

Problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control

2008/2020(INI) - 24/04/2009 - Text adopted by Parliament, single reading

The European Parliament adopted by 372 votes to 12, with 17 abstentions, a resolution in which it addresses a number of recommendations to the Council on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control.

Recall that profiling is an investigation technique made possible by new technologies and commonly used in the commercial sector, but is now also increasingly used as an instrument of law enforcement, notably for the detection and prevention of crime and in the context of border controls.

Given that Member States are making ever greater use of new technologies (via programmes and systems involving the acquisition, use, retention or exchange of information on individuals, as a means of combating terrorism or responding to other threats in the context of the fight against crime), the Parliament calls for **the adoption at European level of a clear definition of profiling**, having in mind the specific objective pursued.

In this context, the Parliament makes the following recommendations:

- all processing of personal data for law enforcement and anti-terrorist purposes should be based on published **legal rules imposing limits on use**, which are clear, specific and binding and subject to close and effective supervision by independent data protection authorities and to stringent penalties for breach (according to the Parliament, mass data storage for precautionary motives is disproportionate in relation to the basic requirements of an effective fight against terrorism);
- a **legal framework should be established providing a clear definition of profiling**, whether through the automated mining of computer data or otherwise, with a view to establishing clear rules on legitimate use and laying down limits; it is also necessary to introduce the necessary data protection safeguards for individuals. According to the Parliament, data-mining and profiling blur the boundaries between permissible targeted surveillance and problematic mass surveillance in which data are gathered because they are useful rather than for defined purposes;
- the collection and retention of personal data and use of profiling techniques in respect of persons not suspected of a specific crime or threat should be subject to particularly strict “necessity” and “proportionality” tests;
- factual and intelligence data, and data on different categories of data subjects, should be clearly distinguished;
- access to police and secret service files should be allowed only on a **case-by-case basis**, for specified purposes, and should be under judicial control in the Member States;
- restrictive legislation on profiling should not prevent legitimate database access as part of such targeted investigations;
- there should be **time limits on the retention of personal information**;
- the creation of a high standard of protection for personal data does not preclude the generation of anonymous statistical data including variables on ethnicity, ‘race’, religion, and national origin that is necessary to identify any discrimination in law enforcement practices;

- the **collection of data on individuals solely on the basis that they have a particular racial or ethnic origin**, religious conviction, sexual orientation or behaviour, political opinions or are members of particular movements or organisations which are not proscribed by law **should be prohibited**; it is also necessary to establish safeguards regarding protection and procedures for appealing against the discriminatory use of law enforcement instruments (according to the Parliament, ethnic profiling raises deep concerns about conflict with non-discrimination norms);
- there should be strong safeguards established by law which ensure appropriate and effective judicial and parliamentary scrutiny of the activities of the police and the secret services, including their counter-terrorism activities;
- redress should be effective and accessible (with clear information being given to the data subject on the applicable procedures);
- a set of criteria should be established for assessing the effectiveness, legitimacy and consistency with European Union values of all profiling activities (if necessary, the Parliament proposes setting **binding rules** which avoid any infringement of fundamental rights).

The Council is also called upon to commission a study, to be conducted under the responsibility of the Commission, covering the actual and potential application of profiling techniques, their effectiveness in identifying suspects and their compatibility with civil liberties, human rights and privacy requirements. Member States should be asked to supply figures on stop-and-search and other interventions which result from profiling techniques.

Lastly, the Parliament highlights the danger that innocent people may be subject to **arbitrary** stops, interrogations, travel restrictions, surveillance or security alerts because information has been added to their profile by a State agent.