list, which constitutes biometric mass surveillance.[6]

Deployments of untargeted (or arbitrarily-targeted) mass biometric processing systems - whether by law enforcement, public authorities (such as schools or local councils), or private actors - do not meet the required justifications or thresholds of **necessity or proportionality** to be considered lawful for the level of violation and intrusion that they create.

This threshold is demanded by the the **Charter of Fundamental Rights**, the **GDPR** and the **LED**. The legal frameworks within which such activities take place often do not meet the requirements of "prescribed for by law" established under the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights, and fail to provide adequate, effective remedies against untargeted, unnecessary, disproportionate surveillance.

This analysis is based on EDRi's 2020 position paper, Ban Biometric Mass Surveillance, available at: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

4 https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como
5 https://www.greenpeace.org/static/planet4-eu-unit-stateless/2020/09/07bf7b31-locking-down-critical-voices_final.pdf
6 https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/