Friday 24 April 2009

RECOMMENDATIONS

EUROPEAN PARLIAMENT

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

P6_TA(2009)0314

European Parliament recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI))

(2010/C 184 E/25)

The European Parliament

— having regard to the proposal for a recommendation to the Council by Sarah Ludford on behalf of the ALDE Group on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (B6-0483/2007),

— having regard to international, European and national human rights instruments, in particular to: the International Covenant on Civil and Political Rights (ICCPR); the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR); the Treaty on European Union; the Treaty establishing the European Community (EC Treaty); the Charter of Fundamental Rights of the European Union (the Charter) and the national constitutions of the Member States, and to the rights and guarantees which they confer on individuals in the field of privacy, data protection, non-discrimination and free movement,

— having regard to European data protection measures from the Council of Europe: Article 8 of the ECHR, Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Recommendations of the Council of Europe's Committee of Ministers to Member States R(87)15 regulating the use of personal data in the police sector [1], R (97) 18 concerning the protection of personal data collected and processed for statistical purposes [2] and R(2001) 10 on the European Code of Police Ethics [3],

— having regard to EU data protection provisions: Articles 7 and 8 of the Charter, Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [4], and Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [5],

— having regard to measures against racial discrimination: the International Convention on the Elimination of all forms of Racial Discrimination (ICERD), Article 14 of and Protocol 12 to the ECHR, Article 13 of the EC Treaty and Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [6],

---

[1] Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Minister' Deputies.
[2] Adopted by the Committee of Ministers on 30 September 1997 at the 602nd meeting of the Ministers' Deputies.
[3] Adopted by the Committee of Ministers on 19 September 2001 at the 765th meeting of the Ministers' Deputies.
[4] OJ L 281, 23.11.1995, p. 31.
[5] OJ L 350, 30.12.2008, p. 60.
[6] OJ L 180, 19.7.2000, p. 22.

Friday 24 April 2009

— having regard to EU instruments in the field of security and the fight against terrorism, including police and judicial cooperation and exchange of information and intelligence, such as Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences ([1]), Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union ([2]), Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime ([3]) and its implementing Decision 2008/616/JHA of 23 June 2008 ([4]),

— having regard to existing and planned EU databases such as the Schengen Information System, Eurodac and the Visa Information System, to biometric data collection measures such as those for residence permits and passports, and to the Commission's Communication of 30 November 2006 entitled 'Reinforcing the management of the European Union's Southern Maritime Borders' concerning the establishment of a Permanent Coastal Patrol Network for the southern maritime external borders (COM(2006)0733), as well as to proposed surveillance projects such as Eurosur (European borders surveillance system),

— having regard to the proposal to create 'e-borders' as mentioned in the Commission's Communication of 13 February 2008 on 'Preparing the next steps in border management in the European Union', where integrated border management envisaging the creation of automated border controls including a registered traveller programme and an entry-exit system is proposed (COM (2008)0069),

— having regard to the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) ([5]) , to the proposal for a Council framework decision on the use of Passenger Name Records (PNR) for law enforcement purposes (COM (2007)0654), as well as to the opinions on that proposal by the European Union Agency for Fundamental Rights (the Fundamental Rights Agency), the European Data Protection Supervisor, the Article 29 Working Party and the Working Party on Police and Justice,

— having regard to relevant national case-law such as the ruling of the German Constitutional Court on *polizeiliche präventive Rasterfahndung* ([6]) and the judgment of the UK House of Lords on the Czech Roma ([7]) and to the case-law of the European Court of Human Rights (ECtHR), in particular Timishev v. Russia ([8]), Nachova and others v. Bulgaria ([9]), D.H and others v. the Czech Republic ([10]) and S. and Marper v. the United Kingdom ([11]), and of the Court of Justice of the European Communities, particularly in *Huber v Germany* ([12]),

— having regard to the report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin ([13]), to the paper on 'Protecting the right to Privacy in the fight against terrorism' by the Council of Europe Commissioner for Human Rights Thomas Hammarberg ([14]), to General Policy Recommendations No 8 on Combating racism while fighting terrorism ([15]) and No 11 on Combating racism and racial discrimination in policing ([16]) of the European Commission against Racism and Intolerance (ECRI) of the Council of Europe and to the report on 'Ethnic profiling' by the European Union Network of Independent Experts on Fundamental Rights ([17]),

([1]) OJ L 253, 29.9.2005, p. 22.
([2]) OJ L 386, 29.12.2006, p. 89.
([3]) OJ L 210, 6.8.2008, p. 1.
([4]) OJ L 210, 6.8.2008, p. 12.
([5]) OJ L 204, 4.8.2007, p. 18.
([6]) Decision of the German Constitutional Court, BVerfG, 1 BvR 518/02 of 4.4.2006, Absatz-Nr. (1-184).
([7]) House of Lords, 9 December 2004, *R v. Immigration Office at Prague Airport and another (Respondents) ex parte European Roma Rights Centre and others (Appellants)* [2004] UKHL 55, paragraph 101.
([8]) *Timishev v. Russia*, 13 December 2005, nos. 55762/00 and 55974/00, ECHR 2005-XII.
([9]) *Nachova and Others v. Bulgaria* [GC], 26 February 2004, nos. 43577/98 and 43579/98, ECHR 2005-VII.
([10]) *D.H. and others v. the Czech Republic*, 13 November 2007, no. 57325/00.
([11]) *S. and Marper v. the United Kingdom*, 4 December 2008, nos. 30562/04 and 30566/04.
([12]) Judgment of 16 December 2008. Case C-524/06, not yet published in the European Case Reports.
([13]) UN document A/HRC/4/26, 29 January 2007.
([14]) CommDH/Issue Paper (2008)3, Strasbourg 17 November 2008.
([15]) CRI (2004) 26, adopted on 17 March 2004.
([16]) CRI (2007) 39, adopted on 29 June 2007.
([17]) CFR-CDF, Opinion 4.2006, available at http://ec.europa.eu/justice_home/cfr_cdf/doc/avis/2006_4_en.pdf

— having regard to Rule 114(3) and Rule 94 of its Rules of Procedure,

— having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinion of the Committee on Foreign Affairs (A6-0222/2009),

Profiling and data mining

A. Whereas 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;

B. Whereas there is a need to adopt, at European level, a clear definition of profiling, having in mind the specific objective pursued; whereas 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;

C. Whereas the practice of profiling, which is often carried out through the automated 'mining' of computer-held data, merits examination and political debate, since it controversially departs from the general rule that law enforcement decisions should be based on an individual's personal conduct; whereas profiling is an investigative technique taking information from various sources about people, which may include their ethnicity, race, nationality and religion, as a basis for trying to identify and potentially take prohibitive measures against those who may be criminal or terrorist suspects, and can be defined as:

'*the systematic association of sets of physical, behavioural or psychological characteristics with particular offences and their use as a basis for making law enforcement decisions*' ([1])

or, making clear the relationship between data-mining and profiling:

'*a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics*' ([2]);

D. Whereas ethnic profiling, which has a specifically racial or ethnic basis and thus raises deep concerns about conflict with non-discrimination norms, can be defined as:

'*the practice of using "race" or ethnic origin, religion, or national origin, as either the sole factor, or one of several factors in law enforcement decisions, on a systematic basic, whether or not concerned individuals are identified by automatic means*' ([3])

or

'*the use by the police, with no objective and reasonable justification, of grounds such as race, colour, language, religion, nationality or national or ethnic origin, in control, surveillance or investigation activities*' ([4]);

([1]) Opinion of the European Union Agency for Fundamental Rights of 28 October 2008 on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, paragraph 35.
([2]) House of Lords Report: Clarke R, Profiling: A Hidden Challenge to the Regulation of Data Surveillance, 1993, para 33, footnote 41.
([3]) De Schutter, Oliver and Ringelheim, Julie (2008), 'Ethnic Profiling: A Rising Challenge for European Human Rights Law,' *Modern Law Review*, 71(3):358-384.
([4]) European Commission against Racism and Intolerance (ECRI) General policy recommendation No 11, above-mentioned, paragraph 1.

Friday 24 April 2009

E. Whereas profiling, whether through data-mining or the practices of police and other agencies, is increasingly used as a tool for law enforcement and border control, and insufficient regard is being given to the evaluation of its effectiveness and to the development and application of legal safeguards to ensure respect for rights of privacy and the avoidance of discrimination;

F. Whereas profiles can be:

i) *descriptive*, when they are based on witness and other information about perpetrators or characteristics of crimes that have been committed, and thus support the apprehension of specific suspects or the detection of current criminal activities that follow the same pattern; or

ii) *predictive*, when they make correlations between observable variables from past events and current data and intelligence in order to draw inferences believed to identify those who may be involved in some future, or as-yet-undiscovered crime ([1]);

G. Whereas 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, amounting potentially to unlawful interference with privacy;

H. Whereas unjustified travel restrictions and intrusive control practices could negatively affect vital economic, scientific, cultural and social exchanges with third countries; accordingly, underlines the importance of minimising the risk of certain groups, communities or nationalities being subject to discriminatory practices or measures that cannot be objectively justified;

I. Whereas the danger exists 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, and that if the information is not promptly removed this could lead through the exchange of data and mutual recognition of decisions to refusals of visas, travel or border admission, placement on watchlists, inclusion on databases, bans on employment or banking, arrest or loss of liberty or other deprivation of rights, all of which may be without redress;

Legal obligations

J. Whereas law enforcement must always be conducted with respect for fundamental rights, including rights to private and family life, the protection of personal data and non-discrimination; close international cooperation is indispensable in the fight against terrorism and serious crime, but all such cooperation must comply with international law as well as European norms and values on equal treatment and proper legal protection, not least so that the EU does not undermine its credibility as a promoter of human rights within its borders and at international level;

K. Whereas the EU should avoid investigative approaches that could unnecessarily harm diplomatic relations, hamper such international cooperation or damage its image in the world and its credibility as a promoter of international law; whereas European standards for equal treatment, non-discrimination and legal protection should continue to set an example;

L. Whereas both descriptive and predictive profiling may be legitimate investigative tools when they are based on specific, reliable and timely information as opposed to untested generalisations based on stereotypes, and when the actions taken on the basis of such profiles meet the legal tests of necessity and proportionality; whereas, however, in the absence of adequate legal restrictions and safeguards as regards the use of data on ethnicity, race, religion, nationality and political affiliation, there is a considerable risk that profiling may lead to discriminatory practices;

([1]) Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, paragraph 33.

M. Whereas, the guidance in the European Code of Police Ethics to the effect that '*police investigations shall as a minimum be based upon reasonable suspicion of an actual or possible offence or crime*', and whereas it is asserted that a likelihood of breach of human rights [1] threatening individuals and society as whole arises in the absence of such reasonable suspicion, when profiling is based on stereotypes or prejudice;

N. Whereas 'predictive profiling', using broad profiles developed through cross-referencing between databases and reflecting untested generalisations or patterns of behaviour judged likely to indicate the commission of some future or as-yet-undiscovered crime or terrorist act raises strong privacy concerns and may constitute an interference with the rights to respect for private life under Article 8 of the ECHR and Article 7 of the Charter [2];

O. Whereas the ECtHR case-law makes clear that derogations from Article 8(2) ECHR are only allowed if they are in accordance with the law and necessary in a democratic society [3], as confirmed in its recent above-mentioned judgment in *S. and Marper v. the United Kingdom*, when it held that '*Blanket and indiscriminate (…) powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences*' was a violation of Article 8 ECHR;

P. Whereas the ECtHR's above-mentioned finding in *S. and Marper v. the United Kingdom*, of a 'risk of stigmatisation' from the fact that persons not convicted of any offence are treated in the same way as convicted criminals in the UK DNA database must also raise questions about the legality of profiling operations based on processing of personal data of persons not found guilty by the courts [4];

Q. Whereas the *Rasterfahndung* programme, in which German police authorities collected personal records from public and private databases of males between 18 and 40 who were current or former students of presumed Muslim faith in an (unsuccessful) attempt to identify terrorist suspects was deemed unconstitutional by the German Constitutional Court in its above-mentioned ruling, which found that data mining is an illegal intrusion into personal data and privacy that cannot be justified as a response to a general threat situation of the kind that has existed continually in regard to terrorist attacks since 9/11, but requires demonstration of a 'concrete danger' such as the preparation or commission of terrorist attacks;

Effectiveness

R. Whereas doubt has been cast on the usefulness of data-mining and profiling in various American studies among which:

(i) A study for the Cato Institute observed:

> '*though data mining has many valuable uses, it is not well suited to the terrorist discovery problem. It would be unfortunate if data mining for terrorism discovery had currency within national security, law enforcement, and technology circles because pursuing this use of data mining would waste taxpayer dollars, needlessly infringe on privacy and civil liberties, and misdirect the valuable time and energy of the men and women in the national security community* [5]';

---

[1] Ibid., paragraph 33. See also the report on 'Ethnic Profiling' of the E.U. Network of Independent Experts on Fundamental Rights, above-mentioned, pp. 9-13.

[2] Opinion of the European Agency for Fundamental Rights of 28 October 2008 on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, paragraph 4.

[3] For a short overview of the relevant case law see E. Brouwer, Towards a European PNR System?, Study conducted for European Parliament Policy department C, Citizen's rights and constitutional affairs, Document PE 410.649, January 2009, paragraph 5, pp. 16-17.

[4] Judgment of the ECtHR in Case S. and Marper v. the United Kingdom, above-mentioned, paragraph 125.

[5] Cato Institute Policy Analysis No 584, 11 December 2006, "*Effective Terrorism and the limited role of predictive data-mining*" by Jeff Jonas and Jim Harper.

Friday 24 April 2009

(ii) A US National Research Council study of data-mining and behavioural surveillance technologies for the Department of Homeland Security concluded that:

'*automated identification of terrorists through data mining…is neither feasible as an objective nor desirable as a goal of technology development efforts* [1]';

S. Whereas the effectiveness of data-mining is weakened by the 'needle in the haystack' problem of analysts having to filter through the huge quantity of available data; whereas the extent of 'digital tracks' left by law-abiding citizens is even greater than that of criminals and terrorists who make considerable efforts to conceal their identities; and whereas there are significant rates of 'false positives' whereby not only do wholly innocent people come under suspicion resulting in potential invasion of individual privacy but real suspects meanwhile remain unidentified;

T. Whereas the inverse problem is the possibility of missing perpetrators who do not fit the profile, an example being the ringleader of the 7 July 2005 London bombings who 'had come to the attention of the intelligence services as an associate of other men who were suspected of involvement in a terrorist bomb plot…but…was not pursued because he did not tick enough of the boxes in the pre-July 2005 profile of the terror suspect' [2];

U. Whereas profiling that upsets good community relations and alienates certain communities from cooperation with law enforcement agencies would be counter-productive in hampering the gathering of intelligence and effective action against crime and terrorism [3];

V. Whereas the efficient collection of information about specific suspects and following of specific leads is the best approach to detect and pre-empt terrorism and as a supplement to this, random checks and controls which affect everyone equally and are impossible for terrorists to evade may be more effective than profiling in preventive counter-terrorism efforts [4];

Ethnic profiling

W. Whereas the use of ethnicity, national origin or religion as factors in law enforcement investigations is not precluded as long as such use conforms to non-discrimination standards, including Article 14 of the ECHR, but it must pass the scrutiny tests of effectiveness, necessity and proportionality if it is to constitute a legitimate difference in treatment that does not constitute discrimination;

X. Whereas profiling based on stereotypical assumptions may exacerbate sentiments of hostility and xenophobia in the general public towards persons of certain ethnic, national or religious background [5];

Y. Whereas the ECtHR case-law has established that where race constitutes an *exclusive* basis for law enforcement action it amounts to prohibited discrimination [6]; whereas in practice it is not always clear if race or ethnicity was the exclusive or decisive basis for such action and it is often only when patterns of law enforcement practice are analysed that the predominant weight of these factors clearly emerges;

---

[1] Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment. Free executive summary available at http://www.nap.edu/catalog/12452.html, page 4

[2] 'Detectives draw up new brief in hunt for radicals,' *The Times*, 28 December 2005.

[3] Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, paragraph 62.

[4] Ibid., paragraph 61.

[5] Ibid., paragraph 40.

[6] Judgment of the ECtHR in Case *Timishev v. Russia*, above-mentioned.

Z. Whereas there is no international or European norm which expressly forbids 'ethnic profiling', ECtHR case-law would suggest that conclusion and both ICERD and ECRI have made clear that such practice does violate the prohibition against discrimination ([1]);

AA. Whereas the Programme of Action adopted at the 2000 World Conference against Racism urged States to design, implement and enforce effective measures to eliminate 'racial profiling' ([2]); whereas ECRI, in its above-mentioned Recommendation No. 8 on Combating racism while fighting terrorism, has asked governments to ensure that no discrimination ensues from legislation and regulations or their implementation in the field of law enforcement; and whereas the EU Network of Independent Experts on Fundamental Rights believes that terrorist profiles on the basis of characteristics such as nationality, age or birthplace 'presents a major risk of discrimination' ([3]);

AB. Whereas there is a need for a comprehensive evaluation of investigative practices and data processing systems within the EU and Member States which employ or supply the basis for profiling techniques, in order to ensure full compliance with national, European and international legal obligations and avoid unjustified discriminatory or privacy-invading impacts;

AC. Whereas the following guidelines should be applied to such operations and whereas a combination of all these protections is required in order to provide full and effective protection;

1. Addresses the following recommendations to the Council:

(a) 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; mass data storage for precautionary motives is disproportionate in relation to the basic requirements of an effective fight against terrorism;

(b) 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 and mechanisms for establishing responsibility;

(c) 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;

(d) factual and intelligence data, and data on different categories of data subjects, should be clearly distinguished;

(e) 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;

(f) profiling activities should not detract from targeted investigative policing by Member States' police services, and restrictive legislation on profiling should not prevent legitimate database access as part of such targeted investigations;

(g) there should be time limits on the retention of personal information;

([1]) Opinion of the European Agency for Fundamental Rights of 28 October 2008 on the Council Framework Decision for a Passenger Name Record (PNR) data for law enforcement purposes, paragraph 39.

([2]) Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance (A/CONF.189/12), Programme of Action, paragraph 72.

([3]) EU Network of Independent Experts on Fundamental Rights, 'The balance between freedom and security in the response by the European Union and its member States to the Terrorist Threats' (2003), p. 21.

Friday 24 April 2009

(h) ethnic statistics are an essential tool to enable the detection of law enforcement practices that focus disproportionate, unwarranted and unjustified law enforcement attention on ethnic minorities; the creation of a high standard of protection for personal data (data linked to an identifiable individual) does not therefore 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 Article 29 Working Party should be asked to issue guidance on this issue;

(i) 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 necessary to establish safeguards regarding protection and procedures for appealing against the discriminatory use of law enforcement instruments;

(j) reliance by private or public bodies on computers to take decisions on individuals without human assessment should be allowed only exceptionally and under strict safeguards;

(k) 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;

(l) in view of the possible consequences for individuals, redress should be effective and accessible with clear information being given to the data subject on the applicable procedures accompanied by rights of access and rectification;

(m) a set of criteria should be established for assessing the effectiveness, legitimacy and consistency with European Union values of all profiling activities; existing and proposed national and EU legislation relating to the use of profiling should be reviewed in order to ascertain that it meets legal requirements under European law and international treaties; and EU law reform should be considered, if necessary, to produce binding rules which avoid any infringement of fundamental rights taking into account the anticipated Council of Europe recommendation on profiling;

(n) there should be an examination of the extent to which Directive 2000/43/EC prohibits or regulates profiling measures and practices, and consideration of reform to remove the exclusion of airports and ports from its scope;

(o) the Council should commission a study, based on the relevant framework and current practices, to be conducted under the responsibility of the Commission, with the consultation of the Fundamental Rights Agency and the European Data Protection Supervisor, as appropriate, and in consultation with law enforcement and with intelligence agencies, 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;

2. Instructs its President to forward this recommendation to the Council and, for information, to the Commission and to the governments and parliaments of the Member States.