in:ex
Converging and conflicting ethical values in the internal/external security continuum in Europe
European Commission, 7th Framework Programme

CEPS CENTRE FOR EUROPEAN POLICY STUDIES
Thinking ahead for Europe

INEX Policy Brief

Profiling in the European Union: A high-risk practice

Gloria González Fuster, Serge Gutwirth and Erika Ellyne

No. 10 / June 2010

ABSTRACT: Profiling through predictive data mining has already found its way onto the security agenda of the European Union (EU). This technique, designed to allow for the automatic flagging of individuals allegedly deserving 'further attention', is increasingly being developed, supported, and even implemented (typically, in the name of counter-terrorism) – but with extremely limited publicity. The debate on the risks to fundamental rights and freedoms of individuals posed by profiling has been sidelined, with worrying implications. This paper summarises a number of key points that are relevant for a much-needed discussion of the challenges ahead.

SEVENTH FRAMEWORK PROGRAMME

Research for this Policy Brief was conducted in the context of Work Package 2 of INEX, a three-year project on converging and conflicting ethical values in the internal/external security continuum in Europe, funded by the Security Programme of DG Enterprise of the European Commission's Seventh Framework Research Programme. The project is coordinated by PRIO, International Peace Research Institute in Oslo. For more information about the project, please visit: www.inexproject.eu

PRIO
International Peace Research Institute, Oslo

PROFILING IN THE EUROPEAN UNION:

A HIGH-RISK PRACTICE

INEX POLICY BRIEF NO. 10 / JUNE 2010

GLORIA GONZÁLEZ FUSTER, SERGE GUTWIRTH AND ERIKA ELLYNE*

Profiling through predictive data mining is already a reality worldwide, including in the European Union (EU). This modern technique relies on the massive processing of personal data in order to identify patterns that allow for the automatic categorisation of individuals.[1] Widely used in the private sector, profiling is now also increasingly being portrayed as a useful, appropriate technique for various security-related purposes – also by the EU institutions.[2] While this is happening, no satisfactory debate is taking place on how the use of profiling in this particular area can encroach upon the fundamental rights and freedoms of individuals.

1. Understanding profiling

There is much confusion about the very essence of the technique, and a degree of misinformation on the subject persists. This is partly due to the multiple meanings of the term

* Gloria González Fuster is a researcher at the Law, Science, Technology & Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB), Serge Gutwirth is a professor at the VUB and chairman of VUB's LSTS and Erika Ellyne is a researcher at VUB's LSTS.

[1] For a general discussion of profiling and the related legal challenges, see Lee A. Bygrave (2001), "Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law & Security Report*, No. 17, pp. 17-24; Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy (2008), *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, 11 January, Strasbourg; and Mireille Hildebrandt and Serge Gutwirth (eds) (2008), *Profiling the European Citizen: Cross disciplinary perspectives*, Dordrecht: Springer Science.

[2] For instance, the Informal High Level Advisory Group on the Future of European Home Affairs Policy (known as 'The Future Group') envisioned in its 2008 report "an increasingly connected world in which public security organizations will have access to almost limitless amounts of potentially useful information" and asked member states to prioritise investment in "technologies that enable automated data analysis" (Informal High Level Advisory Group on the Future of European Home Affairs Policy ('The Future Group') (2008), *Freedom, Security, Privacy: European Home Affairs in an open world*, Report, June, p. 43). Preparatory documents on the Stockholm programme argued that routine data monitoring and analysis should increasingly be handled by machines, and that the systems should flag up exceptions (unusual behaviour and anomalies) for human investigation. Progress was expected in three main areas: developing 'intelligent' responses for the monitoring of a single data stream (for instance, through CCTV); developing 'intelligent' responses for monitoring across multiple data streams, including streams of multiple types (for instance, simultaneous monitoring through CCTV and telecommunications monitoring); and progress in the type of interactions between the monitoring and humans (for instance, issuing certain types of alerts instead of simply 'flags') (Portuguese Presidency of the European Union (2007), *Public security, privacy and technology in Europe: Moving forward: Concept paper on the European strategy to transform Public security organizations in a Connected World*, October, p. 10).

'profiling'.[3] The word is nevertheless commonly used in contemporary security-related discussions as referring to the use of predictive data mining[4] to establish recurrent patterns or 'profiles' permitting the classification of individuals into different categories. Conceptually, it covers a double process: a first analysis of data to look for seemingly relevant patterns, and a second examination to identify the items that correspond to the patterns. When applied in the context of security, profiling is generally used to select a group of people, objects, or actions considered as 'deserving further attention'[5] or 'special treatment'.[6]

Graphically speaking, profiling is not like looking for a needle in a haystack. It is more like collecting information on all the pieces in that haystack, storing the data and analysing it in order to elaborate a profile of something that is yet unknown, but perceived as a possible risk. If the procedure goes well, the obtained 'profile' should consist of a series of features such as 'uncommonly small', 'uncommonly hard', 'uncommonly sharp'. Next, the procedure requires using the collected information again to compare the obtained 'profile' with the features of all the existing pieces. Those that are extraordinarily small, hard or sharp should be flagged as 'potentially risky', and one of the flagged pieces could be the needle in the haystack.

Profiling produces non-representational knowledge. Profiles do not describe reality, but are detected by the aggregation, mining and cleansing of data. They are based on correlations that cannot be equated with causes or reasons without further inquiry; they are probabilistic knowledge. That means that even if a pattern appears to occur each time certain conditions are met, it is not absolutely sure that it will occur again in the future. Based on experience, an animal may associate a situation with danger as a result of the recognition of a certain pattern and act consistently, even if the situation, in reality, is not a dangerous one: the human scent and the shuffling footsteps were not those of a bloodthirsty hunter, but those of an animal rights observer.[7]

As a matter of fact, profiling implies a shift from *searching and measuring* towards *detecting*: while more classical statistical approaches aim at validating or invalidating proposed correlations believed to be pertinent answers to existing questions, with profiling there are no preliminary questions. The correlations as such become the 'pertinent' information, triggering questions and suppositions. The result is that the tracing of behaviour becomes the source of an

---

[3] Ethnic profiling, for instance, refers to the use of ethnic or related features as discriminating criteria to classify individuals and treat them differently (on the possible overlap of the problems caused by ethnic profiling and profiling through predictive data mining, see Wim Schreurs, Mireille Hildebrandt, Els Kindt and Michaël Vanfleteren (2008), "Cogitas, Ergo Sum: The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector", in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross disciplinary perspectives*, Dordrecht: Springer Science, pp. 241-270. The term 'profiles' is sometimes used to refer to plain descriptions of characteristics considered as describing individuals deserving reinforced attention; a measure discussed in 2002 at the level of the Council of the EU went in this direction on the possible definition of 'terrorist profiles' to be used in European counter-terrorism efforts.

[4] In this sense, D.J. Solove (2008), "Data Mining and the Security-Liberty Debate", *The University of Chicago Law Review*, No. 75, pp. 343-362; or Daniel J. Steinbock (2005), "Data Matching, Data Mining, and Due Process", *Georgia Law Review*, Vol. 40, No. 1, pp. 1-86.

[5] Kim Taipale (2007), "The Privacy Implications of Government Data Mining Programs", Testimony before the US Senate Committee on the Judiciary, 10 January, p. 6.

[6] David Lyon (ed.) (2003), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, New York: Routledge, p. 20.

[7] Serge S. Gutwirth and Paul De Hert (2008), "Regulating profiling in a democratic constitutional state", in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European citizen*: *Cross disciplinary perspectives*, Dordrecht: Springer Science**,** pp. 271-291.

almost unlimited network of possible profiling practices generating knowledge with an impact upon individuals.[8]

2. Relevance at EU level

The best example of the EU's support for this type of practice is perhaps Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (generally referred to as the 'Third Money Laundering Directive').[9] Adopted in 2005, the Directive aimed at improving the detection of suspicious financial flows, and extended the obligation to report on suspicious transactions beyond financial institutions.[10] Crucially, it brought about the application of a risk-based approach to customer due diligence for the ongoing monitoring of transaction activities, and obliged member states to require that the designated bodies (i.e. banks, auditors, notaries, etc.) establish policies and procedures of risk assessment to forestall and prevent money laundering or terrorist financing.[11] The designated bodies must report any suspicion of money laundering or terrorist financing obtained through such procedures to their respective national authorities, which will consequently take the appropriate follow-up measures.

Currently, EU institutions are discussing the creation of an EU-wide system designed to use for profiling the personal information of people travelling by air – more concretely, of all passengers travelling by air from EU territory to a third country and vice versa. The official exchange of views on this initiative started in 2007, when the European Commission adopted as a counter-terrorism measure a proposal concerning a common EU approach on the use of air passenger data ('Passenger Name Records', or 'PNR') for law enforcement purposes.[12] According to that proposal, the personal data of passengers was to be processed and shared among all member states in order to "fulfil the purpose of developing risk indicators and establishing patterns of travel and behaviour".[13] Since then, the European Commission has refused to label this activity as a profiling activity, but others have,[14] notably taking into account

---

[8] Serge Gutwirth and Mireille Hildebrandt (2010), "Some Caveats on Profiling", in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data protection in a profiled world*, Dordrecht: Springer Science, to be published in June 2010, p. 11 of current manuscript.

[9] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal of the European Union*, L 309, 25.11.2005, pp. 15–36.

[10] The provisions of the Directive apply to credit institutions, financial institutions, and a series of legal or natural persons acting in the exercise of their professional activities (auditors, external accountants and tax advisors; notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the: (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets; (iii) opening or management of bank, savings or securities accounts; (iv) organisation of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of trusts, companies or similar structures; (c) trust or company service providers; real estate agents; other natural or legal persons trading in goods, only to the extent that payments are made in cash in an amount of EUR 15,000 or more, whether the transaction is executed in a single operation or in several operations that appear to be linked; and casinos (Art. 2(1) of Directive 2005/60/EC).

[11] See Art. 34(1) of Directive 2005/60/EC.

[12] European Commission (2007), *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, COM(2007) 654 final, 6.11.2007, Brussels.

[13] Ibid., p. 10.

[14] Sarah Ludford (2008), *Working Document on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control*, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, 30 September, p. 4.

that the aim of the system would be to identify certain categories of passengers as 'high-risk passengers', presumably to subject them to further examination. The proposal has now lost its pertinence due to the entry into force of the Lisbon Treaty,[15] but in December 2009 the European Council called upon the European Commission to reconsider the subject and propose another initiative setting up an EU Passenger Names Record system for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.[16]

Moreover, the EU is generously supporting technical research in the specific area of security-related predictive data mining.[17]

3. Who is affected?

Profiling for security purposes can have an impact on the fundamental rights of anybody, potentially, as soon as he or she engages in the activity that is monitored, such as performing a financial transaction, or travelling by air, which are not normally unusual activities. As the data used is typically gathered by the private sector initially, individuals are not even required to be in direct contact with any representative of any authority whatsoever.

Affected individuals can be classified in three main categories:

a) the entire population participating in the monitored activity: their personal data is collected, analysed, compared with obtained patterns, and stored for possible re-use;

b) those who mistakenly appear to match the profile as being worthy of further investigation:[18] in addition to their personal data being processed as described, they are flagged as deserving 'more attention' and thus subject to further investigation, unless and until it is made clear that they should not have been flagged; and

c) those who do match the profile: in addition to their personal data being processed as described, they are flagged as deserving 'more attention' and thus subject to further investigation.

It is important to keep in mind that those who match the profile might be or not be the individuals explicitly targeted by the measure (the actual or potential 'terrorists', or the 'money launderers'), and that they should not, in any case, be opposed as a category to the 'innocent majority': being flagged does not imply any statement about the innocence or guilt of the flagged individual.

As currently applied in the security field, profiling appears to serve primarily as a filter. When used at the borders, for instance, it has been said to facilitate the segregation of 'legitimate' mobility from 'illegitimate' mobility,[19] or the separation of "people who are ordinary, happy,

---

[15] Signed on 13 December 2007 by the 27 Heads of State or Government of the Member States of the European Union, the Treaty of Lisbon came into force on 1 December 2009. The Treaty signals the end of the adoption of Framework Decisions.

[16] Council of the European Union (2009), *The Stockholm Programme: An open and secure Europe serving and protecting the citizen*, 2 December, p. 39.

[17] Notably through the projects INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in an urban environment, http://www.indect-project.eu; SAMURAI (Suspicious and abnormal behaviour monitoring using a network of cameras for situation awareness enhancement, http://www.samurai-eu.org; and ADABTS, Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces) (Daniel Moeckli and James Thurman (2009), *Survey of Counter-Terrorism Data Mining and Related Programmes*, D08.1, 11 December, Detection Technologies, Terrorism, Ethics and Human Rights (DETECTER), pp. 30-31).

[18] Generally known as 'false positives'.

[19] Louise Amoore (2006), "Biometrics borders: Governing mobilities in the war on terror", *Political Geography*, No. 25, p. 336.

everyday travellers who are not meeting the profile of people who might be a risk"[20] from the others, maybe less 'ordinary', who happen to meet the profile.

4. Main problems and necessary safeguards

Among the different rights dangerously threatened by security-related uses of profiling, the right to privacy[21] and the right to the protection of personal data[22] are particularly exposed.[23]

The processing of personal data of the entire population engaged in the monitored activity by itself represents an interference with their right to respect for private life. As such, this interference must comply with a series of requirements that ensure that it does not constitute a violation of the standards imposed by the European Convention of Human Rights (ECHR). Not only does the interference need to pursue a legitimate interest,[24] but it must also occur 'in accordance with the law', on the one hand, and be 'necessary in a democratic society', on the other.

As emphasised by the European Court of Human Rights in its case-law,[25] interferences can be considered to take place 'in accordance with the law' only if they meet minimum standards of transparency. The criteria determining the data to be processed must be clear, and those establishing how the data is used must be similarly precise and accessible. Transparency is, however, precisely one of the weakest facets of profiling practices in general.[26] How are profiles

---

[20] Declaration of Ms Meg Hillier at the House of Lords (European Union Committee of the House of Lords (2008), *The Passenger Name Record (PNR) Framework Decision*, HL Paper 106, London, Evidence, p. 11).

[21] Or 'right to respect for private life', as enshrined in Art. 8 of the European Convention of Human Rights (ECHR), signed in Rome on 4 November 1950, and in Art. 7 of the Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights of the European Union, OJ C 303, 14.12.2007, pp. 1-16).

[22] Recognised as an autonomous fundamental right in Art. 8 of the Charter of Fundamental Rights of the European Union, and affirmed also in Art. 16 of the Treaty on the Functioning of the European Union (TFEU).

[23] The two rights are closely related, but different. See notably: De Hert, Paul and Serge Gutwirth (2006), "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power", in Claes, E. A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law*, Intersentia, Antwerp-Oxford, pp. 61-104.

[24] Such as in the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

[25] Of special interest in this sense is the judgement delivered by the European Court of Human Rights in *Liberty v. the United Kingdom* case (*Liberty and Others v. the United Kingdom*, European Court of Human Rights, Application no. 58243/00, Judgement of 1 July 2008, hereafter '*Liberty*'). The case originated in an application against the United Kingdom (UK) and Northern Ireland lodged by a British and two Irish civil liberties' organisations on 9 September 1999 concerning the implementation of the Interception of Communications Act of 1985. It concerned legislation allowing for the interception of communications between the UK and outside territory. In its judgement, the Court asserted that the law questioned did not indicate with sufficient clarity the scope or manner of exercise of the very wide discretion conferred on the State not only to intercept, but also to examine communications, as it did not set out in a form accessible to the public any indication of the procedure to be followed for the examination, sharing, storing and destroying of intercepted material (*Liberty*, § 69).

[26] For instance, in relation with behavioural advertising (Article 29 Data Protection Working Party and Working Party on Police and Justice (2009), *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data*, 1 December, Brussels, p. 16).). See also, more generally, Gutwirth & Hildebrandt (2010), op. cit.: "Citizens whose data is being mined do not have the means to anticipate

constructed, exactly? Who can influence the way in which they are developed and implemented? What precise data determine that an individual is judged as matching the profile? What kind of behaviour transforms an 'uninteresting' individual into an individual that is to be closely monitored? These questions rarely receive comprehensive and unambiguous answers. Thus, much remains to be achieved in this respect in order to ensure full compliance of profiling practices with the basic requirements of Article 8 of the ECHR.[27]

Interferences with the right to respect for private life can only be considered as 'necessary in a democratic society', and thus not in violation of Article 8 of the ECHR, if they are proportionate in the light of the interest pursued.[28] For this evaluation, an important lesson was provided by a landmark judgement delivered by the German Constitutional Court in 2006.[29] The ruling concerned a 'fishing net' initiative, so-called *Rasterfahndung*, aimed at identifying 'sleeper' members of terrorist organisations. The initiative foresaw the screening of data from public and private sources in order to track individuals matching a set of characteristics believed to correspond to the persons sought (such as being male, Muslim, or a student). The German Constitutional Court ruled that such a measure was in breach of the German fundamental right of informational self-determination, and that it could only be justified in the face of a concrete danger to highly valued legal interests. But modern profiling practices are significantly more invasive than any 'fishing net' measures, as even before any data is processed with the aim of selecting individuals matching certain features, massive quantities of data are collected and analysed in order to discern the features in question.[30] Thus, for them to be 'proportionate' and 'necessary', the grounds justifying their adoption should be particularly solid.

The processing of personal data in the context of profiling also has to meet the demands derived from the fundamental right to the protection of personal data. Therefore, the deployment of a satisfactory data protection regime is capital.[31] Various complex issues need careful consideration in this regard, such as, for instance, the problems derived from the mismatch between the aims officially pursued with a specific profiling activity and the actual significance and consequences of being flagged.

---

what the algorithms will come up with and hence they do not have a clue what knowledge about them exists, how they are categorised and evaluated, and what effects and consequences this entails. For individual citizens to regain some control, access is needed to the profiles applied to them and/or information about how these profiles may affect them" (p. 5 of current manuscript).

[27] For example, the profiling of air passengers as discussed at EU level appears, worryingly, to lack clarity on the procedure used for the filtering of individuals (in this sense, see: European Data Protection Supervisor (EDPS) (2007), *Opinion on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 20 December, Brussels, p. 5).

[28] Questioning the proportionality of the 2007 proposal of the European Commission for a EU PNR system, see: European Parliament (2008), *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, P6_TA(2008)0561, Strasbourg.

[29] Decision of German Constitutional Court, BVerfG, 1 BvR 518/02 of 4 April 2006, Absatz-Nr. (1-184).

[30] The extraordinarily invasive nature of profiling through predictive data mining makes it particularly difficult to support the wide implementation of 'behavioural profiling' as the solution to (certainly also problematic) ethnic profiling (with a different perspective, see: European Union Agency for Fundamental Rights (FRA) (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 28 October.

[31] On the unsatisfactory nature of the data protection regime applicable to the processing related to the 2007 proposal of the European Commission for a EU PNR system, see: Article 29 Data Protection Working Party and Working Party on Police and Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, WP 145, WPPJ 01:07, December.

This problem is particularly acute with regard to national provisions implementing Directive 2005/60/EC. This Directive, as explained, is directed towards the fight against money laundering and terrorist financing. The patterns on which the system relies, however, are to be regarded as merely indicative and, when a transaction is flagged, this simply suggests that further investigation may be warranted.[32] Transactions flagged as 'suspicious' are *possibly* related to money laundering or terrorist financing, but in most cases they won't be. The trouble with this that since it occurs in the context of counterterrorism; national provisions implementing those of Directive 2005/60/EC tend to extend to the processing leading to any flagging of transactions (and subsequently thereof); a series of restrictions on the right to personal data,[33] and in particular limitations on the right to access,[34] which are usually applied in the area of counterterrorism to make sure that the individuals placed under surveillance are not aware of this fact. In practice, any citizen can display conduct that will be considered as risky conduct, and thus flagged and reported to the relevant authorities, but they will not be granted the possibility to contest such an assessment[35] even if this limitation will, in most cases, be unfounded, and thus contrary to fundamental rights requirements.[36]

From a regulatory perspective, profiling has often been addressed through the notion of 'automated decisions'.[37] For those who happen to be flagged, it is certainly crucial that no decision with a negative effect is taken without further verification, and such assessment should normally include the intervention of at least a human being, and, depending on the consequences of the decision, a particularly qualified person, such as a judge. When profiling

---

[32] National Research Council of the National Academies (2008), *Protecting Individual Privacy in the Struggle Against Terrorist: A Framework for Program Assessment*, National Academy of Sciences, Washington, D.C., pp. 78-79.

[33] In some member states, a special regime will be applicable to the files of law enforcement authorities to be used for law enforcement purposes, for which important exceptions are foreseen, limiting the right to data protection of those affected by the processing (Solanes Corella, Ángeles and María Belén Cardona Rubert (2005), *Protección de datos personales y derechos de los extranjeros inmigrantes*, Valencia: Tirant Lo Blanch, p. 75).

[34] Which is a core element of the right to the protection of personal data (*College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, Case C-553/07*, Judgement of the European Court of Justice of 7 May 2009, § 49). It should be noted that the restrictions are de facto extended to data processing carried out by private actors.

[35] In the UK, for instance, individuals wishing to make use of their right to access the data related to them stored in the database storing all 'suspicious activity reports' are unlikely to succeed because of exemptions foreseen in data protection provisions in relation to national security and crime (European Union Committee of the House of Lords (2009), *Money laundering and the financing of terrorism*, House of Lords, HL Paper 132, 22 July, London, p. 49).

[36] Any limitations to the fundamental right to personal data should be granted restrictively, for the minimum period necessary. During this time, moreover, the relevant data protection supervisory authority, or the courts, should be granted powers compensating for the limitation of the right of the data subject (Llaneza, Paloma (2007), "El derecho de acceso a los datos de carácter personal contenidos en los ficheros relativos a la prevención del blanqueo de capitales", *Revista Española de Protección de Datos*, No. 3, p. 276).

[37] See, for instance, Art. 7 of Council Framework Decision 2008/977/JHA (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, *Official Journal of the European Union*, L 350, 30.12.2008, p. 60–71). Also, more generally, Serge Gutwirth and Paul De Hert (2008), op. cit., pp. 271-291.

practices are deployed massively, other measures need to be considered, including effective redress and compensation for those who are flagged erroneously.[38]

In any case, it needs to be highlighted that, through profiling practices, a series of features or conducts, which by themselves are fully legitimate and fall with the area of an individual's freedom, are transformed into signs pertaining to a pre-defined mistrusted category. Thus, forms of behaviour that are per se not only innocent, but also constitutionally protected, are obliquely transformed into indications of criminal activity,[39] or at least of undesirability. This requires major reflection, both from a legal (notably in relation with the right to non-discrimination) and an ethical perspective.

5. Concluding remarks

The idea of obtaining useful knowledge by automatically processing massive quantities of otherwise apparently incoherent, seemingly insignificant, 'silent' data can understandably hold some fascination for policy-makers. Profiling techniques are being constantly improved and refined to reinforce the impression that this kind of learning is easily obtainable and that it can be valuable. This paper has not considered whether applying profiling for security purposes is a genuinely effective choice, although that is, in itself, a highly debatable issue.[40]

What has been emphasised is that it is a risky practice, which generates numerous dangers for the rights and freedoms of individuals – not only for a targeted minority, and for those accidentally caught up in the flagging process, but also for the whole population that is de facto placed under generalised surveillance.[41] Safeguards are urgently needed, and they should be discussed in an open, informed debate, which must take into account the very nature of profiling. At the moment, it would appear that no such debate is taking place.

---

[38] On this subject, see Gloria González Fuster and Paul De Hert (2007), "PNR and compensation", in Juliet Lodge (ed.) (2007), *Are You Who You Say You Are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers, pp. 101-109.

[39] Rigaux (1990), op. cit., p. 431.

[40] Calling for an EU-supported study on the effectiveness of profiling, see, for instance: European Parliament (2009), *Report with a proposal for a European Parliament recommendation 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*, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Sarah Ludford, 3 April.

[41] Profiling practices are not the only initiatives currently being discussed and developed that entail such monitoring. For instance, these include so-called 'three strikes' internet disconnection policies that are being implemented in some member states and rely on the generalised monitoring of all internet activities of all internet users (European Data Protection Supervisor (EDPS) (2010), *Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)*, 22 February, Brussels, p. 4). See also Sari Depreeuw and Serge Gutwirth (2010), "Bescherming van intellectuele rechten mag niet ten koste van privacy", *Juristenkrant*, 14 april, p. 12.

References

Amoore, Louise (2006), "Biometrics borders: Governing mobilities in the war on terror", *Political Geography*, No. 25, pp. 336-351.

Article 29 Data Protection Working Party and Working Party on Police and Justice (2007), *Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, WP 145, WPPJ 01:07, December.

———— (2009), *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data*, 1 December, Brussels.

Bygrave, Lee A. (2001), "Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law & Security Report*, No. 17, pp. 17-24.

College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, Case C-553/07, Judgement of the European Court of Justice of 7 May 2009.

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, *Official Journal of the European Union*, L 350, 30.12.2008, pp. 60–71.

Council of the European Union (2009), *The Stockholm Programme: An open and secure Europe serving and protecting the citizen*, 2 December.

Charter of Fundamental Rights of the European Union, *Official Journal of the European Union*, C 303, 14.12.2007, pp. 1-16.

De Hert, Paul and Serge Gutwirth (2006), "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power", in E. Claes, A. Duff and S. Gutwirth (eds), *Privacy and the Criminal Law*, Antwerp-Oxford: Intersentia, pp. 61-104.

Depreeuw, Sari and Serge Gutwirth (2010), "Bescherming van intellectuele rechten mag niet ten koste van privacy", *Juristenkrant*, 14 April, p. 12.

Dinant, Jean-Marc, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy (2008), *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, 11 January, Strasbourg.

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal of the European Union* L 309, 25.11.2005, pp. 15–36.

European Data Protection Supervisor (EDPS) (2010), *Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)*, 22 February, Brussels.

European Parliament (2008), *Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, P6_TA(2008)0561, Strasbourg.

———— (2009), *Report with a proposal for a European Parliament recommendation 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*, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Sarah Ludford, 3 April.

European Union Agency for Fundamental Rights (FRA) (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, 28 October.

European Union Committee of the House of Lords (2008), *The Passenger Name Record (PNR) Framework Decision*, HL Paper 106, London.

———— (2009), *Money laundering and the financing of terrorism*, House of Lords, HL Paper 132, 22 July, London.

González Fuster, Gloria and Paul De Hert (2007), "PNR and compensation", in Juliet Lodge (ed.) (2007), *Are You Who You Say You Are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers, pp. 101-109.

Gutwirth, Serge and Mireille Hildebrandt (2010), "Some Caveats on Profiling", in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data protection in a profiled world*, Dordrecht: Springer Science, to be published in June 2010.

Gutwirth, Serge and Paul De Hert (2008), "Regulating profiling in a democratic constitutional state", in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European citizen*: *Cross disciplinary perspectives*, Dordrecht: Springer Science, pp. 271-291.

Hildebrandt, Mireille and Serge Gutwirth (eds) (2008), *Profiling the European Citizen: Cross disciplinary perspectives*, Dordrecht: Springer Science.

Informal High Level Advisory Group on the Future of European Home Affairs Policy ('The Future Group') (2008), *Freedom, Security, Privacy: European Home Affairs in an open world*, Report, June.

Liberty and Others v. the United Kingdom, European Court of Human Rights, Application no. 58243/00, Judgement of 1 July 2008.

Llaneza, Paloma (2007), "El derecho de acceso a los datos de carácter personal contenidos en los ficheros relativos a la prevención del blanqueo de capitals", *Revista Española de Protección de Datos*, No. 3, pp. 263-279.

Ludford, Sarah (2008), *Working Document on problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control*, Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, 30 September.

Lyon, David (ed.) (2003), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, New York: Routledge.

Moeckli, Daniel and James Thurman (2009), *Survey of Counter-Terrorism Data Mining and Related Programmes*, D08.1, 11 December, Detection Technologies, Terrorism, Ethics and Human Rights (DETECTER).

Portuguese Presidency of the European Union (2007), *Public security, privacy and technology in Europe: Moving forward: Concept paper on the European strategy to transform Public security organizations in a Connected World*, October.

Schreurs, Wim, Mireille Hildebrandt, Els Kindt and Michaël Vanfleteren (2008), "Cogitas, Ergo Sum: The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector", in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen*, Dordrecht: Springer Science, pp. 241-270.

Solanes Corella, Ángeles and María Belén Cardona Rubert (2005), *Protección de datos personales y derechos de los extranjeros inmigrantes*, Valencia: Tirant Lo Blanch.

Solove, D.J. (2008), “Data Mining and the Security-Liberty Debate”, *The University of Chicago Law Review*, No. 75, pp. 343-362.

Steinbock, Daniel J. (2005), “Data Matching, Data Mining, and Due Process”, *Georgia Law Review*, Vol. 40, No. 1, pp. 1-86.

Taipale, Kim (2007), “The Privacy Implications of Government Data Mining Programs”, Testimony before the US Senate Committee on the Judiciary, 10 January.

Acronyms

ECHR European Convention on Human Rights

EU European Union

PNR Passenger Name Records

TFEU Treaty on the Functioning of the European Union