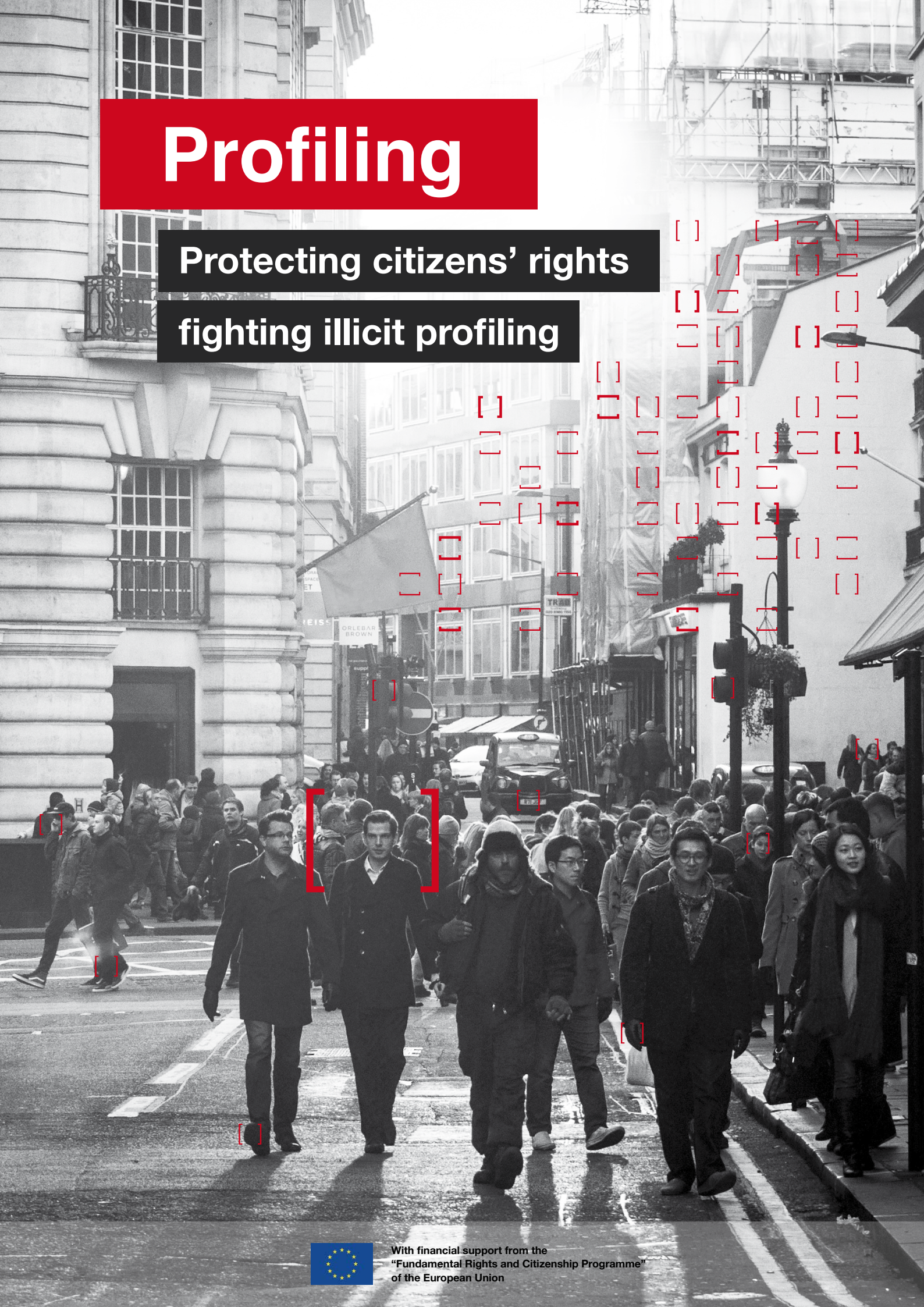
Profiling

Protecting citizens' rights

fighting illicit profiling



With financial support from the
"Fundamental Rights and Citizenship Programme"
of the European Union

Disclaimer

This manual has been produced with the financial support of the Fundamental Rights and Citizenship Programme of the European Commission.
The contents of this manual are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The views expressed are those of the authors and do not necessarily reflect the views of the United Nations or the organizations with which the authors are affiliated.

The designation employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

Cover and layout: Bellissimo and the Beast

Acknowledgments

This report has been prepared within the framework of the “PROtecting citizens’ rights and Fighting ILlicit profilING” (PROFILING) project, funded by the European Commission, DG Justice, under the Fundamental Rights and Citizenship programme. The programme focuses on identifying and tackling the challenges posed by technology to the fundamental right to data protection.

The report results from the work of the 5 partners involved in the project. The three working papers have been drafted by all the partners under the scientific coordination of Bert-Jaap Koops (Tilburg Institute for Law, Technology and Society – TILT). The comparative report has been drafted by the Emerging Crimes Unit of the United Nations Interregional Crime and Justice Research Institute (UNICRI), coordinated by Vittoria Luda di Cortemiglia, including Francesca Bosco, Elena D’Angelo, and Elise Vermeersch and under the supervision of Angela Patrignani. The three fieldworks have been implemented by Marco Sorrentino and Valeria Ferraris (AMAPOLA - Projects on Security and Safety of Cities and Citizens), Daniel Guagnin and Niklas Creemers (Technical University of Berlin – TUB), Bianca Toma, Cristian Ghinea, and Bogdan Manolea (Romanian Center for European Policies – CRPE) and reviewed by Bert-Jaap Koops (Tilburg University).

Special thanks for the support and collaboration provided throughout the research activities goes to: the European Data Protection Supervisor (EDPS), the Council of Europe, the Article 29 Working Party and the Data Protection Authorities of the 28 European Union Member States and, in particular, the Data Protection Authorities of Germany, Italy and Romania which also facilitated the completion of the fieldworks.

Last but not least, we wish to express our appreciation to the High-level experts who participated in the Workshop held in Rome, on 26 September 2014 to discuss the results of the project and to debate on the possible strategies and best practices to be adopted in the future regarding profiling practices and citizens’ rights: Elise Latify (EDPS); Alessandra Pierucci (Council of Europe); Stefan Niederer (Data Protection Authority of Germany); Vanna Palumbo (Data Protection Authority of Italy); Simona Zanfir (Data Protection Authority of Romania); Jędrzej Niklas (Panoptykon Foundation); and Arnold Roosendaal (Netherlands Organisation for Applied Scientific Research – TNO).

Table of Contents

Abbreviations

AFAPDP	Association of Francophone Data Protection Authorities
AFIS	Automated Fingerprint Identification System
AML	Anti money laundering
Art.	Article
BfDI	*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (Federal Commissionerfor Data Protectionand Freedom of Information)
BKA	*Bundeskriminalamt* (Federal Criminal Police Office)
CAHDATA	Council of Europe Ad hoc Committee on Data Protection
CEEDPA	Central and Eastern Europe Data Protection Authorities
CEPOL	Collège Européen de Police
CIS	Customs Information System
CISA	Convention Implementing the Schengen Agreement
CPC	Cost per Click
CPM	Cost per Thousand
CRID	Centre de Recherche informatique et droit
DPA	Data Protection Authority
DPD	Data Protection Directive
EAO	*Errichtungsanordnung* (Legal Ordinance for the Construction of a Database)
EC	European Commission
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
e.g.	For example
EU	European Union
EU-LISA	EU Agency for large-scale IT systems
EURODAC	European fingerprint database
EUROPOL	European Union's law enforcement agency
FoI	Freedom of Information
GDPR	General Data Protection Regulation
IAB	Interactive Advertising Bureau
ICT	Information and Communication Technologies
ID	Identification
IP	Internet Protocol
ISP	Internet Service Provider
IT&C	Information Technology and Communications
IWGDPT	International Working Group on Data Protection in Telecommunications

JSB	Europol Joint Supervisory Body
LKA	*Landeskriminalamt* (State Office of Criminal Investigations)
MIFID	Markets in Financial Instruments Directive
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal of the European Union
PC	Personal Computer
PET	Privacy Enhancing Technologies
PMK	Politisch motivierte Kriminalität (political motivated crime)
RBL	Romanian Black List
RTP	Registered Traveller Programme
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengen Information System
SDPI	State Data Protection Inspectorate
TCN	Third Country National
UNICRI	The United Nations Interregional Crime and Justice Research Institute
UK	United Kingdom
URL	Uniform Resource Locator
VIS	Visa Information System
WP	Working Party
WPSPDE	Working Party on Security and Privacy in the Digital Economy

The Profiling Project

One of the biggest challenges posed by the global technological evolution to the right of data protection is the processing of such data in the context of automated profiling: the automated processing of data to develop predictive knowledge in the form of profiles that can subsequently be applied as a basis for decision-making. UNICRI is leading a consortium of partners (Amapola, Turin, Italy; Romanian Centre for European Policies, Bucharest, Romania; Technical University of Berlin, Berlin, Germany; Tilburg University, Tilburg, The Netherlands) in a project that seeks to outline the main challenges to human rights involved in profiling practices.

The PROFILING project has been funded by the European Commission, DG Justice, under the Fundamental Rights and Citizenship programme. The programme focuses on identifying and tackling the challenges posed by technology to the fundamental right to data protection.

The main **objectives** of the PROFILING project are:

- analyzing the issue of automated profiling by exploring the definition, the evolution of technologies and the fundamental rights implications;
- identifying the level of awareness of the responsible authorities in the Member States on the potential risks and benefits deriving from the use of profiling;
- considering the measures adopted in all EU Member States to regulate and tackle the main challenges posed by profiling;
- investigating three interesting fields of application of automated profiling through a fieldwork in the partner countries (Romania, Germany and Italy).

The main **activities** of the project are:

- A background analysis and the publication of three working papers:
    - Defining profiling
    - Evolution of technologies in profiling
    - The impact of profiling on fundamental rights
- The elaboration of a checklist for studying the risks of profiling. This document can be a useful tool for stakeholders, policy-makers, governments, civil society and EC officers when approaching issues related to profiling.
- A questionnaire submitted to the national Data Protection Authorities of the 28 EU Member States + Switzerland, to assess the present European legal framework on profiling and issues such as application domains; complaint procedures and remedies; citizen awareness; and impact on fundamental rights.
- Fieldwork in three selected countries – Romania, Germany and Italy – exploring automated profiling in different domains of application:
    - Political activism (Germany)
    - Border control (Italy)
    - E-commerce (Romania)

The final comprehensive analysis provides input for the different stakeholders involved in the field of automated profiling, in order to expand the knowledge on the phenomenon and provide useful information to policy-makers, governments and civil society.

The main activities come along with a set of dissemination activities. These enable the partners to share the achievements gained during the implementation of the project and possibly inspire follow-up initiatives.

An international meeting was held in September 2014 in Rome to present the main results of the project and to debate with high-level experts and representatives of national authorities working on protection of personal data and privacy at European level on their experience and on possible strategies and good practices to be adopted in the future regarding profiling practices and citizens' rights.

An international Conference was organized in November 2014 at the European Parliament in Brussels to discuss the issue of profiling and related risks for citizens' fundamental rights with Members of the European Parliament and relevant stakeholders.

More information is available on the project webpage:

www.profiling-project.eu

Comparative report on automated profiling in the 28 EU Member States and Switzerland

Final results from the survey with the National Data Protection Authorities

Francesca Bosco, Elena D'Angelo and Elise Vermeersch
UNICRI

Executive summary

Definition and legislation

General questions on profiling

Sixteen DPAs consider it necessary to adopt a legal definition of automated profiling, particularly in order to clarify the concept and the procedures used. Three countries already have a legal definition of automated profiling, and five DPAs have proposed one.

The main risks involved in the use of profiling techniques mentioned by DPAs concern the challenges posed to an individual's liberties and fundamental rights and the lack of transparency and awareness among data subjects about the existence of profiling. On the other hand, DPAs recognise that profiling is a useful tool for tailored commercial services, predictive medicine and the identification of fraud and other criminal offences.

All of the responding DPAs (except Estonia) agree that profiling is a challenging area to be regulated, and the majority believe that all steps[1] of automated processing should be subject to strict regulation, both at the EU and national level.

Questions related to national legislation

Almost all of the responding EU countries (except Greece) have transposed Article 15 of Directive 95/46/EC on automated decisions.

No country has implemented Recommendation (2010) 13 of the Council of Europe on profiling.

Thirteen countries have (directly or indirectly) implemented Article 7 "Automated individual decisions" of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Questions related to the General Data Protection Regulation (GDPR)

According to the DPAs, the main profiling issues that should be included in the GDPR are: a precise and broad definition of profiling; adequate safeguards for individuals; a right to transparency; and increased responsibility for the data controller.

1 As defined by the Council of Europe, namely: 1) collection and storage of data, 2) correlation and analysis of data and 3) practical application of profiles.

Five DPAs support the present draft of Article 20 of the GDPR "Measures based on profiling," and eight DPAs are of the opinion that it must be improved. The main weaknesses of this Article are: its scope, which should be broader and cover the processing of personal data, not only the result of the processing operation; some terms are unclear, which may undermine legal certainty; and there is also a lack of clarity regarding the future use of sensitive data. Its main strengths are: the fourth paragraph on the data controller's obligations; and its expanded scope.

Five DPAs support the current version of Article 9, "Measures based on profiling and automated processing" of the proposed Directive on Data Protection in the Law enforcement sector; three DPAs consider it sufficient but still have some hesitations; four DPAs do not find it to be sufficiently protective.

Domains of application

According to the DPAs, finance and marketing are the domains in which profiling is applied most and which also pose the greatest challenges.

Complaints and remedies

A general procedure whereby data subjects can lodge complaints concerning data protection violations directly with the DPA, can be designed in accordance with national legislation: the plaintiff lodges a complaint with the DPA about an act or omission by the data controller violating the law or his/her rights. If the complaint is admissible, the DPA initiates an investigation and then makes a decision in order to correct the violation. The individual is generally kept informed about developments and notified of the final decision.

While there are numerous reasons for lodging complaints, the most common refer to: the violation of data subjects' rights, data breaches, or complaints against data processing for marketing purposes.

Half of the DPAs have already received a complaint related to profiling.

All the responding DPAs are also able to investigate data processing practices on their own initiative, and seven out of fifteen have already used this right.

Compensation mechanisms are usually in place in European countries, embedded in National Data Protection Acts through general civil, penal or administrative procedures.

There are only three countries where DPA officials receive specific national training, instruction or guidance on profiling.

Fundamental Rights: how fundamental rights/principles relate to profiling

The main fundamental rights and principles challenged by profiling are private life, data protection and respect for the principle of purpose limitation, proportionality, and necessity.

Nine DPAs follow a "prior checking" procedure (examination of processing operations likely to present specific risks for data subjects' rights prior to the start thereof), while three DPAs utilise other similar procedures.

The risk of infringement of citizens' rights regarding the protection of their personal data is highest in the financial sector and lowest in the education sector.

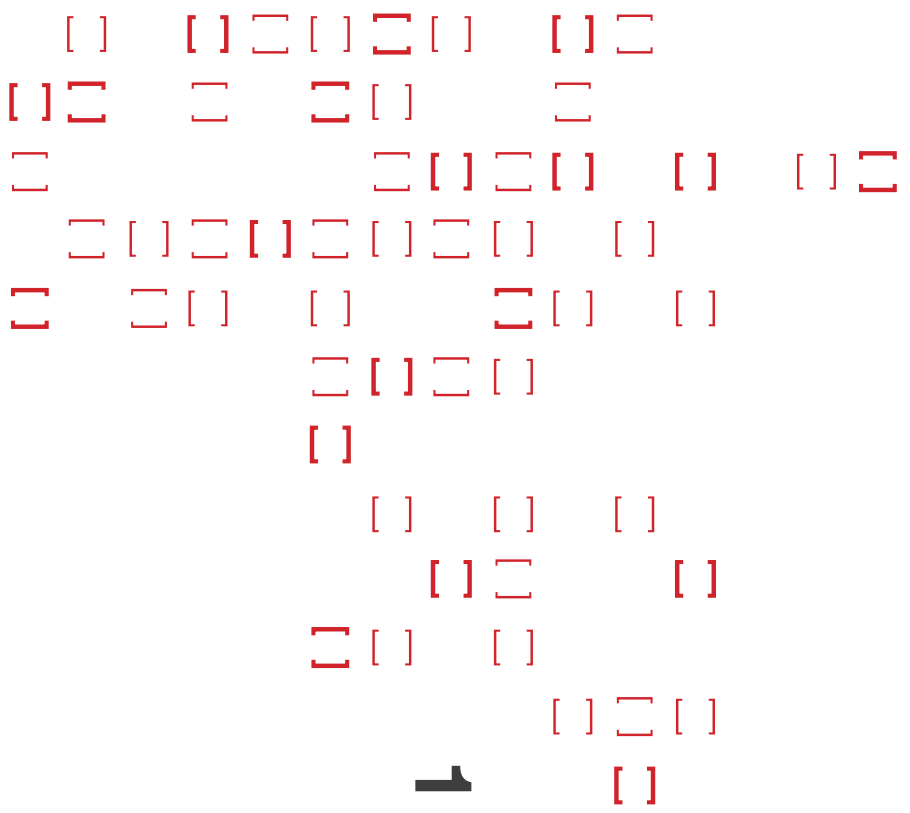
Six DPAs have processed a concrete case of infringement of fundamental rights.

Citizen awareness

Awareness of the legal effects of individual profiling measures is the main reason why data subjects decide to submit complaints in regard to automated profiling. Conversely, the lack of knowledge and transparency regarding profiling is the main limitation for data subjects' understanding of profiling risks and implications.

Strategies for awareness

DPAs use many methods to improve awareness among the general public about their rights as regards data that have been collected/used for profiling purposes (e.g. websites, reports, guidelines, conferences, media). Ten DPAs have already produced a report or study on the issue of profiling in order to meet this aim. Lastly, almost all DPAs think data subjects' awareness of automated profiling and its possible implications should be increased.



The aim and scope of the survey of this report

[1.1.] Methodology of work

In its aim to collect and compare information on the issue of profiling and, in particular automated profiling, UNICRI, together with its partners, developed a questionnaire to be sent to the Data Protection Authorities of EU Member States and Switzerland.

The questionnaire was finalised thanks to the contribution of the consortium and the inputs and feedback provided by the DPAs of Romania, Germany and Italy, the European Data Protection Supervisor (EDPS) and the Council of Europe.

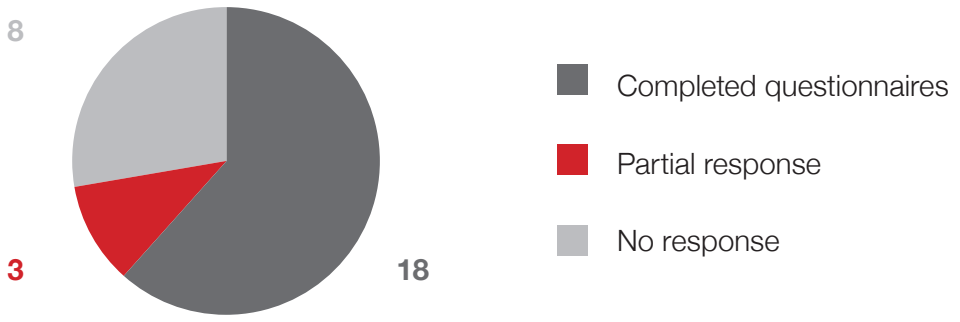
The structure of the questionnaire is as follows:

- Definition and legislation
  - General questions on profiling
  - Questions related to national legislation
  - Questions related to the General Data Protection Regulation
- Domains of application
- Complaints and remedies
- Fundamental rights: how fundamental rights/principles relate to profiling
- Citizen awareness
- Strategies for awareness

The DPAs were also invited to share their opinions on the relevance of the survey to their everyday activities or to the current policy debate on data protection.

The questionnaire was sent to the twenty-eight EU DPAs and Switzerland through the Secretariat of the Article 29 Data Protection Working Party (hereafter Article 29 Working Party). Within two months UNICRI had received feedback from twenty-one countries. Eighteen DPAs completed the questionnaire: Austria, Bulgaria, Croatia, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, and the United Kingdom. Three DPAs informed us that they would not be able to complete the questionnaire, mainly due to a shortage of human resources: Denmark, Luxembourg and the Netherlands. The DPAs from Luxembourg and the Netherlands did nonetheless provide some information related to the issues covered in the questionnaire, which has been included in the analysis. Eight DPAs did not reply: Belgium, Cyprus, the Czech Republic, France, Latvia, Poland, Portugal and Spain.

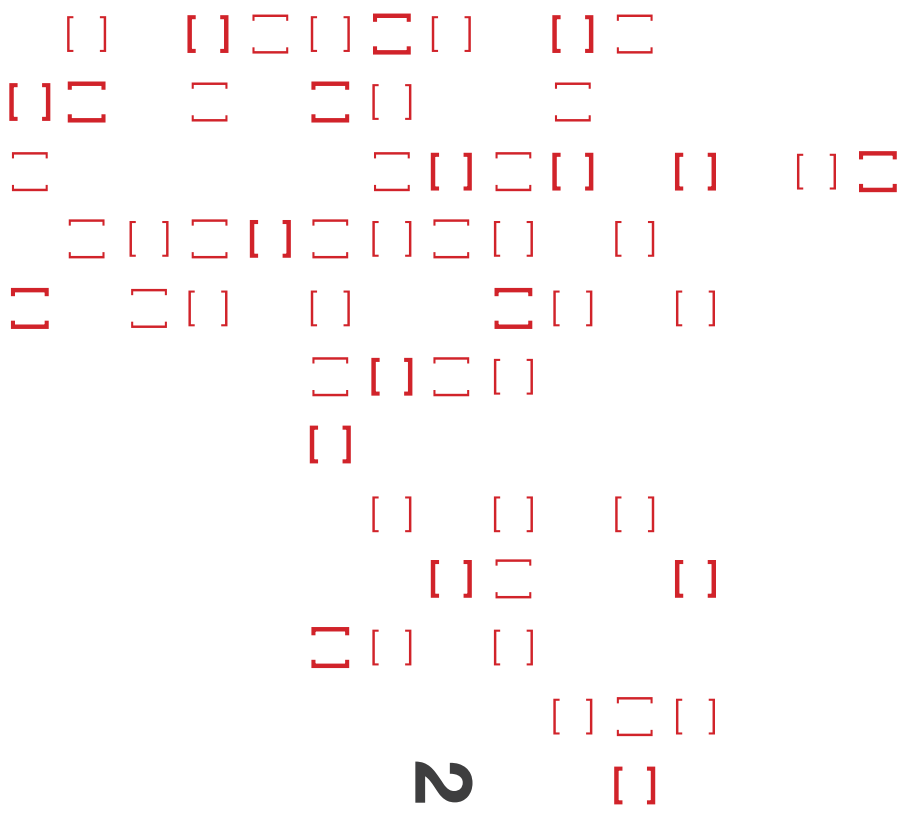
Response rated over the 28 European DPAs and Switzerland



This report begins by presenting some background information based on previous studies carried out by the PROFILING project on the definition of profiling and its legislative and normative basis. It then goes on to provide a descriptive analysis of the results of the survey, following the structure of the questionnaire[2].
The presentation of the results of the survey is based entirely on the answers of the DPAs and does not reflect the viewpoints of UNICRI or its partners.

While we were compiling and analysing the answers from the DPAs, the first draft findings of the questionnaire were presented at the annual Computers, Privacy and Data Protection Conference in Brussels on 22 January 2014.

2 The first draft of the survey was sent back to the partners of the project and the responding DPAs for review. The final report integrates feedback from the partners and three DPAs (Croatia, Italy and Switzerland).



Profiling: definition and previous research

[2.1.] The definition of profiling

The PROFILING project has defined profiling as follows:

> Profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (human or non-human, individual or group) subject. Constructing profiles is the process of discovering unexpected patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific subject or to identify a subject as a member of a specific group or category and taking some form of decision based on this identification and representation.

The entire working paper is available on the PROFILING project website[3] and aims to clarify the debate on the definition of machine profiling. The definition was further refined during the course of the project, nonetheless, the definition provided above is the one used for the report as well as for the questionnaire.

[2.2.] Legislative and normative background

Profiling is currently regulated through Directive 95/46/EC on data protection[4] (herein Directive 95/46/EC). Although the term "profiling" is not mentioned and ad hoc measures concerning profiling issues are not foreseen, Article 15 of Directive 95/46/EC is of particular relevance. The provisions of this article concern 'automated individual decisions' and are thus closely related to profiling. Article 15(1) states that every person has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." At the same time, Article 15(2) states an exception, in that a person may nevertheless be subjected to an automated individual decision "if that decision: (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests".

3 Ferraris V., Bosco F., Cafiero G., D'Angelo E., Suloyeva Y. (2013), Defining Profiling, Working Paper 1 of the Profiling project, p.15. Available at: http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_definition_0208.pdf

4 Directive 95/46/EC of the European Parliament and of 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, OJ L 281 , 23/11/1995 P. 0031 – 0050. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

In summary, Article 15 does not take directly prohibit a particular type of decision making; rather, it directs each European Union Member State to confer on persons a right to prevent them from being subjected to purely automated decision making in general[5].

Since Directive 95/46/EC does not provide for sufficient protection in a fast-developing information society and globalised world, the increasing issues relating to data surveillance and use call for a new legal framework for the protection of personal data in the European Union. In response to these issues, the European Commission released a draft General Data Protection Regulation (GDPR) in January 2012[6], which contains a set of proposed reforms to the existing EU data protection law. Article 20 of the GDPR does not offer a definition of profiling as it pertains to regulating the processing of data derived from profiling. It considers profiling as "automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour". Accordingly, it gives every 'natural person' "the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person," based on automated processing for profiling purposes.

The European Commission also released a draft Directive proposal[7] (hereinafter "proposed Directive") to replace the existing Council Framework Decision 2008/977/JHA[8] on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Law enforcement has been identified as an area where improvement is needed, and the previous framework decision did not provide a comprehensive framework of data protection by law enforcement and judicial authorities in criminal matters, as it only regulated supranational data flows.

5 Bygrave L. A., Data protection law: approaching its rationale, logic and limits, The Hague, Kluwer Law International, 2002, p.3.

6 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD). Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

7 European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012 COM(2012) 10 final 2012/0010 (COD). Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

8 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, OJ L 350/60, 30/12/2008. Available online at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008F0977

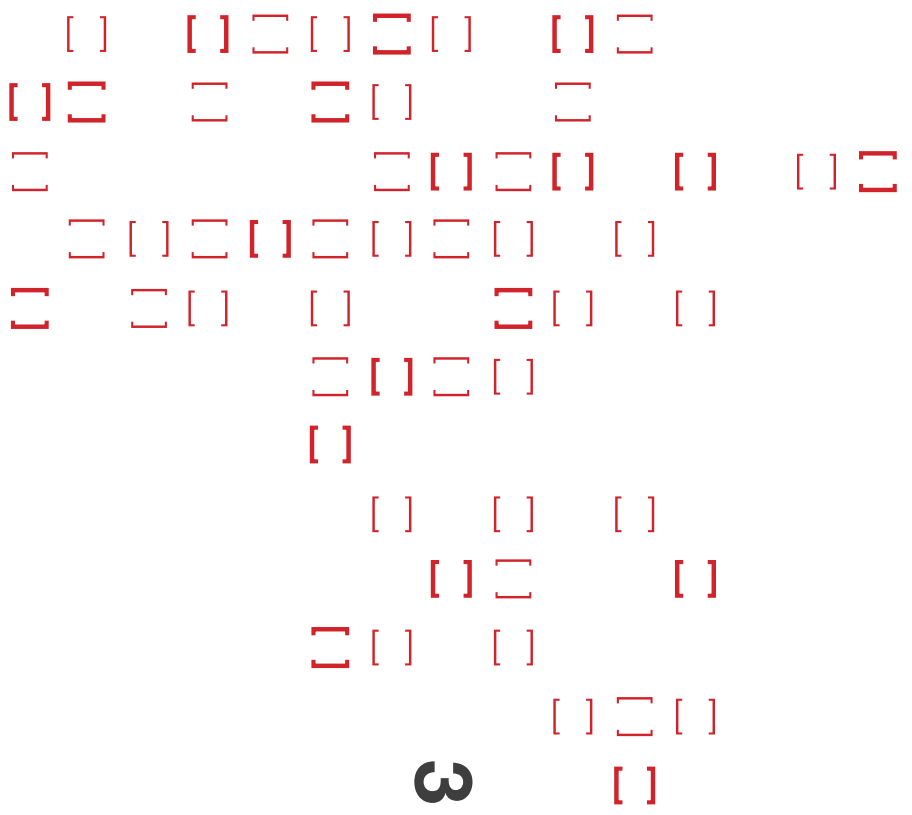
Aside from Article 15 of Directive 95/46/EC, the Council of Europe[9] has drafted an outline of the profiling process. It offers a definition that divides the process into three stages: an observation stage, which can also be referred to as the data-warehousing stage, in which data from a variety of different sources are collected and stored; a stage where these data are analysed, which can also be referred to as the data mining stage; and a final implementation stage. According to the Council of Europe's Recommendation CM/Rec(2010)13[10], profiling is an "automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

More information regarding the legislative and normative background is available in the previously mentioned working paper, "Defining Profiling", of the PROFILING Project[11].

9 Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy, 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, 11/01/2008, Strasbourg. Available online at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profiling_2008_en.pdf

10 Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies. Available online at: https://wcd.coe.int/ViewDoc.jsp?id=1710949

11 Supra, note 3.



Survey on automated profiling

[3.1.] Definition and Legislation

The survey envisaged a first set of questions aimed at:

a) shedding light on the different definitions in use within the EU;

b) assessing the legislative implementation of the Data Protection Directive and national legislation on the issue;

and

c) collecting input on the issues to be covered by the proposed General Data ProtectionRegulation.

[3.1.1.] General questions on profiling

The first section related to the understanding of automated profiling. According to the replies received from the DPAs, profiling is a new concept that is difficult to grasp. The understanding of the meaning of automated profiling varies from country to country. However, by pooling the answers of all the European DPAs it was possible to identify a general "structure". Basically, three principal aspects emerged: first, it requires the collection, storage and/or analysis of different kinds of data (mostly personal data); second, it must be based on automated processing using electronic means; third, it involves an objective of prediction or analysis of personal aspects or personality (preferences, attitudes, behaviour, health, economic situation, location, movements, performance at work...) and/or the creation of a profile. For six DPAs (Croatia, Estonia, Ireland, Lithuania, Slovakia and UK), the final aim of automated profiling is to take decisions concerning a specific data subject, which means that profiling results in legal consequences for data subjects or significantly affects them. It is interesting to note that several countries directly refer to the Article 29 Working Party definition[12] (Romania, Slovakia and Sweden), the definition provided by the

12 Article 29 Working Party, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, 13/05/2013. Available online at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf. The proposed definition states that: "Profiling means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements".

Council of the European Union in its draft proposal on the GDPR[13] (Bulgaria and Slovenia) or the definition given by the Council of Europe[14] (Slovakia and Switzerland).

A specific legal definition of automated profiling is not currently provided under European Union Law. Sixteen DPAs believe that such a legal definition would not only be important for clarifying the concept of profiling, but also for specifying how it may be executed and delineating the powers and liabilities of data controllers. A unitary interpretation will enforce safeguards for individuals subjected to profiling measures. Three DPAs (Hungary, Sweden and the UK) are not in favour of a definition in terms of law because it would create risks of misinterpretation (Hungary), or because it would be difficult to provide an exhaustive definition that includes every imaginable profiling situation (Sweden). Throughout the survey, the UK DPA explained that it might be better to see profiling as just another form of personal data processing that should be regulated within the normal data protection framework, and should therefore be treated as just one variant of data processing.

Three countries have already adopted a legal definition of automated profiling (the Netherlands[15], Estonia and Slovenia, which refer to national articles transposing Article 15 of Directive 95/46/EC on automated individual decisions). Moreover, five DPAs have proposed a legal definition (Germany has its own proposal[16], Bulgaria and Slovenia refer to the definition envisaged in the draft compromise text on GDPR[17], Finland and Switzerland support the definition of the Council of Europe[18]).

---

13 Council of the European Union, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Key issues of Chapters I-IV, Brussels 31/05/2013 10227/13 ADD 1. Available online at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010227%202013%20ADD%201. According to the draft compromise, "profiling means any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to a natural person, in particular the analysis and prediction of aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements."

14 Supra, note 10. According to the Recommendation, 'profiling' means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.situation, health, personal preferences, or interests, reliability or behaviour, location or movements."

15 The definition provided by the Dutch DPA is: "Profiling is collecting, analysing and combining personal data to classify someone in a certain category, to predict his or her behaviour or to make a decision concerning someone". According to the Dutch DPA the profiling process consists of three steps; 1. Collection of personal data about (a group) of people; 2. Analysis and linking of these, or even other data to establish patterns or correlations; 3. Application of the patterns and correlations (profiles) to (a group of) people to classify them as belonging to a certain category or to predict their behaviour."

16 The definition provided by the German federal DPA is: "profiling is the processing of personal data for the purpose of drawing conclusions about a person's personality or part of that personality, in particular to make statements or predictions about personal preferences, attitudes, behaviour, including movement and location, health or about the data subject's economic situation."

17 Supra, note 13.

18 Supra, note 10. According to the recommendation, profiling is an "automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviours and attitudes".
Moreover, Sweden's DPA considers that Article 29's definition "can be helpful" in establish-

ing a definition, and the Italian DPA does not propose a definition but has set out the necessary conditions in order to establish one[19].
An important section of the survey aims to highlight the main benefits and risks of profiling techniques. One issue of concern is the challenges posed to an individual's liberties and fundamental rights at large (privacy and data protection, self-determination, dignity, personal integrity, personality, free speech and movement), and the lack of transparency and awareness among data subjects about the existence of profiling. DPAs also highlight the risk of automated decisions – in particular decisions with possible legal consequences – based on inaccurate/outdated information and/or poor or flawed criteria which may result in the creation of a negative profile. Such processing can lead to exclusion of deserved benefits, discrimination or infringement of other fundamental rights. For this reason DPAs stress the key importance of error-handling procedures and of data subjects' control over their information. In addition, excessive collection of data is problematic, particularly considering that private companies could have access to enormous amounts of data, including highly sensitive data. Finally, DPAs mention other dangers such as the use of profiling in behavioural monitoring or the "long term consequences on minors' life through the creation of profiles for them, even more so as they are unable to express informed, specific and unequivocal consent to their processing", both mentioned by the Romanian DPA.

DPAs also recognise the beneficial role of profiling in some sectors, particularly in that of tailored commercial services (such as market segmentation, development of marketing and advertising strategies), in the health sector to aid predictive medicine, and in the identification of fraud and criminal offences. In addition, DPAs mention that profiling can improve the effectiveness or efficiency of processing (greater speed and cost-effectiveness, enhanced quality and security of services, easy-to-use decision tool, and reduction of bureaucracy). Because information is constantly collected from different sources, the Lithuanian DPA also mentions that profiling helps the data controller to analyse behaviour more precisely. For the Maltese and British DPAs, profiling can

19 The answer from the Italian DPA is as follows: "The setting up of a definition may be appropriate in order to provide more clarity and certainty in the application of the necessary safeguards. However, we believe that such definition should be carefully drafted and in such a way as to cover the many and challenging aspects of profiling in use today, in particular with regard to the consequences for individuals' rights. As emerged in the debate over the last few years within the data protection community, one of the biggest challenges for data protection in this context is that profiling is based on different phases (data warehousing, data mining, inference), which are not all necessarily based on the collection of "personal" data (Data warehousing for example is the collection of large quantities of data – either personal or anonymous – derived from observation of the behaviour and characteristics of individuals). Although the processing of anonymous data is beyond the scope of data protection legislation, it should be underlined that profiling, through statistical inference, creates "new data" that are then referred to the individual and have relevant repercussions on such individual. Therefore, the definition of automated profiling should be able to mirror this conceptual shift, from a more "traditional" data protection approach based on a literal and narrow application of the notion of personal data, to a more dynamic understanding of an individual's identity and rights. Not to mention the fact that data that appear to be anonymous may nevertheless, in certain cases, allow the identification of the related individual. As for our national legislation, please note that although our DP Code (legislative decree 30 June 2003, No. 196 available at http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf) does not contain a specific definition of profiling, Section 14 (Profiling of Data Subjects and Their Personality), Section 22.10 (Principles Applying to the Processing of Sensitive Data as well as to Judicial Data in the public sector) and Section 37 (Notification) set forth some specific rules in respect of profiling (see answer No. 7). Please note that in a decision dated 25 June 2009 (and published in Italy's Official Journal) concerning profiling carried out by telecommunication providers in respect of their clients, the Italian DPA described such technique though without giving a specific definition of profiling, in particular highlighting the different kinds of data (personal, aggregated) which can constitute the basis for profiling (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1636001). Such decision is relevant also because the DPA highlighted that if a provider plans to use aggregate personal data for profiling purposes and there is no proof that the data subjects consented thereto, the said provider will have to lodge a prior checking application with the Italian DPA. As a consequence of such decision the Italian DPA received and continues to receive requests for prior checking in respect of profiling."

even be protection-friendly when targeting a small segment of the population. The Slovenian DPA mentions that profiling can be beneficial in regard to "predictions about future events, personalisation of individual experience [and] may benefit social development."

All the DPAs agree that regulating profiling is a challenge for numerous reasons (with the exception of the Estonian DPA for which "if the laws and regulations are clear it is not a problem"). This is because of the previously mentioned risks to fundamental rights, and also because profiling is a fast-moving and expanding domain that influences various fields, involves large amounts of data and affects numerous people. Thus, it is very difficult to find a definition that will apply in all situations.

As for the role of technology, the growing use of profiling and its application are directly related to the rapid evolution of information and communication technologies (ICT). Indeed, the DPAs' answers indicate that various technologies are used in profiling contexts, such as Internet technologies (cookies, web crawlers, web beacons, web bugs, social networks, mobile apps), Internet of Things (RFID), tracking technologies (GPS, WI-FI, web tracking, video-surveillance), biometric databases, data warehouse technology (recording of information from data available in public data files or the online environment or from data subjects themselves or from other data controllers), data mining (big data processing and analysis techniques), computerised data analysis involving the use of algorithms, and credit reporting systems.

As previously mentioned, the Council of Europe[20] offers a definition of profiling that divides the profiling process into three stages: 1) collection and storage of data, 2) correlation and analysis of data and 3) practical application of profiles. On this subject, a majority of DPAs (Austria, Estonia, Finland, Germany, Hungary, Malta, Romania, Slovenia, Sweden, and Switzerland) believe that these three steps should be subject to strict regulation at both the European Union and the national levels. Three DPAs (Bulgaria, Lithuania and Slovakia) insist on the second and third steps, while one DPA calls for a stricter regulation of the first step only (Croatia) and one DPA of the second step only (Ireland). For the Greek and Italian DPAs, profiling should be considered and regulated as a whole process rather than in different stages, in order to apply the regulation to the entire profiling procedure, at any stage. For the British DPA, there is no particular need for stricter legal regulation of profiling than of other forms of data processing.

20 Supra, note 10.

[3.1.2.] Questions related to national legislation

Directive 95/46/EC[21] is the reference text at the European level for the protection of personal data. Therefore, this is the principal legislative instrument dealing with the notion of data profiling. In particular, Article 15 of Directive 95/46/EC establishes the ban on automated individual decisions with two exceptions to this general principle:

> Article 15 - Automated individual decisions
>
> **1.** Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
>
> **2.** Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:
>
> **a)** is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
>
> **b)** is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

Out of the nineteen replies received on this issue, seventeen countries (Austria, Bulgaria, Croatia, Estonia, Finland, Germany, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta, Romania, Slovakia, Slovenia, Sweden and the UK) have transposed the provision into their national legislation. In Greece, "Article 15 has not been exactly transposed into the data protection law", while Switzerland, although not bound by Directive 95/46/EC, has included a definition of profiling in its national Data Protection Act (see box 1). Basically, all national legislation follows Directive 95/46/EC, albeit with different degrees of protection for the data subject's rights.

21 Supra, note 4.

Box 1 - National legislation transposing Article 15 of Directive 95/46/EC

Austria
Section 49 "Automated Individual Decisions" of the Austrian Data Protection Act
Available at: http://www.dsk.gv.at/DocView.axd?CobId=41936 (English)

Bulgaria
Art. 34b of the Law for Protection of Personal Data.
Available at: https://www.cpdp.bg/en/index.php?p=element&aid=373 (English)

Croatia
Article 22a of the Personal Data Protection Act (OG 106/12 – consolidated text).

Estonia
§ 17 "Automated decisions" of the Estonian Personal Data Protection Act.
Available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse+seadus (English)

Finland
Section 31 "Automated decisions" of the Finnish Personal Data Act.

Germany
Section 6a of the German Federal Data Protection Act.

Greece
"The only relevant provision in the Greek data protection Law is that of Article 14".
Available at: www.dpa.gr

Hungary
Section 11 of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

Ireland
Section 6B of the Irish Data Protection Acts of 1988 and 2003.

Italy
Section 14 "Profiling of Data Subjects and Their Personality" of the Italian Data Protection Code.

Lithuania
Article 28 "Evaluation of Personal Aspects by Automatic Means" of the Law on Legal Protection of Personal Data.

Luxembourg
Article 31 of the 'loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel' (Luxembourg modified Act of 2 August 2002 relating to the protection of the persons with regard to the processing of personal data).

Malta
Article 24 of the Maltese Data Protection Act.
Available at: http://www.idpc.gov.mt/dbfile.aspx/DPA_amended2012.pdf (English)

Romania
Article 17 "The Right not to be subject to an individual decision" of Law no. 677/2001, as modified and amended.

Slovakia
Section 28 paragraph 5 of Act No. 122/2013 Coll. on Personal Data Protection and about Amendment of Other Acts.

Slovenia
Article 15 "Automated decision-making" of the Personal Data Protection Act.

Sweden
Section 29 "Automated decisions" of the Swedish Personal Data Act.

Switzerland
Article 3 letter d, defining profiling, of the Swiss Federal Act on Data Protection.

United Kingdom
Section 12 of the UK Data Protection Act 1998.
Available at: http://www.legislation.gov.uk/ukpga/1998/29/section/12

Regarding the implementation of Recommendation (2010)13 on Profiling of the Council of Europe[22], although all the survey countries are members of the Council of Europe, none have implemented this Recommendation. Only Bulgaria intends to do so by establishing a working group in order to amend the national Data Protection Act or the specific laws under which profiling is performed. However, it is worth noting that several DPAs (Estonia, Finland, Germany, Lithuania, and the UK) stated that their regulations meet the requirements of the Recommendation. Furthermore, the Italian DPA asserts that it "has taken into account and quoted Recommendation (2010)13" in its decisions on profiling, the Slovenian DPA "would […] refer to the Recommendation in a profiling case" and the Swiss DPA would "take it into account in [its] advising activities."
Within the specific context of police and judicial cooperation in criminal matters, which potentially involves greater risks for citizens' rights, profiling needs to be more regulated. In fact, this question is addressed by Article 7 of Council Framework Decision 2008/977/JHA[23] which was drafted in light of Article 15 of Directive 95/46/EC:

> Article 7 - Automated individual decisions
>
> "A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests."

One section of the survey related to the transposition of Article 7 asked the question: How has this provision been transposed into corresponding provisions in national measures? And furthermore: Can you share your opinion on possible limitations from the data protection perspective, of this provision and/or its national implementation?

Among seventeen responding countries, five have directly implemented this provision through a specific Law or Act[24]. Seven refer to their general personal data protection regulation[25], while Hungary is a signatory to an agreement[26] that refers directly to the Decision. Only four responding countries have not transposed this provision[27].

---

22 Supra, note 10.

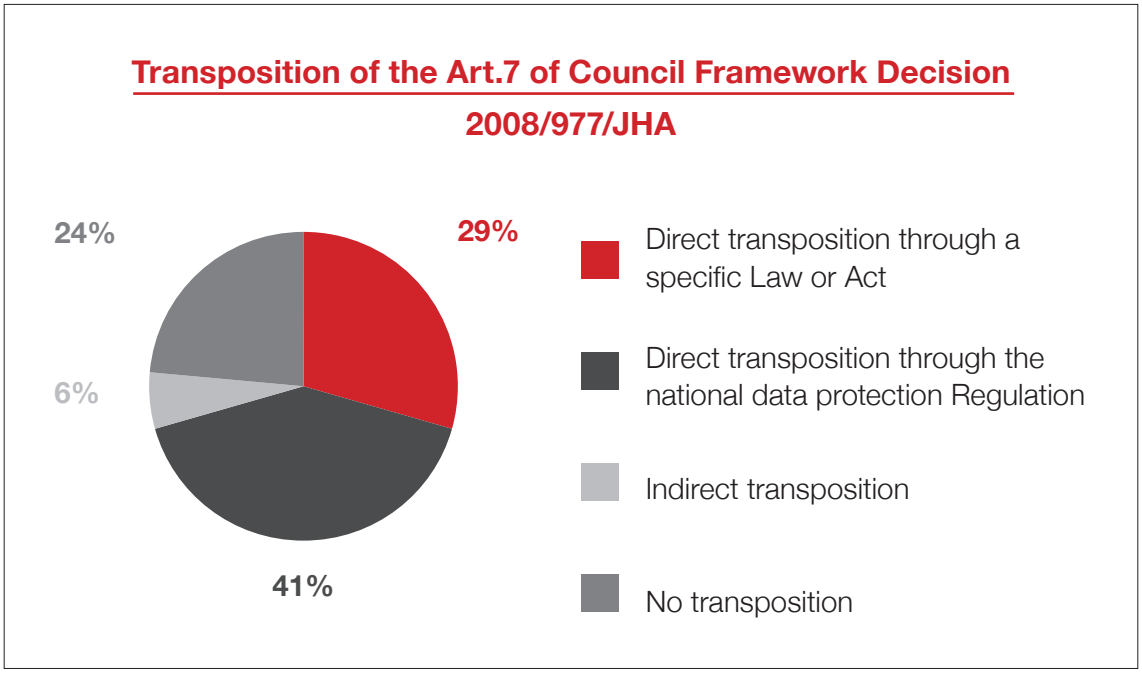
23 Supra, note 8.

24 Malta through subsidiary legislation, Romania through a national law that does not, however, contain a specific provision on individual automated decisions, Slovenia through the Police Tasks and Powers Act, the UK through a Ministry of Justice circular and in Switzerland Art. 7 of the decision is directly applicable.

25 Bulgaria, Croatia, Estonia, Finland (which also refers to two other Acts), Lithuania (although there is no reference to the police sector), Slovakia, and Sweden (which also refers to a specific data protection provision for the law enforcement sector).

26 Salzburg Forum Ministers, Agreement on cooperation in the area of witness protection, 24/05/2012. Available online at: http://www.mzz.gov.si/fileadmin/pageuploads/Mednarodno_pravo/Zascita_pric_-_CTC.pdf

27 Germany, Greece, Ireland (but the Irish DPA has supervisory powers in relation to the national police force, Europol national unit, Customs Information System and Eurodac) and Italy.



On the possible limitations of Article 7 of Council Framework Decision 2008/977/JHA and/or its national implementation, six DPAs (Germany, Hungary, Lithuania, Malta, Switzerland, and the UK) recommend a better explanation of certain notions, strengthening the principle of purpose limitation, excluding sensitive data as a matter of principle, with exceptions only if necessary and with appropriate safeguards, and adding the right to review, delete and correct the profile unless it skews the case in question. Austria and Ireland find the existing legislation adequate.

Only Germany and Italy have implemented other specific legal provisions or rules/regulations on automated profiling in the national legal framework in addition to national provisions transposing Article 15 of Directive 95/46/EC. For example, profiling is addressed in the German Telemedia Act for the purposes of advertising, market research or in order to design telemedia in a needs-based manner. In Italy, legal provisions on the assessment of income tax provide for some form of profiling. In addition, a code of conduct for information systems managed by credit referencing agencies - which is attached to the Data Protection Code and compliance with which is a prerequisite for processing operations to be lawful - sets forth the main principles for data processing as indicated in the Community Reinvestment Act, which includes the issue of credit scoring. In Greece, internal policies of financial institutions can contain rules on profiling, and credit profiling performed by credit referencing agencies is regulated by decisions of the DPA[28].

The absence of such specific national provisions does not mean that there are no other ways in which citizens are legally protected against profiling. Indeed, in Croatia and Estonia, citizens can file a complaint with the DPA and, in Estonia, also with the courts. In Hungary, the DPA can lead investigations or launch administrative procedures. This issue will be further addressed in part 2.6 “Complaints and remedies” of the report.

28 Under a recent Greek Law, No. 2238/2010 (Art. 82), banks and financial institutions are required to share details about their customers’ financial assets, savings, real estate etc. with the tax authorities, for the purpose of creating a profile of individual taxpayers.

National Data Protection Authorities are the guarantors of data protection in their countries. In this regard, Directive 95/46/EC on data protection envisages several powers, such as "monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive" (Article 28 §1). One section of the survey was aimed at understanding whether DPAs have written internal guiding policies for their employees or public policies addressing data controllers on the implementation of Articles 15 and 12[29] of Directive 95/46/EC with regard to automated decisions based on profiling. Only two DPAs answered that they have such written policies: Finland has a guide on the processing of personal data in the context of direct marketing and a guide on data subjects' right of access to their data[30]. The UK has also provided guidance on subjects' access rights[31]. Two other DPAs mention that they have incorporated Decisions on the implementation of Articles 15 and 12: Austria has incorporated nine Decisions which may serve as guidelines for their activities[32], and Italy has issued several Decisions on profiling, for example on loyalty cards[33], customer profiling as carried out by telecom operators[34], profiling in the employment sector[35] and profiling in respect of interactive TV[36]. Six DPAs[37] mentioned other policies related to those articles, though not specific to profiling. From the survey, it appears that policies produced by DPAs mostly concern data subjects' awareness and the assertion of their rights, rather than being addressed to DPA employees or data controllers for clarifying how to carry out profiling.

29 Article 12 "Right of access" of Directive 95/46/EC states: "Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1); (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort."

30 Guides are available on the Finnish DPA's website: http://www.tietosuoja.fi/.

31 Access to information held in complaint files (available online at: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/access_to_information_held_in_complaint_files.ashx), Regulatory activity exemption (Available online at: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/regulatory_activity_exemption_section_31_guidance.ashx), Subject access: code of practice (Available online at: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF), Subject access: responding to a request checklist (Available online at: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-checklist.pdf).

32 Available online at: http://www.ris.bka.gv.at/Dsk/

33 Available online at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1109624

34 Available online at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1636001

35 Available online at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1829641

36 Available online at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1116787

37 The Hungarian former commissioner for data protection and freedom of information issued a report, in cooperation with the commissioner for ethnic and minority rights, on the processing of data relating to ethnic origin (No. 754/H/2009-7); the Irish DPA provides general information and advice on the right of access of data subjects to their personal data, but not specifically tailored to the issue of automated profiling; the Italian DPA has issued "Guidelines on processing personal data for dissemination and publication on exclusively health-related web sites", not explicitly mentioning the issue of profiling but recommending the acquisition of information about the specific "risk notice" on the ground that users' health data disseminated on the Internet may also be the subject of profiling; Slovenia has issued some non-binding opinions on a creditworthiness system, both to the data controller and to data subjects; the Swedish DPA has published a leaflet on Article 12 that contains information about which public and private actors process personal data and how to proceed in exercising the right of access to personal data; and the Swiss DPA has provided guidance on subject access rights.

According to Article 28 §2 of Directive 95/46/EC, "Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data". The survey reveals that all DPAs are entitled to comment and advise on government and other state bodies' proposals which interfere with a citizen's right to data protection. Among other things, they can participate in or scrutinise the pre-legislative phase and deliver opinions or recommendations. Moreover, they can make proposals for new regulations and for the amendment of legislation, advise on policy issues or carry out audits. This specific activity of a DPA is generally based on national law and, in particular, on the national Data Protection Act, except for Ireland and the UK where there is no specific legal basis for pre-legislative activity.

[3.1.3.] Questions related to the General Data Protection Regulation

In 2012, the European Commission proposed a major reform of the EU legal framework on data protection and the introduction of a General Data Protection Regulation[38] to replace the current Directive 95/46/EC. Therefore, Article 15 of Directive 95/46/EC on profiling should be replaced by Article 20 of the proposed General Data Protection Regulation (in the originally proposed version of January 2012):

> Article 20 - Measures based on profiling
>
> **1.** Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.
>
> **2.** Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:
>
> **a)** is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention;
>
> or

38 Supra, note 6.

b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

The first paragraphs are more or less similar to the current Article 15 of Directive 95/46/EC, for examples. The second paragraph provides exceptions to the general prohibition of profiling that has legal effects on, or significantly affects, individuals. The future article replaces the data subjects' right to give their point of view via the right to a human intervention and adds the data subjects' consent as a new exception. A third paragraph points out that profiling must not be based solely on sensitive data. Furthermore, a fourth paragraph increases the data controller's responsibility by stipulating additional obligations.

Regarding the DPAs' opinions on the main aspects of profiling that should be included in the General Data Protection Regulation, they first call for a precise and broad definition of profiling and for adequate safeguards for individuals (right to information, control, consent/objection, data correction, human intervention). According to the responding DPAs, transparency and the increased responsibility allotted to data controllers are also important issues. These issues are correlated and confirm the main risks of profiling techniques mentioned above. To a lesser extent, DPAs support limiting the use of sensitive data to guarantee the principles of necessity and proportionality, to strictly regulate the transfer of data to third parties and to regulate the use of profiling in cloud computing contexts.

The opinions of the responding DPAs on the present draft of Article 20 of the General Data Protection Regulation are basically divided into two camps. One group supports the new provision in its entirety (Ireland and Malta) or with some improvements (Croatia, Hungary and Slovakia). The other group (Finland, Germany, Greece, Italy, Romania, Slovenia, Sweden, and the UK) is more critical of the proposed regulation and states that it must be improved. Several DPAs refer to the argument developed by the Article 29 Working Party in the Advice paper on the essential elements of a definition and a provision on profiling[39].

39 Supra, note 12.

This argument basically asks that the Article encompass a broader scope, greater transparency and control for data subjects, more responsibility and accountability of data controllers, and the empowerment of the European Data Protection Board (EDPB) to issue guidelines on the interpretation and application of Article 20 in specific processing contexts. Another frequent criticism concerns paragraph 3, which does not clearly explain if and how sensitive data could be used, or if a combination of sensitive and non-sensitive data could be used in automated processing.

In particular, countries identify the following main weaknesses and strengths in the proposed Article 20 of the GDPR. First, the scope of the article should be broader, covering the processing of personal data, not only the result of the processing; second, some unclear terms which may be dangerous for legal certainty ("based solely on automated processing", "legal effects" and "significantly affects" in the first paragraph, "suitable measures" or "safeguards" in the second paragraph and "envisaged effects" in the fourth paragraph) should be reworded; finally, the future use of sensitive data is also unclear. However, countries have noted that the fourth paragraph on the data controller's obligations is an improvement. Following the opinion of the EDPS[40], they also recognise that the scope has already been expanded thanks to the substitution of "decision" by "measure" and the addition of a number of categories of personal aspects which would fall under the scope of this provision (such as processes concerning an individual's economic situation, location, health and personal preferences).

The European Parliament, the European Data Protection Supervisor and the Article 29 Working Party have provided general opinions on the General Data Protection Regulation, and DPAs were asked to give their position on their reports, specifically concerning profiling issues.

On the European Parliament report[41], which contains numerous Amendments (in particular Amendments 158 to 167 specific to the future Article 20 of the GDPR), DPAs did not limit their answers to profiling, but gave a general opinion on the Regulation. Thus, a majority of answering DPAs (Bulgaria, Finland, Germany, Hungary, Italy, Malta, Romania, Slovakia and Slovenia) consider the European Parliament report to be beneficial for establishing a final version of the Regulation (having a broader scope, clarifying the transparency obligations of data controllers so it improves data subjects' rights, and banning the use of sensitive data). However, three DPAs see this report as having limitations: for Austria it "doesn't appear to address the issue of consent in questionable cases"; for Croatia the text discussed in the Council of Europe is of higher quality; and for Ireland the suggestions would "make profiling very difficult except on the basis of law" which "may not always be practical or proportionate, given other provisions on information and consent included in the GDPR".

---

40 European Data Protection Supervisor (EDPS), Opinion on the data protection reform package, 7/03/2012. Available online at: http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf

41 Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 17/12/2012 COM(2012)0011-2012/0011 (COD), Rapporteur Albrecht J.P. Available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

The EDPS[42] supports Article 20 with three main arguments, as summarised in a working paper produced by the PROFILING Project[43]:

> The EDPS supports the clarification provided by the Proposal on its scope of application and the development of the list of definitions (EDPS, 2012). With regard to the measures based on profiling, the EDPS supports the provisions of Article 20 of the proposed Regulation. The Article builds upon the existing Article 15 of Directive 95/46/EC on automated individual decisions, and extends its scope to all types of measures which produce legal effects on a natural person, not only to decisions. Firstly, the positive aspect is that it would apply not only to processing intended to evaluate certain personal aspects but also to those activities carried out to analyse or predict these aspects, therefore encompassing a broader category of processing. Secondly, it introduces a number of categories of personal aspects, which would fall under the scope of this provision, such as processing concerning an individual's economic situation, location, health and personal preferences. Thirdly, Article 20(2) sets forth the conditions under which this type of processing may take place by way of derogation and recognises the data subject's right to human intervention but not the right to submit their point of view, as is currently provided for in Article 15 of Directive 95/46/EC.

A majority of answering DPAs (Austria, Bulgaria, Croatia, Hungary, Ireland, Italy, Malta and Slovenia) support these three main arguments, especially the recommendation to restore the right for individuals to submit their point of view. Five (Finland, Germany, Greece, Romania and Slovakia) are in favour of a more far-reaching regulation of profiling.

Finally, in its Advice paper[44], the Article 29 Working Party provides a definition of profiling[45] and several suggestions[46] on how to improve Article 20 of the GDPR, which are supported by almost all the answering DPAs (Austria, Bulgaria, Croatia, Finland, Germany, Greece, Hungary, Malta, Romania, Slovakia, Slovenia and Sweden) except for Ireland which prefers the proposal version, considering that "the focus should be on the outcomes of profiling – i.e. on adverse legal effects or significant affects".

---

42 Supra, note 40.

43 Supra, note 3.

44 Article 29 Working Party, Advice paper on essential elements of a definition and a provision on profiling within the European Union General Data Protection Regulation, 13/05/2013. Available online at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf.

45 Supra, note 12.

46 The main proposals for improvement concern the scope: "It […] welcomes Rapporteur Albrecht's proposal to broaden the scope of Article 20 covering processing of personal data for the purpose of profiling or measures based on profiling. The Working Party regards this as a necessary step towards more legal certainty and more protection for individuals with respect to data processing in the context of profiling". The other proposals concern a greater transparency and control for data subjects; more responsibility and accountability of data controllers; and a balanced approach to profiling and the role of European Data Protection Boards.

The British DPA also explains that it has no particular comments to make on the papers of the European Parliament, EDPS and the Article 29 Working Party except that "profiling does not differ from ordinary forms of personal evaluation in that it involves the allocation of a particular individual to an existing general profile […]. If profiling is to be treated separately from other forms of similar data processing then this needs to be reflected in the relevant definition and regulatory approach".

As previously stated, the European Commission has proposed a major reform of the European Union legal framework on data protection. Decision 2008/977/JHA, which complements Directive 95/46/EC providing for specific data protection rules in the area of police and judicial co-operation in criminal matters, should be replaced by a Directive on Data Protection with a larger scope[47]. The current Article 7 on profiling will be replaced by Article 9 of this proposed Directive.

> Article 9 - Measures based on profiling and automated processing
>
> **1.** Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.
>
> **2.** Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.

The first paragraph is similar to the current provision except that "decision" will be replaced by "measure". However, the proposed article adds a second paragraph prohibiting automated processing based solely on sensitive data, which raises the same questions as Article 20 of the GDPR (see above).

As for DPAs' opinions on Article 9 of the proposed Directive, five DPAs (Bulgaria, Hungary, Croatia, Slovakia and Sweden) support the current version or do not have any comment or serious concern about it. Three DPAs have a mixed opinion because even though they consider Article 9 as generally sufficient, they have some hesitations: the Italian DPA recognises the modification of "decisions" to "measures" as an improvement but would open the scope to "sensitive data which may also be generated by profiling and not only included in such activity" and would prefer reference to "data" rather than to "personal data"; the Maltese DPA considers that "more specific guidance could be necessary on the application of this article when this is incorporated under national law"; and the Romanian DPA recommends the adoption of "legislative acts regulating the use of profiles in order to avoid the excessive collection of data" and the inclusion of "additional safeguards in order to protect data subjects' rights, similarly to those provided by Article 20 of the draft Regulation".

47 Supra, note 7.

Four DPAs deem Article 9 not to be sufficiently protective: the Austrian and Irish DPAs do not support the addition of "solely" in the second paragraph related to sensitive data because, as previously explained, this may not provide a real protection against the use of these special categories in automated profiling if they are combined with other data; the Finnish DPA asks for sufficient safeguards and assurance of the purpose limitation principle; and the Greek DPA considers that Article 9 of the proposed Directive "essentially only reiterates the relevant Art. 7 of Council Framework Decision 2008/977/JHA" and that "the content of this article is inconsistent with the Regulation" (the proposed article does not explicitly provide for the analysis and evaluation of behaviour, the prohibition of profiling is conditioned by the production of an "adverse" legal effect, which adds a condition, and the relevant subjects' rights are not specifically detailed), and it asks for provisions more in line with the equivalent ones of the Regulation. It is interesting to underline that the only two DPAs (Austria and Ireland) that find Article 7 of Council Framework Decision 2008/977/JHA adequate, highlight that the future Article 9 of the proposed Directive is not protective enough for sensitive data. For the Slovenian DPA, the GDPR should be binding for all sectors, including appropriate modifications and exemptions. Finally, the German and British DPAs are awaiting other debates at the European or national levels before giving their opinion. Germany hopes the proposal will "prompt a necessary debate on the legal bases for and the limits to access to and analysis of personal data under new technological circumstances"; the UK is anticipating other debates in order to understand if "it will apply to domestic processing or cross border processing".

After a first set of questions aiming to highlight the general legal framework related to automated profiling at the national and European levels, a second set of questions concerned the possible domains of application of automated profiling.

[3.2.] Domains of application

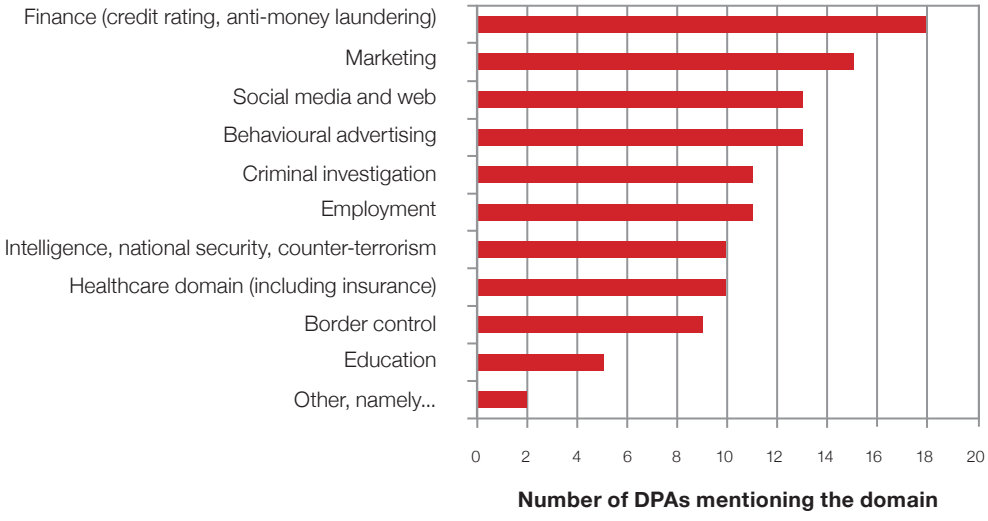
Automated profiling can apply to numerous sectors and this part of the survey aims to identify the main risks and benefits and the principal challenges of the use of automated profiling in each domain.

From this section, the survey applied the working definition of profiling specified in the framework of the PROFILING project:

> Profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (human or non-human, individual or group) subject. Constructing profiles is the process of discovering unexpected patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific subject or to identify a subject as a member of a specific group or category and taking some form of decision based on this identification and representation.

The questionnaire listed a number of domains where profiling is likely to be used, and DPAs were invited to identify in which of them profiling is applied in their country at the national level. The finance sector (credit rating, anti-money laundering) is considered the most inclined to apply profiling (18 DPAs), followed by marketing (15 DPAs), social media and web and behavioural advertising (13 DPAs), criminal investigation, employment (11 DPAs), intelligence/ national security/ counter-terrorism, the healthcare sector (including insurance) (10 DPAs) and border control (9 DPAs). Education is the least mentioned domain (5 DPAs). The Irish DPA highlights that profiling happens in "insurance quotation generally" and the Bulgarian DPA also mentions domains which were not predetermined, namely "sociological agencies" and "TV and radio programme rating research".

Domains in which profiling is applied in the countries



As far as you know, in which of the following domains is profiling applied in your country, at the national level?

	Number of Yes / 18 countries	Countries
Finance (credit rating, anti-money laundering)	18	Austria, Bulgaria, Croatia, Estonia, Filand, Germany, Greece, Hungary, Ireland, Italy (incoma tax), Lihuania, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Marketing	15	Bulgaria, Croatia, Estonia, Filand, Germany, Hungary, Italy, Lihuania, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Social media and web	13	Bulgaria, Estonia, Filand, Germany, Hungary, Ireland, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Behavioural advertising	13	Bulgaria, Estonia, Filand, Germany, Hungary, Ireland, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Criminal investigation	11	Bulgaria, Croatia, Filand, Germany, Hungary, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Employment	11	Bulgaria, Filand, Germany, Hungary, Italy, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Intelligence, national security, counter-terrorism	10	Bulgaria, Croatia, Germany, Hungary, Malta, Slovakia, Slovenia, Switzerland, UK
Healthcare domain (including insurance)	10	Bulgaria, Filand, Germany, Ireland, Malta, Slovakia, Slovenia, Sweden (insurance), Switzerland, UK
Border control	9	Bulgaria, Croatia, Estonia, Filand, Hungary, Slovakia, Slovenia, Switzerland, UK
Education	5	Estonia, Filand, Slovakia, Slovenia, Switzerland, UK
Other, namely...	2	Bulgaria (namely-sociological agencies, TV and radio programmes rating research) Ireland (insurance quotation generally)

Referring to the categories above, the DPAs were asked to list the potential risks and benefits brought about by the application of automated profiling. They provided numerous examples, except in the field of education, which was not listed by any of the DPAs.

Risks are considered more important than benefits, according to the DPAs' answers, and some risks are mentioned for all sectors. This is the case for discrimination, which can result in various forms of infringement for the individuals involved. In security domains (intelligence, national security, counter-terrorism, criminal investigation and border control) there is a high risk of ethnic profiling. In the other domains, discrimination of certain groups of people depending on their age, gender, health or place of living may lead to exclusion from obtaining certain benefits of services (credit, insurance, health insurance, other contracts, etc.) or receiving them at unequal terms or costs compared to everyone else. Also, non-transparent data processing or poor notification and information about profiling and its consequences are potential hazards likely to occur in all the aforementioned domains. Two DPAs (Finland and Hungary) consider that the risk of disregarding the principle of proportionality and purpose limitation is relevant for almost all the mentioned domains. The Slovenian DPA makes reference to the risk of losing one's right to self-determination for all sectors.

More specifically, in the fields of national security (intelligence and counter-terrorism), criminal investigation and border control, a main problem is the creation of inaccurate profiles that are likely to produce serious prejudices to individuals. Attempts to infringe upon fundamental rights and liberties (especially privacy, but also violation of immigrants' rights) are major concerns in these domains. Although the risks in these three domains are strong, automated profiling can also carry benefits. Indeed, better and faster interaction between systems (with proactive and fast procedures) allows for a correlation of information obtained from different databases, which aids in the prediction and prevention of crime and terrorism, the identification of criminal offenders, the reduction of recidivism, a wider control of groups considered potentially dangerous, and in the reduction of illegal immigration. Automated profiling can also improve the allocation of police resources, based on information gathered and analysed.

In the finance (credit rating, anti-money laundering) sector, as mentioned above, inaccurate profiles can increase discrimination and produce serious prejudices against individuals. This is therefore an important risk to be controlled. The absence of consideration for the individual case and the specific context in the assessment of validity is also a negative aspect of automated profiling. Finally, DPAs mention a high risk of error, which can result from the huge volume of data processed and the impossibility of correcting mistakes and inaccurate data. On the other hand, automated profiling can also benefit the financial sector in many ways: improve the effectiveness of the system by reducing the decision-making process; avoid payment default by granting credit, which is to the benefit of both the client (knowledge of customer to offer a personalised and protective solution) and the bank (security and stability); offer better prices, rates and discounts for loyal customers; and, as in the criminal sector, the correlation of information can improve the prevention and identification of fraud and tax-evasion and aid in the fight against money laundering.

Regarding the healthcare domain (including insurance), DPAs point out that automated processing is particularly sensitive in cases of violation because of the nature of the data. The Irish DPA highlights that the context needs to be taken into account in assessing health insurance because health issues are too sensitive and context-specific to be suitable for broad categorisation. Here, automated profiling can have great benefits, such as enabling the creation of a complete record of a person's health, which influences future policies and allows preventive medicine or proactive personalised solutions. It can also play a role in the evaluation of treatment effectiveness. In addition, automated profiling can be used in order to improve the health care system: lower prices, customised service and detection of fraud and abuse.

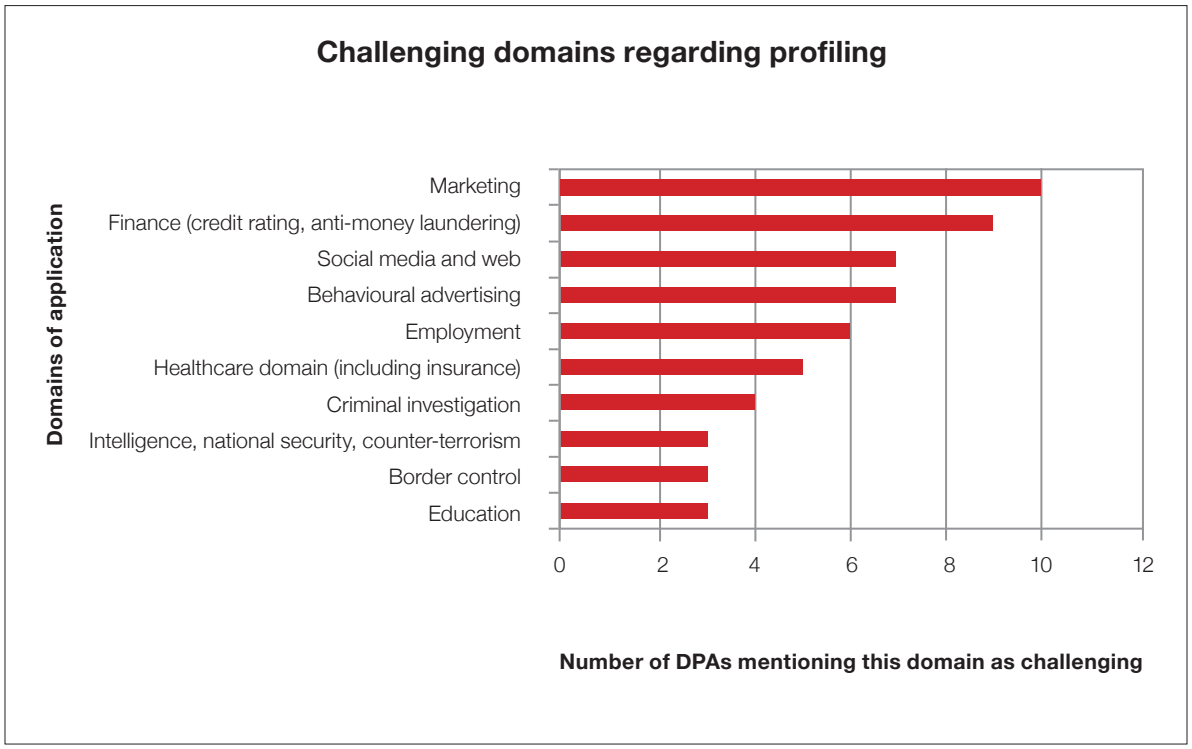
In the employment sector, the risks come from the lack of respect for the principle of necessity, if too much data is collected and/or stored without any legal ground and if the data are processed for reasons other than the actual employment relationship. Automated profiling can also lead to an intrusive monitoring of employees, which results in the infringement of their rights. On the other hand, automated profiling can also improve Human Resource management and increase the efficiency of the organisation through the detection of employees' capacities and lead to the subsequent placement in the most suitable and effective position within the company. For the Finnish DPA, methods used for such purposes are objective and, perhaps, more equalizing for employees. Furthermore, profiling could also prevent fraud (embezzlement).

The risks mentioned in the marketing domain are various. First, the possibility of sharing the information gathered with other data controllers (private and public, such as law enforcement agencies), without informing the individuals concerned, leads to a loss of control over their personal data. The violation of consumers' privacy and other rights are therefore a risk in the marketing sector. In addition, data controllers collect a huge amount of data, subjective or even erroneous, which may result in inappropriate decisions. But automated profiling can also have benefits both for the consumer and the data controller. On the one hand, it aims to provide tailor-made services for consumers and eventually lower prices. On the other hand, the detection of the customers' current preferences, the means of predicting future behaviour and consequently developing targeted advertisements can maximise or optimise companies' functioning and profits.

Where social media and behavioural advertising are concerned, the future use of information by other actors (private and public bodies, such as law enforcement agencies) without informing individuals can lead to a loss of control over their personal data. The Romanian DPA also mentioned a special risk to minors in these two sectors, "the creation of profiles for minors may have serious long term consequences on their lives even more so as they are unable to express an informed, specific and unequivocal consent for the processing of their data. For example the later use of data within the context of employment." Then, there is an obvious risk of intrusion of individuals' privacy. In the behavioural advertising sector specifically, wrong decisions based on inappropriate information are another source of concern. However, automated profiling in social media is also a tool for gathering and sharing information, making contacts and reuniting with other individuals in a more accessible and quicker manner. It can also be used to provide customised services at a lower price. Benefits in behavioural advertising are the same as those mentioned in marketing: customised services for consumers and the maximisation and optimisation of functioning and profits for companies. Obviously, it can also facilitate individuals in their search for products and services.

The answers from the Italian, Romanian and Slovakian DPAs have not been taken into account in the previous paragraphs because they provide comprehensive, general input. Regarding the potential risks of profiling, these three DPAs mention the risk of discrimination through exclusion from certain goods and services and also the risks to fundamental rights and liberties (human dignity, right to privacy and personal data protection). The Italian and Slovakian DPAs highlight the possible lack of transparency and awareness of profiling. On the benefits of automated profiling, the three DPAs answered in a more diverse way, mentioning, among others, anti-discrimination policies, better market segmentation, better analysis of risks and fraud, provision of better services and better collection of statistical data for the purpose of finding resolutions to any serious problems, and the identification of areas dangerous to health.

As previously mentioned, all DPAs think that regulating profiling is a big challenge. When asked to name the most challenging domains regarding profiling, the DPAs responded as follows: marketing (10 DPAs), finance - credit rating, anti-money laundering - (9 DPAs), social media and Internet, behavioural advertising (7 DPAs), employment (6 DPAs), healthcare (5 DPAs), criminal investigation (4 DPAs) and finally border control, national security and education (3 DPAs).



As regards profiling, which of the above mentioned domains is more challenging in your country?

	Number of Yes / 14 countries	Countries
Marketing	10	Bulgaria, Croatia, Estonia, Filand (commercial purposes), Hungary, Italy, Malta, Romania, Slovakia, UK
Finance (credit rating, anti-money laundering)	9	Bulgaria, Estonia, Germany, Ireland, Italy, Lithuania, Slovakia, Slovenia, UK
Social media and web	7	Bulgaria, Croatia, Estonia, Hungary, Romania, Slovakia, UK
Behavioural advertising	7	Bulgaria, Croatia, Estonia, Hungary, Romania, Slovakia, UK
Employment	6	Bulgaria, Croatia, Filand, Germany, Hungary, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Healthcare domain (including insurance)	5	Bulgaria, Filand, Germany, Hungary, Italy, Romania, Slovakia, Slovenia, Sweden, Switzerland, UK
Criminal investigation	4	Estonia, Slovakia, Slovenia, UK
Intelligence, national security, counter-terrorism	3	Estonia, Slovakia, UK
Border control	3	Estonia, Slovakia, UK
Education	3	Estonia, Slovakia, UK
Not answered	4	Austria, Greece, Sweden, Switzerland

Data collected for processing is likely to circulate between different data controllers working in the public or private spheres. All DPAs state that the exchange of data between public bodies and private actors is regulated by law (Data Protection Act or specific laws related to particular fields). Some countries also have specific regulations, such as Government acts, normative acts of other public authorities (Romania) or Constitutional provisions (Sweden), dealing with such forms of information sharing.

Regarding the existence of national law or regulations governing the collection of personal data and the use of databases containing such data, numerous responding countries have passed regulations through their Data Protection Act (Austria, Estonia, Finland, Ireland, Italy, Lithuania, Malta, Romania, Slovakia, Sweden, Switzerland and the UK) and/or through specific regulations (Bulgaria, Estonia, Finland, Greece, Hungary, Italy, Romania, Slovakia, Slovenia and Sweden) or also through a Code of conduct approved by the DPA (Bulgaria and Italy). According to the DPAs, the domains involved in this process are both diverse and numerous. Financial and banking rules (general provisions but also credit rating, the Markets in Financial Instruments Directive (MIFID) and Anti Money Laundering (AML) requirements, provisions on quality assurance and customer relations, etc.), police and law enforcement, healthcare, traffic, telecommunications/electronic communications, freedom of movement, insurance, environment, schools and Courts are mentioned as areas in which relevant sectoral rules may be found. The Croatian DPA answered that "there is no provision which explicitly refers to profiling".

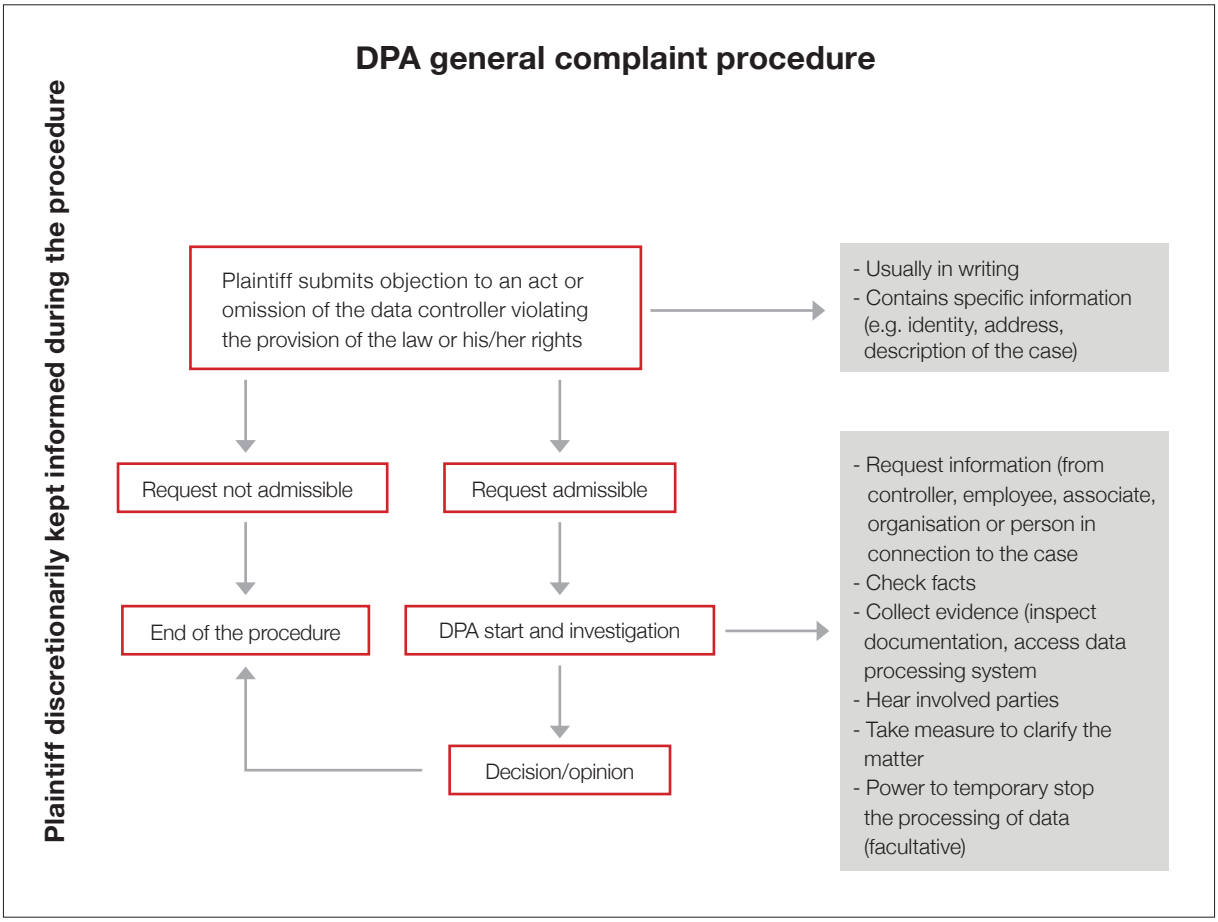
The next part of the survey focuses on complaint mechanisms, available remedies and practices.

[3.3.] Complaints and remedies

Article 28 of Directive 95/46/EC deals with Data Protection Authorities' powers. In particular, the fourth paragraph envisages the capacity for a DPA to "hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data." There are no indications in Directive 95/46/EC on how data subjects' complaints are to be processed. Thus, DPAs were asked about the national procedures in place for data subjects to lodge direct complaints addressing data protection violations and how DPAs deal with the complaints received.

The general procedure that emerged from the responses is as follows: the plaintiff submits a complaint to the DPA (usually in writing and containing specific information such as name, address and a description of the case) against an act or omission of a data controller that allegedly violates the provisions of the law or the individual's rights. If the complaint is admissible, the DPA initiates an investigation that can consist of requesting information, checking facts, collecting evidence, hearing all involved parties and taking measures to clarify the matter. DPAs have several investigational powers (for example, the Hungarian DPA it is able to inspect documents, access data processing systems and request information from the controller, employee, associate, organisation or person in connection with the case) and sometimes have the ability to temporarily stop the processing of data (Austria, Croatia and Italy). Then, the DPA issues a decision/ recommendation/ guidance/ direction/ opinion (which is generally not as powerful as a court decision)

in order to correct the violation. In agreement with Article 28, the individual is generally kept informed on the developments and notified of the final decision. Although national legislation generally follows the procedure described above, there are still numerous particularities among European countries concerning the formalities that must be carried out by individuals in order to file a complaint and for the DPAs to investigate the claim. Furthermore, some national data protection acts associate profiling complaints with various types of procedures (administrative, penal, mediation). For example, in Austria the procedure is different, depending on whether the complaint is against a public body (all complaints are brought before the data protection commission) or the private sector (all complaints must be brought before the courts, except for those concerning the right of access, which are handled by the data protection commission).



The data subject is not the only actor in the complaint procedure. Indeed, sixteen DPAs (Bulgaria, Croatia, Estonia, Finland, Germany, Greece, Hungary, Italy, Lithuania, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, and the UK) also receive data subjects' complaints through legal entities, institutions, associations, law firms, attorneys, representatives of natural persons, bodies, organizations, NGOs, Trade Unions, foundations or local and central public authorities (such as Consumer Protection Commission, Communications Regulation Commission etc.). However, Germany specified that "in the large majority of cases the data subjects appeal directly and in person to the" DPA.

Regarding the most common reasons for complaints, DPAs' answers varied. For clarity, these can be divided into three categories:

- complaints related to the sectors involved;
- complaints based on a violation of data subjects' rights; and
- complaints based on violation of other data protection rules.

The main sectors involved in complaints are marketing - by phone, email, post (mentioned by 10 DPAs) or even spam (2 DPAs) - the unlawful usage of CCTV (video surveillance) (5 DPAs), the processing of data in the credit and banking sector (7 DPAs), the employment sector (4 DPAs) and the healthcare sector (2 DPAs). The telecommunications sector, police sector, public sector and the Internet are also sources of complaints. The processing of personal data for journalistic purposes, especially in respect to on-line journalism and media archives, is also an issue (each mentioned by 1 DPA).

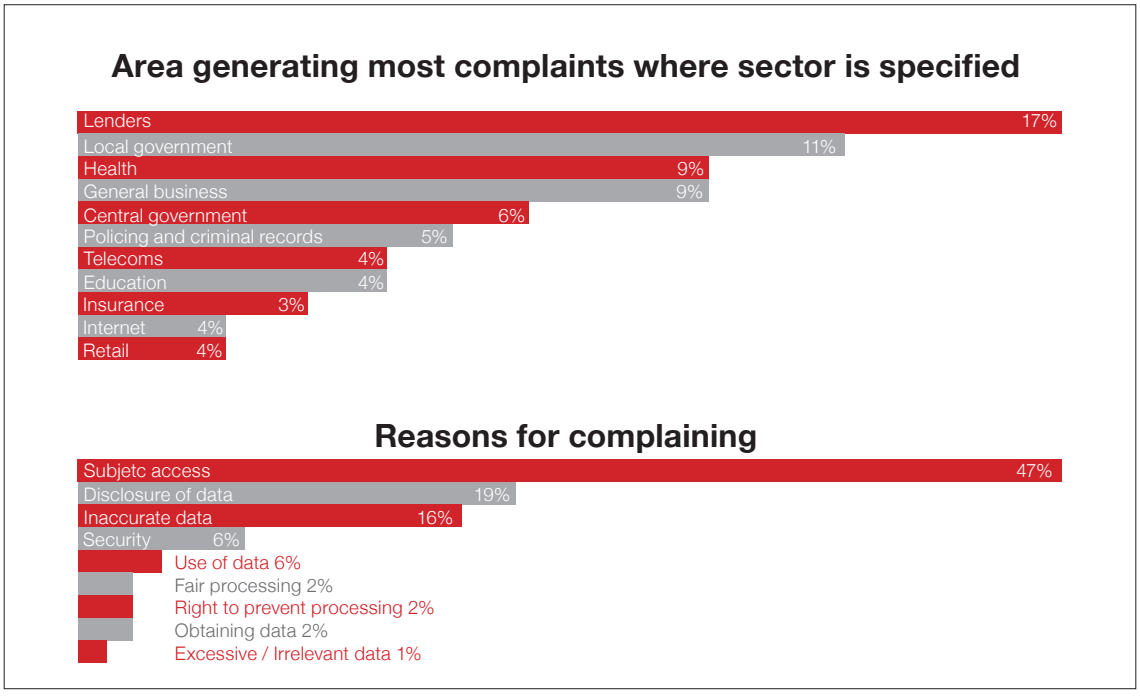
Complaints are also frequent when processing is not performed in compliance with data subjects' rights as stipulated in the Data Protection Directive 95/46/EC: right of access (3 DPAs), right of information, correction, or deletion, and right to consent or object to the processing of personal data (each mentioned by 2 DPAs).

The third category of complaints concerns violations of other data protection rules, such as disclosure of personal data (6 DPAs), violation of principles of proportionality and necessity (3 DPAs), lack of security of personal data (3 DPAs), excessive storage periods, unfair obtaining and processing of personal data, unlawful disclosure of personal data to third parties, inaccuracy of data (each mentioned by 2 DPAs), violation of the principle of lawfulness in general and violation of the conditions set forth by the law allowing the processing of data (each mentioned by 1 DPA).

The following is a detailed list of the types of reasons for complaints provided by the Irish DPA.

Reasons for complaining	Number of complaints
Electronic Direct Marketing	606
Access Rights	442
Disclosure	106
Unfair Processing of Data	35
Failure to secure data	35
Use of CCTV Footage	32
Excessive Data Requested	24
Accuracy	19
Unfair Retention of Data	17
Unfair Obtaining of Data	13
Postal Direct Marketing	10
Other	10

The following is the detailed information on reasons for complaints provided by the British DPA.



Source: Information Commissioner's Annual Report and Financial Statements 2012/13, p.21[48]

48 Information Commissioner's Office, Information Commissioner's Annual Report and Financial Statements 2012/13, Independent, authoritative, forward looking. Available online at: http://ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/ico-annual-report-201213.ashx.

One section of the survey related to the actual receipt by DPAs of complaints on automated profiling and the quantification of these. Half of the answering DPAs have received one or more complaints on automated profiling (see box 2).

Box 2 - DPAs having received complaints on automated profiling

Austria
Since automated profiling is used a lot for credit reporting, we have several complaints in this area.

Croatia
Yes, approximately 10 complaints.

Finland
The DPA has received complaints on profiling of personal data for commercial and e.g. marketing purposes.

Germany
Yes, but not very often. In this area the Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) is only competent in view of the calculation of score values by telecommunications companies.

Hungary
The Authority only received a few complaints on automated profiling.

Lithuania
Yes, we have had a complaint on automated profiling (credit rating).

Malta
Some complaints were received on the use of publicly available databases such as the election polls to build up customers' profiles.

Romania
The supervisory authority received few complaints concerning the application of Article 17 of Law no. 677/2001 and in only one case the data controller had not observed these requirements (a financial institution).

However, quantifying such complaints is difficult because responding countries generally do not have such statistics, never receive complaints on automated profiling, or explain that they have only received a "few" complaints (only Croatia mentioned that it had received approximately ten complaints).

With regard to the possibility of investigating data processing practices on their own initiative, all the responding DPAs are entitled do so, and seven (Finland, Germany, Hungary, Ireland, Italy, Slovakia and Sweden) have already used this right.

Article 23 of the current Data Protection Directive 95/46/EC invites Member States to provide compensation for "any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions". In this regard, the survey aims to establish whether compensation mechanisms (or similar practices) are envisaged at the national level for data subjects whose rights have been infringed by profiling and whether DPAs are aware of any other legal procedure whereby data subjects are entitled to compensation if their rights are infringed by automated profiling. The survey also serves to establish if there are any relevant court cases on automated profiling in their country. According to the DPAs' answers, such compensation mechanisms are usually envisaged in European countries[49]. Sometimes the national Data Protection Acts regulate the compensation procedures, giving competencies to the DPA or referring them to the general procedure and the general competencies of the court. If the national Data Protection Acts do not foresee such compensation, data subjects can resort to civil, penal or administrative procedures. In some countries they may also resort to other entities, such as a Competition Authority or an Authority for Consumer Protection, as in Hungary. Concerning relevant court cases on automated profiling, only the Italian DPA mentioned that "a case is currently pending before the Italian Supreme Court of Cassation regarding the case of profiling carried out by the National Printing Institution on its employees, in particular as a result of the monitoring of the employees' activities on the Internet. The case originated from the challenging of a decision adopted by the Garante [i.e., the Italian DPA] on 21 July 2011" prohibiting "the unlawful data processing operations which had been carried out, inter alia, without informing the data subjects and notifying the processing to the Garante[50]".

Profiling is a new data processing technique that is difficult to grasp and DPA officials often lack the training to deal with it properly. Currently, there are only three countries where DPA officials receive specific national training, instruction or guidance on profiling: the Finnish DPA has issued a number of guidance mechanisms (particularly on marketing practices); the Italian DPA has organised some internal seminars regarding the most controversial aspects of profiling; and the Slovakian DPA trains its employees in the area of profiling.

49 Drawing directly from the DPAs' answers: Austria (before a court but not in practice), Bulgaria (under civil law not in the DP Act which foresee administrative penalties-fines/sanctions), Croatia (before a court of general jurisdiction), Estonia (not specified), Finland (before a district court in civil procedure), Germany (the DPA of the non-public sector can impose a fine and civil procedures also apply), Greece (through civil procedure), Hungary (through civil and other procedures), Ireland (no direct compensation before the DPA but possible through civil procedure), Italy (judicial authorities' competence), Lithuania (civil courts' competence), Malta (civil courts' competence), Romania (competence of the court of Law), Slovakia (not under the DPA but through civil courts), Slovenia (the civil law gives competence to the courts and relevant authorities), Sweden (the Data Protection Act envisages compensation but not specific to profiling), UK (courts' competence).

50 Decision of the Garante available online at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1829641 (Italian).

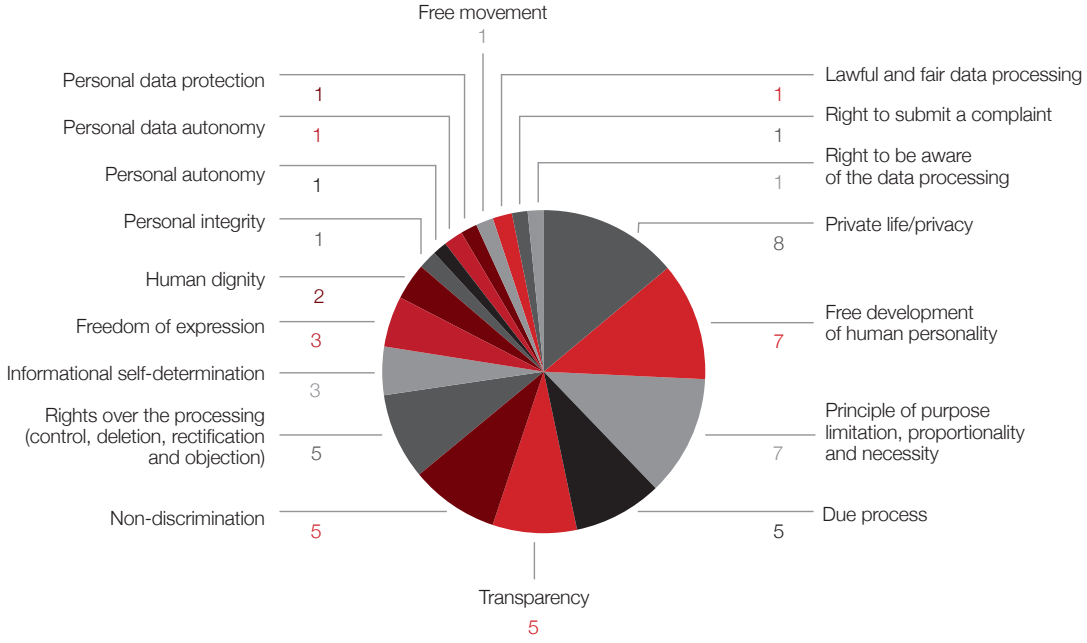
[3.4.] Fundamental rights: how fundamental rights and principles relate to profiling

The protection of fundamental rights[51] is an issue frequently highlighted by DPAs throughout the survey since these are likely to be affected by the use of profiling.

Among the main fundamental rights and principles challenged by profiling, the DPAs principally mention private life, personal data protection and respect of the principles of purpose limitation, proportionality and necessity. Other principles and rights include awareness about and the transparency of processing, non-discrimination and rights with respect to the processing of data (such as right of control, deletion, rectification and objection). To a lesser extent, the DPAs refer to informational self-determination, freedom of expression, human dignity, personal integrity, personal autonomy, free development of human personality, one's own image, free movement, lawful and fair data processing, right to submit a complaint and due process.

Main fundamental rights and principles challenged by profiling

Number of DPAs mentioning the right or principle



51 European Convention, Charter of Fundamental Rights of the European Union, OJ C 364/1, 18/12/2000. Available online at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf. The Charter of Fundamental Rights of the European Union envisages numerous rights divided into six categories: dignity, freedoms, equality, solidarity, citizens' rights and justice.

With the aim of protecting fundamental rights and principles, Article 20 of Directive 95/46/EC envisages a "prior checking" procedure as follows:

> Article 20 - Prior checking
>
> **1.** Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
>
> **2.** Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
>
> **3.** Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

The survey aims to determine whether DPAs envisage any specific procedure to be carried out to assess possible cases of infringement of fundamental rights and freedoms in profiling processes. Nine responding DPAs have noted this possibility: Austria, Bulgaria (a prior checking procedure is envisaged for processing in general and only for sensitive data), Croatia (the prior checking procedure is not explicitly mentioned in the Data Protection Act but the DPA has delivered prior notifications on establishing a filing system of evidence), Hungary (audit and impact assessment are envisaged as a prior checking procedure), Italy (the DPA's prior checking procedure is provided for by the Data Protection Code, as profiling is likely to present specific risks to data subjects' fundamental rights; the Italian Data Protection Code also considers profiling a high risk procedure, making notification by the data controller to the DPA absolutely mandatory), Malta (a prior checking procedure is envisaged if the profiling activity involves a particular risk of interference), Slovakia, Slovenia and the UK (prior checking is in the Data Protection Act but has never been enforced). There are, however, some options available to DPAs which do not envisage a prior check: the Finnish DPA points out that it can control codes of conduct drafted by controllers; in Germany, prior checks are carried out by the data protection officers of public authorities and of private companies; and the Romanian DPA can perform a preliminary control before the start of certain processing operations which are likely to present special risks for persons' rights and liberties.

Referring to the above-listed domains of application of profiling, the DPAs were asked to state which of them pose a considerable risk of infringement of citizens' rights to the protection of their personal data. According to the responding DPAs, such risk is highest in the financial domain (14 DPAs). The intelligence, national security and counter-terrorism, criminal investigation, healthcare (including insurance), employment and marketing domains are also frequently mentioned (10 DPAs). These are followed by border control, behavioural advertising (9 DPAs) and social media and the web (8 DPAs). In the education domain, seven DPAs think that infringements of the right to personal data protection are likely to occur. Four DPAs do not refer to the specific domains but provide interesting points of view: Croatia considers that any processing of special categories of personal data (data regarding criminal offences, health, racial and ethnic origin, trade union membership, political, religious or other beliefs) using profiling would be measured as risky; Germany explains that "the

domain of application of profiling is not decisive, but the quality and amount of data used and the penetration of the personal characteristics of a person involved" are; Malta deems that "By its very nature, profiling carries a considerable risk of violating the right to privacy" and that is why "Good practice needs to be present in all the processes and various steps involved"; and finally, for Slovakia "It is not possible to determine which domain poses the greatest risk in terms of protection of personal data. We are of the opinion that profiling should be evaluated consistently and complexly. As stated above, we have to have general conditions and guidelines for profiling as such, after which we will be able to approach the issue of solving problems of individual domains."

In which of the above listed domains of application of profiling (see question no. 19 Domains of application) is there considerable risk of infringement of citizen's right to the protection of their personal data?

	Number of Yes /14 countries	Countries
Finance (credit rating, anti-money laundering)	14	Austria, Bulgaria, Estonia, Filand, Greece, Hungary, Ireland, Italy (income tax), Lithuania, Romania, Slovenia, Sweden, Switzerland, UK
Intelligence, national security, counter-terrorism	10	Austria, Estonia, Hungary, Ireland, Lithuania, Romania, Slovenia, Sweden, Switzerland, UK
Criminal investigation	10	Austria, Bulgaria (police and justice field), Estonia, Hungary, Lithuania, Romania, Slovenia, Sweden, Switzerland, UK
Healthcare domain (including insurance)	10	Austria, Bulgaria, Estonia, Hungary, Lithuania, Romania, Slovenia, Sweden, Switzerland, UK
Employment	10	Austria, Estonia, Finland, Hungary, Italy, Romania, Slovenia, Sweden, Switzerland, UK
Marketing	10	Austria, Bulgaria, Estonia, Filand, Hungary, Italy, Romania, Slovenia, Sweden, UK
Border control	9	Austria, Estonia, Hungary, Ireland (immigration), Romania, Slovenia, Sweden, Switzerland, UK
Behavioural advertising	9	Austria, Bulgaria, Estonia, Filand, Hungary, Romania, Slovenia, Sweden, UK
Social media and web	8	Austria, Bulgaria, Estonia, Hungary, Slovakia, Romania, Slovenia, Sweden, UK
Education	7	Austria, Estonia, Hungary, Romania, Slovenia, Sweden, UK
Countries giving another kind of answer:	4	Croatia, Germany, Malta, Slovakia

In practice only six DPAs (Austria, Germany, Hungary, Lithuania, Italy and Slovakia) have ever processed a concrete case of infringement of fundamental rights and principles in the context of profiling (see box 3). Seven DPAs (Croatia, Estonia, Greece, Ireland, Slovenia, Switzerland and the UK) have never processed this type of case. It should be noted that Bulgaria, Finland and Malta report that they have processed concrete cases of infringement of fundamental rights, but not in profiling contexts.

Box 3 - Infringements of fundamental rights and principles in the context of profilin - Examples and concrete cases

Austria
We have processed several cases. Here is a typical example, a right to access case about credit ratings, in which the data protection commission ordered a bank to hand over information on how it determines a person's credit score:
http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Dokumentnummer=DSKTE_20100827_K121599_0014_DSK_2010_00

Germany
In a couple of cases in the BfDI's area of competence the data subjects were not informed about the possibility (cf. Art. 15 Directive 95/46/EC) of having the vital reasons of a measure based on profiling explained.
In other cases the rights to information concerning the creation of score values have not been properly complied with.
In part the profiles were not based decisively on personal characteristics, but on address data. This was the reason why solvent customers were not given mobile phone contracts.

Hungary
Concrete case: A direct marketing data broker created profiles of individuals with contact details using data mining algorithms. The database linked personal data from public and private sources with no regard for the purpose of the data processing operation and delivered marketing emails to the data subject. The database contained false data on several data subjects, because they had a common Hungarian name and the algorithm mixed their data with data of other individuals. The content of the marketing email was based on data from the above mentioned database.

Lithuania
The State Data Protection Inspectorate (SDPI) received a complaint against a mobile network operator in 2012. The person complained that the mobile network operator had collected information about his credit rating illegally. The SDPI stated that the mobile network operator could only collect credit rating information if the data subject was party to a new contract and if that contract was related to risk acceptance. The SDPI drew up a record of administrative offences for the responsible employee of the mobile network operator. Vilnius Regional Court sustained the position of the SDPI.

Italy
Italy refers to cases mentioned under the previous section 2.4.2 related to the DPA's decision on the implementation of Articles 15 and 12 of Directive 95/46/EC with regard to automated decisions based on profiling.

Slovakia
In 2009 the Office found in one case of profiling which involved the processing of personal data that were not up-to-date and had been stored for longer than necessary for the initial purpose.

The survey asked DPAs to rank a list of predetermined fundamental rights and principles in terms of how seriously they are challenged by profiling, in relation to concrete cases of infringement. The analysis of the answers shows that the most challenged right is the right to data protection, followed by the right to privacy. The right to non-discrimination, the right to transparency, the right to autonomy and self-determination and the right to due process followed. Note that there are not huge differences amongst those rights. Hungary also mentioned two rights not listed in the questionnaire: proportionality and data minimisation.

Thinking about concrete cases of infringements, can you rank the following fundamental rights/principles in terms of how they are challenged by profiling (7=the most challenged, 1=the least challenged)?

Please include the rights/principles you mentioned in question 34 if they are not already mentioned.

	Right to data protection	Right to privacy	Right to non-discrimination	Transparency	Autonomy and self-determination	Due process	Other
Austria	7	7	7	7	7	7	
Bulgaria	6	7	6	5	1	1	
Croatia	5	6	6	7	N/A	N/A	
Finland	5	2	4	3	7	6	
Germany	7	3	4	6	5	2	
Hungary	7	7	1	3	4	2	
Ireland	6	7	4	3	2	5	
Italy	5	4	7	3	6	2	
Lithuania	6	7	4	5	3	2	
Malta	5	5	4	4	5	N/A	
Romania	7	7	6	6	6	5	
Slovakia	7	7	3	5	5	5	
Slovenia	3	2	6	4	7	3	
Total	76	71	62	61	58	40	
	Data minimisation 6						
	Proportionality 5						
	N/A: Estonia, Greece, Sweden, Switzerland, UK						

In this section, the survey aims to gain an overview of DPAs' participation in bodies or institutions dealing with human rights protection. While all the DPAs (except Switzerland) are part of the Article 29 Working Party, twelve DPAs (Austria, Bulgaria, Croatia, Estonia, Greece, Italy, Lithuania, Malta, Romania, Slovakia, Switzerland, and the UK) mention that they are also affiliated with bodies or institutions involved in human rights protection (see box 4).

Box 4 - Bodies and Institutions involved in human rights protection of which DPAs are part.

Austria
Not specified.

Bulgaria
Consultative Committee of Convention 108/81 of the Council of Europe (member).
Global Privacy Enforcement Network (member).

Croatia
Cooperates with the relevant institutions in Croatia promoting privacy and data protection.

Estonia
International cooperation of freedom-of-information commissioners (member)
Baltic cooperation of Data Protection Authorities (member)
Supervision Coordination Group of the European fingerprint database (Eurodac) (member)
Europol Joint Supervisory Body (JSB) (member)
Joint Supervisory Authority for the Customs Information System (CIS) (member)
European Visa Information System (VIS) Supervision Coordination Group (member)
Schengen Joint Supervisory Authority (member)
International Working Group on Data Protection in Telecommunications (Berlin Group member)
Organisation for Economic Co-operation and Development (OECD) Working Party on Security and Privacy in the Digital Economy (WPSPDE member)
Consultative Committee of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (member)
Global Privacy Enforcement Network (member)

Greece
Participation in Work Programmes, Committees, Bodies and Conferences with peer authorities, mainly in the EU.

Italy
Supervision Coordination Group of the European fingerprint database (Eurodac member)
Europol Joint Supervisory Body (vice-chair)
Joint Supervisory Authority for the Customs Information System (member)
European Visa Information System Supervision Coordination Group (vice-chair)
Schengen Joint Supervisory Authority (member)
Article 29 Working Party
Consultative Committee of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (member)
Bureau of the Consultative Committee of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (member)
Council of Europe Ad hoc Committee on Data Protection CAHDATA (member)
Working Party on Security and Privacy in the Digital Economy (member)
Working Party on Security and Privacy in the Digital Economy Bureau (member)
International Working Group on Data Protection in Telecommunications (Berlin Group member)
The International Conference for Privacy and Data Protection Commissioners
The Spring Conference of European Data Protection Commissioners
Global Privacy Enforcement Network (member)

Lithuania
Lithuanian institutions involved in human rights protection:
Equal Opportunities Ombudsperson's Office
The Seimas Ombudsman's Office
Institution of the Ombudsman for Children's Rights of the Republic of Lithuania
State Labour Inspectorate
Others

Malta
European fora (not specified)

Romania
International Working Group on Data Protection in Telecommunications - IWGDPT
(Berlin Group)
Central and Eastern Europe Data Protection Authorities (CEEDPA)
International Conference of Data Protection Commissioners
Association of Francophone Data Protection Authorities (AFAPDP)
Bureau of the Consultative Committee of the Council of Europe Convention for the
Pro tection of Individuals with Regard to Automatic Processing of Personal Data [ETSNo 108]

Slovakia
Slovakian offices (cooperation)
Consultative Committee of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No 108] (member)
Data protection authorities (participation in conferences)

Switzerland
Article 29 Working Party for Schengen relevant matters
The International Working group on Telecommunications
The International Conference for Privacy and Data Protection Commissioners
The Spring Conference of European Data Protection Commissioners
Association francophone des autorités de protection des données personnelles

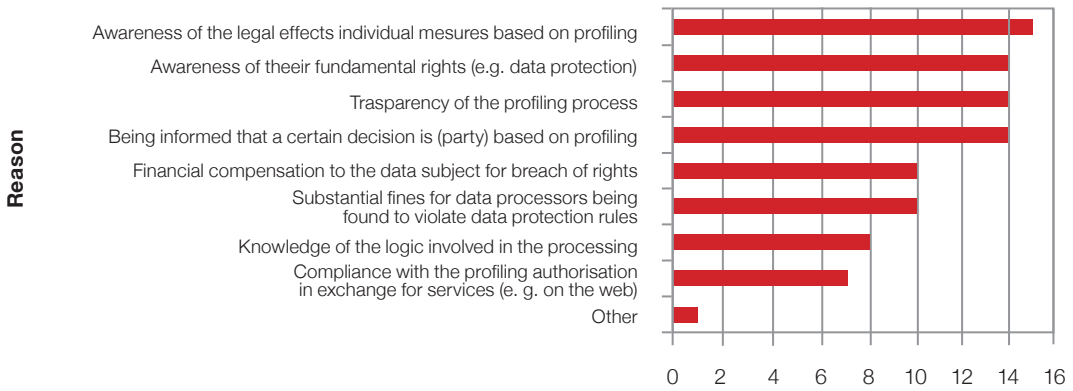
United Kingdom
The International Working Group on Telecommunications
The International Conference for Privacy and Data Protection Commissioners
The Spring Conference of European Data Protection Commissioners

The last two sets of questions concerned citizen awareness and DPAs' strategies to improve general awareness.

[3.5.] Citizen awareness

As shown throughout the report, data subjects' awareness is an important and worrisome issue for DPAs. In this regard, DPAs were asked to give their opinion on several points which could have a major effect on data subjects' decisions to submit a complaint in case of automated profiling that significantly affects them. They principally mention awareness of the legal effects of individual measures based on profiling (15 DPAs). They also frequently quote the awareness of their fundamental rights (such as data protection), transparency of the profiling process and the need to be informed that a certain decision is (partly) based on profiling (each mentioned by 14 DPAs). These are followed by concerns about financial compensation or substantial fines for data processors in the case of rights violations (10 DPAs). This suggests that the awareness of the existence of profiling and of individuals' rights when their personal data are used in automated processing is considered more important than financial issues. Last but not least, about half of the responding DPAs think that knowledge of the logic involved in the processing (8 DPAs) and compliance with profiling authorisation in exchanges of services (for example on the web) (7 DPAs) can have an effect on data subjects' decisions to submit complaints. Austria also mentions swift redress and governmental action, which were not predetermined reasons.

Reasons likely to influence data subjects to submit a complaint in case of automated profiling that significantly affects them



As for DPAs' experience regarding the main limitations for data subjects' understanding of profiling risks and implications, the most frequently mentioned are the lack of knowledge about the existence of profiling and lack of transparency in processing. A misunderstanding of what profiling is and a general lack of information on profiling risks are also mentioned. Finally, the indirect link between the data controller and unfamiliarity amongst data subjects with the possibility of complaining could also limit the understanding of profiling risks and implications.

[3.6.] Strategies for awareness

The next section examines the methods used by DPAs to inform the general public of the rights of data subjects as regards data collected or used for profiling purposes. It also addresses the issue of whether or not DPAs face any significant technical or practical challenges in providing this information. DPAs employ numerous strategies in order to improve awareness on this particular topic. They mainly use their websites for this purpose. However, they also utilise written documentation (such as reports, guidelines, newsletters, leaflets and press releases), internal and external seminars/conferences (workshops, roundtables, study visits to other agencies and ministries, press conferences, campaigns, interviews released by Commissioners, institutional communications), media (television, radio, social networks, newspapers), and annual surveys, and/or they give their citizens the option of writing or calling their DPA (hotline). No country mentioned significant technical or practical challenges in this mission except for the Finnish DPA "in cases where data subjects are not actually aware of concrete circumstances or have misunderstood the processing activities in question".

Following the previous question, DPAs were asked whether they have produced any report, study or website on data protection, especially on profiling, to increase data subjects' awareness of such issues (see box 5). Ten DPAs answered positively. However, it should be noted that among the countries answering negatively, some provided written material on general data protection (Austria, Hungary and Romania).

Box 5 - Reports, studies, websites on data protection (especially on profiling) produced by DPAs

Austria
No, nothing particular on profiling. We issue a bi-annual report on our work: http://www.dsk.gv.at/site/6207/default.aspx (Austrian).

Bulgaria
The Commission for Personal Data Protection has prepared and maintains its own web site, containing information on the various privacy and data protection issues inBulgaria, namely: https://www.cpdp.bg/en/index.php?p=rubric&aid=4- in English. We have not prepared specialised information about profiling.

Croatia
Yes, our Agency has a website www.azop.hr where we inform all those concerned about the effects of our activities in the field of personal data protection. News and information about events relating to the Agency are updated on a daily basis, and we also monitor and publish news and developments in the world concerning the protection of personal data and (il)legal actions.

Estonia
The activity is included in the Estonian DPAs 2014 work plan.

Finland
Profiling has been addressed in guides published by the DPA. These guides address the matter according to the focus of the guidance, e.g. direct marketing.

Germany (refers to a previous answer)
The dangers of profiling are regularly the subject of the activity reports which the BfDI submits biennially to the German Bundestag [i.e. federal Parliament] and makes available to the public. General and contextual information on profiling - for example by credit reporting agencies - can be found on the website of the BfDI.

Greece
We have produced and published a lot of information on the subject of data protection in general and on specific processing domains, but not on automated profiling, since we have not considered this as a priority so far.

Hungary
The Hungarian DPA has not produced any report/study/website on this matter.

Italy
Our DPA has not produced specific reports/studies/websites on profiling. However, our DPA highlights its decisions, including those on profiling, through its website and its newsletter that is published regularly. It also emphasises the international dimension with particular regard to the Council of Europe Recommendation on profiling and the Report study - by the scientific experts of the Centre de Recherche informatique et droit (CRID) - which constituted the theoretical basis for the preparation of the Recommendation.

Lithuania
Our DPA has not produced any reports on data profiling because we have limited experience in this area.

Malta (refers to a previous answer)
Data protection awareness is normally dealt with generically. On the issue of behavioural marketing or advertising, this Office has in the past issued a newspaper article and also stated its views in programmes on the radio.

Romania
Not as regards profiling.

Slovenia
Yes: https://www.ip-rs.si/publikacije/prirocniki-in-smernice/ (Slovenian)

Sweden
We have not issued any reports that specifically deal with profiling, but other information includes parts about this, e.g. information about data processing in the employment context.

Ireland, Slovakia, Switzerland, United Kingdom
No.

Finally, almost all DPAs agree that data subjects' awareness of automated profiling and its possible implications should be increased. In order to achieve this aim, they suggest using numerous methods or tools (guidelines, CPDP website, online videos, promotional campaigns, conferences, etc.), involving private entities (responsibility for transparency), public officials and consumer protection bodies, and addressing all remaining aspects of the issue (particularly, by providing information on data processing/profiling in general and on specific issues, on good practices in risky domains, on legal effects of individual measures based on profiling, on data subjects' rights or financial compensation for a breach of rights).

[3.7.] Relevance of the Questionnaire

On the relevance of the topic of the questionnaire to the DPAs' everyday activities or to the current policy debate on data protection, seven (Bulgaria, Estonia, Finland, Italy, Romania, Slovakia and the UK, which deems that "This was a very useful questionnaire that touched on some very important issues, and we appreciate the opportunity to have shared our views with you") consider that it is completely relevant and five (Croatia, Hungary, Lithuania, Malta and Switzerland) answered that the questionnaire was "more or less" relevant. For the Greek and Irish DPAs, although they did not consider this questionnaire at all relevant for their everyday activities, it is relevant to the current policy debate on data protection. For the Slovenian DPA, the questionnaire was not sufficient. Austria, Germany and Sweden did not answer the question.

4

Conclusions

From the survey it emerged that, overall, the national legal frameworks on automated profiling within the surveyed countries (European Union member states and Switzerland) look quite similar. Moreover, the DPAs have largely similar points of view in their understanding of automated profiling, even though this is a new and fast-moving domain, and a majority of the DPAs express the need for legal regulation. The British DPA has a particular view on the issue: it is not against legal regulation, but it believes that automated profiling does not necessarily need stricter legal regulation than any other form of data processing.

However, when discussing future regulation, differences emerged among DPAs, in relation to both Article 20 of the GDPR and Article 9 of the proposed Directive. Whereas one group supports the new proposals, the other group thinks that they can, and should, be improved to reinforce data protection. It is important to note that the groups supporting or opposing Article 20 of the GDPR are not altogether the same groups supporting or opposing Article 9 of the proposed Directive. This suggests that research is needed in order to better identify the levels of risk associated with the use of automated profiling and to identify the importance given to fundamental rights protection, in particular data protection, in general and in the criminal and justice sector.

There is also a largely shared understanding among DPAs concerning the sectors in which automated profiling is applied and the challenges, risks and benefits emerging from the use of profiling techniques. Major concerns refer to respect for fundamental rights (in particular private life, data protection and freedom rights), particularly in the domains of finance and marketing. This is not surprising, since these two sectors use automated profiling most frequently and on a large scale.

National legal frameworks usually envisage two main ways of protecting data subjects' rights: a priori, through the prior checking procedure and a posteriori, through a complaint procedure.

In effect, the first way to protect data subjects' rights is to address the cause of the problem through the identification and examination of automated profiling activities likely to present specific risks to rights prior to the start of processing. This is carried out through the prior checking procedure of Article 20 of Directive 95/46/EC, but only nine DPAs use such a procedure. Better implementation and reinforcement of this procedure would enable the prevention of rights infringements[52].

The second way of protecting data subjects' rights is to redress the infringement. All the countries surveyed envisage a particular procedure whereby data subjects can lodge complaints directly with the DPA in the case of a data protection violation. This process seems quite similar among the surveyed countries. This type of procedure frequently

52 Note that "prior authorisation" and "prior consultation" procedures, based on the current "prior checking" procedure, are also envisaged in Article 34 of the GDPR.

results in decisions aiming to stop the violation. Compensation mechanisms, in almost all countries queried, are in the hands of the courts.

Although the reasons for complaining are quite numerous, the DPAs within the European Union and Switzerland have only received a few complaints on profiling to date. This might be due to the novelty of the use of automated profiling, but also to a general lack of awareness among the public. Awareness of the legal effects of individual measures based on profiling, awareness of their fundamental rights and awareness of the profiling process are all factors likely to influence data subjects' abilities to submit complaints in cases of automated profiling that significantly affect them. Our survey reveals that even though awareness among data subjects is an important and worrisome issue for DPAs, most of them do not seem to have dedicated much effort towards raising awareness so far, for example through reporting and/or guidance specifically dedicated to profiling. Therefore, DPAs need to provide more comprehensive and understandable information on the concept of profiling, its uses and its potential risks and implications. Such information can be provided by strengthening all the means already used by DPAs - including, among others, websites, written documentation (such as reports, guidelines, newsletters, leaflets, annual surveys), conferences, campaigns and contributions in the media - with a focus on profiling techniques.

All DPAs are entitled to investigate data processing practices on their own initiative. Thus, they must ensure that data controllers respect their obligations under Directive 95/46/EC regarding the information to be given to data subjects and the respect of data subjects' rights. DPAs are also responsible for advising data controllers on their responsibilities and ensuring that they are following the rules in practice.

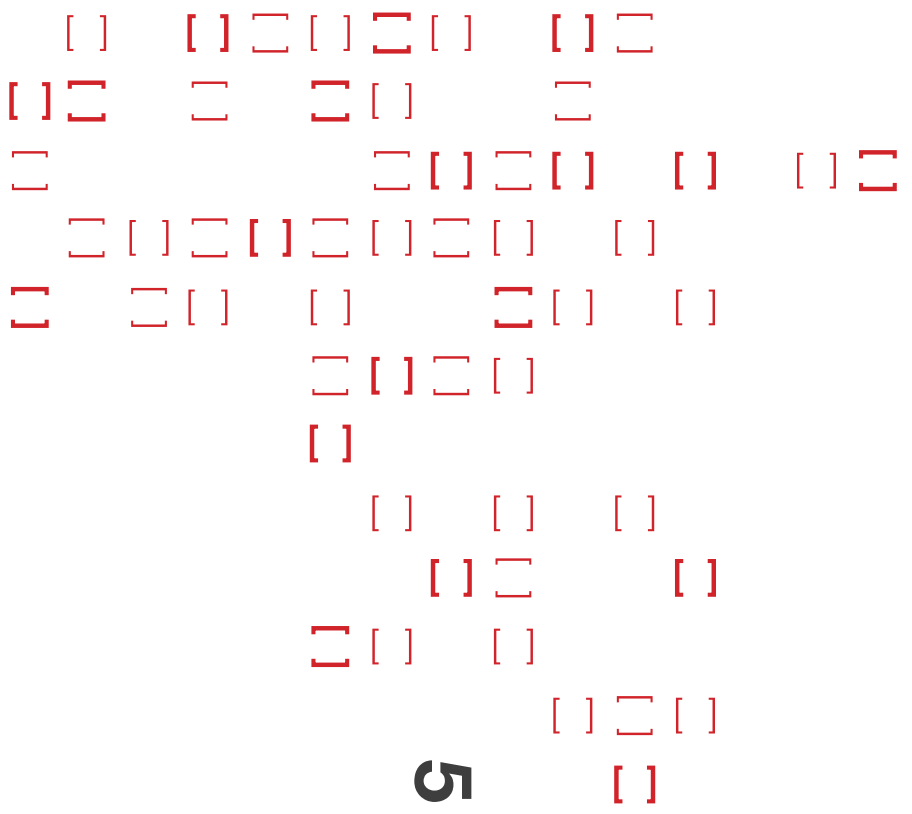
The most challenged rights according to DPAs are privacy and data protection rights when considering the relationship between respect for fundamental rights and principles and profiling. Only a few DPAs have ever processed a concrete case of infringement of those rights. Hence, although there is a generally-held opinion among DPAs that automated profiling frequently occurs and can lead to violations, it seems that citizens are not aware of it, do not appreciate the risks or do not realise when an infringement of their rights has occurred. Again, the lack of knowledge about the existence of profiling and the lack of transparency over processing are the main limitations for data subjects' understanding of profiling risks and implications. There may possibly be other legal or institutional obstacles that hamper citizens' access to justice besides a lack of awareness; this is difficult to assess on the basis of the survey, and requires further research.

Aside from the need to enhance citizens' awareness, DPA employees also need to be more familiar with profiling issues. Indeed, our survey reveals that DPA officials in only three countries receive specific national training, instruction or guidance on profiling. DPA officials cannot correctly perform their mission without a clear and complete understanding of the profiling technique itself, the challenges and risks associated with it and the scale and scope of its use. DPAs therefore need to develop and implement more training schemes and seminars for their employees on the issue of profiling. Given the scarce experience with such training or guidance within national DPAs, possibly the Article 29 Working Party or the EDPS could take the initiative to identify and disseminate best practices.

To conclude, national Data Protection Authorities admit that profiling is a challenging and risky application. To better address these challenges and risks, they need to take the necessary measures to:

- make data controllers more aware of their responsibilities;
- significantly enhance the awareness of citizens; and
- improve the training of DPA employees.

DPAs already employ a number of methods to raise awareness among the general public about their rights regarding the use of personal data for profiling purposes or other processing activities, but our findings suggest that they need to substantially step up their efforts to increase data subjects' awareness of automated profiling and its possible implications. It is up to all stakeholders involved in data processing and data protection to address this issue. Therefore, national Data Protection Authorities and the Article 29 Working Party, the EDPS, the Council of Europe, the European Parliament, consumer protection bodies and also data controllers and public officials need to take measures to ensure that better information is provided to citizens on all issues related to profiling.



References

[Article 29 Working Party, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, 13/05/2013. Available online at:http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf.

[Bygrave L. A., Data protection law: approaching its rationale, logic and limits, The Hague, Kluwer Law International, 2002, p.3.

[Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 17/12/2012 COM(2012)0011- 2012/0011 (COD), Rapporteur Albrecht J.P. Available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

[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, OJ L 350/60, 30/12/2008. Available online at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008F0977

[Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies. Available online at: https://wcd.coe.int/ViewDoc.jsp?id=1710949

[Council of the European Union, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Key issues of Chapters I-IV, Brussels 31/05/2013 10227/13 ADD 1. Available online at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010227%202013%20ADD%201.

[Directive 95/46/EC of the European Parliament and of 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, OJ L 281, 23/11/1995 P. 0031 – 0050. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement ofsuch data, Brussels, 25.1.2012 COM(2012) 10 final 2012/0010 (COD). Available online at:

[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

[European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD). Available online at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[European Convention, Charter of Fundamental Rights of the European Union, OJ C 364/1, 18/12/2000. Available online at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[European Data Protection Supervisor (EDPS), Opinion on the data protection reform package, 7/03/2012. Available online at: http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf

[Ferraris V., Bosco F., Cafiero G., D'Angelo E., Suloyeva Y. (2013), Defining Profiling, Working Paper 1 of the Profiling project, p.15. Available online at: http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_definition_0208.pdf

[Information Commissioner's Office, Information Commissioner's Annual Report and Financial Statements 2012/13, Independent, authoritative, forward looking. Available online at: http://ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/ico-annual-report-201213.ashx.

[Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy, Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD), Expert report on the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, 11/01/2008, Strasbourg. Available online at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profiling_2008_en.pdf

[Salzburg Forum Ministers, Agreement on cooperation in the area of witness protection, 24/05/2012. Available online at: http://www.mzz.gov.si/fileadmin/pageuploads/Mednarodno_pravo/Zascita_pric_-_CTC.pdf

Note: All the websites were last accessed on 31.03.2014.

E-commerce and profiling in Romania: what is going on and who cares about privacy?

Bogdan Manolea, Bianca Toma and Cristian Ghinea
Romanian Center for European Policies

Executive summary

As a contribution to "PROFILING – Protecting Citizens' Rights Fighting Illicit Profiling" the Romanian Center for European Policies (CRPE) conducted a case study about the use of profiling in Romanian e-commerce domain. The purpose of this study is to identify what are the current profiling practices related to e-commerce in Romania and their privacy implications. We focused more on deciphering on what are the current practices and how do the local actors see the process – both in technical and legal terms – also trying to probe certain key-issue from a data protection point of view.

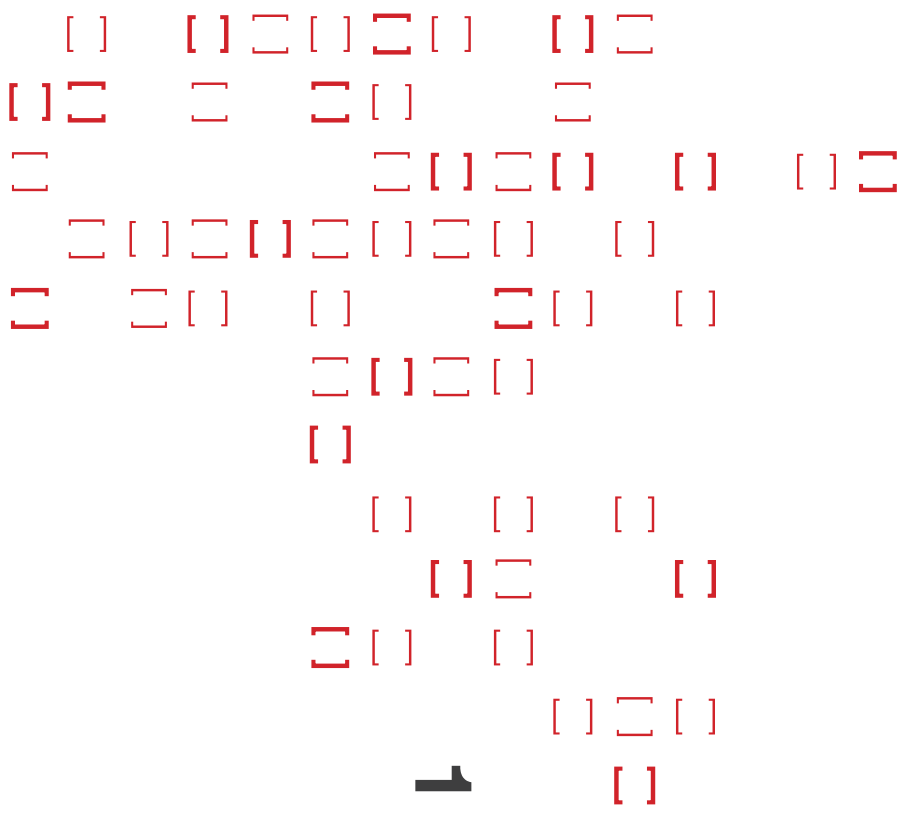
Based on a analysis of the initial phase it turned out that actually most of the knowledge related to profiling practices in e-commerce would be obtained not only directly from e-commerce shops, but rather from companies or consultants that are working specifically on this niche. Therefore the 10 interviews with different actors from the Romanian market spanned across a large spectrum of professionals related to e-commerce: e-commerce shops, profiling and targeting software companies, e-commerce consultants, marketing experts, e-commerce platform owners and e-mail marketing companies. The interviewees were complemented by a series of informal private talks made by the author during the e-commerce and e-marketing events.

The general image of the current practices of profiling in Romania points to a limited usage of these practices among current players. Without being possible of having an exact picture, the average estimation show that a 5-10% of the national e-commerce players are involved in some kind of the profiling activities. However, this doesn't need to be confused with the number of e-commerce shops that are currently gathering data about customers and visitors that they could use in the future for profiling purposes. Most of the e-commerce shops are gathering a lot of data from their customers which are kept for an undetermined period and this is a basic feature of any e-commerce platform. Therefore, using profiling in e-commerce activities is on the uprise, at least for medium and big e-shops.

The analysis revealed a grim picture of privacy awareness on profiling among all e-commerce stakeholders. Consequently the data protection issues are often ignored, such as:

- The scope of profiling is actually broader than just "increasing sales" and may be used in unexpected secondary uses;
- Any action can be technically tracked, so profiling is limited only on business reasons for data that could be relevant for an e-commerce shop;
- Profiling may be used in e-commerce for producing a significant or legal effect: usually price differentiation but also giving other benefits and/or blacklisting;
- Re-targeting raises specific privacy concerns, especially in the case of using shopping cart recovery techniques;
- Sharing data with Google and/or Facebook is the rule. However, those companies are giving back less data to the e-commerce shop;

- Most of the e-commerce shops are claiming they are obtaining consent for profiling based on the acceptance of the online documents – privacy policy or terms and conditions and/or actions (such as subscription to the newsletter or finalizing the order)
- Our empiric analysis of the relevant public documents of 150 e-shops shown that this information on using profiling is lacking from all the websites that we have visited. Some of them have included the scope of "personalizing information that we show to you" as a part of the purpose or usage for personal data.
- As regards the cookie policy, none of the e-commerce websites that we visited said anything specifically about profiling as the specific purpose for using cookies. Most of the texts – if existent - are copy&paste with general information on what cookies are.
- Although technically feasible, it is impossible to opt-out on e-commerce profiling, apart from the case in which the user deletes the cookies or uses an Ad blocker.
- There is no incentive on data minimisation, except for commercial reasons (data no longer useful or could lead to better e-commerce conversion).
- Currently, there is no enforcement on profiling and no information among e-commerce stakeholders if and how this could be in breach of data protection rules.



Introduction

The rapid increase in Internet access has brought several benefits including the availability of a faster way to shop online: electronic commerce. Although it seems - for a novice, at least – a more anonymous way of shopping, the information that is sent electronically to an online store may actually be more invasive from a privacy point of view. Although until some years ago, the personal information gathered directly or indirectly by e-shops was not used at all or only to a very limited extent by e-commerce businesses, the situation is changing significantly day by day as new profiling tools are used.

These new ways of using personal information raise significant challenges to the right of privacy:

> *"Profiling may challenge the essence of democracy because it moves to the background the role of human beings in the decision-making process and creates unbalanced distribution of power and knowledge asymmetries among citizens on one side and government and corporate business enterprises on the other side. Decisions based on automated profiling techniques do not allow the citizens to challenge the reasoning behind the process. This clearly hampers a full and free development and expression of one's personality and his/her effective participation to the democratic life"*[60].

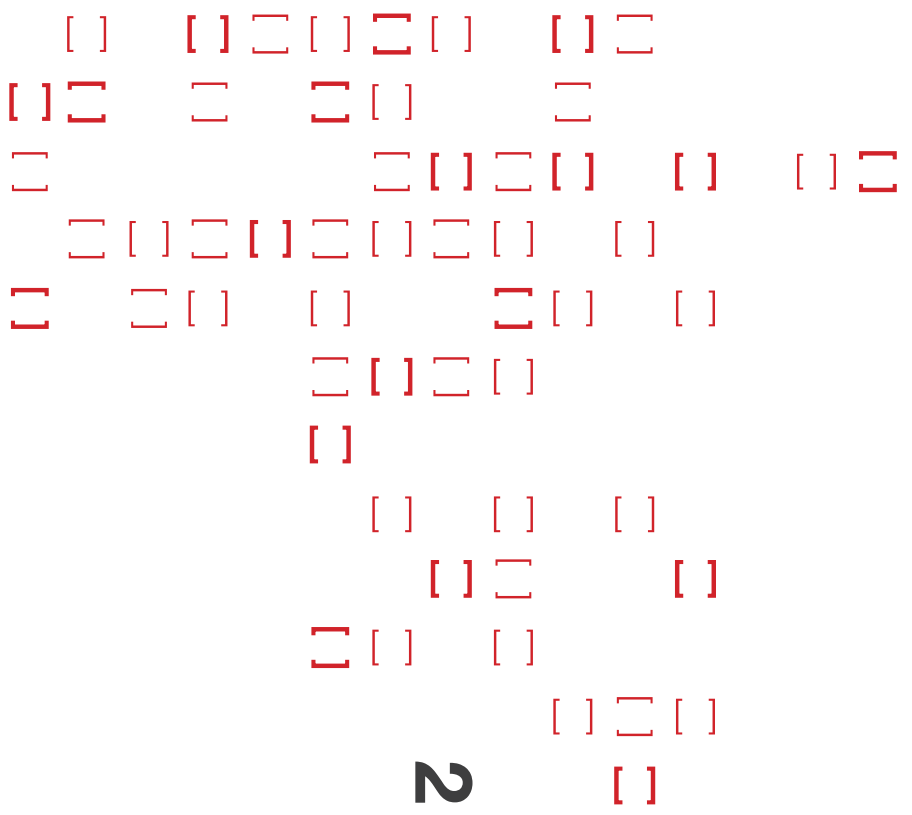
The development of new Internet technologies has made this profiling not only possible, but also easier, especially with the digitisation of sensors and the generation of data through logs and user engagement[61]. Although much attention has been paid to behavioural advertising and third-party cookies, especially on the occasion of the 2009 amendments to the ePrivacy Directive[62], the usage of profiling techniques in e-commerce and its potential implications for privacy are still fairly recent issues – especially on the Romanian market where no similar studies have so far been undertaken.

---

60 See Profiling project – working paper - The impact of profiling on fundamental rights V. Ferraris (AMAPOLA); F. Bosco, E. D'Angelo (UNICRI) Internal reviewer: B.J. Koops (Tilburg University), p34 available at http://profiling-project.eu/wp-content/uploads/2013/10/PROFILINGproject_WS1_Fundamental_1110.pdf (all pages, last accessed on 30 August 2014)

61 More details in the Profiling Project – working paper - Evolution of Technologies in Profiling, DANIEL GUAGNIN, LEON HEMPEL (Technische Universität Berlin) and JUSTIN JUNG (Philipps-Universität Marburg) available at http://profiling-project.eu/wp-content/uploads/2013/08/Evolution-of-Technologies-in-Profiling_0208.pdf

62 Directive 2009/136/EC, text available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF



Purpose and methodology

The purpose of this study is to identify the current profiling practices related to e-commerce in Romania and their privacy implications. As this was the first national study of its kind and we expected awareness about the implications of profiling on privacy to be rather limited, we decided to focus more on deciphering the current practices and how local actors see the process – both in technical and legal terms – while also trying to probe certain key issues from a data protection perspective. Chapter 5 includes a more detailed discussion on how the actual findings are related to data protection principles relevant for the profiling domain.

The perspectives of e-commerce stakeholders were gathered through a series of 10 interviews with different actors from the Romanian market. Right from the initial planning phase it became clear that in order to get more honest answers from the interviewees, we would need to guarantee the anonymity of those who decided to talk to us. During the actual interviewing phase it became even more obvious that – due to the limited size of the market, where almost everyone is familiar with the other market players - in this study we would only be able to quote the types of e-commerce businesses that we met in order to ensure the real anonymity of the interviewees[63].

Moreover, during the initial planning phase and informal talks, it actually turned out that most of the knowledge related to profiling practices in e-commerce would be obtained not only directly from e-commerce stores, but also from companies or consultants working specifically in this niche sector.

Therefore our target group of 10 interviewees spanned a large spectrum of professionals related to e-commerce: e-commerce stores, profiling and targeting software companies, e-commerce consultants, marketing experts, e-commerce platform owners and e-mail marketing companies.

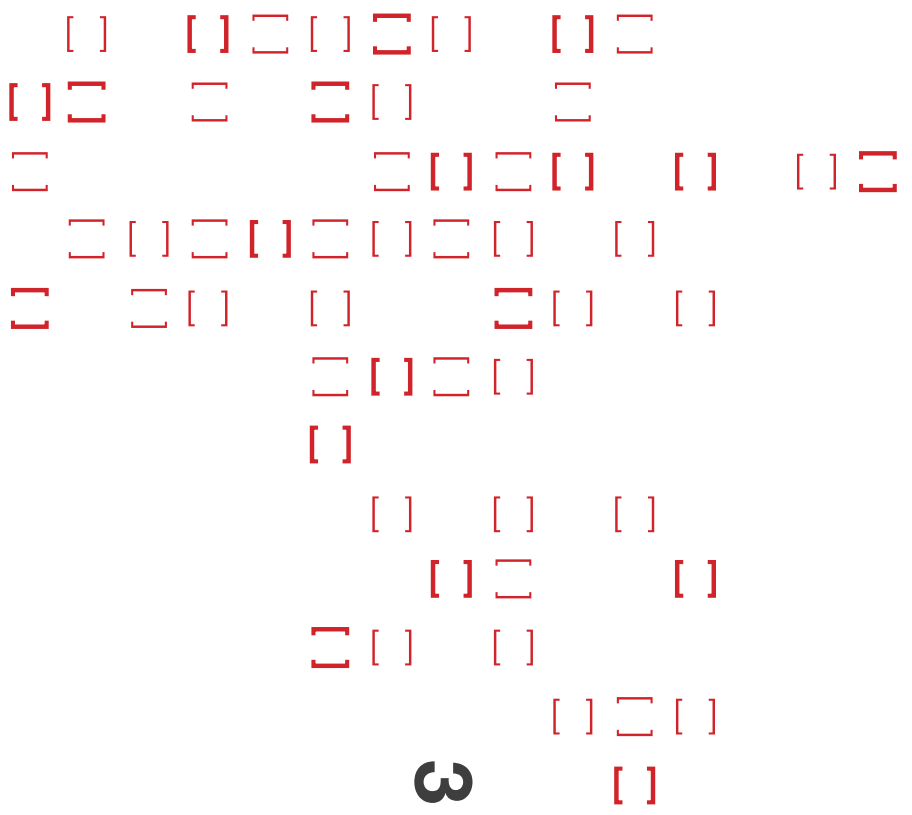
The findings from the interviewees were enhanced through a series of informal private talks by the authors during e-commerce and e-marketing events attended in the last two years. The study is also based on one of the authors' experience in auditing the Romanian e-commerce websites in the Romanian E-commerce Gala Awards (GPeC) in 2013 and 2014 (only the first phase in 2014). On the latter occasion, the author analysed and graded more than 150 Romanian e-commerce stores on several legal criteria, including the content of their privacy policies.

63 For a similar reason we also decided in the final publication not to specifically quote which interview the citations refer to, as it would be quite easy for anyone familiar with the market and the connections, to understand exactly who said what, at least for some parts.

During the interviews and for the purposes of this working paper, we have used the following definition of profiling, developed in the first paper of the project[64]:

> *"Profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (human or non-human, individual or group) subject. Constructing profiles is the process of discovering unexpected patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific subject or to identify a subject as a member of a specific group or category and taking some form of decision based on this identification and representation".*

64 See Profiling project – working paper - Defining Profiling V. Ferraris (AMAPOLA); F. Bosco, G. Cafiero, E. D'Angelo, Y. Suloyeva (UNICRI) Internal reviewer: B.J. Koops (Tilburg University) available at http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf



Basic technical issues related to profiling

We identified two main profiling methods, according to how data are obtained:

[3.1]

Data provided directly by users in order to create their account or to place an order or in any other interaction with the website.

Such data are usually obtained through the registration form or user profile (or more often in recent years through Facebook Login[65] or similar social networks), but can also be obtained manually through other interactions with the website.

[3.2]

Data automatically given by users when they visit the e-commerce web page.

Such data are usually obtained via cookies or other tracking technologies.

As our colleagues pointed out in their paper on the Evolution of Technologies in Profiling[66] there are "several methods to reconstruct the session of a web user, such as log file analysis, session tracking, user and multi-server user tracking". Most of the profiling that we analysed in the e-commerce arena is actually done via cookies: "Cookies are information sent by the server and stored on the computer of the user. The cookie is usually set when the user visits a website for the first time. During future website visits, the server can retrieve information about former visits from the cookie and update the information stored in the cookie – if the user does not actively prevent it. Accordingly cookies facilitate the creation of individualised user profiles" (E. Benoist, 2005).

65 See details at https://www.facebook.com/about/login/

66 More details in the Profiling Project – working paper - Evolution of Technologies in Profiling, DANIEL GUAGNIN, LEON HEMPEL (Technische Universität Berlin) and JUSTIN JUNG (Philipps-Universität Marburg) available at http://profiling-project.eu/wp-content/uploads/2013/08/Evolution-of-Technologies-in-Profiling_0208.pdf

4

Romania: e-commerce and profiling

[4.1] Current profiling practices in e-commerce in Romania

Overall, the use of profiling practices among Romania's current players appears to be rather limited. Although it is not possible to have an exact picture of the situation, it is estimated that on average 5-10% of Romanian e-commerce players are involved in some kind of profiling activity.

This also depends on the size of the e-commerce business – smaller players do not have an incentive to use profiling, as they usually need to deal with more basic issues:

> *A: Unfortunately, a high percentage of clients haven't focused on creating a database of emails on their own. Therefore, as their customer databases are so small, whenever we try to apply any type of segmentation tool, we are left with only 300 emails. Summing the costs of publishing/sending/creating a newsletter, it is just not worth it. But in the coming years this will certainly be the trend and this is what we are trying to suggest to our clients, segmentation tools, to prevent them from sending ads for children's shoes to a 50-year-old man.*

However, this should not be confused with the number of e-commerce stores that are currently gathering data about customers that could be used in the future for profiling purposes. Most e-commerce shops gather a lot of data from their customers which are kept for an undetermined period and this is a basic feature of any e-commerce platform. As far as we know, there is no platform today that would automatically delete the personal data gathered, after a certain period.

As regards data obtained automatically via web browsing leading to and in the e-commerce website, anything can be tracked on a web page that you own - from a purely technical point of view.

But in practice this depends on the e-commerce platform used and/or whether an external specialised (or not[67]) third party service[68] is being used. As regards the e-commerce platforms, some of them noted that these tracking features are not implemented at all, while others sold it as an add-on package that could be bought as an extra (but only 4-5% of their clients actually buy them).

> *A: It has several modules, and its implementation depends on the shops and their budget. It also depends on the basic function that displays the latest products on the site that the user visited for the second time, and on the recommendations that depend on the history you create on the platform, while you surf the page. If you search for products of a brand for a certain price, we will begin to follow you with the same product category. If the system and the store have the products, we will show you products of the same brand, with the same features and same price level. All this while you are surfing the page. Then we have the e-mailing part, from which we can draw very simple accurate data, for follow-up and also for custom emails. I mean we can see who has bought a pair of size 44 brown slippers in May or even all the women called Maria who bought a specific product in a specific size and so on.*

or

> *Q: Are certain elements already "built in" to the application?*
>
> *A: Most of them are built in, as I told you, the data are there. The formula is simple, what products is he buying and what pages is he visiting, that's his area of interest. And after that you find an algorithm and create his real area of interest.*
>
> *Q: So the platform can tell you: 1. Track all users who enter the website. 2. Link what I just told you with the tracking system.*
>
> *A: Yes, and other empirical elements. What you have searched on Google, how you entered the website and so on.*

From a practical perspective, there are two ways of implementing profiling in your e-commerce shop:

- develop an in-house expertise in this direction, but this is difficult, since this is rather a new domain, and especially because it requires knowledge not only about profiling, but also about statistics and algorithms.
- buy a specialised service capable of offering not only the tracking technology, but also the interpretation and correlation of the data. Several such services have appeared in the last 2-3 years, some of them localised for the national market.

---

67 Internet analytics software (such as Google Analytics, currently used by over 99% of Romanian e-commerce shops) can be used for this purpose. See here a practical guide on how this can be done. How to Create Custom Audience Segments in Google Analytics, 7.11.2013 http://blog.hubspot.com/marketing/how-to-create-custom-audience-segments-in-google-analytics-quick-tip

68 This would be a third party in relation to the e-commerce shop and the e-commerce platform, but the tracking code is actually placed by the e-commerce store itself, so this would be a first party cookie – from a technical perspective – for further details see section 5 of this report

A: We have developed a software tool that allows us to track each user, individually, and, depending on his pattern on a specific website, to identify the products that he will buy in the near future in terms of price range, category, sub-category and so on.

Although this goes in the direction of profiling, most of the companies offering this service are still mainly working on the technical aspects and less on the data interpretation issues. As explained by one expert who decided not to work with such a company:

A: I wanted to do this for myself and, of course, no formula tool was good enough. They are not necessarily doing statistics, rather averages (..) But, look, I'll give you an example. There are people who buy half of the products for their wife who weighs 80 kg, and half for their mistress who weighs 40 kg. Basically, in Romania, profiling will be something like, so the wife is 80 kg, the mistress 40 kg, therefore an average will show you products for 60 kg. Whereas what you would really need in this case is two different categories of products.

There is also an area of relatively new developments in the field of profiling, where information obtained from behavioural advertising or similar techniques could be used not only in targeted ads (such as Google Adwords[69] or Facebook Ads[70]), but also for more specialised services for e-commerce shops – such as to discover their audience's profile or to target certain sectors of the public on their website[71].

As regards the limits of profiling in the activities of online shops, we did not identify any concerns with regard to privacy or legal requirements that would make the players on the market cautious about using profiling techniques. The overall attitude (with a minor exception – see chapter 5 for details) is that profiling would not give rise to any legal or moral issues:

Q: At present, few people engage in profiling. Is that because it is way too complicated, technically speaking, or the market is too small or you would be too intrusive? Or is it a combination of these?

A: Certainly, I wouldn't say it would be intrusive. I do not believe that anyone involved in marketing in Romania is faced with this problem. Probably, except people who work for corporations who have to abide by certain rules and would have more to lose if someone caught them doing I don't know what, but I don't think anyone would say "I could do something to boost my business by 10% but I'm not doing it because it's too intrusive". I think the lack of profiling is based on the shortage of resources, there are small teams that handle online stores, they don't have a strong business background, they have other basic problems, such as with suppliers or trying to obtain lower prices. Still, the success of online shops is based more on the offer/price range, than on anything they do regarding marketing.

69 Available at https://adwords.google.com

70 Available at http://www.facebook.com/Ads

71 See more details in section 4.2 and 4.3 of the current report

So, as is clear from the above, the limits of profiling are related to size and costs. This is also one of the main reasons why certain information that online stores are already able to obtain (such as data aggregated from online advertising programs such as Google Adwords or Facebook Ads) is not used much in profiling by e-commerce stores.

> *Q: What I have noticed, and this is quite interesting, is that although there are shops that use Facebook Ads or Google Ads, they only use that information to attract people to their website, and not for any other reason. The moment the user enters the website, he becomes a "nobody" for the shop. And this surprises me. Initially I thought that, once you had targeted the customer, you'd have used the information.*
> *A: But different people do that. On Facebook, as a marketing person, you depend solely upon yourself. You need technical support to make changes on the website. And that costs, I mean it is complicated, but not that complicated. The market is small, resources are few.*

There are also limits related to the products sold by e-commerce shops, that would make certain profiling techniques very difficult or almost impossible to identify.

> *A: For example, on the PC market, it is easy to profile. But when you have shops selling flowers, underwear or other things for which there are no clear benchmarks "you looked at the red ones, so we will only recommend red underwear to you".*
>
> *Q: But surely this is because it hasn't been done, not because it is impossible to do?*
>
> *A: We didn't do it because we didn't find any clear connections. There can be different links, such as level, size, but we don't have a clear formula.*
>
> *Q: So, in practice, you don't use this profiling part for your shop?*
>
> *A: Suggesting products, according to your profile, no, not really.*

[4.2] Scope

The scope of profiling in e-commerce should be obvious and simple: to sell. At any time and at the maximum price that the user is willing to pay.

> *Q: So you see the profiling tool from a marketing perspective. I mean your interest is to bring the customer to your website, identify the right people to buy your products and increase your conversion rate*[72].
>
> *A: And the customer should also be happy (…) There are certain shops that now sell products on the Internet, which was impossible before. Say their target group is just 2000 people worldwide, before the Internet it would have been impossible to find them, it would have been much more expensive, incredibly expensive, compared with what they would have got in return. And now it's become cheaper to find them and earn money.*

72 The conversion rate is defined as the percentage of visitors to the website who take a specific action. In the case of e-commerce, the action is usually a sale (although it may also be defined differently – for example subscribing to a newsletter). For further details see Marketing Terms – Conversion http://www.marketingterms.com/dictionary/conversion_rate/

In order to do that you would first need to segment those users and to send out a personalised communication:

> *A: So my profiling tool is designed to tackle the individual level. For 20,000 users, I am thinking of sending 20,000 different e-mails.*
>
> *Q: What do you mean by "users"?*
>
> *A: Users who are subscribers to our newsletter. Others use profiling based on targeting interest groups: This week let's send a newsletter to people who have bought laptops in the last six months. And, somehow, you are profiling them, but at group level.*

But with the data that is currently being collected, this scope means not only being able to tap into the willingness of a user to buy something at a certain price, but also requires you to know what other similar users might be looking for. As the provider of a specialised profiling solution explains:

> *A: It started from our need to be able to communicate with every person individually. As I like to say: just as customers are individuals, so campaigns should be individualised. And two years ago I had an experience that made me think about this. I had ordered an Xbox from one of the biggest retailers in Romania. Two weeks later, I received a newsletter with an Xbox in the title and I immediately opened it cause I needed a controller, some games, etc. The content was "Discount for Xbox" and I said "But I already have one, I don't need another, thank you. Give me anything else". It is difficult for an online retailer with tens of thousands of products to make the appropriate associations between them. You would need to have an entire data entry department working on it to make some related recommendations. We are dependent on collective intelligence. So if you have 10 people who bought X, then Y, for the next person who buys X, it is logical to recommend Y to him.*

But this scope is sometimes linked to a different one – for example one of our interviewees specialising in targeting newsletters initially saw this as a technical issue – how can you make the content of a newsletter relevant to the user, so that the email provider will send it to the Inbox (and not to the Spam folder):

> *A: This area of targeting was somehow used as a tool to optimise your Inbox placement. It's a huge factor. The call to place something in the Inbox or not depends on a certain user.*

Another example is the need for websites to identify what actually is their target group, so they can change their attitude or even products, accordingly:

> *A: He conducted general campaigns on Facebook by age group, targeting women between 18-20, 20-24, etc. He gave different URLs, analysed these and saw different types of behaviour in each category in Google Analytics. And they learned that their target group was women aged 35. Up until then, they thought it was women aged 25-30. The others visited the site, but bought less. And the tool is there, but he had the patience. It took longer, but he understood the business. Speaking of focus: Focus is two inches wide, two miles deep. The same applies for targeting women between 35 and 37 years, who buy the most, you start to understand them, you know when they wake up in the morning, what coffee they drink, and then you can offer them different products. I think it will end up as a consumer-generated product. This means that the producer establishes what the customer wants and produces in order to satisfy his need.*

A common concern related to processing of personal data is the possibility that this could be used in the future for another purpose, not related to the initial one. This risk emerged clearly in three particular cases, as did the data processor's current lack of understanding about privacy issues:

A. One of the companies we have spoken with – in the field of online marketing – has already created a significant database with profiles (estimated to contain around 8 million profiles) from different websites. (e.g. online publishing networks, individual publishing sites, bank sites, company sites, e-shops, blogs). But if the purpose of collecting the profiles is unclear or at least very vague, the future usage of the data (or, to be precise, of the aggregated data, as the data operator made it clear that no one else would get the whole data from them) is open to any kind of new ideas of business:

> *A: And stores can use this thing in many ways. For example they can see what kind of people visited their site and do data mining on statistical data, for example, "What kind of people who navigated on my site are interested in cars and are parents?" And you make a socio-demographic split. There are so many uses, we managed to surprise everyone, "Well, what do we do with such a large amount of information?" The idea is that if one day you might need something, you'll find it.*

B. In one interview we also investigated whether information obtained via cookies with data gathered for a clear and specific purpose might be used for a totally different purpose in the future.

> *Q: You said that you have practical information like "when exactly Romanians buy online and stuff like that." So basically you are sitting on a pile of data that could lead to some very interesting profiling. Have you ever thought about monetising it?*
>
> *A: I have thought about it a few times. The easiest way of monetising is to launch a retargeting study in our country. We had some interesting discussions with some Ad servers who said "would you give me your cookies? So that I sell more, for example, on a CPC or CPM basis and tell my clients "I will only target online shoppers on all Romanian sites. And those guys will sell at higher prices and they will give me something for that." I thought about giving them reports that I could sell. I mean, detailed reports and to ask 100 per piece, and that's it. I don't have the resources for it or I'm not good enough. It comes in handy but I'm not doing it, and this hurts me directly because it involves a large proportion of my resources. We're still involved in other aspects of the business where we solve basic issues, but for a business like ours, this type of development is natural."*

C. But probably the most intriguing and complicated purpose emerged from a part of an interview that we had not planned. In this case certain profiling activities – using Google Adwords searches, so before the user enters a website - were initially performed for a clear purpose: to target a specific category of clients who could obtain a discount. But due to the type of products sold by the e-shop (sexy underwear and other related products) a differentiation could be made between professionals and amateurs:

> *A: Girls who buy for home use are generally interested in stuff that can be delivered tomorrow, that is guaranteed, and that doesn't ruin the surprise. Girls who buy for business are like people who buy for business, good quality and low price. And the prices must be high so I can lower them afterwards. And obviously, the price will change.*

Q: And how do you change it?

A: By giving discounts. Happy hour deals, like you have 3 days of discounts.

Q: But the happy hour deal applies for everyone.

A: No, only for her.

Q. M: And how do you identify her through the newsletter?

A: For professionals, I launched a separate campaign on AdWords with certain keywords which are generally interesting for these types of girls. And I have a parameter in the link, depending on which it triggers the happy hour deal. The problem is that I now find out who are prostitutes, which is not OK. I mean, I can find out.

Q: You find out or you can find out?

A: If I look in the list, yes, I can find out.

Q: So basically you can make a list of customers who can be called "Prostitutes"?

A: Well, with a margin of error, I do not know, about 40%. But it's pretty big.

Q: OK. And if the police were to come to you and say, "You are the right person, you have the best site in this area and we want to have the official list of prostitutes from you"?

A: Well, if they come with a warrant, what can I do?

It should be explained more clearly that the list does not actually exist as such and the interviewee pointed out that this is a moral problem for him, so he is trying to avoid any unnecessary profiling. Not because of the existence of any laws that would not allow him to do this, but because it is not actually compatible with his business ethics. Besides, even if the list did exist, the law enforcement bodies would not have the actual know-how on data interpretation (how or what to search in the list) to get the information they wanted. Due to the very specific nature of the data gathered, one would need to know the specific domain very well before being able to perform any reliable interpretation of the data.

[4.3] What is "being used" in profiling

In order to have a consistent approach, we first need to distinguish between the different types of profiling (explained above – point 3).

In the case of data provided directly by the client, any data could be stored and used for profiling (e.g. email and telephone, demographics - city, sex, birth date, name and surname – although only the surname is traditionally used for addressing in newsletters). It is however important to point out that due to market changes, it is becoming more and more fashionable to ask for fewer data when registering an account with an e-shop, or even to allow customers to place an order without opening a new account – not as part of any data minimisation requirements under data protection law, but for purely commercial reasons.

Asking customers to provide fewer data when placing an order proves to be better for conversion[73] (i.e. more sales).

> *A: I believe that 95% of customers have opted for simplified shopping carts. This is a trend we have seen in recent years for shopping carts in a single step, to increase conversion and therefore many people have renounced adding many fields. In principle, we can collect the dates of birth, or the names of the children, if this is a site for children, but in practice no one in Romania is currently interested in this type of segmentation.*

However, other data that the user gives the e-commerce shop could also be used for further profiling – if it proves beneficial to the store.

> *Q: (...) Do you take into account the period when he placed his order and whether the child will have grown up?*
>
> *A: Yes, I must.*
>
> *Q: Has anyone ever asked, how did you know how old my child is?*
>
> *A: No. We have a very well developed customer service system, where I also keep a database on every client, I know the children's age if I can get his date of birth, not automatically, but manually; then we check who confirmed the client's order. We also have records of all previous e-mail conversations. So far, we have never upset anyone.*

As regards data submitted automatically by the user – as already explained above, from a technical perspective – anything can be tracked. This includes data directly linked to the shopping activity (e.g. order history) on the website but also tracking users' activity on the website or activities related to the website (newsletter, referral, search string used to enter the website etc.).

Even though some interviewees asked us not to share some of the data, based on the overall interviews we were able to get a picture of what is tracked in e-commerce and what makes sense from a commercial perspective. We split the data in the two categories mentioned above, but the lists are randomly ordered:

Data obtained directly from shopping activity:

- history of shopping
- addition of a product to the shopping cart
- use of a voucher or not
- finalising an order
- searches on the website
- customer value
- customer acquisition cost.

---

73 Simply explained: "As one shopper told us, "I'm not here to enter into a relationship. I just want to buy something.": see http://www.uie.com/articles/three_hund_million_button/

Data from user browsing:

- categories of products visited
- visiting a product X times
- time spent on products – with spending more than 1 minute on a product seen as a notable interest
- opening the pictures of a product at least Y times
- seeing the entire set of pictures of a product
- price ranges
- how active a user is on the website
- clicking discount links on the website
- opening the newsletter (if the email client allows this)
- clicking on a link in the newsletter (if the email client allows this)
- time stamp when the user visited the link in the newsletter together with the IP address
- for products with different sizes (e.g. for shirts), the size the customer looked for
- comment on a product
- location (based on IP)
- type of products seen (e.g., men's vs. women's shoes)
- mobile or desktop usage
- Facebook Like on a product (its relevance depends on the market though) A: If it is a very expensive fashion product, the like on this product is a kind of "I appreciate this product, I know I will never have the money to buy it". If you give her a wedding dress worth 150 million, she puts a like because she likes it, not because she will buy it.

The lists shown above are obviously not exhaustive. The objective of tracking is better explained by one of the interviewees:

> *A: Look, the point is that I'm trying to collect data, everything being empirical from scratch. I can't tell the man, I'll give you 20 words and you choose 3. You can't ask for that. I can try to profile each product and give it 5-10 criteria (...) and depending on what the customer visits, extract product criteria and somehow profile him depending on what he looks at.*
>
> *Q: Depending on the visitor's pattern.*
>
> *A: Yes, so to speak. I extract the information from the products you visited; I do not extract it directly from you. From this information I outline other important information. That's what I do. Others do approximately the same thing.*

Based on information from e-commerce platforms, only a small minority of their clients (less than 5%) actually use the tracking visitors features embedded in the e-commerce platform. Most e-commerce platforms just track the clients' data, but if they collect both data from clients and from simple visitors to their website, they can easily link the two sets of data.

> *Q: Are they even related to shopping?*
>
> *A: Yes and no. If you have an account, I know who you are and then everything is linked. If not, it links to the user's ID. If you have deleted your cookies, we'll take it from 0.*

The same situation would probably apply if some other Privacy Enhancing Technologies that did not accept cookies were used, but the percentage of users who regularly employ such techniques represents an insignificant percentage of profilers.

Although profiling is not based on the presumption of identifying the user, but rather of segmenting the target audience, in one interview we investigated whether, in some situations, identifying a simple visitor to a website would make sense from a commercial perspective:

> *A: In recent years, the market has become more professional in many ways, but at the moment the possibilities are frightening. If you hook up data from Google Analytics and Facebook, I can follow you and know when you are on my site, I know all your history and everything. I know that is not OK, but I know this.*
>
> *Q: So you are saying that you can do it for me, B. M., but how do you identify that I am Q?*
>
> *A: If you have set up an account using the e-mail address or you connected via Facebook. Nevertheless, you must be extremely important for me or I would have to have a very small number of customers.*
>
> *Q: But if you have a yachting site, a niche product, where the product is super expensive...*
>
> *A: Then it makes sense.*

The situation is slightly different if we consider data obtained from behavioural advertising or similar tracking tools. In this situation, a lot of data are gathered, but these are not 100% accurate, and used to create a standard profile – over 100 issues related to the "level of interest" on specific subjects – from interest in furniture, holidays, politics, business and even horoscopes. Other issues are related to social-demographic factors, such as age, sex, location, income, education, decision making profile, relationship status, parent or not, car owner, house owner, etc.

In order to be useful from a commercial perspective, these profiles need to be high in number and refreshed on a permanent basis in order to be relevant for the potential customers of these data. One of our interviewees estimated it had 14 million profiles, with 7-8 million individual profiles that are currently updated[74].

On the other hand, due to the high number of profiles and the type of business in this sector, there is absolutely no interest in identifying a user or importing data from other sources:

> *A: We do not accept data import, I don't want to know the names of particular persons, hence we know nothing about these profiles, nor do we want to know.*

It is still complicated to assess how these data are used for e-commerce. On the one hand we know they are currently mainly used for targeting online advertising, but on the other hand they can also be used for linking this type of profile with the profiling done by e-commerce shops on their own platforms. Technically, the two profiles (the one from the e-commerce website and the one from behavioural advertising) can be linked, but this

---

74 This is a huge number compared with the number of Romanians who use Internet. A recent Gemius Report for South East Europe estimated that in December 2013 there were 8.8 million users. See full report at http://files.gemius.pl/Reports/2014/gemiusKnowledge_South-EastEurope

option is not available to be purchased by online stores, at least not with the programs we assessed. However, there is no guarantee that this may not happen in the future, especially in cases where targeting is of crucial importance for the e-commerce store.

> *A: But I do not know that the tracked ID is a particular person. You find that out when the person fills in the form and subscribes to your website. Then you discover that the name of the person is John Doe and is linked to that ID.*

Finally, we need to explain that the profiles that are created are only important for a limited period of time (the exact period depends on the market and the products sold), and that after a few months most of the data are not really useful any more for correct profiling – this aspect is discussed in further detail in chapter 5.4.

However, in most cases, data processors still keep the data because it is technically possible and the law is not seen as a potential barrier in this case.

[4.4] Decisions made based on profiling

In the current legal regime, profiling is indirectly regulated by Art 15[75] of the EU Data Protection Directive. That specific article has been transposed into Romanian law almost literally by Article 17 of Law 677/2001[76]: The right not to be subject to an individual decision (discussed in more detail in chapter 5).

In practice, decisions based on profiling relate to the basic aim of any e-commerce store – to get customers to return to the e-store and make them an offer they cannot refuse. Although this is usually based on an automated decision making process, the algorithms or conditions used in order to make the decisions are set manually and usually reviewed quite often, to check whether or not the campaign is working.

> *Q: To what extent are automated decisions based on profiling?*
>
> *A: Fully automatic, never. Decisions are based on the conditions imposed by the shops.*
>
> *Q: Which is practically automatic.*
>
> *A: You can fill them in once and then they are taken into consideration.*
>
> *Q: All the actions that we initially established are based on what the shops check.*
>
> *A: There are certain decisions, for example, whether in that particular segment to offer*

---

75 The text of Article 15 (1) of the EC Data Protection Directive states that every person has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, credit-worthiness, reliability, conduct, etc." For further details see p 15 of the Profiling project – working paper - Defining Profiling V. Ferraris (AMAPOLA); F. Bosco, G. Cafiero, E. D'Angelo, Y. Suloyeva (UNICRI) Internal reviewer: B.J. Koops (Tilburg University) available at http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf

76 Law 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed
. Published in the Official Journal of Romania, Part I, No. 790/12 December 2001
. An unofficial English translation of the law can be found here http://dataprotection.ro/servlet/ViewDocument?id=174

a voucher or display a banner. Those decisions are made automatically according to what's happening on the website and apply indefinitely, until they decide to stop them.

On the basis of the classification according to Article 15(1) of the EU Data Protection Directive (implemented by Article 17 of Romanian Law 677/2001 on data protection) we decided to split the actions that are usually undertaken by an e-commerce store based on profiling data into two main categories, depending on whether the action could be expected to produce a significant or legal effect:

[A] Producing a significant or legal effect

A.1 Price differentiation (e.g. offering a discount)

A.2 Offering other benefits

A.3 Blacklisting a user

[B] Not producing a significant or legal effect

B.1 Targeted communication

B.2 Retargeting (trying the get the user back to the website)

A.1 PRICE DIFFERENTIATION

One of the most important decisions an e-commerce store has to make is whether to offer different prices to different users. The reason for this differentiation is that e-shop owners are convinced that certain users are only willing to buy if they are offered a discount or that, to stay in business, it is important that customers keep returning to the site, so this must be encouraged by offering them discounts.

A: As a consumerist generation, I've also noticed something else. We have a moral depreciation of things. And by that I mean that depreciation is very high. If you bought a car now, in six months time you would be fed up with it, you would want something else. And the best example is me. Meaning that the software meets my needs, as a shop owner, but also as a client. And, because of this moral depreciation, business automatically increases. And I link this to different prices. And it's normal for a retailer to have different prices. If you are a regular customer, you should be able to buy things cheaper.

In all of the interviews we conducted, we only found out about situations where a discounted price was offered, based on specific criteria. However, it is technically possible that price differentiation strategies could involve price increases.

A: You can customise the Shopping Cart. I know which products you are interested in, you receive a 5-10% discount in order to convince you to buy them.

Q: Is it basically an automatic voucher? Or a different price tag?

A: A voucher that is produced automatically. I tell him that the product costs 150, but it is shown at 135 lei and I tell him "Buy it". The client, who does not have those products at 135 lei in his database, receives a voucher code. We do not make the code visible because, if it was, all users would use it and start buying with discounts.

Q: So the voucher is specifically for the client, for a specific shopping session.

A: Yes, yes.

Q: So the price can be customised with a voucher. And is all of this automatic?

A: The client sets when and what to send, but the sending process is automatic. The software also decides if you are the type of person who purchases with discount vouchers and then gives you the voucher, and if not, it does not show you the discount.

Q: How do you do that?

A: Depending on your previous purchases.

Q: But I think that everyone would buy with discount vouchers if they could.

A: Yes, but if you have placed 5 orders without discount vouchers, you will also place the sixth one without it..

Q: And if am the type of client who only buys with discounts, then the discount will be displayed.

A: Yes

It is also important to note that all the people we interviewed said that they did not show the discounted price directly, but showed the price reduction instead – though not for legal reasons and mainly for marketing purposes.

Q: So in practice the clients see the changed price?

A: Yes, they see the price, like, if the price is 100 lei, that is struck out and 85 especially for you as a happy hour deal is written instead.

Q: So basically it says that it's specifically for you?

A: Yes

Q: And what about in the "Shopping Cart"?

A: In the shopping cart the client will probably see 100 minus 15.

Q: And why do you do this, instead of showing the price of 85?

A: So that he *knows it is not a fake.*

Q: And how can he know that?

A: I don't know, he might use Chrome Incognito and see that the price is 100 lei. Plus it is actually more marketing orientated.

A.2 OFFERING OTHER BENEFITS

Most e-commerce platforms or shops may create a special category or categories for the most important customers – based either on the total amount of the money spent in the store or number of orders, but also on other elements of profiling.

Q: So, basically, you only know who the Top customers are and the store has to implement the algorithm. Like "If he exceeds a specific amount, he will receive something"?

A: Yes, you can set that. Within the platform we have a lot of marketing features, discount rules, etc. There I believe we are the best on the market. The things you can do there, without having any advanced technical knowledge, I have not seen anywhere else.

Q: And basically the marketing features are based on specific information that the store must provide from its back office, is that right?

A: Or on what it collects. What we want is to make the client understand that he pays us an amount of money, but that helps him to get the most from his customers. Reducing marketing costs.

Other benefits offered to this category of VIP customers can be set up manually or automatically by the e-commerce shop, so there is no standardised list of incentives – which may either be incentives that are visible to the user (e.g. the offer of free shipping with a product for which a shipping fee is usually charged) or invisible (e.g. on BlackFriday when website traffic peaks, the e-shop may prioritise orders of visitors marked as important).

A.3 BLACKLISTING A USER

The segmentation of users based on their profile or shopping history can also be used in a negative way. The concrete example described by interviewees, and which we actually knew about even before we started this report, regards the blacklisting of so-called "problem-customers" - mainly customers who have ordered a product with payment on delivery[77], but then failed to pick up the product.

Q: Can you use the profiling tool to remove certain users from your list of customers? For example, people who ordered something and did not pay for delivery?

A: Yes.

Q: So it is like a black list. And do you use it internally?

A: Yes. Meaning you don't deliver to him or ask for payment in advance.

Q: And do you share it with other shops or is your personal list?

A: We tried that about 10 years ago, but it failed.

Based also on information acquired from the market before the study, we also probed to what extent customer blacklisting data could be shared among clients – at least in the case of similar e-commerce companies using the same e-commerce platform.

Q: Do you have the possibility of blocking specific customers who you don't like on the website?

A: With the new version of the website, yes. We also had a black list on the previous one, of customers who turned down orders.

Q: Paid by cash or ...?

77 On the Romanian e-commerce market payment on delivery is used in more than 80% of cases according to figures presented at the GPeC 2013

A All the people who turned down orders.

Q: And what do you do with the blacklist?

A: We identify them when they order new products and ask for payment in advance.

Q: Is there a specific list for each store or not?

A Yes, we don't pass data from one client to another.

Q: Why don't you pass data on?

A: We think this wouldn't be ethically correct. Every store has its own customers. A customer might not feel confident enough to buy from one store, but might then buy from another one. It doesn't mean he will have the same experience. Or maybe the shop was charging too much or wasn't polite over the phone, so he gave up his order. The biggest problems are not usually with stores. Our clients' customers can sometimes be very difficult. Sometimes orders are confirmed by phone and then not collected.

From a recent press release by the Romanian Data Protection Authority (DPA)[78], it emerged that such a blacklist was actually shared by a few e-commerce websites[79]: The DPA had ruled that this was in breach of Romanian data protection legislation and the owner had received a fine of 15 000 RON (approx. 3300 Euro).

From a technical point of view, profiling data may also be used for negative discrimination of buyers or even exclude them from certain activities (buying, commenting, sharing on social networks or even accessing any part of the website). Discrimination could be based on objective criteria (e.g. the IP number that has abused the comments section with spam) or subjective (e.g. refusal to deliver products in a certain area renowned for the high level of criminality).

B.1 TARGETED COMMUNICATIONS

One of the most used decisions based on profiling regards the creation of different types of communication for different audiences. Targeted communication can be used with any kind of communication medium used by the e-commerce shop, and can either be sent to the user (such as text messages or newsletters) or presented to the user (the e-commerce website) or a mixture of the two methods (live messages sent to the user on the website). The purpose of targeting communication is to show users what they are interested in and not "noise", which they would very likely just discard. As far as newsletters or even text messages are concerned, targeted communication means different texts or images (in terms of their content or subject-matter) are sent to the user depending on the profile allocated to them.

Q: How do you use these data received from tracking tools?

78 Press release of 7 July 2014 - http://www.dataprotection.ro/?page=Comunicat_de_presa_09_07_2014&lang=ro

79 The website was called – clientineseriosi.ro (a rough translation would be "not reliable customers") and it claimed that the e-commerce website had the right to draw up and share the blacklist (where the names of the people would be made public), provided it simply included something to that respect in its privacy policy.

A: For the moment, we store them and give them to the client in order to use segmentation tools. The client can say "Give me information about all my subscribers who clicked on a product yesterday and are from Bucharest". We extract an automatic list and he can send a follow-up message.

Q: Do you have lists with e-mails or an ID you create?

A: The segment that is created is based on emails. In practice, it is a list of e-mails. They remain within the application. He has all the data, he has an ID, so he can also use the name, surname, e-mail. You can see that on the segmented list. This is what you can see on that particular list. The client can choose to upload all types of information. He can also use them for tracking.

As regards targeted communication through e-commerce websites, although ideally everything can be changed, making such changes and showing different websites (or parts of websites) to different clients may use up a lot of the organisation's resources, and so only makes sense when it really does carry benefits. Through our interviews we were able to identify the following key issues that could be changed on a website for different users, depending on their profile (the order is random):

- Personalised text used on the website (e.g. Hello John or Other X people from Bucharest bought this)
- What the first page looks like and what products and discounts are shown
- Product recommendations
- The order of the products
- Different landing pages (especially for ads or newsletter campaigns) – including different (discounted) prices (see also A1 above)
- Articles with information about products, based on the type of products you have seen
- Facebook Trust (explained below):

A If you know that a user came from Facebook, you can show him the Facebook page higher up and there is a good chance of him becoming your fan.

Q: So if he "liked" the store, what do you show?

A: Not if he liked the store. If he came from Facebook, you know there is a good chance that he will become our fan. So if you show him "You know, we have 100,000 fans like you", it is a social proof thing. Basically, we show the page higher up, because our goal is to sell products, not to receive likes. But you are showing him something familiar "Look, there are 100,000 more people like you"

B.2 RETARGETING

Retargeting can be explained as a marketing technique that aims to target users who have previously visited a website, usually with banners or text ads across other Internet websites they are visiting[80]. Sometimes people also refer to another term related to the same

80 See more details in Moz Blog - Retargeting: What It Is & How to Use It – 5.04.2011 - http://moz.com/blog/retargeting-basics-what-it-is-how-to-use-it

technology – remarketing, which was actually coined by Google for their retargeting services in their display network[81]. However, both terms are used in practice, and this is sometimes a source of confusion, as remarketing can be used beyond the sphere of Google products.

When an e-commerce shop engages in retargeting, it might also identify some specific features of the users it is targeting (e.g. just users who have visited a special category or users who have stayed on a website more than x minutes or even users who have initiated an order but not finalised it).

Or more basically explained in one of our interviews:

> *A: For example, the user enters the website and a cookie is added. More than that, through the remarketing features, I can know what pages and categories you visited. I open my marketing tool and "tell" it: "I want to retarget all the users who entered the DSLR category and did not buy". You add a tag to the IP that was on the website, where the user navigated, after which I can tell my marketing tool "advertise on all pages where Google is showing advertising through its AdSense publishers programme and target users who entered my website and did not buy". And I create a banner saying I have a special offer for you, a Nikon Z, I know you have seen it, but you did not buy it and I am tracking you. The idea is that the advert will follow you on all the websites you enter, depending on the budget.*
>
> *Q: But is it pay per click? Or pay per impression?*
>
> *A: Both. But the idea is that the banner gives you the impression that that ad by that specific company is everywhere on the Internet. But it is not like that, only you see that specific ad. Other people won't see it. The feeling is that you are being tracked by the ad.*
>
> *Q: But what happens after I click on the ad and re-enter the website.*
>
> *A: You re-enter the website and do whatever you want to, it doesn't' matter.*
>
> *Q: So the website knows than that I was the one that…*
>
> *A: No, it doesn't, not at individual level, but at group level.*

It is possible to identify three different types of retargeting with different privacy implications, depending on the kind of ad being served on other websites:

- Generic ads that just show you the ad for the website you have already visited, but give you no indication as to whether you have visited that website or not.
- Specialised ads that show you an ad saying that you have visited the website and inviting you back to it.
- Shopping cart recovery - Specialised ads that show you that you have added some products to the shopping cart at the shop, and invite you back to the website to finalise your purchase (possibly with a discount).

The last category poses some significant privacy concerns, especially if more than one person is looking at the websites that you are visiting:

---

81 See more details at http://www.google.com/ads/innovations/remarketing.html

"For example, you enter my website, you put some underwear in your shopping cart and then you go on another website and I show you a banner "you have products in your basket. 5% discount to finish your transaction". I find it quite intrusive: You might be sitting at your desk and there you see "you have these products in your basket". That is not OK. (…)

When doing remarketing I always pay attention to the expressions I use, to make sure they are general ones. I don't say "X, you've visited My Website. Come again". I try to say something different. I don't do this stuff even though if you are with someone on Facebook and it pops up like a normal ad, I could have written "I know you clicked three times, I know...."

But this approach was rather unique in the context of discussions with people from the e-commerce industry, as most of them simply looked at the conversion rate without considering whether or not customers would find their retargeting techniques intrusive. And conversion rates are clearly much higher than with any kind of traditional advertising, so this is very convenient in terms of price/result from the e-commerce shop's point of view.

[4.5] Data sharing

One of the issues that we identified as potentially posing privacy concerns was the possibility of sharing profiling data. Profiling data may be shared in two different ways: with a third party e-commerce business (either the e-commerce platform or the profiling services or other shops) or with one of the Internet Advertising platforms (usually Google or Facebook). However, regardless of the practice used, the interviewees showed little or no interest from a privacy perspective.

A. SHARING OF DATA BETWEEN E-COMMERCE PLAYERS

As regards the sharing of profiling data with other e-commerce players, there is a tendency not to accept data sharing between e-commerce stores, for two main reasons: companies regard data about customers and visitors (including their profiling) as confidential, but also because such profiling data are only relevant within the context of that respective shop and might have no significance in the other company's e-shop or have little significance in terms of competition.

Q: Can you mix data received from various customers?

A: No, our clients don't want to. We tried this, we had the idea a couple years ago, and they did not want it.

Q: Why?

A: Because those are their users, their data. If I am a big store I don't want to give that information to a smaller one, if I am a small shop I want to, but...

Or

A: From my point of view, the client's database is the most important part of a store. The more complex the database, the more it is worth. Moreover, you can't use it. Let's say you have the database of a big fashion store. What are you supposed to do with it, go and open a similar fashion store? You can't use it, if you send e-mails they will have no idea who you are. You might raise, let's say, 200-300 customers, but that's it.

B. DATA SHARING WITH GOOGLE

The situation is much different when we talk about data sharing with the one of the biggest Internet companies – Google. Most e-commerce companies in Romania use Google Analytics for traffic analysis and Google Adwords (including the remarketing option) for buying ads that attract users to their e-commerce shop.

In this case, companies actually send a lot of data to Google (and indeed their entire traffic details if they use Google Analytics), but get limited information back (which is a source of frustration for some, especially since up until quite recently Google used to give more personal data[82] about website traffic). The reason why they still use Google's services is related to the quality of the product, which is free, and the fact that there are not many alternatives that actually work for them, so they look very much like captive customers (although some of them mentioned that they are actively looking for alternatives).

On the other hand, the online stores have no information about how Google uses the information gathered from their websites, beyond what is made available to the shop. It is even more unclear for the final user how Google uses the data gathered from the websites that use Google Analytics[83] . What we can infer is that if a remarketing tag is included in a website, Google uses this information for retargeting[84], so that users will be tracked (and possibly profiled) extensively on other websites that display Google Ads.

It is however clear that, at present, Google services send a very limited amount of personal or even non-personal information about online users that could be helpful for profiling – and focus much more on aggregated data. Even if you use two Google services, the company actually locks the information within the products, and only gives the aggregated data to the e-store.

Q: And what about from the Google Analytics area?

A: We introduce new data, we don't extract them. There you see reports, not data that you can use afterwards. For example, you cannot ask "tell me something about the users who did this".

Q: But I know that it has some sort of demographic data.

---

82 See for example Google Puts A Price On Privacy, 22.10.2011 available at http://searchengineland.com/google-puts-a-price-on-privacy-98029

83 Part of the subject of the Article 29 WP investigation

84 With special cookies that have a standard period of 30 days, but which could be extended – as explained in the technical implementation of retargeting - https://support.google.com/adwords/answer/2454064

A: Ah, but you cannot extract and use them. I mean, you can extract them as a report, but you cannot use them, like "we identified this user as being 30-40 years old (…)"

It is interesting in this respect that the new Google Analytics traffic analysis software – called Universal Analytics - supports data collection without browser cookies[85], which raises more privacy questions on how users can control information about them. According to Google, this can only be done by installing a browser add-on produced by Google[86], which in practice only amounts to an opt-out procedure.

C. SHARING DATA WITH FACEBOOK

As regards sharing data with Facebook, the service used most by the Romanian e-commerce sector[87] is Facebook Login[88] (featured as a service that lets users use the Facebook account to sign into other websites, so there is no need to create a new account with different websites), but Facebook Ads are also gaining traction – especially in recent months following improvements to their retargeting services.

Surprisingly enough for someone not too familiar with the e-commerce industry, most of the e-commerce players who use Facebook Login are actually not interested in having many details about their users, apart from those needed to finalise the order:

Q: When Facebook Login is activated, what type of information is sent to the shop or platform?

A: Only to the shop. The shop works on our platform and the back office part comprises a panel where you can see information about customers who have logged in with Facebook. We use the standard functionalities of Facebook Login.

Q: I know that as part of the standard information you can extract data checked as "Public View" on my profile, can't you?

A: No, we are not interested in this type of information. We are not concerned with data collection or processing. And we have never received this type of request from shops. They are only interested in obtaining contact data which they use to process the order and so on.

But by skilfully integrating the different services and playing with their limits, some data can be imported/exported from one service to another (from the website's internal data to Google, Facebook or newsletters) in order to profile a certain user target group. One concrete example is explained below:

Q: Do you want to integrate the data you obtain from your e-mail subscribers with other services such as Google Analytics or other related services?

---

85 See Security and Privacy with Google Analytics - https://support.google.com/analytics/answer/2838718

86 See Google Analytics opt-out browser add-on ttps://support.google.com/analytics/answer/181881

87 Facebook reported 7.2 million accounts from Romania in July 2014 – see the data at http://www.manafu.ro/2014/08/social-media-in-romania-august-2014/ (only in Romanian)

88 See details at Facebook Login https://www.facebook.com/help/405977429438260

A: Yes, we actually tried targeting customers using Facebook by exporting the database of newsletter subscribers, uploaded with Facebook, and after that you can manage the customers who have subscribed to your newsletter only. Meaning you can use Facebook campaigns for those who have not subscribed. But I have to say it didn't really work. In terms of conversion rates, you wouldn't say "wow", but it is clearly something more than just direct or standard Facebook targeting, in terms of gender or age targeting.

[4.6] Profiling Efficiency

From an e-commerce shop's perspective the efficiency of profiling can be measured simply on the basis of the increase in the number and value of sales after using profiling in its activities. But there are also other indicators of improved performance due to profiling, which need not necessarily be a final sale (called micro-conversions. e.g. subscribing to a newsletter, engagement with the website, etc.).

An example of the efficiency of profiling is given below. However, since the people we interviewed worked in this sector and may have been interested in selling their services, their answers must be taken with a pinch of salt. Nonetheless, the mere fact that profiling is beneficial for e-shops is confirmed by the fact that they continue to use and develop it.

Q: And what is the added value for the store? About how much does the conversion rate increase?

A: It brings an increase of about 25-50% in total sales. The personalised newsletter increases the conversion rate by personalized newsletter, between 3-7%, live messages by 5-12% and triggers by anything between 8-40%. One day we had a conversion rate of 175%. Meaning 4 individual customers placed 7 orders. We brought them to the website for some cheap products, they bought them, then saw that there were others that were just as cheap and placed another order. Google Analytics analyses where the order comes from and tells the shop if it's from my software or from my e-mail.

A concrete example illustrated during a recent e-commerce workshop[89] concerning a newsletter campaign on a travel website provides more reliable details about the conversion rate of a profiling-based personalised newsletter compared with a traditional one:

	Profiling-based personalised newsletter	Conventional standardised newsletter sent to active users (who have visited the website in the past 30 days)	Conventional standardised newsletter sent to inactive users
Open rate	45%	17%	6%
Income/email sent	5.56 Euro	0.72 Euro	0.02 Euro

89 Presentation by an email marketing provider at the GPeC Summer School 2014

[4.7] Future plans for profiling

Although the use of profiling in e-commerce is still somewhat limited in Romania, we wanted to explore the general trend in this practice, based on the experience of our interviewees, some of whom also operate in more advanced e-commerce markets. As some of the companies we interviewed also provide services in the field of profiling, their plans for development are also relevant for the direction of the entire market in Romania. Even those that do not actively work in the field of profiling may be able to forecast the general trend.

The overall conclusion is that this is only the very beginning of the use of profiling in e-commerce, at least in Romania. In the future, e-shops will work to optimise the way they approach visitors to their websites as prospective customers – and that will include offering them what (they think) they want, in order to increase sales.

> *Q: What future plans do you have in order to develop your profiling activities? Or what will the trend be?*
>
> *A: To profile the design, the content of the message, e-mail, website and user patterns. To make recommendations not only based on their history on the website, but also on their online experience. And I mean tracking not only on the website, but their whole online activity.*
>
> *Q: And how will you do this?*
>
> *A: Now, I don't know if you can. With cookies, but I don't know if you can. If you ask me where I think we'll be 5 years from now, I say here, with everything personalised. And I think that's normal. I am a guy, so why should you recommend me products for women on the shop's web page? Only if you knew it was my wife's birthday and you could recommend something. But If I am a guy, show me products for guys.*

Changing the website, so that each user can see it differently, based on their profile could also be extended to the ads you see on publishing websites, as one of our interviewees explained:

> *A: A well designed profiling software will do the next thing. Let's target people who need wooden tables because I have a wooden table to sell.*
>
> *Q: But how do you know who needs wooden tables?*
>
> *A: The profiling software will know. What profiling means is that, if you need a wooden table and I have one, I will come and sell it to you. If someone has a mobile phone for sale, he won't be able to sell it to you if you need a wooden table instead. You start reading an article and you have just one ad banner with a wooden table. And a well written article, with spaces, arranged nicely on the page and well linked to that banner. No other ads.*

Another future trend will be the tendency to pass from reactive attitude to pro-active activities, which means in practice more profiling and more targeting:

> *A: At present, we are re-active, meaning that for certain actions on the website, we define what the software should do: give you a discount, display something, etc. The trend is to be pro active, meaning to anticipate certain things the user will do.*

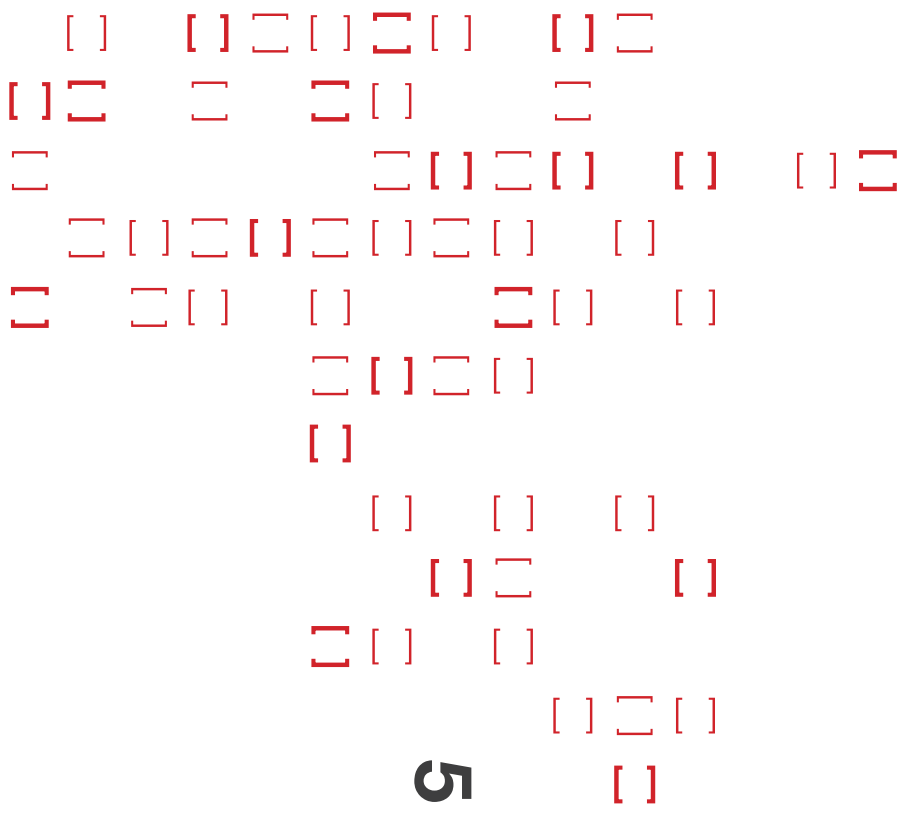
If he repeatedly buys 10 bottles of beer at 9 pm it means he is probably a student partying or something similar. In 5 years he will have a job and the store knows that, he will have a higher income, and during those 5 years will develop a relationship with me so he could come back to the store when his income has increased. Things are moving in that direction.

Q: Isn't the example with the beers a bit of an exaggeration?

A: Yes, maybe the best example is with pregnant women. There I see a clear example, you can offer products for children, their behaviour changes.

One of the worst examples from the US of how privacy-invasive profiling can be was actually quoted in one of our interviews as a very clear possibility in the future in e-commerce – the example of the campaign by a US company called Target that sent coupons for baby items to customers according to their pregnancy scores[90].

90 Forbes.com: See the entire story at How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did (16.02.2012) http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ and NY Times: How companies learn your secrets (19.02.2014) http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html



Privacy and Profiling

As discussed earlier, profiling activities fall under the text of Art 15[91] of the EU Data Protection Directive. That specific article was transposed into Romanian law almost literally by Article 17 of Law 677/2001:

> *Article 17: The Right not to be subject to an individual decision*
>
> *(1) Any person has the right to demand and receive the following:*
>
> *a) the withdrawal or the cancellation of a decision that produces juridical effects concerning him/her, adopted exclusively on a personal data processing basis, carried out through automatic means, destined to evaluate some aspects of his/her personality, such as professional competence, credibility, behaviour or any other similar aspects;*
>
> *b) re-evaluation of any decisions regarding him/her, that affect him/her in a significant manner, if the decision was adopted exclusively on a basis of data processing that meets the requirements stated under letter a).*

Romania has not yet implemented the Recommendation of the Council of Europe (2010)13 on Profiling[92].

Some significant and relevant changes are being discussed in relation to the new General Data Protection Regulation (GDPR), but this has already been extensively covered in one of the projects' earlier working papers[93].

As regards the current legislation governing the use of cookies (which are widely used for profiling in e-commerce) the Romanian law transposing Directive 2009/136/EC has implemented the cookies' consent part of the Directive that refers to users' consent to their use: Article 4 of Law 506/2004[94] mentions that consent for storing information or obtaining access to the information stored on the terminal device of a subscriber or of a user can be given using the settings of the 'Internet navigation application or other similar technologies through which it can be considered that the subscriber or user has expressed consent'.

This text was created on the basis of Recital 66 of Directive 2009/136/EC which mentions

---

91 The text of Article 15 (1) of the EC Data Protection Directive states that every person has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." For more details see p 15 of the Profiling project – working paper - Defining Profiling V. Ferraris (AMAPOLA); F. Bosco, G. Cafiero, E. D'Angelo, Y. Suloyeva (UNICRI) Internal reviewer: B.J. Koops (Tilburg University) available at http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf

92 Text available at https://wcd.coe.int/ViewDoc.jsp?id=1710949

93 Chapter 2.2. of the Profiling project – working paper - Defining Profiling V. Ferraris (AMAPOLA); F. Bosco, G. Cafiero, E. D'Angelo, Y. Suloyeva (UNICRI) Internal reviewer: B.J. Koops (Tilburg University) available at http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf

94 Law 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, with the modifications of the Government Emergency Ordinance 13/2012. Full consolidated text available in Romanian at http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-privind-prelucrarea-datelor-cu-caracter-personal-si-protectia-vietii-private-in-sectorul-comunicatiilor-electronice.html

that: “Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.”

However, the Romanian law seems to entirely overlook the part of the text that says “where it is technically possible and effective”, which is actually the key to understanding the text correctly[95].

To make things even more complicated, the current obligations regarding the use of cookies are also a constant source of confusion. The problem specifically arises when cookies are put in place by a party other than the e-shop, but integrated in the source code by the e-shop itself. Although technically speaking these could be regarded as first party cookies[96], they are really third party cookies and so require explicit consent according to Directive 2009/136/EC and the Article 29 Working Party explanatory documents[97].

> *Q: When stores opt for this type of profiling or segmentation, how do you obtain users’ consent? Isn’t that your job, or is it the store that has to do it?*
>
> *A: Initially for all of our clients we wanted to integrate an area with information on Privacy, Cookies and the rest, but due to lack of time, this hasn’t been done yet.*
>
> *Q: But don’t the stores usually ask you, “Is it legal or not”?*
>
> *A: No, they don’t ask. There is a general Privacy form, it is all set out in writing with information that can be given to the user “We use cookies, we try to offer you the best recommendations. Do you accept or not? So the user can be informed transparently”.*
>
> *Q: But the cookie is really owned by the store, right?*
>
> *A: Yes.*
>
> *Q: Actually, they are not being asked for their consent to use the cookie, they are just being informed “The store uses cookies”.*
>
> *A: Yes.*

Although the part of our interviews related to privacy was quick and vague, as most of the interviewees (with one exception) did not have a lot to say on the matter, in each interview we tried to probe key issues on profiling and privacy, such as: consent, transparency, anonymisation, opting out of profiling, complaints or other privacy concerns.

---

95 In our opinion, the EU legislator was referring to the possible adoption of the Do Not Track feature as the W3C standard – for further details see http://donottrack.us/

96 See for example the Google Analytics explanation of cookies - “The analytics.js JavaScript library is part of Universal Analytics and uses a single first-party cookie containing an anonymous identifier used to distinguish users.” https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

97 Article 29 WP Working Document 02/2013 providing guidance on obtaining consent for cookies http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf and Article 29 Opinion 04/2012 on Cookie Consent Exemption http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

[5.1] Consent

As regards consent to profiling, most e-commerce shops claim that they obtain consent based on the acceptance of online documents – privacy policy or terms and conditions and/or actions (such as subscription to the newsletter or completion of an order).

However, there is some debate as to whether this actually constitutes informed consent, as defined by the Data Protection Directive[98] and the Article 29 WP guidance documents[99], since most of the information provided states generally that personal data are being processed, without any clear emphasis on the fact that some data (and exactly which data) will be used for profiling.

The relationship between third parties offering technical solutions for profiling to online shops and their clients is a more complicated issue. In this situation, the third parties involved claim that all responsibility lies with the e-commerce actors, who should be the ones providing the proper information and obtaining consent:

> *Q: How do you inform customers about data collection?*
>
> *A: We are not required to inform them, the stores are. We offer a software product. The e-commerce business buys the services and is responsible for informing. As far as I know, all online shops have to state that they are using cookies and you have the option of saying "OK" or leaving the website.*

[5.2] Transparency

We tried to investigate to what extent profiling was included in the scope of data processing, as requested by the Romanian data protection legislation. Our empirical analysis of the relevant public documents of 150 e-shops at the GpeC revealed that this information was absent on all the websites we visited (and we know that at least some of them use profiling techniques). Some have included the "personalisation of the information we show you" among the purposes for which personal data are used.

We also probed the issue of whether they provide adequate information regarding cookies, as these are used for almost all or most profiling activities. In practice, also based on our experience with the e-commerce companies registered at the GPeC, if the e-commerce website uses cookies, be it first party or third party cookies – it falls within one of the following categories:

- They have no information on their website as regards the use of cookies.
- They provide some general information such as "We may use cookies on our website to .." in their Privacy Policy or Terms and Conditions.

---

98 Directive 95/46/EC of the European Parliament and of 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 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

99 Article 29 WP Working Document 02/2013 providing guidance on obtaining consent for cookies http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

- They have a special so-called Cookie Policy, which is usually just a copy&paste of the information document on cookies provided by IAB Romania.
- They have a pop-up widget which loads at the top or bottom of the page, saying "We use cookies on this website. By continuing to use it, you accept that" and with a link to the Cookie policy.

We were unable to find any clear or direct information on the Romanian e-commerce websites (with just one exception in about 150 e-commerce shops visited) about exactly what cookies they used and exactly what for, whether and how they used cookies for profiling and how users could opt-out from using them. Furthermore, none of the e-commerce websites that we visited said anything specifically about profiling as the specific purpose of using cookies.
This practice was also acknowledged in our interviews:

> *Q: How do stores that use profiling or targeting inform clients about data collection?*
> *A: I don't think I've ever seen any modified "Terms and Conditions". The only change that I've seen was regarding AdWords remarketing, some people reacted and made the changes within the "Terms and Conditions". But once they've signed with these profiling platforms, I don't think I've seen any changes made.*

Still on the subject of transparency, but at a much higher level, we looked into whether the personalised information shown to the user is somehow identified or presented as information based on profiling activities using the personal data collected:

> *Q: And what about the newsletter? Did you mention that it's personalised or not?*
>
> *A: Indirectly, yes. Meaning, you send him a marketing message "Look, your favourite products" or "You might be interested in the following products"*
>
> *Q: So he should realise from the message that the information is only for him.*
>
> *A: Kind of, yes. But you can't go too far because…*
>
> *Q: Because?*
>
> *A: Meaning…You can't say "Look, I know you saw this, you did not buy it, but if you buy it now, I'll give you a discount because I know you want it. It is our offer to you".*

[5.3] Opting out of profiling

We also tried to find out whether any of the companies that use profiling techniques had thought about providing an opting-out solution – not for all communications, but just for profiling related to e-commerce. Although technically feasible, we were unable to find a single case where this is done:

> *A: The store has the option to stop the software for some users. I mean not to interact with that user. Basically, it stops sending customised messages.*

It is also interesting to note that some service providers assume there is no need to opt out of profiling and that it is up to the customer to be careful and knowledgeable about what he is subscribing to.

A: We had something in the field of pregnant women …meaning there were some campaigns that were set for nine months and, depending on the stage of your pregnancy, you received certain emails, clients who do this.

Q: With this type of newsletter, I suppose you can give an output. Is this possible at any time?

A: You must realise that she already knows it is this kind of newsletter from the time of registering. You can't register with the happymama.ro website and not know..... I think that if the magazine asked you exactly how many months pregnant you are ... it must be clear why ... meaning that we send you the newsletter and you must wait.

The situation is different in the cases of profiling from publishing websites, or of retargeting, where such option is available based on the Ad Choices format already made available by IAB:

A: We have designed a function, in a section of the page the user is visiting and the system tells you what the user suspects about you and gives you the option of disabling the profile. In other words, the cookie continues to be valid, the system sees that it's still you, but deletes all the information about you, deletes everything and notes that on this particular ID nothing should be registered.

Q: And how do you do this?

A: Simple, you go to a URL.

Q: And how do I know which is the URL?

A: At present you don't know, but when the public service is launched you'll definitely see it. It is very likely that this will happen, however we will need to go to those who have already used it and run an update with the cookie policy.

The situation would be more complicated in the case of future technologies that are not based on cookies (see the case of Google's Universal Analytics[100]), where basically the only option available is to install an add-on specifically for this purpose, but that would need to be created, probably just by the software company performing the profiling.

[5.4] Data limitation and other related issues

One interesting issue in relation to profiling is the technical possibility of identifying a person by using other non-personal data from the profile. Based on information from several interviews it became clear that most of the profile data was of interest to the e-commerce website without having a direct identifier of the person. However, if the e-commerce business wanted to identify one of its customers behind a profile, that would be quite easy to do. Even in the case of simple visitors (meaning people who do not complete an order), the option to identify the person could be used either when the user creates an account, or uses social network features, or in more complicated ways in other circumstances.

100 Op cit footnote 24

Q: And have there been any instances in which the shop wanted to identify a particular customer?

A: No.

Q: Is that because they weren't interested?

A: It's going to involve a huge amount of data. You can identify them; we usually identify them when we're checking things. For example: "he bought 20 million worth this month, how about we send him a private message? No, we don't do that."

We also learnt from the interviews that even though a lot of data are tracked, their value is not so important over time – depending on the market where the website operates. In the Fashion domain, for example, the decision to buy has been estimated to take an average of 4 hours, whereas in the case of IT&C products, this could take on average 7-8 days. Thus, the data actually become irrelevant within a matter of weeks or even months. In order not to keep too much information that is of no interest (and not for privacy concerns), some companies that sell profiling software services actually limit the time for which the data are used – whether actively or not:

Q: Do you recommend a storage period for the client depending on the market category as we have just discussed?

A: To be honest, yes, but it's not our decision. It's each client's decision. It depends on the time it takes for a purchase. For example, in the fashion field, none of my clients communicate for more than 5 or 6 days for the same product or for the same range of products. If customers haven't bought anything within 5 or 6 days, they will not buy at all. On the other hand, in the IT&C field, the process can take a month or two. For example, the decision to buy a Smartphone. Because there is a possibility that you don't have the money, you might enter the site after a week or two to see if the price has gone down and later, when you have enough money to buy it.

Q: And in this case, if a fashion store says "I do not want a customer who is willing to buy after 6 days because he might not buy the product at all.". What happens to that user, is he inactive, or what?

A: No, we keep the history, but just so that we can use it in another campaign. A new history will start for him; all that is relevant will be taken from his last session or from the action during a certain time frame or if he didn't place an order. When the user makes a purchase, we then close the session and keep the history. Because we need to bring him back to us not using the same products but with related segments.

Q: What do you mean when you say "keep the history"?

A: We store it in an archive, which is available for 6 months, after which it is deleted.

Q: Can the store download the history?

A: The store can access the database at any time.

The relevance of data for just a limited period of time and only to the specific website where they were collected is a factor that actually prohibits data sharing or data transfer. Moreover, some specific profiling software could give you the raw data, but it would be impossible (or extremely difficult) to be used outside that software:

Q: And what if you have all their browsing history?

A: It is difficult to use their browsing history because, after a certain amount of time, the information is useless. OK, you were interested in shirts, but you might not be in one month. A user's profiling data can't be used for more than 4-5 months. And there is another problem. The problem is that our software compiles the data. Meaning I can give them to you, but you can't use them. There is not a .txt file, you said OK, Mr. Popescu wants that.

Q: What do you mean by compiling?

A: Meaning you still need our software to understand the data.

[5.5] Data minimisation

As already explained in chapter 4.3, there is a strong commercial incentive not to ask directly for a lot a personal data when users open a new account on an e-commerce website. One of the e-commerce platforms that we interviewed took this even further in order to have as many orders as possible – even from users who are reluctant to give their data online. The platform sees this not as a form of data minimisation, but rather as a means of getting access to inexperienced e-shoppers.

A: We have a very nice function, the fast order, in which you only give your e-mail address, telephone number and are not asked to provide any other data.

Q: And do they call the user in order to obtain their address?

A: Yes, and it's being used, quite often. Especially if I order something from my mobile, it is easier to enter just those 3 pieces of information. Following the same principle, some customers order by telephone in order not to give any data.

Q: Are a significant number of orders made by telephone?

A: It depends. Orders are also sent by e-mail, like "I saw something on your web-site and I would like to buy it".

Q: And is this beca*use they are not technical enough to follow the order process or because they have trust issues or because they don't want to use the site?*

A: It is not about lack of confidence, they are just used to ordering things like that. But now older people are discovering online shopping, a lot of older women, aged over 60, and they don't have an e-mail address, they have never ordered anything online before, but their grandchild's birthday is coming up and they want to buy a present. So, of course, she calls and you have to explain "left click, right click". Or, another thing, if the products sold on the website are extremely expensive, the website might act more as an information area.

[5.6] Complaints and concerns about profiling

In most of the interviews we were unable to identify any kind of privacy-related concerns among our interviewees, with only one exception. In this case the interviewee acknowledged that an average Internet user would not realise if he/she was being profiled. But this interviewee has to perform some kind of reverse-engineering process and understands the issues at stake – especially in the context of retargeting. This could also be related to the fact that he has an e-shop selling products that are somehow related to special categories of personal data:

> *Q: But, given all these issues concerning privacy, would you still think about doing profiling or would it be unpleasant for the customer?*
>
> *A: Well, what I'm talking about is re-marketing, because few people know that those ads which appear on a blog are linked to the user's profile. Usually, when people see those ads with ABC Shop on all the sites they start to think, "oh look, how much money they have, they put ads on all the websites". (..) As long as you show things that look impersonal, for me it is OK. (...)*
>
> *Q: So, is it a sort of business philosophy?*
>
> *A: I'm that kind of man.*
>
> *Q: So you stick to the idea of profiling within the website?*
>
> *A: Yes, profiling, I told you about the website. If it happens on external websites, I have a problem. If it is on my website, I don't have a problem, or if it is in your mail. So, I am talking about re-marketing on external websites where things sometimes might get out of hand.*

It was also interesting to note that the interviewee did not see this as a legal issue, but rather as a moral one – of respecting his customers or business ethics:

> *A: The first strange thing that happened was the ad that I saw: "You have items in your cart and I will give you a 5% discount if you complete your order now". Maybe I was about to buy a gift for my wife and we were both looking on a blog at that time and she told me "Oh, you've ruined the surprise". This is exactly what I told them. From then on, this started to be strange. It is a tool that should be used but with certain limitations. But, it depends on how you see things. It is my computer, my cookie, it is not my fault that I have someone next to me.*
>
> *Q: But you - as a shop or third party -, don't you know whose computer it is?*
>
> *A: When I do re-marketing I am always careful to make unisex statements, and use generic expressions. I don't say, 'Oh, you visited X Shop, come again'. I try not to make it obvious. I am not like that, even if you're with someone, on Facebook it appears like a normal ad, although I could write I know "You clicked on this three times, you want this product, come and get it." (...)*
>
> *Q: Are you like this because there's a business need or are you afraid?*
>
> *A: No, I am fair, I try to respect the customer. I mean, I can attract 2000 new customers, and for sure there will be one that might create a conflict, not neces-*

sarily a huge conflict, but it would be unpleasant. I can give you an example that actually happened to me; I was writing on the site that our products are packed in non-customised cartons. And the products are packed in like this, but the name of the website was written on it by mistake. It was a mess, I ruined his wife's gift. But, he was right, he was counting on me for his privacy and… My answer is that I respect my customer. I mean, legally, he was warned that we use cookies, but morally I don't know if it is OK.

[5.7] DPA and enforcement

In this context, as explained so far, e-commerce actors have an extremely limited understanding of privacy issues in the domain of profiling, to use a euphemism. Thus, it is hardly surprising that none of the interviewees were aware of any audit or intervention by the DPA on this topic.

The current image of the Romanian DPA – a bureaucratic entity which asks for mandatory registration and a document that no one looks at – emerged from several answers provided by the e-commerce actors and demonstrates the lack of relevant information concerning the issue of data protection in general, but also specific to the e-commerce market.

Q: Have any Romanian or foreign authorities performed an audit?

A: Oh, no.

Q: Or privacy checks?

A: Ah, the data protection authority - the document where you write what you want and nobody looks at it. Yes, there has been one.

It is also interesting to note how the relationship between the different actors in the e-commerce field is not clear with regard to data protection issues and legal responsibility.

Q: Have you analysed the issue of profiling in terms of privacy?

A: No, it's not the customer's job to perform an analysis, it's the client's business.

On the other hand, the Romanian DPA also acknowledged in its answer to the Profiling project[101] that it had received few complaints concerning the application of Article 17 of Law No. 677/2001 and that only in one case the data controller had not observed these requirements (a financial institution). It also said that it had not investigated any cases of automated profiling on its own initiative.

101 Answer from the Romanian DPA to the Profiling Project questionnaire - Questionnaire on Profiling for National Data Protection Authorities – 31 October 2014

6

Complaints to the DPA or courts concerning Ecommerce and profiling

As stated above, the Romanian DPA has received no specific complaints concerning e-commerce and profiling. Moreover, even the most important courts in Romania[102] replied that they have only dealt with a few cases related to data protection and none related to profiling.

The majority of complaints received in 2012 and 2013 concerned unsolicited commercial communications (mostly related to online commerce activities). In 2013 these types of complaints accounted for one third of the total number received. This is confirmed by the statistics of the Romanian Blacklist – abuse.ro[103] which in its report for 2013 notes that 5% of checked emails were reported as spam in Romania. Romania is still one of the top 20 spam source countries, ranking 13th according to the latest Kaspersky Lab report[104].

According to the answers provided by the Romanian Data Protection Authority (DPA) to our Freedom of Information request[105], as yet this DPA has not investigated any cases regarding profiling techniques.

We also received similar answers from the Appeal Courts[106] which answered our FoI request stating that they had not dealt with any cases based on Romanian data protection law 677/2001.

However, the Romanian DPA has investigated one case related to profiling in the digital age by an ISP – with the collaboration of a company called Phorm, which aroused much attention in the UK[107] just two years before it set up in Romania (however the case was not classified under Art. 17 of the Romanian law).

---

102 In some cases the courts also claimed that they do not hold any specific evidence for data protection cases.

103 See Abuse.ro - Raport de activitate - septembrie 2013 https://www.abuse.ro/blog/raport-de-activitate-septembrie-2013-n2614 (only in Romania18.10.2013)

104 See Wall-street.ro: Romania – one of the top countries for number of spam messages sent (only in Romanian 27.01.2014) available at http://www.wall-street.ro/articol/IT-C-Tehnologie/160600/romania-in-topul-tarilor-cu-cele-mai-multe-mesaje-spam-trimise-in-2013.html

105 14th of April 2014/ Answer to CRPE's request FoI no 7668 – Romanian Data Protection Authority

106 16th of April 2014/ Answer to CRPE's request FoI/ 43- Romanian Court of Appeal Timis (Romanian courts Arad, Timis, Caras-Severin, Hunedoara counties)/ National Council for Magistracy, Romania

107 EDRi-gram: Phorm case sends the UK to the European Court of Justice (6.10.2010)
See http://edri.org/edrigramnumber8-19uk-infringement-data-protection/

The company described its service as “Internet personalisation”, whereas in fact it was an invasive profiling technique, as explained in simple terms below[108]:

> *“Phorm works by looking at the web traffic between you (an ISP client) and the sites you visit. Phorm examines the content of the web pages you visit, and logs keyword information derived from it. Phorm can then deliver adverts to you based on keyword information.*

For instance, if you visit car related sites, and make searches for new car models, you would start seeing car adverts when you visit Phorm’s partner’s websites.”

The case – reported by the Romanian DPA in its 2012 Report – was classified not as a breach of Art. 17 of Law 677/2001 (the national law implementing Art 15 of the DPD) that makes reference to ‘automated individual decisions’ which are thus closely related to profiling[109], but rather a breach of the e-privacy law 506/2004 and its articles related to cookies.

The DPA noted in its 2013 Report that it had investigated the implementation of the Phorm Romania profiling software at Romtelecom (a major Romanian ISP) – the service called MyClicknet was an added value service – the purpose of which is to personalise Internet navigation in order to provide behavioural advertising and which consists in “redirecting a copy of the traffic history, in order to be analysed and the related data to be collected and processed, before and after accepting this service, by installing cookie files on the computers of the subscribers/its users”. The DPA also concluded that basically the cookies were added without consent.

Following the investigation, the DPA sanctioned the ISP with two fines, which were contested in court. The courts finally confirmed the reasoning of the DPA with a final decision in 2014. Phorm decided not to continue its activities in Romania[110].

---

108 Explanation by Jim Killock in article UK: Phorm threat in EDRi-gram 7.2 (28.01.2009) – http://history.edri.org/edri-gram/number7.2/phorm-uk. For further technical analysis see also The Phorm “Webwise” System (18.05.2008) http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf

109 See Profiling project – working paper - Defining Profiling V. Ferraris (AMAPOLA); F. Bosco, G. Cafiero, E. D’Angelo, Y. Suloyeva (UNICRI) Internal reviewer: B.J. Koops (Tilburg University) available at http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf

110 According with their annual report - http://www.phorm.com/sites/default/files/Annual_Results_27-June-2014.pdf

7

Conclusions

From the interviews performed and the above analysis, it seems that profiling in e-commerce in Romania is still in its infancy. Despite its limited development and its obvious advantages for e-shops, but also for consumers in certain cases, it has already raised a large number of concerns and question marks especially in relation to data protection issues.

Our work in this domain has revealed the need for clearer regulation in this respect, so the GPDR would definitely fill a loophole in the current legislation, including in the e-commerce field. In this respect it is important to note that all the key elements requested by the Article 29 Working Party[111] (scope, transparency and accountability and responsibility of data controllers) are essential for a properly functioning legal framework. We would especially like to underline that if the scope of the regulation would still be limited to "a measure which produces legal effects concerning this natural person or significantly affects this natural person", many of the profiling activities already described above would still not be covered by the future legal text.

But even a "perfect" new legal text on profiling will need to be backed by functional enforcement mechanisms, that cannot be bypassed simply by using the service in another country, which is rather easy to do from a technical perspective given the nature of the Internet.

It also seems clear that the national DPA lacks authority in this field and is largely ignored by the e-commerce market players – qualities which would be essential to have an effective and efficient regulator. This is obviously due to the fact that the DPA is under-staffed and under-financed, but also depends on a lack of adequate technical knowledge in order to enable it to independently assess the real risks that the current profiling techniques pose to privacy (and not only in the area of e-commerce).

There is plainly still much that needs to be done in order to put legal profiling activities in place. In our opinion, many problems could be solved by providing the right information, fostering dialogue and the will to understand the needs of the other party. At present there is no form of dialogue between the e-commerce industry and the DPA authority. Future actions by the DPA to investigate profiling issues in the field of e-commerce, in which it simply intervenes, applies the laws (with the usual fines) and then steps aside (as it has been doing up to now), would probably have no long-term effect and, based on our experience, would simply arouse an instinctive reaction from within an industry that has traditionally been exempted from a lot of tough regulation.

The interviews in which we needed to explain what "personal data" actually means (and not just quote the law), gave us the full picture on why an extensive awareness campaign (by the DPA, but also by other actors) is needed more than any sanctions. With the correct implementation of the principles of privacy by design and privacy by default, the situation could significantly improve. Given the current limited development of profiling activities in e-commerce, starting as soon as possible will limit the headaches later.

111 Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation (13.05.2013) available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/annex_one-stop_shop_20130513_advice-paper-on-profiling_en.pdf

Border control: a new frontier for automated decision making and profiling?

Valeria Ferraris and Marco Sorrentino
Amapola

prof[i]ng
PROTECTING CITIZENS' RIGHTS FIGHTING ILLICIT PROFILING

Executive summary

Borders have always been tools of classifications, aimed at sorting welcome and unwelcome people. Compared to the past, nowadays borders are increasingly mobile and are one of the privileged arenas for implementation of risk-based strategies. Thus, information exchange and databases have over the last 15 years been the new frontiers for migration control. This paper seeks to draw attention to one specific aspect of this subject, namely the issue of automated decision making and profiling, aiming to understand if and to what extent this new trend in immigration control involved such measures. In particular, this study focuses attention on the newly developed Schengen Information System II and on Eurodac, examining how these biometric databases are implemented and used in Italy for immigration control. Moreover, it explores the development at EU level in terms of new databases for migration control (the so called smart borders package) and the information exchange initiatives aimed at increasing surveillance in the Mediterranean area.

Key findings:

- Some of the new functions of SIS II, in particular the interlinking between alerts, are elements of profiling.
- There is a hiatus between the design of the database and its implementation.
- There is a clear trend to multi-purpose databases.
- There is a clear trend to grant access to new authorities, unrelated with the original scope of the data collection.
- Data protection rights are clearly established on paper but not fully enforced in practice.
- Databases classify people according to degrees of suspicion.
- Databases make easier the exchange of information.
- Profiling is not yet a common practice in the present use of databases for migration control but there is room for profiling practices in the future.

Introduction: theoretical background, aim and methodology

Borders seemed to lose most of their significance after 1989, but then, after 9/11, all of a sudden – they were back on the agenda. Borders were once again performing the role they first acquired in the 20th century: as barriers against terrorism and to prevent other violations of security.

In Europe, this new centrality of borders was accompanied by an increasing harmonisation of the European migration policy framework and the growing relevance of a risk-based approach in many policy fields, e.g., policing, justice, welfare and immigration (see Feeley and Simon, 1992; Ericson and Haggerty, 1997).

Borders are therefore one of the privileged arenas for implementing risk-based strategies; borders have increasingly become a tool of classification, aimed at sorting individuals into deserving and undeserving foreigners (Bosworth, 2008). Technology adds a new complexity to this action of sorting, as it enables automated profiling. The nature of borders has also changed, as they have become gradually more mobile, in a way that was unforeseeable just a few years ago.

The concept of mobile borders (first introduced by Weber, 2006) focuses on the different strategies developed by receiving countries to prevent and deter unwelcome arrivals. They are not new border control measures but strategies of manipulation of the "location and meaning of borders themselves" (Weber, 2006, p.22). These include three different ways of border-shifting – functionally, spatially and temporally – plus a fourth one, the personalised border, when the foreigner embodies the border.

The functional shift occurs when the border is not the sole location where border functions are performed. Migration control is not confined to the border as a geographical site but is a combination of checks implemented inside and outside the country. The spatial shift refers to the removal of a part of the country's territory[1], whereas the temporal shift underlines that for a specific period of time the border is moved somewhere else.

1 Australia is the land of experimentation in this extreme practice. Since 2001 Australia has excised some northern islands from the so-called migration zone (area where people land by boat, have the possibility to apply for asylum and have access to the Australian judicial system) declaring them 'excised offshore places' and, as a consequence, putting the migrants who land there in a sort of no man's land. (see Coombs, 2004 and Ferraris, 2014 for more details).

The personalised border has been conceptualised as “fragmented and fully portable, its location defined, not by sites of enforcement action by state officials, but in terms of the current whereabouts of certain intending visitors” [Weber, (2006), p.36], in other words, as a border that would-be migrants incorporate and carry around, regardless of where the functional or spatial boundary lies.

Technology plays a significant part in making borders highly personalised. Border control is a challenging task because of the mobility of the target: as effectively underlined by Koslowski (2011, p.7) “border control officers often compare their task to squeezing a balloon: if you squeeze one end, it expands at the other”. Technology - at least in the desire of the policy makers - is pictured as the solution to the mobility of migrants. Databases appear as the most efficient and effective way of exercising remote control (Zolberg, 1997).

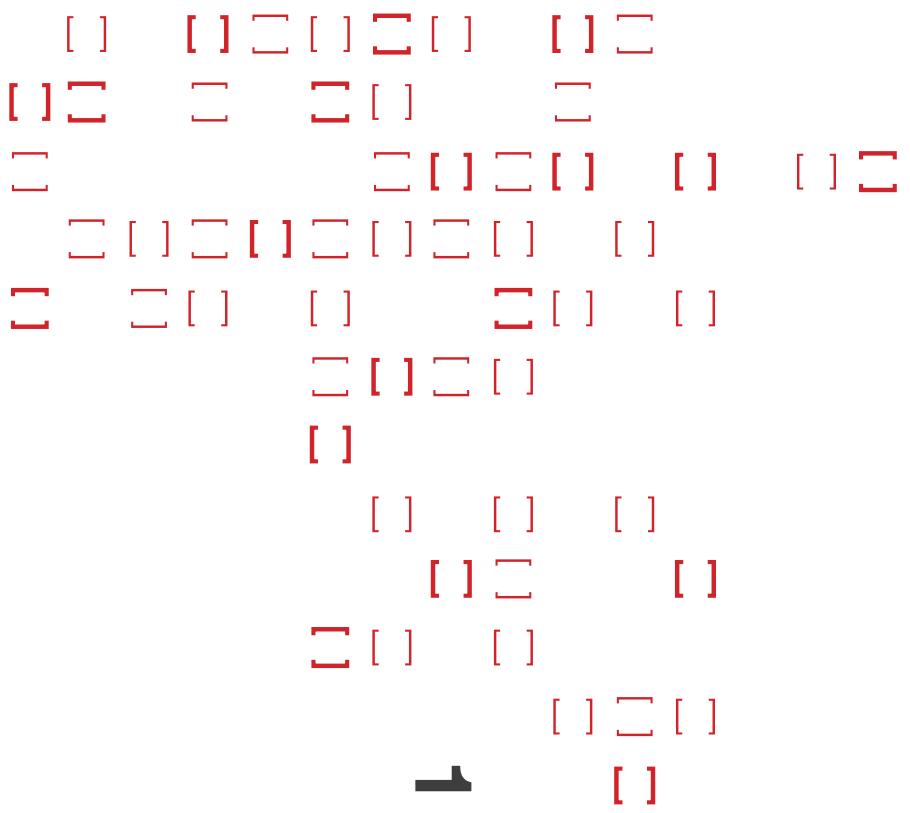
Thus, the exchange of information and databases have, over the last 15 years, been the new frontiers for migration control. This paper seeks to draw attention to one specific aspect of this subject, namely the issue of automated decision making and profiling, in order to understand whether and to what extent this new trend in immigration control involves such measures. In particular, this study focuses on the newly developed Schengen Information System II and on Eurodac, examining how these databases are implemented and used in Italy for migration control. This means that the databases, especially the SIS II, will not be explored in detail, but the discussion will focus on aspects concerning Third Country Nationals. The choice of Italy, apart from the fact that it is the author’s native country, is due to its centrality as a gateway to Europe from the South. This is even truer now than it was a few years ago, with the Italian border being placed under increasing pressure as a consequence of the crisis in Northern Africa and the Middle East.

- Chapters 1 and 2 draw attention to the main features of SIS II and Eurodac, examining their implementation in Italy and their daily use by immigration offices.
- Chapter 3 explores further developments at EU level in the so-called smart borders package and other initiatives aimed at increasing surveillance in the Mediterranean area.
- The last section provides some reflections on profiling and automated decision making in border control.

This research is exploratory in nature. The issue of automated decision making and profiling is fairly new and has not been described in depth in relation to immigration databases, in particular not in terms of how it works in recent practice. Some contributions (Broeders and Hampshire, 2013; Bigo et al, 2012) have pointed out that the logic of profiling and data mining pertains to these EU databases and represents a risk, but have not explored this in detail. Some scholars (in particular Brouwer, 2007, 2008a, 2008b and Karanja 2008) have focused their attention on the risks of infringements of fundamental rights and remedies, also analysing the implementation of the SIS databases in some EU countries (France, Germany, The Netherlands). Also worth mentioning is the research carried out by the National Ombudsman of the Netherlands, the only public body to have conducted an assessment of the implementation of the SIS database in the Netherlands (De Nationale Ombudsman, 2010).

The research was conducted through fieldwork and desk research. Before starting the fieldwork, legal texts at EU and country level together with the relevant literature were reviewed. The empirical research relies mainly on individual or group interviews with MEPs (3); EDPS assistant supervisor; lawyers (4); EU Commission DG Home Affairs Unit A3 – Police cooperation and relations with EUROPOL and CEPOL (1); the Italian DPA; police authorities at a central and local level (N-SIS Italian Division; Immigration office of two cities in Italy). The Italian Sirene Office refused the interview.

It is worth mentioning that we encountered some difficulties with gaining access to the information and obtaining authorisation to perform the interviews. In general, these were due to the fact that the topic concerns police databases and so specific authorisations or additional checks were necessary. Although this does not limit the generalisability of the findings, it does mean we were only able to draw a partial picture of the situation. As already underlined, this study is exploratory in nature. The issues raised certainly require further in-depth analysis.



The Schengen Information System (SIS)

The Schengen Information System (SIS)[2] is the oldest and one of the most important large-scale databases in the European Union. It was originally created as a compensatory measure to allow for the free movement of persons in the Schengen area. Furthermore it enhances cooperation and coordination between the police and the judicial authorities in order to safeguard internal security by countering illegal migration and fighting crime, namely organised crime.

It was operational from the entry into force in 1995 of the Convention Implementing the Schengen Agreement - hereafter Schengen Convention or CISA - until its replacement (on 9 April 2013) by the new information system SIS II[3], which has more functions and allows the expansion of the original SIS to the new Member States.

The switch to SIS II occurred in response to two main issues: the inclusion of new Member States, which required a new IT infrastructure, and the need for new functionalities. The new system also involves changes in the supervision and management of this database. A coordinated structure of the national DPAs and the EDPS now supervises SIS II and has replaced the Schengen Joint Supervisory Authority (JSA), which supervised the Schengen Information System up to 2013.

The new European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) assumed the operational management of SIS II on 9 May 2013.

2 For an overview of border control systems see Peers 2011.

3 For a critical view on the development of SIS II and the actors involved see: Joanna Parkin (2011).

SIS II has a dual legal basis, formerly falling under the first and third EU pillars: a Decision[4], which focuses on the use of the system for policing and criminal law purposes, and a Regulation[5] that implements the rules on immigration matters[6].

Its purpose — according to the two legal texts — "shall be to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the Treaty relating to the movement of persons in their territories" (Article 1, Regulation No. 1987/2006 and Decision 2007/533/JHA). Compared to the purpose laid down in the Schengen Convention[7] the objective appears wider and more ambitious, moving forward from a largely administrative purpose for which the Schengen Information System had been established to one of a more general policy.

[1.1] The data stored and the alerts

In contrast to the original SIS, SIS II also contains biometric data (see table No. 1 below). The legal basis requires a specific quality check of biometrics to be determined according to an identified procedure. However, there are no common obligations or requirements related to biometric data.

Biometric data are currently only used to confirm the identity of a Third Country National who has been located as a result of an alphanumeric search in SIS II. Both the Decision and the Regulation allow the use of fingerprints to identify a person when "this becomes technically possible". Until this functionality is implemented, the Commission must present a report and the European Parliament needs to be consulted, but there will be no further vote on this new functionality. As soon as it becomes technically possible to compare the biometric data of an unidentified person with all the biometric data in the database (the so called "one to many" search), it will also be in compliance with the law (see Article 22 of the Regulation and of the Decision).

4 Decision 2007/533/JHA

5 Regulation No. 1987/2006

6 Another regulation is on the use of SIS II by vehicle registration authorities.

7 The general purpose of the Schengen Information System is described in Article 92 as: "the SIS shall enable the authorities (…) by means of an automated search procedure, to have access to alerts on persons and property for the purposes of border checks and other police and customs checks". In the case of the specific category of alerts referred to in Article 96, the purpose is the issuing of visas, residence permits and the administration of legislation on aliens.

Table No. 1 Data stored: evolution from the CISA to the present rules

CISA	Article 20 Regulation No. 1987/2006	Article 20 Decision 2007/533/GAI
(a) surname and forenames, any aliases possibly entered separately; (b) any specific objective physical characteristics not subject to change; (c) first letter of second forename; (d) date and place of birth; (e) sex; (f) nationality; (g) whether the persons concerned are armed; (h) whether the persons concerned are violent; (i) reason for the alert; (j) action to be taken.	a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately; (b) any specific, objective, physical characteristics not subject to change; (c) place and date of birth; (d) sex; *(e) photographs;* *(f) fingerprints;* (g) nationality(ies); (h) whether the person concerned is armed, violent or has escaped; (i) reason for the alert; (j) authority issuing the alert; *(k) a reference to the decision giving rise to the alert;* (l) action to be taken; *(m) link(s) to other alerts issued in SIS II in accordance with Article 37.*	(a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately; (b) any specific, objective, physical characteristics not subject to change; (c) place and date of birth; (d) sex; *(e) photographs;* *(f) fingerprints;* (g) nationality(ies); (h) whether the person concerned is armed, violent or has escaped; (i) reason for the alert; (j) authority issuing the alert; *(k) a reference to the decision giving rise to the alert;* (l) action to be taken; *(m) link(s) to other alerts issued in SIS II pursuant to Article 52;* *(n) the type of offence.*

* In Italics the new data included under the Regulation and under the Decision that were not included under the CISA.

As shown in the table, the two other new pieces of data included in the SIS II system, besides biometric data, are a reference to the decision giving rise to the alert and links between alerts.

The reference to the legal basis of the alert should make it possible to check its legitimacy more quickly. But the links between alerts are the most relevant and sensitive novelty. This functionality allows one alert to be associated with another.

Alerts concerning persons or objects. Objects include: motor vehicles, boats, aircraft; firearms; stolen, misappropriated or lost official documents, identity papers, residence permits, travel documents; banknotes; etc. (see Article 100 of the CISA; Article 38 of Decision 2007/533/GAI).

Persons include:

- Persons wanted for arrest for surrender or extradition purposes (Article 95 of the CISA; Article 26 of Decision 2007/533/GAI);
- Unwanted Third Country Nationals (Article 96 of the CISA; Article 24 of Regulation No. 1987/2006);

- Missing persons (Art. 97 of the CISA; Article 32 of Decision/2007/533/GAI);
- Persons sought to assist with a judicial procedure (Art. 98 of the CISA; Article 34 of Decision 2007/533/GAI);
- Persons for discreet surveillance or specific checks (Art. 99 of the CISA; Article 36 of Decision 2007/533/GAI).

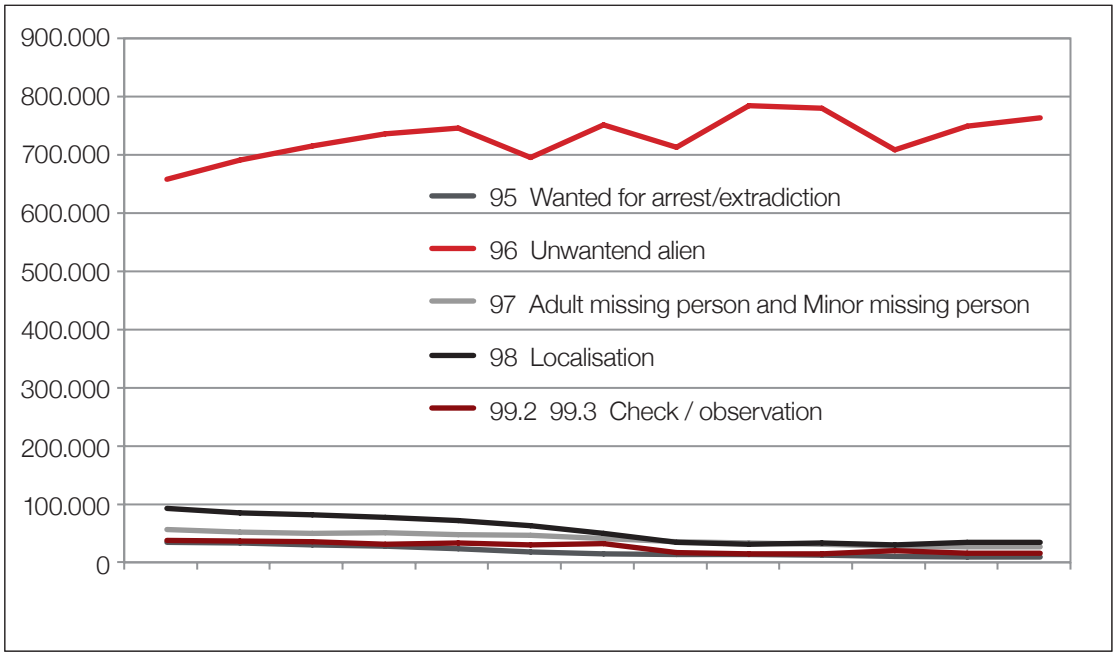
The sensitiveness of such links was well stressed in the EDPS opinion on SIS II: "Interlinking of alerts can have a major impact on the rights of the person concerned, since the person is no longer 'assessed' on the basis of data relating only to him/her, but on the basis of his/her possible association with other persons. Individuals whose data are linked to those of criminals or wanted persons are likely to be treated with more suspicion than others. Interlinking of alerts furthermore represents an extension of the investigative powers of the SIS because it will make possible the registration of alleged gangs or networks (if, for instance, data on illegal immigrants are linked with data of traffickers)" (EDPS, 2005). To give an example: an alert for an unwanted TCN could be linked to an alert for a stolen vehicle where the person was found. If there was another person in the car, these two persons would be linked by the alert on the vehicle.
Over the last five years the number of alerts entered for persons has been about 900,000 per year (and more than 10 million for objects). The overwhelming majority of alerts on persons are in respect of unwanted Third Country Nationals. However, compared to 1999, the number of alerts issued under Article 24 of the Regulation has decreased and all those related to police investigation or judicial proceedings have increased.

Table No. 2 - Alerts issued according to type

Type of alert	01/01/13		01/01/10		01/01/07		01/01/03		1/1/1999	
	N.	%	N.	%	N.	%	N.	%	N.	%
Wanted for arrest/ extradition	35,919	*4.05*	28,666	*3.08*	16,047	*1.79*	14,023	*1.60*	10,491	1.23
Unwanted TCNs	659,347	*74.43*	736,868	*79.27*	752,338	*84.08*	780,992	*88.99*	764,851	*89.36*
Missing persons	57,302	*6.47*	52,319	*5.63*	42,500	*4.75*	32,211	*3.67*	27,436	*3.21*
Arrest in view of a judicial procedure	94,292	*10.64*	78,869	*8.48*	50,616	*5.66*	34,413	*3.92*	35,806	*4.18*
Discreet or specific checks	38,947	*4.40*	32,824	*3.53*	33,275	*3.72*	16,016	*1.82*	17,365	*2.03*
Total	885,807		929,546		894,776		877,655		855,949	

Source: own elaboration of EU Council data

Graph No. 1 – Issued alerts according to type



Source: own elaboration of EU Council data

The eu-LISA statistical report presents the composition of the SIS II database[8] on 31 December 2013. Italy is the country with the highest number of alerts entered into the system, followed by Germany (with less than ½ of the Italian alerts) and the Netherlands and Spain (with less than ¼ of the alerts). As regards persons, Italy and France have the highest numbers, followed by Germany and Greece.

Table No. 3 – Numbers of alerts by country

COUNTRY	Persons	Documents (issued and blank)	Vehicles	Licence plates	Firearms	Others*	Total
Italy	294,101	13,819,029	1,143,745	471,905	51,511	387,539	16,167,830
France	125,058	2,263,170	326,824	1	32,557	35,319	2,782,929
Germany	76,302	6,230,209	234,818	626,111	148,227	204,133	7,519,800
Spain	71,454	3,187,767	632,581	380	45,848	764	3,938,794
Greece	65,885	396,640	165,303	119,017	14,433	28,301	789,579
Poland	29,953	679,061	210,721	144,712	17,121	3,247	1,084,815
Switzerland	29,386	828,930	21,175	0	9,780	1,460	890,731

8 Twenty-eight countries are connected to SIS II. Member States of the EU connected to SIS II are Austria, Belgium, Bulgaria, Czech, Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. Associated Countries connected to SIS II are Iceland, Norway, Switzerland and Liechtenstein. Moreover, the authorities of the United Kingdom, Ireland and Croatia are in the process of making preparations for their technical connection to SIS II.

Austria	27,043	317,438	24,999	13,833	5,658	548	389,519
Netherlands	24,393	3,872,084	89,331	194	1,517	420	3,987,939
Portugal	20,147	87,385	57,204	1	9,369	10	174,116
Hungary	16,888	767,931	32,518	28,615	397	213	846,562
Czech Republic	14,462	2,443,655	81,988	113,524	16,989	153	2,670,771
Norway	14,161	129,777	7,009	6,669	1,493	746	159,855
Sweden	11,002	242,286	34,406	19	17,819	27	305,559
Belgium	10,450	2,494,023	56,863	184,119	36,234	4,229	2,785,918
Slovakia	7,370	718,799	20,657	12,510	4,424	44	763,804
Romania	6,587	1,329,120	7,343	0	537	17	1,343,604
Denmark	3,061	556,732	26,487	182	4,563	115	591,140
Finland	2,789	125,491	4,391	174	8,070	77	140,992
Malta	2,451	87,197	836	8	174	14	90,680
Lithuania	2,339	799,157	27,298	276,719	3,255	44	1,108,812
Estonia	1,574	339,518	2,442	2	254	0	343,790
Latvia	1,414	72,817	1,756	1,068	10	4	77,069
Bulgaria	1,247	955,647	22,302	121,554	61	0	1,100,811
Luxembourg	1,220	19,318	1,085	107	156	169	22,055
Slovenia	896	138,103	7,652	35,819	645	273	183,388
Liechtenstein	231	2,311	72	84	8	34	2,740
Iceland	36	15,736	3	1	11	0	15,787
Total	861,900	42,919,331	3,241,809	2,157,328	431,121	667,900	50,279,389

* The category “others” includes: aircraft, banknotes, boats, boat engines, containers, industrial equipment, licence plates, securities, vehicle registration documents.

Source: own elaboration of eu-LISA (2014b)

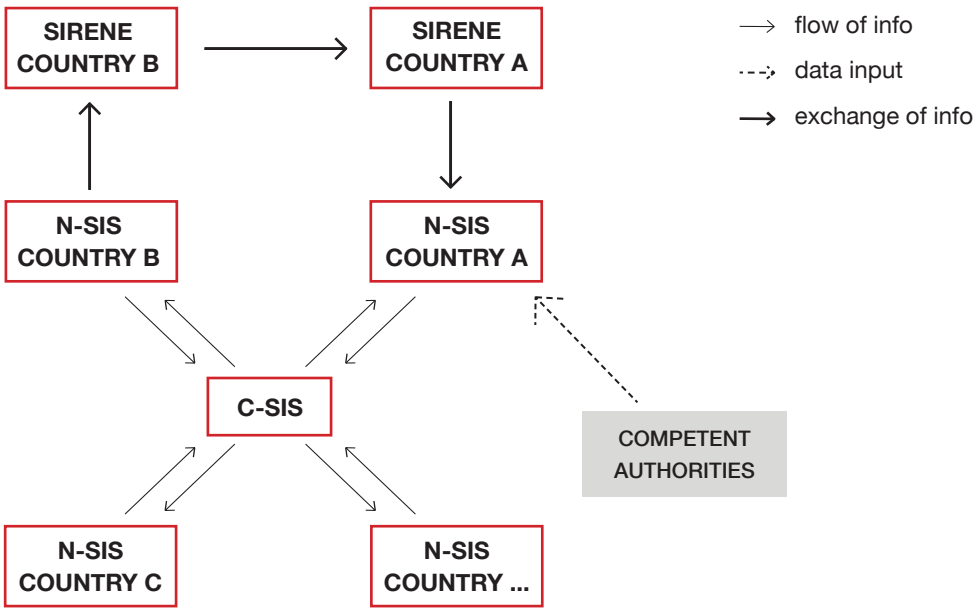
[1.2] The architecture of the system and information searches

The system is an interconnection of a national database (N-SIS), via a secure communication infrastructure, with a central server in Strasbourg (C–SIS) that sends and receives data to and from the Member States (radial shape). Each Member State accesses the system through a common interface. The national database may contain a national copy of the data (Article 9 of the Regulation). However this is not necessary: access is guaranteed by the central system. During the interview, the SIS office clarified that in actual fact the biggest countries have a national copy for their own purposes.

When an alert needs to be entered, the N-SIS of a Member State sends the request to the central server. After checking the alert to verify its compliance with technical requirements, the C-SIS validates it and then enters it into both the National system and the C-SIS. Consequently the permanent updating of the central database and the uniformity of the national system are guaranteed. Each MS adopts a security plan to guarantee the security of the system. If a Member State has a copy of the data, the copy is under its own responsibility.

Information searches in each Member State only take place within that country's N–SIS. The authorities of a Member State cannot search the N-SIS of another country. An N-SIS Office in each Member State is responsible for the operational management of the N-SIS. In addition, an office (called SIRENE, Supplementary Information Request at the National Entry) is established to provide additional information. Member States exchange information through the respective national SIRENE offices.

Figure No. 1 - The circulation of information in the system



[1.3] Right to access and retention period

Having outlined the architecture of the system and the types of data it contains, a subsequent important aspect is to define who is authorised to access the system and under which conditions. Access to the system refers to "a query - regardless of whether a hit is achieved or not - or to a transaction intended to create/update/delete (CUD) an alert. Every access is counted, even if an access resulted in an error and an error message was returned from the system (e.g. if the operator commits an error)" (eu-LISA, 2014). Access is granted on a hit/no-hit basis. The searched object or person can be entered as a search query in order to obtain a yes/no answer. If the response is positive and the alert has been issued by the country performing the search, additional information can be searched through national databases. If the alert has been issued by another country, the SIRENE office of the country that did the search will contact the SIRENE office of the country that issued the alert to ask for additional information (see figure No.1 above).

According to the rules set forth in Article 27 of Regulation No.1987/2006 and in Article 40 of Council Decision 2007/533/JHA, the authorities that have access to the information entered in the SIS must be identified by each Member State. As regards Third Country Nationals (TCNs), Article 27 of the Regulation gives the right to search data to the authorities responsible for the identification of TCNs for the purpose of border control and for other police and customs checks. In addition, the right to access data entered in SIS II is given to judicial authorities and to those issuing visas. In both cases access by these authorities is governed by national legislation.

The statistical report (eu-LISA, 2014b) provides figures on the numbers of accesses from April to December 2013, with a distinction between manual and automated processes. As shown in the following table, few countries were able to provide separate figures for the number of manual and automated accesses. Belgium, Hungary, Malta, the Netherlands, Poland and Sweden reported not using any automated data processing systems. Some countries (Estonia, Spain, Italy, Austria, Romania, Slovenia, Norway, and Switzerland) reported that they use automated data processing systems to a certain extent but that they cannot separate the data. The table also reveals notable differences between the various countries. It is hard to entirely understand these differences. Several countries that do not insert many alerts appear to use the system a lot. Other countries, especially Italy, enter a large number of alerts but do not access the system as frequently as others. It is also reasonable to suppose that not all countries understand the meaning of automated processes in the same way (no definition is provided at EU level). Moreover a high number of automated processes could be related to the use of automatic licence plate readers. This could explain the high figure in countries (such as Germany) with intense road traffic.

Table No. 4 – Numbers of accesses to SIS II from April to December 2013

	Country	Manual processes	Automated processes	Total
1	Spain			343,655,015
2	Germany*	2,148,704	237,047,720	239,196,424
3	Poland	128,744,291	0	128,744,291
4	Romania			64,593,255
5	Czech Republic	30,522,148	19,485,451	50,007,599
6	Bulgaria	3,038,194	45,266,498	48,304,692
7	Switzerland			43,028,560
8	France	38,869,603		38,869,603
9	Finland	23,532,727	14,604,394	38,137,121
10	Austria			37,623,689
11	Hungary	36,161,651	0	36,161,651
12	Netherlands	33,286,351	0	33,286,351
13	Estonia			28,477,900
14	Italy			25,229,296
15	Slovenia			23,897,408
16	Greece	21,982,593	1,473,291	23,455,884
17	Lithuania	22,559,080		22,559,080
18	Latvia	14,681,460		14,681,460
19	Sweden	13,887,614	0	13,887,614
20	Portugal**	6,988,878		6,988,878
21	Belgium	6,968,088	0	6,968,088
22	Slovakia	3,903,002	1,449,740	5,352,742
23	Norway			4,728,876
24	Denmark	2,727,000	1,500,000	4,227,000
25	Malta	1,053,529	0	1,053,529
26	Luxembourg	241,116	269,914	511,030
27	Iceland	292,192	179,121	471,313
28	Liechtenstein	106,801	307,320	414,121

* Partial data, for CUDs only alerts and flags are counted
** Figures only for the second semester 2013

Source: eu-LISA (2004b)

The retention period is limited to the time required to achieve the purposes for which the alert was entered. In addition, the Member State has a duty to review the need to keep the alert after three years. A Member State "shall, where appropriate, set shorter review periods in accordance with its national law" (Article 29 of Regulation 1987/2006).

[1.4] Implementation in Italy

The authorities in charge of the Schengen Information System are the SIS Office and the SIRENE Office. In Italy these two offices are located at two different branches of the Public Security Department of the Ministry of the Interior.

The N-SIS Division is a branch of the *Ufficio Coordinamento e Pianificazione delle Forze di Polizia* (Coordination and Planning Office of the Police Forces). This Office performs several tasks, aimed at increasing the efficiency of the police forces and improving cooperation between them in Italy and between the Italian law enforcement offices and those of foreign countries.

The Sirene Office is located at the *Direzione Centrale per la Polizia criminale* (Central Directorate of the Criminal Police).

This Central Directorate coordinates police investigations at the national level, collects and analyses data on criminal phenomena and is in charge of the international cooperation with foreign countries aimed at fighting organised crime.

The SIS interface

The police forces may access the SIS database through the SIS II native interface or the SDI (*Sistema Di Indagine*) interface, which is the national police information system. Access for queries is more frequent through the SDI because this is the commonly used police information system and offers more functionality than SIS II. Access for create/update/delete (CUD) an alert is possible for objects but not for persons. The two databases are hosted on different servers but, provided they have the appropriate privileges, users can access the data in SIS II through the SDI interface. Accessing the SDI and SIS involves different authorisation procedures, and the authorisation of users to access SIS is an exclusive competence of the N-SIS office. When law enforcement officers access the SDI interface, they enter or search the relevant information in the SDI and the system is able to link the information that has been entered or the search queries to the SIS database. Thus, if the information entered in the SDI is relevant for the SIS, the system automatically copies it in the SIS databases. If the person or object searched in the SDI is also present in the SIS, a link to the SIS alert appears. This happens if the officers searching the system have the required level of authorisation, otherwise no information appears. If the alert has been issued by another country and the officers need more information besides that included in the alert, they must contact the Sirene Office of their own country and request an exchange of information.

The issuing of alerts under Article 24 of the Regulation

The reasons for issuing an alert differ from one Member State to another. Reports by the JSA[9] and the 2013 eu-LISA report show a high level of discretion among Member States in issuing alerts. This is because Article 24 of the Regulation (and previously Article 96 of the CISA) provides the general framework but also allows National States considerable discretion.

Article 24 provides for the issuing of an alert in two situations: when a TCN has been subject to a measure involving expulsion, refusal of entry or removal that is accompanied by a re-entry ban and when a TCN could represent a threat based on the fact that s/he has been convicted in a MS of an offence carrying a custodial sentence of at least one year or there are serious grounds for believing that s/he has committed (or intends to commit) a serious criminal offence.

National immigration laws regulate several aspects of expulsion and refusal of entry. Moreover, penalties for crimes or the reasons why a person could be defined as a threat to public policy or public security are a matter of State sovereignty. This results in different methods of enforcement across Member States. In Italy, the local Police authorities we interviewed affirmed that the alerts envisaged under Article 24(2) had never been implemented and that they had only ever issued alerts based on Article 24(3) (see table below).

9 Over the years, the JSA has carried out several inspections on the implementation of The Schengen Convention. See http://schengen.consilium.europa.eu/reports/inspection-report.aspx?lang=en

Table No. 5 – Rules on the issuing of the alert for unwanted TCNs.

Article 96 Schengen Convention	Article 24 Regulation No. 1987/2006	Article 10 Legislative Decree No. 286/1998*
1. Data relating to aliens who are reported for the purposes of being refused entry shall be included on the basis of a national report resulting from decisions taken, in compliance with the rules of procedure laid down by national legislation, by the administrative authorities or courts responsible. **2.** Decisions may be based on a threat to public order or national security and safety which the presence of an alien in national territory may pose. Such may in particular be the case with: **(a)** an alien who has been convicted of an offence carrying a custodial sentence of at least one year; **(b)** an alien who, there are serious grounds for believing, has committed serious offences, including those referred to in Article 71, or against whom there is genuine evidence of an intention to commit such offences in the territory of a Contracting Party. **3.** Decisions may also be based on the fact that the alien has been the subject of a deportation, removal or expulsion measure which has not been rescinded or suspended, including or accompanied by a prohibition on entry or, where appropriate, residence, based on non-compliance with national regulations on the entry or residence of aliens.	**1.** Data on third-country nationals in respect of whom an alert has been issued for the purposes of refusing entry or stay shall be entered on the basis of a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law taken on the basis of an individual assessment. Appeals against these decisions shall lie in accordance with national legislation. **2.** An alert shall be entered where the decision referred to in paragraph 1 is based on a threat to public policy or public security or to national security which the presence of the third-country national in question in the territory of a Member State may pose. This situation shall arise in particular in the case of: **(a)** a third-country national who has been convicted in a Member State of an offence carrying a penalty involving deprivation of liberty of at least one year; **(b)** a third-country national in respect of whom there are serious grounds for believing that he has committed a serious criminal offence or in respect of whom there are clear indications of an intention to commit such an offence in the territory of a Member State. **3.** An alert may also be entered when the decision referred to in paragraph 1 is based on the fact that the third-country national has been subject to a measure involving expulsion, refusal of entry or removal which has not been rescinded or suspended, that includes or is accompanied by a prohibition on entry or, where applicable, a prohibition on residence, based on a failure to comply with national regulations on the entry or residence of third-country nationals.	**1.** The border police may refuse entry to foreigners who arrive at border posts without the legal requirements foreseen by this law. **2.** The refusal of entry is also ordered by the police authority for foreigners: **(a)** who are stopped at an entry point or immediately after entering the territory of the State while avoiding border controls; **(b)** who while being in the circumstance provided for under paragraph No.1, have been temporarily admitted on the grounds of public assistance needs. **3.** Should a carrier transport a foreigner to the national border without the required documents to enter the country, or a foreigner who must in any case be rejected, that carrier shall assume responsibility for immediately accompanying the foreigner back to the country that he or she came from. **4.** The measures provided for by article 10(2) and (2) do not apply in those cases envisaged by the existing provisions regulating political asylum, recognition of refugee status or the adoption of measures of temporary protection for humanitarian reasons. **5.** The rejected foreigner shall be granted due assistance at national borders. **6.** All rejections shall be recorded by the border police.

* Decreto legislativo n. 286/1998 Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero. Translation is by the author.

In Italy, the only authority that can issue alerts in accordance with Article 24 of Regulation No. 1987/2006 is the Immigration Office of the local Police Headquarters[10]. This office is responsible for issuing the alert, and for its subsequent deletion or any amendments as required.

In Italy the reasons for issuing an alert ensue from the implementation of the rules set forth under EU Regulation No. 1987/2007, the Return Directive (2008/115/EC) as transposed into Italian law and Italian immigration laws. There is no national legal text that clarifies the reasons for issuing a SIS alert. This complex legal framework made up of different European instruments and Italian legal rules is therefore subject to the interpretation of the local offices.

As regards alerts based on a removal measure (Article 24(3) of the Regulation), Italian immigration law does not provide for the issue of an alert as a consequence of a refusal of entry (Article 10 of the Italian Immigration Act). This is because in the Italian legislation there is no re-entry ban following a refusal of entry measure. In contrast, expulsion decisions are always accompanied by a re-entry ban and consequently an alert is always issued. This difference in the rules is problematic, since Italian Immigration law envisages a specific type of refusal of entry, namely delayed refusal of entry, which is difficult to distinguish from expulsion. Article 10 of the Italian Immigration Act provides for refusal of entry to migrants who are not entitled to stay within the territory of the Italian State. Delayed refusal of entry applies when migrants have avoided border controls and have been stopped upon entry or immediately after entering the country or are entitled to enter temporarily in order to be rescued (this is often the case with people entering Italy via Lampedusa or other areas of Sicily[11]). This last reason for delayed refusal of entry overlaps with one of the reasons for expulsion — envisaged under Article 13(1)(a) of the Italian Immigration Act — in cases where migrants have entered avoiding border controls and have not been removed.

In actual fact, regardless of whether the persons were rescued or landed on their own, the Authority has full discretionary power to choose between expulsion and delayed refusal of entry. The two procedures differ significantly; for the purposes of this discussion, expulsion implies the issue of a SIS alert whereas delayed rejection at the border does not.

If a case requires the issuing of an alert, Article 24(1) of the Regulation states that the decision to issue the alert be taken “on the basis of an individual assessment” (see table No. 5 above). This means that the authorities must always assess the concrete circumstances and evaluate whether or not the case warrants the issuing of a SIS alert (see Brouwer 2008b, Peers 2011). On the other hand, this could be interpreted as meaning that the issuing of one alert for a group of people based on a collective decision (e.g. a collective expulsion order) is prohibited.

10 Each province in Italy (there are 110 in all) has a police headquarters (“Questura”). Every Immigration office is responsible for the administrative decisions taken in respect of Third Country Nationals resident or present within the territory of the province.

11 Since the insurgence of the political crisis in the regions of North Africa, Italy has experienced a significant rise in the number of illegal immigrants arriving from the coasts of North Africa by boat. Lampedusa and other areas in Sicily are the main places of arrival.

According to the lawyers interviewed, alerts are, however, issued automatically after an expulsion order. The authorities interviewed confirmed this. The existence of an expulsion order is a necessary and sufficient condition for issuing an alert.

In addition, Article 21 of the Regulation states: "Before issuing an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant entry of the alert in SIS II". In practice, this proportionality assessment does not take place, since there is no discretionary power to issue an alert as a consequence of an expulsion order.

Both the individual assessment requirement and the proportionality clause therefore do not work as limitations for entering alerts in respect of TCNs. The issuing of the alert appears to be the consequence of a highly routinised procedure.

The retention period of alerts based on a removal measure (Article 24(3) of the Regulation) is calculated according to the length of the entry ban. In the interview the SIS office underlined that the retention period is calculated from the day on which the TCN leaves the Schengen territory (not just that of Italy). Thus, if there is no proof that the migrant has left the territory, the alert is maintained and renewed. This could partially explain the high number of alerts on persons in Italy.

Access to the database by the authorities

Access depends on the type of alert and level of authorisation. All five Italian law enforcement bodies (Carabinieri, Police, Guardia di Finanza, Polizia Penitenziaria and Corpo Forestale dello Stato) have access. The city police only have access to vehicle registration data. The Foreign Affairs Ministry has access according to Article 27(3) of the Regulation.

There is no national legislation regulating access to the databases. Decrees of the Chief of the Police establish who has access to the database. These are administrative acts, circulated internally. The list of authorities that have access to the database is not published but, in accordance with Article 31 of Regulation 1987/2006, it must be sent to the eu-LISA, which will ensure its annual publication in the Official Journal of the EU.

According to the authorities interviewed, there are 140,000 accounts with access to the Schengen Information System. Each access account refers to a name but not to a specific IP address; this means that the same person can have access from different computers. Data are not downloadable.

The right to information and the right of access, correction and deletion

According to Article 42 of the Regulation, Articles 10 and 11 of the Directive 95/46/EC regulate the right to be informed when an alert has been issued in respect of third country nationals for the purpose of refusing entry and stay, but there are some specific exceptions. The information must not be provided if the personal data have not been obtained from the TCNs or when provision of the information would involve a disproportionate effort or proves impossible. Moreover there is no right to information when the Third Country National already has the information or where "national law allows for the right of information to be restricted, in particular in order to safeguard national security, defence, public security and

the prevention, investigation, detection and prosecution of criminal offence". This leaves the doors open to a wide interpretation of these exceptions by the Member States. All the lawyers interviewed agree that most TCNs do not know anything about the alert, but they usually understand the meaning of the re-entry ban. Moreover, the information "shall be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert" (Article 42(1) of the Regulation). According to the lawyers and the immigration officers interviewed, the Third Country National receives a copy of the decision, that states the length of the re-entry ban but provides no specific information about the SIS alert.

Both Article 109 of the CISA and Article 41 of the Regulation provide for the right of access, correction and deletion. The Italian Data Protection Act[12] also establishes the rules for exercising these rights. The procedure is explained on the websites of the Ministry of the Interior and of the DPA[13].

Since 1 January 2004 the right of access, correction and deletion has been exercised directly through the Ministry for Home Affairs - Public Security Department - SIS Office. Prior to that date, the data subject could exercise these rights through the Data Protection Authority, which had the duty to request information from the Ministry for Home Affairs. According to the lawyers interviewed, lawyers exercise the right of access when they need to know if the existence of a SIS alert is hampering the possibility for the Third Country Nationals involved to receive a visa or a residence permit. Immigration lawyers seem not to consider data protection as a right that needs to be protected in itself. If the answer provided is unsatisfactory, data subjects may lodge a complaint with the Data Protection Authority. No complaint has ever been processed by the DPA.

According to the authority interviewed, the duty of information is the responsibility of the local authorities that issue the alert. The information is not centralised. The interviewees revealed that information about data protection aspects is almost never given. Expulsion orders always include information on the length of the ban on entry but nothing is written on the issue of a Schengen alert.

In the experience of the lawyers, foreign nationals are rarely aware of the issued alert. It is difficult to say whether this is due to their not being informed, or whether they were informed but did not realise the content of the information they were given or perhaps simply forgot it.

In addition, the lawyers reported a lack of information when an alert is deleted. When they ask for an alert to be deleted they are not always informed that it has been erased. In practice, what happens is that the foreign national receives the residence permit that could not previously be issued because of the alert. Consequently it is clear that the alert must have been cancelled or expired, although the lawyers did not receive any official communication in that respect.

12 Legislative Decree No. 196 of 30 June 2003.

13 The websites are available in Italian and English. See the following links: http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/servizi/come_fare/banca_dati_delle_forze_di_polizia/dati_schengen.html; http://www.garanteprivacy.it/home/attivita-e-documenti/attivita-comunitarie-e-internazionali/cooperazione-in-ambito-ue/schengen

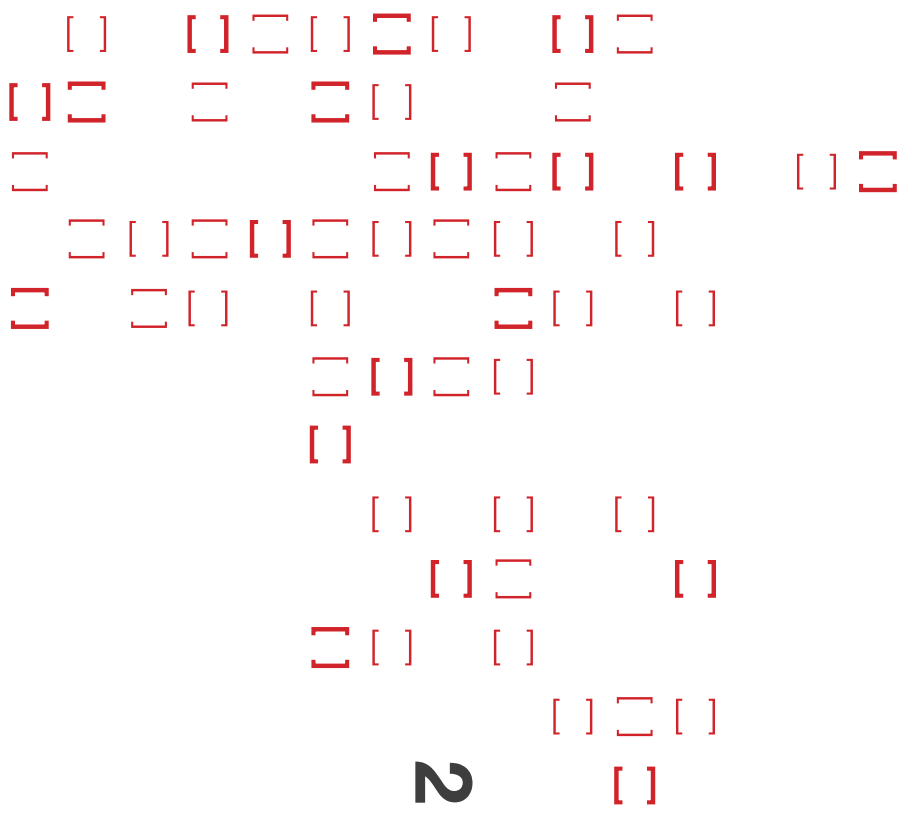
The interlinking of alerts

The interlinking of alerts is a useful tool for policing purposes because it permits the identification of associations between persons or persons and objects, such as documents or vehicles. Consequently, the authorities can take action based not only on single persons but on their link to alerts issued for other people or objects. This appears to be a particularly sensitive issue for TCNs alerted for their irregular status. The purpose of an alert as provided for under Article 24 should be limited to immigration control and the fight against illegal migration. In practice, linking two alerts adds a new and different purpose to the alert, compared to that for which it was originally issued: it also means that the TCNs involved are now targeted as "persons of interest" for investigative reasons. This appears to go beyond the scope of the SIS alert *ex* Article 24. According to Article 37 of the Regulation, the link is based on national law and it should be used "when there is a clear operational need".

The authorities at the central level underlined that this new functionality represents an investigative lead, but this does not in itself imply that there is "a clear operational need" to use SIS II in this way also as a database for policing purposes. There is a grain of truth in the statement, but this does not alter the fact that the data of thousands of undocumented migrants are in the database and can be used for other purposes, completely unrelated to that for which they were originally included, and thus affecting many people for whom there is no particular suspicion that they are involved in crimes.

Moreover there are no legal rules on the criteria for issuing a link. The N-SIS provides an operational manual that explains the meaning and the technical aspects of the alerts. This gives wide discretionary powers to the police authorities.

One of the two local immigration officers interviewed affirmed that they do not implement links or enter fingerprints into the database. However, this does not mean that the law enforcement officers do not collect these data. Fingerprints are included in other national databases. For example, the national AFIS (Automated Fingerprint Identification System) database stores fingerprints of all TCNs who apply for a residence permit, who are expelled and who are convicted of a crime. Moreover, the SDI database, which allows the addition of links and has more functionalities than SIS II, is used by the Italian police on a daily basis. It could therefore be argued that the full enforcement of a database that is more relevant at the international than at the domestic level is not yet regarded as a priority by some local police authorities.



EURODAC

Eurodac is the oldest EU biometric database. It was established in 2000 (Regulation No. 2725/2000) and became operational in 2003. Since then several proposals have been enacted by the Commission to comply with modifications in the Common European Asylum System and to extend access to new authorities. The present Regulation (No. 603/2013) is a revised version that takes these changes into account. It will come into force on 20 July 2015.

The original purpose was to help establish which Member State is responsible, in accordance with the Dublin Convention, for the reception of asylum applications. Eurodac was introduced to avoid so-called "asylum shopping", i.e. the risk that applicants submit several applications or travel across Europe in order to choose the Member State they prefer.

The 2013 Regulation adds a new purpose, described as follows: "This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the Central System for law enforcement purposes" (Article 1(2))". This will be discussed later on.

As for SIS II, the new European Agency eu-LISA is now in charge of the operational management of the database. Changes have also been made to the supervisory authority, which will bring it in line with the structure envisaged for SIS II. When the new Regulation comes into force, the Eurodac Supervision Coordination Group (composed of representatives from the DPAs of each of the participating States and the EDPS) will be replaced by the EDPS that will supervise all the data processing activities concerning the Eurodac. National DPAs will supervise the processing of data within the Member States.

The architecture of the system

The system consists of a computerised central fingerprint database (so called "Central system") and a communication infrastructure between the Central System and Member States, which provide an encrypted virtual network dedicated to Eurodac data. Each Member State has a single national Access Point. In Italy the authority in charge of Eurodac is the *Direzione Centrale Anticrime – Servizio di Polizia scientifica (*Central Department of the Forensic Police). At the sub-national level there are fourteen branches (the *Gabinetti Regionali di Polizia Scientifica* – The regional offices of the Forensic Police) which are the national Eurodac focal points.

The Eurodac focal points enter the fingerprint data and the system immediately processes the information and replies whether the fingerprints are already in the system or not. When hits occur (i.e. the fingerprints are already in the system because the person has already asked for asylum in another Member State), the Member States involved are likely to exchange additional data via a system called DubliNet. The data that are exchanged regard the individual's name, date of birth, nationality, photos and even information about the family and address.

Types of data stored and retention period

The new Regulation, like the previous one, defines three categories of people whose data can be stored in the system:

- Category 1: applicants for international protection over 14 years old;
- Category 2: TCNs or stateless persons over 14 years old apprehended in connection with the irregular crossing of an external border;
- Category 3: TCNs or stateless persons over 14 years old found illegally staying in a Member State, with the aim of checking whether the data subject has previously lodged an application for asylum in another Member State.

The data stored are specific for each category and the retention period varies. The table below summarises the new provisions, which contain just a few changes compared to the previous Regulation. They will come into force on 20 July 2015.

Table No. 6 – Data stored in Eurodac

	Category 1	Category 2	Category 3
Data stored	• fingerprint data (all ten fingers) • MS of origin, place and date of the application for international protection • sex • reference number used by MS of origin • date on which the fingerprints were taken • date on which the data were transmitted to the Central System • *operator user ID* • *dates related to transfers, removals or other specific movements of the persons according to Article 10**	• fingerprint data (all ten fingers) • MS of origin, place and date of the application for international protection • sex • reference number used by MS of origin • date on which the fingerprints were taken • date on which the data were transmitted to the Central System • *operator user ID**	No data storage. Fingerprint data may be transmitted to the Central system in order to check whether a person has previously lodged an application for international protection
Transmission of data to the Central System	Within 72 hours + additional 48 hours in specific cases *(under the previous Regulation there were no rules)*		Within 72 hours + additional 48 hours in specific cases (under the previous Regulation there were no rules)
Retention period	10 years from the date the fingerprints were taken	18 months *(under the previous Regulation it was 2 years)*	data shall not be recorded
Erasure of data	As soon as the State becomes aware of: • acquisition of citizenship;	As soon as the State becomes aware of : • acquisition of citizenship; • issuing of a residence permit; • departure from the MS	N.A.
Marking of data	*When a MS grants international protection, the applicant's record will be marked. The marked data will be available for three years for law enforcement purposes, as laid down in Article 1(2). Upon the expiry of the three year period the data will be blocked and then erased, when the retention period expires.*		

* info in italics was not included in the previous Regulation.

Source: Own elaboration of legal texts.

As the table above shows, under the new Regulation, when TCNs receive international protection[14], their data are not erased but marked so that they can be used for law enforcement purposes for three more years. Under the previous regulation, data of persons recognised as refugees[15] were blocked and hits concerning them were not transmitted. As soon as the retention period expired, the data were erased. The regulation made no provision for an asylum seeker was recognised as beneficiaries of subsidiary protection.

Data are entered in the system by the fourteen focal points within the Italian territory through the national AFIS (Automated Fingerprint Identification System) interface. Due to the specificity of recent immigration flows, this activity is most extensively performed by the focal points in the South of Italy, mainly in Sicily, where the number of people apprehended while unlawfully crossing the country's border is highest. Since the beginning of the recent operation called Mare nostrum[16] migrants' fingerprints have also been taken immediately on board the search and rescue ships.

As shown in the table below, at the end of 2013 2,378,008 data sets were stored in the Eurodac Central system. Data differ between countries due to geographic or geopolitical reasons (see the high number of Category 2 data in Italy and Greece) and rules on granting residence permits and citizenship that allow erasure. Moreover, as underlined in the 2013 Eurodac annual report, levels of blocked data vary among MS, several of which are working in order to comply with the Regulation[17] (eu-LISA, 2014, p.11). In fact the number of data sets that were blocked increased from 16,573 in 2012 to 56,013 in 2013.

14 Under the new Regulation this rule applies to any type of international protection (from refugee to subsidiary protection).

15 There were no rules for other types of international protection. Consequently the data remained in the system.

16 http://www.marina.difesa.it/EN/operations/Pagine/MareNostrum.aspx

17 The report underlines: "In several cases (in Cyprus, Denmark, France, Greece, Iceland, Latvia, Malta, Norway and Slovakia) fewer than 10 data sets had ever been blocked since Eurodac became operational in 2003, whilst in Germany, Sweden and the UK the figure was in the tens of thousands. In most cases where very few data sets had been blocked, the Member States informed the Commission that they intended to undertake projects to apply the Eurodac Regulation correctly in future as well as to conduct retrospective corrections. France informed the Commission that they would need to block around 110,000 cases, which would require a fifteen-month project to complete. Having each blocked 0 cases in 2012, in 2013 Belgium blocked 8,072 data sets, Cyprus blocked 15, France blocked 4,417, Greece blocked 76. Norway blocked 16,640 (which, they explained to the Commission, included historic cases that had previously not been blocked). Slovenia blocked 91 and Slovakia blocked 59 – both appearing to have resolved their previous problems concerning the blocking of data" (p.11)

Table No. 7 - Numbers of data sets in Eurodac on 31.12.2013

	Category 1	Category 2	Blocked Category 1
France	359,742	796	4,247
Germany	334,535	122	19,405
United Kingdom	256,692	456	29,712
Sweden	219,594	0	23,408
Italy	189,400	33,883	3,208
Belgium	152,615	16	7,972
Greece	121,315	28,888	76
Austria	118,177	197	7,463
Netherlands	90,384	30	4,714
Switzerland	82,625	4	5,897
Norway	76,601	89	16,558
Poland	52,128	48	556
Spain	32,895	7,645	489
Hungary	32,659	1,688	302
Cyprus	30,272	52	14
Finland	24,687	7	1,062
Denmark	22,953	0	0
Ireland	21,666	8	966
Slovakia	16,187	64	59
Czech Republic	14,935	0	434
Bulgaria	10,217	9,856	12
Romania	8,419	52	622
Malta	8,096	58	70
Luxembourg	7,652	2	9
Slovenia	3,793	48	98
Lithuania	2,122	5	57
Portugal	1,632	1	29
Latvia	784	0	0
Iceland	478	0	0
Croatia	335	38	0
Estonia	283	1	32
Liechtenstein	81	0	0
Total	2.293.954	84.054	127.471

Source: eu-LISA 2014a

Besides the above-mentioned changes, there are some relevant new provisions regarding the rights of data subjects and the rights of law enforcement authorities to access data.

The rights of law enforcement authorities to access data

For the new purposes that have been added under the 2013 Regulation, in 2015 Europol and the law enforcement authorities of the Member States will have access to the database for the comparison of fingerprint data with the data stored in the central system. According to Article 20, Member States' law enforcement authorities can only gain access if the search in other databases did not lead to the establishment of the identity of the data subject. The mentioned databases are national fingerprint databases, other Member States' databases, accessible through the network of national DNA databases established by the Prüm Decision (2008/614/JHA), and the Visa Information System (VIS) database.

In addition, access has to be:

- "necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences" which means that there is "an overriding public security concern which makes the searching of the database proportionate";
- "necessary in a specific case", which means that systematic comparisons are not allowed; and
- based on reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question.

As outlined in the table above, this right of access includes the right to access the fingerprints of people granted recognition as asylum seekers for three years.

The law enforcement authorities with power to access such data are designated at MS level and, according to Article 5 of the 2013 Regulation, must be authorities that are "responsible for the prevention, detection or investigation of terrorist offences or other serious criminal offences".

The rights of the data subject

Article 29 of the 2013 Regulation establishes the rules governing the rights of the data subject. It replaces Article 18 of the 2725/2000 Regulation, adding some new obligations for data controllers. This is a consequence of the findings of the inspection carried out by the Eurodac Supervision Coordination Group in 2009. The inspection identified a need for a general improvement in the quality of information given to the data subject. In particular, it reported that asylum seekers (Category 1) are provided with better information than illegal border crossers (Category 2). Some Member States give information in writing, others only orally. Information on data protection is generally included in the information regarding the whole asylum procedure, and no attention is paid to providing this information in an accessible and understandable language. Finally the moment the information is given differs among Member States (see Eurodac Supervision Coordination Group, 2009).

The 2000 Regulation did not set out any rules on the form of information, whereas the 2013 Regulation stipulates that a person must be informed "in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand". Moreover a common leaflet, clear and simple, written in a language that the person concerned can understand (or is reasonably supposed to understand) has to be drawn up in such a manner as to enable Member States to complete it with additional Member State-specific information.

The content of the information given and the right to access, correct and delete data are the same as those envisaged under the 2000 Regulation. It is worth underlining that the above-mentioned inspection report refers to very few requests to access data submitted by data subjects and "in general the countries where such requests are being presented are the same ones in which the information which is being provided to data subjects is deemed to be complete, adequate and in compliance with Eurodac Regulation" (Eurodac Supervision Coordination Group, 2009, p. 15). During the interview, the Italian DPA stated that they have never received any requests.

Successful transactions and hits

The annual report on the activities of Eurodac shows the number of so-called successful transactions, namely data transactions, which have been correctly processed, without rejection due to a data validation issue, fingerprint errors or insufficient quality.

This number represents the times a member State has sent fingerprint data to the system and the data were successfully processed by the system. As the table clearly shows, the use of Eurodac is increasing, albeit not steadily. However, in the last 3 years the number of transactions has grown significantly.

Table No. 8– Successful transactions from 2003 to 2013

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Cat 1	246,902	232,205	187,223	165,958	197,284	219,557	236,936	215,463	275,587	285,959	354,276
Cat 2	7,857	16,183	25,162	41,312	38,173	61,945	31,071	11,156	57,693	39,300	48,276
Cat 3	16,814	39,550	46,299	63,341	64,561	75,919	85,554	72,840	78,753	85,976	106,013
Total	271,573	287,938	258,684	270,611	300,018	357,421	353,561	299,459	412,033	411,235	508,565

Source: eu-LISA 2014a

Hits indicate matches. When a hit occurs it means that the searched fingerprints were already in the system. There are three categories of hits:

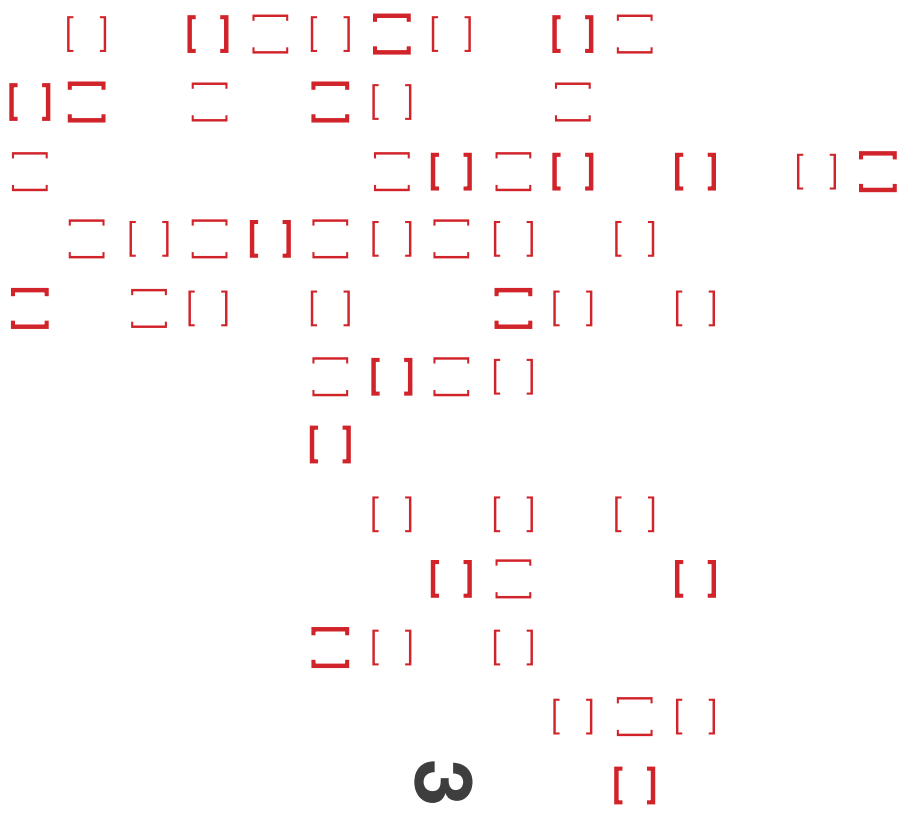
Cat. 1 against cat. 1, asylum seekers' fingerprints against asylum seekers' fingerprints. This shows how many migrants have repeatedly applied for asylum in the same country (local hits) or in another one (foreign hits);

Cat. 1 against cat. 2, asylum seekers' fingerprints against those of persons apprehended while irregularly crossing an external border. This shows how many persons who irregularly crossed the border later lodged an asylum application and where they did so;

Cat. 3 against cat. 1, fingerprints of irregular migrants found in a MS against asylum seekers' fingerprints. This shows how many irregular migrants previously requested asylum and where.

According to the data published by eu-LISA (2014a), Italy is the country with the highest number of hits. This means that when other countries enter fingerprints and find a match, the data are already in the system because the same fingerprints have already been entered by Italy[18].

18 10 % of the hits on cat. 1 against cat. 1 and on cat. 3 against cat. 1 and about 50% of hits on cat. 1 against cat. 2 are Italian.



Current and forthcoming developments

Several other databases and information-sharing schemes are currently under implementation or discussion, besides SIS II and Eurodac. All of these instruments have a twofold objective: to improve border management and counter serious crime. None of them have the exclusive aim of border control (with the sole exception of API, the Advanced Passenger Information system). Almost all of them have multiple purposes, either from the outset or having acquired more purposes during their development or implementation, and are aimed at managing borders, fighting serious crimes and enhancing judicial cooperation. Some of the schemes involve exchange of data with third countries, others explicitly forbid this exchange.

It is beyond the scope of this research to provide an overview of all of these, but it is worth underlining the main features of some of them, as they have many characteristics in common with SIS II or Eurodac or are closely linked to the Italian context.

The first database, already in an advanced phase of implementation, is the Visa Information System (VIS)[19], which allows the exchange of data between Member States on short-stay visas. Like SIS II and Eurodac, the architecture of this system is composed of a central database, a national interface and a communication infrastructure between the Central VIS and the national interfaces. In particular SIS II and VIS share the same communication system and system for processing biometric data. Operational management is performed by eu-LISA and EDPS and DPAs supervise the system.

The VIS has a very broad purpose. It aims to improve the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and decisions, in order to:

- facilitate the visa application procedure;
- prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application (i.e. asylum shopping);
- facilitate the fight against fraud;
- facilitate checks at external border crossing points and within the territory of the Member States;
- assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence in the territory of the Member States;
- facilitate the determination of the MS responsible for an asylum application lodged in one of the Member States;
- contribute to the prevention of threats to the internal security of any of the Member States.

19 VIS has a dual legal basis, formerly falling under the first and third pillars: Regulation No. 767/2008, concerning the exchange of data between Member States on short-stay visas and Council Decision 2008/663/JHA concerning access by several authorities for the purposes of preventing, detecting and investigating terrorist and other criminal offences.

It clearly links the implementation of the common visa policy with security interests of the EU and MS.

The database contains ten fingerprints[20] (as does Eurodac) and a digital photograph of the visa applicant along with data provided in the visa application form[21].

Visa authorities are the only authorities allowed to enter the relevant information but a wide range of authorities can have access for consultation (from the border control authorities and those performing checks within the country to the designated authorities of the MS for the purposes of the prevention, detection and investigation of terrorist offences or other serious offences). Searches may be performed for the purposes of verification and identification: verification consists of checking that the fingerprints scanned at the border crossing point correspond to those associated with the biometric record attached to the visa; identification consists of comparing the fingerprints taken at the border crossing post with the contents of the entire database.

Similarly to SIS II and Eurodac, the VIS envisages the rights of data subjects to information, access and deletion.

Similar to the VIS are the databases in the Smart Border Package[22]. This proposal provides for the establishment of an Entry-Exit System (EES) and a Registered Traveller Programme (RTP). The EES, modelled on the US-VISIT system, is aimed at identifying overstayers[23], by registering the time and place of entry and exit of all TCNs who travel to the European Union for a short stay (estimated to stand at around 150 million people every year). When a person overstays, the system sends an alert to the competent authorities to enable them to take the appropriate measures (the proposal does not specify the measures to be taken, which could amount to a fine or the issuing of an expulsion order).

The aim of the RTP is to speed up border crossing for frequent, pre-vetted, pre-screened TCNs, who are estimated to number between 4 and 5 million. The system would allow these travellers to cross borders through Automatic Border Control Gates.

Both of these proposed new systems will collect alphanumeric and biometric data. Like SIS II, they will be under the operational management of a new European Agency established for the operational management of large-scale IT systems and they will share the same communication and biometric data processing systems.

---

20 Article 9 of Regulation No. 767/2008 refers to the Common Consular Instructions that require the fingerprints of all ten fingers to be taken.

21 These data include: surname, name, sex; date, place and country of birth; current nationality and nationality at birth; type and number of the travel document, the authority which issued it and the date of issue and of expiry; place and date of the application; type of visa requested; details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay; main destination and duration of the intended stay; purpose of travel; intended date of arrival and departure; intended border of first entry or transit route; residence; current occupation and employer; for students: name of school; in the case of minors, surname and first name(s) of the applicant's father and mother (Articles 9 and 10 of Regulation No. 767/2008). When the visa is issued further data concerning the visa will be added.

22 http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228_01_en.htm

23 Those who enter the EU with a valid travel document but then become unlawful migrants because they do not leave the EU territory when their authorisation to stay expires.

Specifically relevant for the Mediterranean area is EUROSUR (the European Border Surveillance System), which became operational in December 2013. Its aim is to facilitate the exchange of information and cooperation between Member States and Frontex[24] and - in certain cases and on the basis of bilateral and multilateral agreements - with third countries. The purpose of the exchange of information is the empowerment of the "ability to monitor, detect, identify, track and understand illegal cross-border activities in order to find reasoned grounds for reaction measures on the basis of combining new information with existing knowledge, and to be better able to reduce loss of lives of migrants at, along or in the proximity of, the external borders" and the "ability to perform actions aimed at countering illegal cross-border activities at, along or in the proximity of, the external borders" (Article 3 of Regulation No. 1052/2013). Information is obtained from several sources (national border surveillance systems, sensors, patrol activities, drones, etc.) and is collected and analysed in order to obtain pictures of the situation organised in three different layers:

- an events layer, which contains events such as unauthorised border crossings, detected cross-border crimes, suspect objects or persons, crisis situations;
- an operational layer, which contains information on the authorities involved in border activities and on weather conditions;
- an analysis layer, which contains information such as indicators, risk analysis, maps. In the proposed version of the regulation[25] it also includes migrant profiles.

The purpose of EUROSUR is not to collect personal data, but given the wide range of information collection activities performed and the use of advanced technologies such as drones and smart cameras, it could result in more collection and processing of personal data than originally foreseen.
Moreover EUROSUR is one of the surveillance systems that will be interoperable within the Common Information Sharing Environment (CISE)[26] in the EU maritime domain. The aim of the CISE system, which is currently under development, is to enhance the exchange of information between national authorities and EU agencies on maritime surveillance. Flows of migrants to the Schengen Area via the Mediterranean Sea are one of the areas of interest (for details see the recent COM 2014 451 final[27]).

24 Frontex is the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. It was established by Regulation No. 2007/2004.

25 Proposal for a regulation of the European Parliament and the Council Establishing the European Border Surveillance System (EUROSUR) COM(2011) 873 final

26 http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance/index_en.htm

27 Communication from the Commission to the European Parliament and the Council. Better situational awareness by enhanced cooperation across maritime surveillance authorities: next steps within the Common Information Sharing Environment for the EU maritime domain

4

Discussion: some reflections on profiling and automated decision making in the context of Italian border control

The EU databases and in general the use of technology in border control have been analysed from several points of view. In particular, the lack of transparency in the decision making process and the lack of democratic control over these information systems have been underlined by several authors (Parkin, 2011; Brouwer 2008a; Petermann et al. 2006). Although this fieldwork did not analyse these aspects, its findings do confirm a lack of information and understanding among the experts, in particular lawyers, who work in the field of immigration. They only take data protection issues into consideration when problems arise which affect the possibility of their clients being able to stay in the country. None of them ever consider data protection as a right in itself that needs to be enforced.

Besides this lack of awareness among experts, the results of this fieldwork revealed that data protection rights are clearly established on paper but not fully enforced in practice.

TCNs are often unaware that their data are being collected, even though this is done according to the law, they are not properly informed about the fact that they are being registered and what this registration implies and how they can dispute it. Moreover, data are collected lawfully but - as discussed more in detail later on in this paper - the purpose of their collection changes over time. New authorities have access to the data, the retention of data is extended and new purposes are added that justify the use of previously collected data. In conclusion, it would not appear to be an exaggeration to say that the spirit of data protection principles is undermined by these databases.

In general, these databases allow the storage of a huge amount of information about a growing number of people or objects and aim to make it easier for countries to exchange information. However, the findings of this fieldwork have underlined that the effective implementation of all of their functions (such as the addition of fingerprints and links between alerts) has not yet been achieved. Bureaucracies need time to implement new functions and this appears to be one of the biggest obstacles to their effectiveness.

Notwithstanding this, the addition of new functions (in the case of SIS II) and new purposes (both for SIS II and Eurodac), and the features of forthcoming databases (EES and RTP), have blurred the distinction between border control, counter terrorism, the fight against transnational crimes and migration management.

This confusion is strictly related to the power of the law enforcement authorities at EU (Europol) and Member States level to access data.

The original collection of data for a well-defined and narrow purpose has been combined with further storage for new purposes.

The clear-cut example is Eurodac. This database, originally created to better implement asylum policy, will store data about persons who have been granted refugee status and grant access to law enforcement agencies. It appears clear that these data will not serve the original purpose (to identify the competent state for the asylum procedure) but rather plant a seed of suspicion as to the motives of people asking for international protection (innocent and even vulnerable people) whose data are stored with a view to fighting future crimes, even though there is no indication that those people whose data have been withheld will ever commit a criminal offence.

The original nature of SIS II has also changed. From being a tool to guarantee the enforcement of the Schengen Agreement, it is slowly moving towards becoming a tool for investigative purposes. This transformation is now at the embryo stage. But an extensive interlinking of alerts and the collection of fingerprint data in a format that allows comparison will modify the present – certainly limited – use of the database. The VIS, RTP and EES clearly have a multi-purpose nature and this clearly indicates that the trend is towards multi-purpose databases.

Moving closer to the specific issue of this paper, all the EU databases (existing and forthcoming) share the common feature of being tools aimed at classifying people (i.e. TCNs and travellers) into various categories, whose access to rights is differentiated. The aim of this classification is to make it easier to control borders, or better to say, control mobility of the target population.

Those identified as trusted travellers (and who will be included in RTP databases in the future) will be granted the highest degree of mobility and given the green light, thanks to previous checks, which will allow them to be included in the databases.

Those with criminal records or bans on entry to EU territory will be given the red light. They are the Third Country Nationals included in SIS II.

Those whose motives are questionable, whose data are requested and held for future use, get the amber light. This is the case of those whose data are entered in the EURODAC database and those who apply for a visa. All such TCNs are looked upon as possible troublemakers, and their data are kept well beyond the time needed for the administrative and purely migration-management purposes for which they were collected. Amber is also the colour assigned to potential overstayers who will be included in the forthcoming EES.

As already suggested in the introduction, owing to this differentiation, these databases are the perfect tool for regulating personalised borders, where controls can be performed at multiple sites because the border is embodied in the traveller.

In order to be efficient, this personalisation certainly finds a good ally in automated decision making and profiling systems.

The databases in their current forms contain some traces of automated decision making. In the daily use of SIS II it appears clear that law enforcement officers enter the alert without any individual assessment. The alert is the automatic consequence of the administrative act of expulsion.

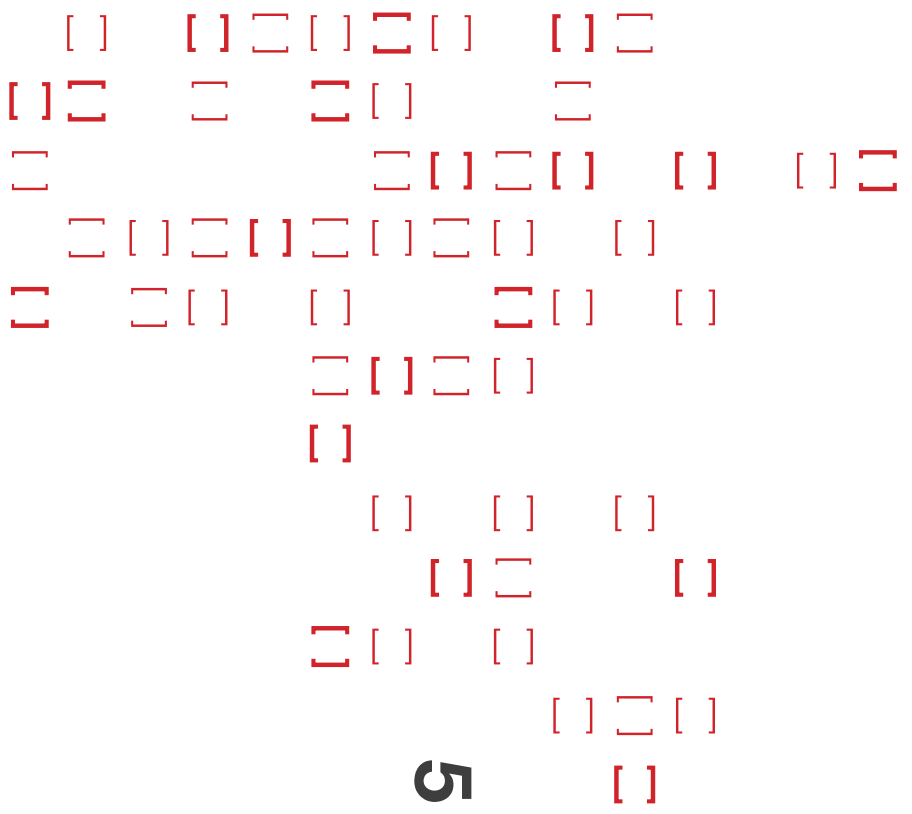
Moreover the new function of the interlinking of alerts represents a fruitful tool for profiling purposes. It allows the assessment of the person to be performed on the basis of the links between that person and other people and/or objects.

The evolution of the situation over the last ten years has shown the information stored in these databases to be of a rather dynamic character. Information that might have been gathered for a very limited purpose can be turned into valuable knowledge when combined with other data or when used for different purposes (and this is clearly the case of the extension of access to law enforcement officers).

Moreover, the EUROSUR system and the CISE currently under development are clearly directed towards the exchange of information with the aim of building new knowledge from the available information[28].

Profiling is certainly not a common practice in the present use of databases but the classification of the population according to different risk levels through the creation of new databases and the development of new information exchange schemes makes border control an area of increasing interest for profiling and automated decision making.

28 Maritime borders are affected by EUROSUR and CISE. However, other EU projects - such as PNR (passenger name record) have made it clear that land and air borders are also increasingly reliant on the exchange of information for border control.



References

[Besters, M. and Brom, F. (2010) "'Greedy' information technology: the digitalization of European migration policy", European Journal of Migration and Law, 12(4): 45-70.

[Bigo D et al. (2012) Evaluating current and forthcoming proposals on JHA databases and a smart borders system at EU external borders, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462513/IPOL-LIBE_ET(2012)462513_EN.pdf

[Boehm Franziska (2012) Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level, Springer

[Bosworth, M. (2008) 'Border control and the limits of sovereign state', Social & Legal Studies, Vol. 17, No. 2, pp. 199-215.

[Broeders Dennis and Hampshire James (2013) Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe, in Journal of Ethnic and Migration Studies, vol 39, No. 8, pp. 1201 - 1218

[Brouwer Evelien (2007) "The use of biometrics in EU data bases and identity documents. Keeping track of foreigners' movements and rights", in Juliet Lodge (ed.), Are you who you say you are? The EU and Biometric Borders, Nijmegen: Wolf Legal Publishers.

[Brouwer Evelien (2008) Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System. Leiden and Boston: Martinus Nijhoff.

[Brouwer, E. (2008b) The Other Side of the Moon: The Schengen Information System and Human Rights – A Task for National Courts, CEPS Working Document, No.288, April 2008.

[Coombs, M. (2004) Excisions from the Migration Zone. Policy and Practice, http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/J4TB6/upload_binary/j4tb66.pdf;fileType=application%2Fpdf#search=%22library/prspub/J4TB6%22> (Accessed 6 August 2014)

[Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

[Council Decision 2008/663/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences

[Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention

[De Nationale Ombudsman (2010) No entry. Investigation of the registration of foreign nationals in the Schengen Information System and the provision of information in this connection, available at http://www.nationaleombudsman.nl/sites/default/files/report_2010-115_no_entry.pdf

[EDPS Opinion of 19 October 2005, 2006/C 91/11, available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2005/05-10-19_SISII_EN.pdf

[Ericson, R. and Haggerty, K. (1997), Policing the Risk Society, Oxford University Press, Oxford

[EU Lisa (2014) Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/docs/eulisa_report_eurodac_en.pdf

[EU Lisa (2014b) SIS II – 2013 Statistics, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/docs/20140709_sis_ii_stats_2013_public_en.pdf

[EU Regulation No 1987/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

[EU Regulation No 767/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

[EU Regulation No. 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems

[Eurodac Supervision coordination Group (2009) Second inspection report, available at https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac

[Feeley, M. and Simon, J. (1992) 'The new penology: notes on the emerging strategy of corrections and its implications', Criminology, Vol. 30, No. 4, pp. 449-474.

[Ferraris V. (2014) Trapped by stand-by borders, in International Journal of migration and border studies, n.1, forthcoming

[Karanja, S. (2008) Transparency and Proportionality in the Schengen Information System and Border Control Cooperation, Leiden, Martinus Nijhoff.

[Koslowski Rey (2011) The evolution of Border Controls as a Mechanism to Prevent Illegal Immigration, Washington, DC: Migration Policy Institute, available at http://www.migrationpolicy.org/research/evolution-US-border-controls-illegal-immigration

[Lodge Juliet ed. (2007) Are you who you say you are? The EU and Biometric Borders, Wolf Legal Publishers.

[Lyon, D. (2007) 'Surveillance, Security and Social Sorting: Emerging Research Priorities', International Criminal Justice Review. 17 (3), pp. 161-170.

[Lyon, D. (2009) Identifying Citizens ID Cards and Surveillance. Cambridge: Polity.

[Parkin Joanna (2011) The difficult road to the Schengen Information System II: the legacy of laboratories and the cost for fundamental rights and the rule of law, available at http://www.ceps.eu/book/difficult-road-schengen-information-system-ii

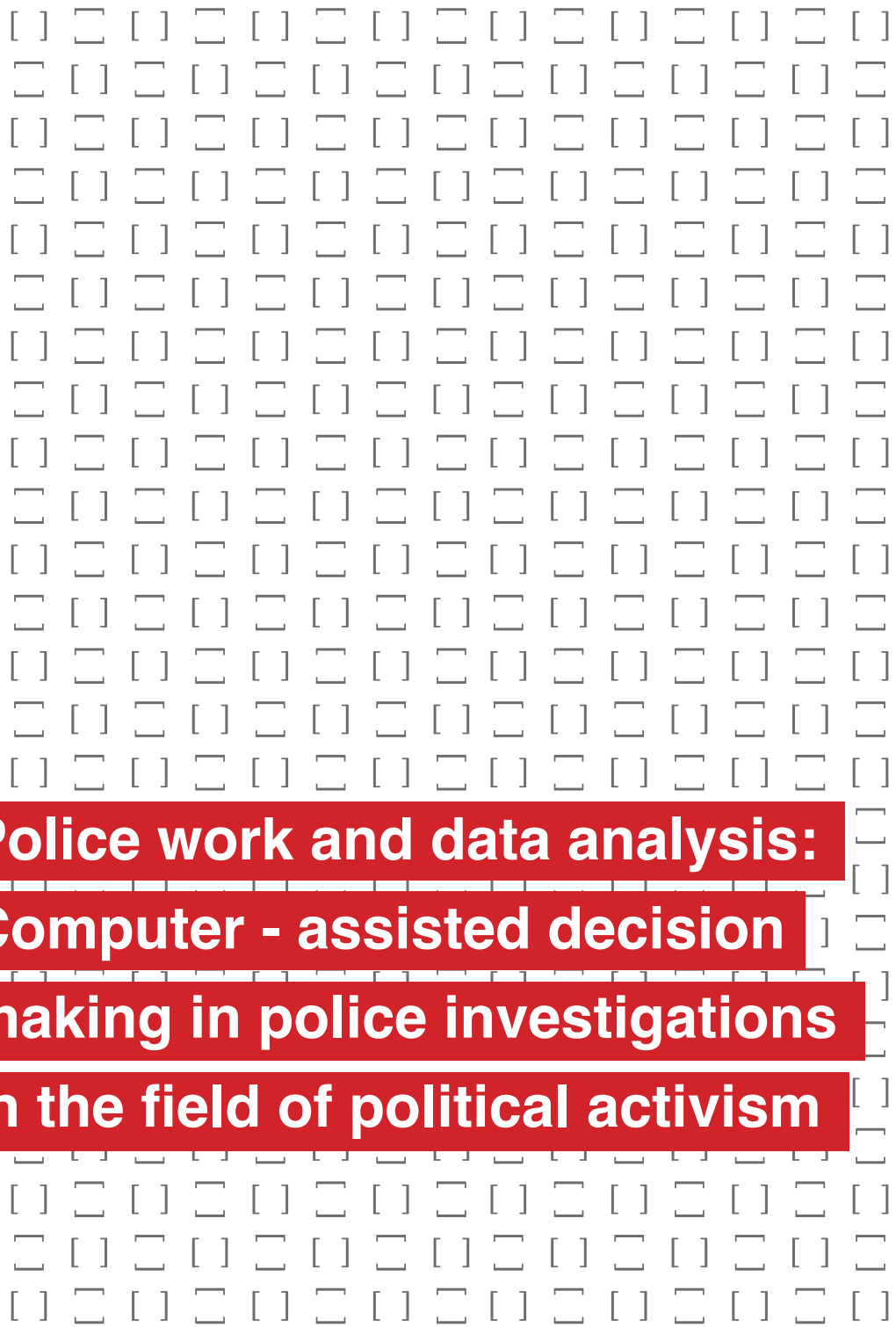
[Peers Steve (2011) EU Justice and Home Affairs Law, Oxford University Press.

[Petermann Thomas, Arnold Sauter & Constanze Scherz (2006) Biometrics at the borders. The challenges of a political technology, International Review of Law, Computers & Technology, vol. 20, No. 1-2, pp. 149-166.

[Valverde, M. and M. Mopas, (2004) "Insecurity and the Dream of Targeted Governance," in W. Larner and W. Walters (eds.), Global Governmentality: Governing International Spaces, London: Routledge.

[Weber, L. (2006) "The shifting frontiers of control", in Pickering, S. and Weber L. (Eds.). Borders, mobility and technologies of control, Springer, Dordrecht, pp. 21-43.

[Zolberg (1999) "The Great Wall Against China: Responses to the first Immigration crisis, 1885-1925", in Jao Lucassen and Leo Lucasses (eds) Migration, Migration History, Migration. Old Paradigms and new perspectives, pp. 291- 315



Police work and data analysis: Computer - assisted decision making in police investigations in the field of political activism

Niklas Creemers and Daniel Guagnin
Center for Technology and Society
Technische Universität Berlin

prof[i]ng
PROTECTING CITIZENS' RIGHTS FIGHTING ILLICIT PROFILING

Executive summary

This report presents research results about the collection, storage and evaluation of digital information by German police authorities, especially in their efforts to combat so-called political extremism and/or so-called politically motivated crime. An analysis is also provided of how the use of digital information, databases and data analysis tools changes police practices and of the effects these changes have on civil rights as well as fundamental democratic values.

A case study on the role of digital processing in police work was carried out based on literature and document research. For this purpose, a sample of experts from the areas of police, law, data analysis software development and political activism were interviewed. The interviews were carried out as open guided interviews. The material was evaluated based on the methods of qualitative content analysis.

Digital data that is stored in databases and its organisation and evaluation with the help of (partially) automated data analysis software has become increasingly important for police work over the past decades. This trend will continue. On the one hand, by digitising their daily work, the police can provide larger amounts and new forms of information for criminal investigations and preventive purposes for addressing threat and averting danger. On the other hand, (partially) automated data analysis methods make it possible to correlate this new type of information in a way that it was not possible during the pre-digital age of conventional police procedures for knowledge discovery and establishing suspicion. By being able to connect different types of information from different databases, the police are able to acquire new types of information. This innovation is an advantage above all when investigating network-based activities. In addition, databases allow to exchange digital information, based on certain legal conditions, on a continuous basis and across agencies, on a national and even a European or international level. An expansion of the possibility to use cross-agency and cross-national databases for legal purposes is being intensively discussed on both these levels.

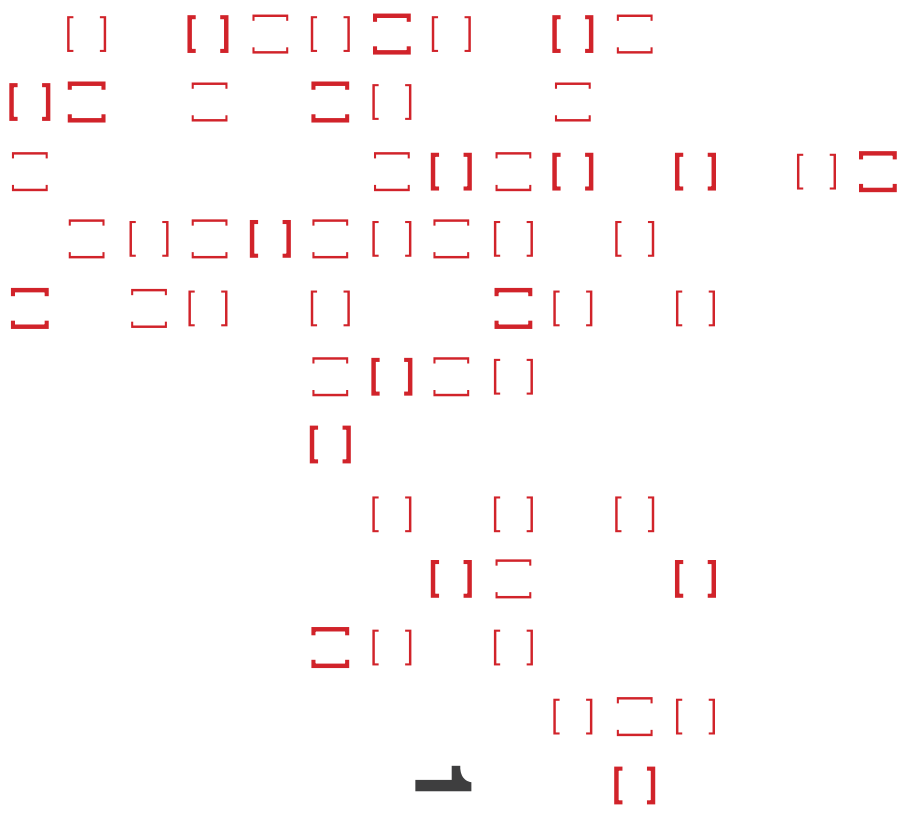
New possibilities for knowledge discovery and constructing suspicion are leading to fundamental changes in police work, which can also have an impact on the preservation of the fundamental rights of citizens and the exercise of fundamental democratic values. The large amount of data that police can access in comprehensive databases or through publicly accessible online sources jeopardises the rights of citizens to the protection of their private data as well as protection of the core areas of their private life. This is because these new technical possibilities permit far-reaching intrusions in this fundamental right with little effort. Therefore a critical examination must be carried out regarding the proportionality of data processing and the effectiveness of the given legal framework.

This case study provides evidence that the new knowledge available to the police is characterised by an increasing uncertainty regarding its quality and validity, so that new processes for checking this knowledge and for documenting the investigation procedures must be established and used in the training and further education of officers.

The interviews suggest that insufficient documentation in this regard can lead to an asymmetric level of information in the evidence. This could result in a structural disadvantage for the accused during a criminal case.

Furthermore, new methods of collecting information and the (partially) automated construction of knowledge facilitate non-transparent processes of the construction of suspiciousness. It is difficult for parties concerned in the preliminary investigations to understand how the information about them is compiled, stored and used and which consequences this could have. Due to the expanded possibilities for data collection, storage and analysis, the right to the self-determination of personal data is infringed in a qualitatively new manner and partially in a disproportionate manner.

The possibility of being able to store information for a long period of time and evaluate it in a (partially) automated manner benefits a future-oriented approach to police work, especially in network-based areas, such as in the case of the fight against so-called politically motivated crime. Here, the assessment of groups and individuals, based on information as it is stored in databases, such as the “politically motivated crime left” database, becomes more important. This leads to police measures against people or groups that can possibly be classified as dangerous based on a partly probabilistic affiliation to certain networks. The attention of the investigator is shifted from concrete acts to potential dangers and consequently, suspicion is abstracted and possibly de-individualized. The decontextualisation of information that is made available in databases, and its recontextualisation through database queries is beneficial to the evaluation of evidence for everyday activities or legitimate political activities as an element of construction of suspiciousness. In light of the increasingly non-transparent processes of establishing suspicion and the resulting police measures regarding politically active citizens there is, in this regard, an incipient uncertainty in the area of political engagement, which limits the exercising of civil rights and fundamental democratic values thereby undermining a critical culture of political protests.



Introduction

The case study presented here by the Technische Universität Berlin (TUB) analyses the application of databases and data analysis tools by the German police authorities. The focus of this study lies on their use in the fight against so-called politically motivated crime. Police investigations in this area involve a wide scope of political activities, which range from civil society engagement to politically motivated crime. They take place in a societal area that is constituted on the basis of exercising rights such as freedom of opinion, freedom of assembly and freedom of association. Consequently, this area is particularly susceptible to having these civil rights and fundamental democratic values violated. There is a risk that legitimate - and from a democratic point of view desired and necessary - political activities will come into the focus of the police and that therefore these activities will be limited. Furthermore, the activities by authorities to collect and use data affect the fundamental right of data protection, of informational self-determination and the protection of the core areas of private life.

After describing the methodical basis of the case study (section 1), section 2.1 will show which personal data can be collected and stored by police authorities and which databases are used in order to manage the information and make it available for software-based data analysis (section 2.2). Furthermore, the technological capabilities of the data analysis instruments that the police have available and their integration in police practices will be described (section 2.3). On this basis, an analysis will be carried out about the importance that databases and data analysis tools have when defining suspicion and which technology driven transformations this involves. The challenges that these changes represent for the given legal framework and how the fundamental democratic values are compromised will also be described (section 3).

[1] Data processing and suspiciousness in police practices: a case study

The case studies carried out in the PROFILING project substantiate the question concerning the societal consequences of the application of automated data analysis technologies when used in specific social contexts. In addition to the case studies in Italy and Romania, which address the use of profiling within the scope of border security and e-commerce, the case study carried out by TUB investigates the use of data, databases and data analysis tools by the German police. Here the focus is on combating so-called politically motivated crime.

[1.1] Police work in view of the increasing importance of data

On the 10th anniversary of the first German federal police information system INPOL, Hans-Georg Stuff declared the following at the autumn conference of the German Federal Criminal Office (Bundeskriminalamt, BKA) in 1982:

> *"Criminal police activities - both from preventive as well as from repressive points of view - have always required collecting, evaluating and using information, that is, data. In order to perform its tasks the criminal police has, and always has, created its own information collections" (Stuff 1982, 221).*

If the collection and evaluation of information for criminal prosecution and avoidance consequently represent a historical constant in police work, it can be assumed that the possibilities and forms of acquiring information and producing knowledge will be conditioned by the application of specific technologies, and that consequently technological change will involve a change in police work and its focus as well as its access to its object, the population. Thomas Scharff refers to the introduction of written documents in criminal proceedings in the Middle Ages: "[…] [T]he increase in the pragmatic written form since the middle of the 12th century, i.e. the use of writings in administrative and other contexts, also increased the repression of dissenters in various areas." (Scharff 2008, 255-256) Nikolas Rose determined that the discovery of statistics created specific practices for the acquisition of information and knowledge, which provided the knowledge of new forms and therefore created new methods for controlling the population. (Rose 1991) Consequently, the increased use in police work of computerised methods for acquiring information as well as for managing and evaluating it causes changed knowledge practices which then change the practices of establishing suspicion. (See Cope 2004, Oevermann et al. 1994, Reichertz 1994)[1] This reconfiguration of police work is also a part of a societal digitisation process,

1 For a comprehensive overview of how police work has been transformed by the increased implementation of information technologies and the related challenges that have resulted, also refer to Ericson/Haggerty: 1997, Chan et al.: 2001, Manning: 2008 and for the German speaking area, Bundeskriminalamt 1982, Busch et al.: 1988, Heinrich: 2007.

which creates a constantly increasing body of knowledge about people, groups, institutions and social processes due to the computerisation of information and communication. In police work, this therefore increases the significance of digital data as an information source and of (partially) automated data management and data analysis tools. (See Koops, 2009, van Brakel/de Hert, 2011) to access these information (See Harcourt, 2014).

In view of the research results obtained from the PROFILING project, we can assume that this trend leads to changes in acquiring, storing and evaluating information by the police and produce new forms of knowledge. (See Ferraris et al. 2013a; Guagnin et al. 2013) This also involves a reconfiguration of the construction of suspicion in the practices of law enforcement authorities, because more information as well as new types of information can and must be involved in investigations. Furthermore, by using databases to organise data storage, also the form in which the information must be transformed and its contextual embedding changes. This leads to new demands on the interpretation of information. (See Cope, 2004; Oevermann et al. 1994; Reichertz 1994) This also applies to handling the results from (partially) automated data analysis, how they are dealt with by the police, for example during preliminary proceedings. Furthermore, the collection and (partially) automated evaluation of large, new amounts of data makes new object areas visible for the police in certain work areas and addressable for police measures, which were difficult to access prior to computerisation. This applies in particular when confronting network-based, long-term phenomena, such as the so-called politically motivated crime. New forms of the construction of suspicion lead to an alteration in how the population is accessed, in which the suspicion describes the framework that justifies the measures of the police towards people or groups. (See Schulz, 2001, 1-2) Thereby, the intensity of the suspicion determines which measures can be implemented. Based on the concept of suspicion, the population can be accordingly classified into zones of different levels of intensity of suspicion in police-related contexts, (see Amoore 2011, Lyon 2003) based on which certain police measures can be applied in each case, for example increased monitoring measures or house searches.

In the police area of activity of averting danger, the term of danger fulfils a complementary function to the term suspicion. The processes for defining the dangerousness of people or groups, which have also changed due to new technological developments, mean it is possible for the police to resort to measures such as the obligation to register with the police, travel bans or warnings to potential offenders, according to the level of danger. In the area of combating so-called political extremism, these types of measures can be used, for example, in order to prevent people or groups from participating in political events. (See Laufer 2009) A requirement for this is the demonstration of a suspected risk. This makes it possible to carry out risk investigation measures that permit the investigation of a possible situation of danger and possible troublemakers, for example with the help of police databases. Potential offenders are people who are suspected of committing offences in the future. (See Deutscher Bundestag 2011a) Within the scope of fighting terrorism, or combating so-called political extremism, political motives are also assumed. Dangerousness can be considered the future-oriented aspect of the police field of suspiciousness, which establishes the scope of access for police measures depending on the intensity of suspicion towards people or groups. Within the scope of measures for combating so-called political extremism, political activities, personal connections or even positions in political-social discussions can also be included in the assessment as a potential offender or a “relevant person”, that is people who are suspected of playing a central role in extremist networks, which also permits

more intensive police measures. (See Deutscher Bundestag, 2011a) By using the category of suspiciousness, a differentiation is made between legitimate and illegitimate forms of political engagement. Creating zones of suspiciousness potentially impacts the expression of political opinions and the perception of fundamental democratic rights: Suspiciousness can also lead to the exercise of legitimate political activities resulting in police measures, which may also involve unpleasant consequences.

The project results let us assume that the use of automated data analysis processes leads to a shift in the production of knowledge, towards increasingly prognostic knowledge, which favours the valuation of future-oriented strategies of police work. (See Ferraris et al. 2013a, Guagnin et al. 2013) As the collection, storage and use of data takes place within a given institutional and legal framework, it must be assumed that the introduction of new technologies, which involve such far-reaching consequences, will also place these societal boundaries of police work under pressure to transform. This assumption is supported by the risks and dangers identified in the project that the use of profiling technologies can have with regard to fundamental rights and civil rights. (See Ferraris et al. 2013b)

In short, the following assumptions guide the examination:

- There is a trend towards changing the acquisition, storage and evaluation of information in police work, which leads to new forms of knowledge.
- This changed basis of knowledge leads to a reconfiguration of the construction of suspicion in the practice of law enforcement authorities.
- The creation of new information sources and types and the resulting new forms of information collection and use by the police adversely impact fundamental rights such as data protection, informational self-determination and the protection of core areas of private life as well as the privacy of post and telecommunications and therefore require appropriate legal regulation.
- The informed creation of zones of suspicion based on new methods of acquiring and using information leads to the potential of influencing the expression of political opinions and the perception of fundamental democratic rights.
- The use of automated data analysis processes leads to a shift in the production of knowledge, towards increasingly prognostic knowledge. This favours the valuation of preventive strategies of police work.

[1.2] Procedures and methods

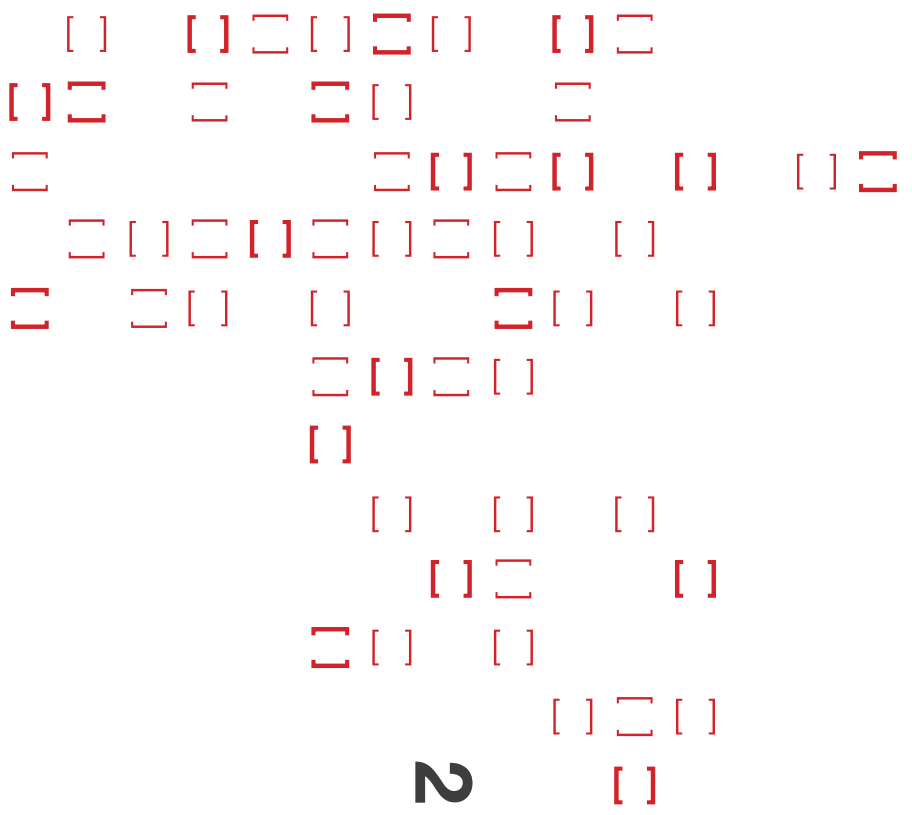
In order to check the above assumptions, it was first determined what data is available to the police and under which conditions and for what purpose such data is collected. Consequently, it was investigated how available information is stored and organised and with which technological aids data inventories are analysed and evaluated, in order to determine which (partially) automated data analysis methods (such as profiling) are used and how they are integrated into police practices. The objective was to analyse if and how the processes for acquiring knowledge and establishing suspicion change, and if that is the case, which institutional, legal and social consequences result from this. The focus of the study thus lies on the practical use of data, databases and data analysis systems. Given the explorative nature of this study, it is only able to highlight this field and only provide a limited presentation of political, social and legal discourses.

Within the scope of the case study, a sample of eight experts[2] in the area of police, data analysis software, political activism and law[3] were selected and guided interviews were carried out with them. (For the structure of the guidelines, see Gläser/Laudel 2008) The purpose of this selection was to connect the different perspectives from the field of consideration to create a multi-sided panorama in order to collect empirical data about an area that is difficult to access and highly normative. The limited number of interview partners is due to the difficulty in accessing this field as well as the limited resources of the case study. Based on a literature research and evaluation, various categories were identified for selecting the sample, which permit a comprehensive examination from various perspectives. First of all, it was important to interview police experts who have practical knowledge and experience in the use of new technologies regarding information collection and processing and have an overview of their development in recent times. In order to obtain an overview of the legal framework that conditions police work, the legal experts who were interviewed have field knowledge in the areas of research and data registration. In order to learn more about the technological possibilities and their integration into policing practices, technical experts in the field of case processing software were interviewed. As for the experts in the field of political activism, people were selected who have long-standing knowledge of relevant discourses and have good knowledge about the field of political protest movements or who are personally involved in the field.

In order to increase the significance of the explorative case study, critical statements made in the interviews were substantiated with available documents such as parliamentary requests, official documents as well as newspaper articles and academic literature. The data evaluation is based on the qualitative content analysis method (Mayring: 2008).

2 In this report, reference to male and female is alternated in a general manner. This is also done for reasons of anonymisation of those who were interviewed.

3 Quotes and supporting text excerpts will be assigned to the respective interviewees with the following abbreviations: Police experts, POL1/2; software development experts, SW1/2; political activism experts, AK1/2; legal experts, JUR1/2.



Databases and analysis software in police practices

The following section provides an overview of the use of databases and data analysis tools in police work. This section is structured according to the different phases of data use: collection of digital information, storing of information in databases and data management as well as the evaluation of the data using data analysis software.

[2.1] Collecting data and metadata

With the digitisation of our everyday life and the progressive digitisation of forensics as well as the digital archiving of police knowledge, on the one hand, and technological advances in the area of data processing on the other, the amount of information available to the police has increased enormously, as well as the spectrum of their capabilities of using this data both quantitatively as well as qualitatively. This makes new information, technologies and methods for controlling criminality available to the law enforcement authorities.

> *"All data that plays a role today in our life is also important for criminal investigations. It depends on the investigation, which data is taken into particular consideration." (POL2)*

During investigation proceedings, the police have the possibility to seize technical devices and read out information contained on data carriers. Due to the computerisation of our daily activities, it is possible to obtain a wide range of information about activities, social networks and the behaviour of suspects. The data carriers and digital devices can therefore contain a multitude of information about the planning and preparation of an offence or course of events of a crime, for example in the form of documents or email conversations.

> *"This is the classical criminal work of the past, which focuses, for example during an investigation, on finding the plan of action of the perpetrator, that is any sketch, a hand sketch, a hand drawing, a recording […]. Due to these technical changes in the area of information and communication technology, new requirements have emerged as these plans of action can no longer be found in paper form on a desk, written in a journal, or similar, or only in a few cases. [...] This means that we must find new ways of handling this new media [...] and […] [...] that then can be utilised with completely new technical possibilities. (POL2)*

During criminal proceedings, the police are also able to request data from private companies such as internet providers, service providers or even banks and under certain circumstances can even seize data carriers. (JUR1/2) Data that internet providers, homepage operators, email providers and similar service providers possess provide the police with access to a wide scope of information about the activities of individuals and institutions. So-called metadata can be used to draw conclusions about networks of individuals as well as their communication and movement habits. Information that used to be very difficult or impossible to find and investigate is much easier to find today. This type of structural knowledge is very important especially in the areas of police work where network based operations of the suspects is assumed, for example in the case of complex white-collar crime, organised crime or political groups. (JUR2)

A tool that has gained a great deal of public attention is the querying of telephone base stations, which creates a data record that contains all the cell phone calls recorded on a cell phone tower at a certain point of time. This tool was used in a prominent case by police in order to determine who was present at the time of riots at a certain demonstration. According to news reports, the metadata obtained in this manner was also used for other proceedings. (See Biermann, 2011) From a data protection law point of view, this creates the problem of violating the principle of purpose binding and the proportionality of the measure. In particular, in the case of the base station query, the data of numberless innocent people was inevitably processed. The lawfulness and proportionality was criticised by the responsible data protection officers and legally found as having been partially illegal. (See Landgericht Dresden, 2013) This incident caused the Berlin data protection officer to perform a general check of the use of this tool in Berlin during the period between 2009 and 2011, and he came to this conclusion:

> *"Telephone base station queries, which based on their intensity of intrusion and wide range may only be used in exceptional cases, have become everyday tools in certain crime areas that are used on a routine basis and without sufficient observance of legal guidelines." (Dix 2013)*

The great usefulness of metadata also explains its increasing importance for police work.

> *"Of increasing interest, or perhaps of greater interest, is traffic data and metadata, because much more can be reconstructed from this type of data than only the contents of conversation or conversational contacts, for example movement profiles from traffic data, or social data, as social networks can be reconstructed from metadata." (JUR1)*

The collection and handling of this type of data is only insufficiently regulated, although this implies deep-reaching intrusion in the fundamental rights of citizens. This type of data collection enormously jeopardises above all the right to protection of personal data and the right to the protection of the core areas of private life. (See Singelnstein, 2012) In connection with the possibility of digital storage and evaluation, such large data records are problematic. Their use in connection with the recording of citizens who are exercising a fundamental right during a demonstration is particularly precarious.

There is also a need for regulations regarding the use of publicly accessible information on the internet, which originate in the form of user generated content, for example on Twitter, Facebook, Blogs or Wikis, and permit new possibilities for the police to collect information.

(See Singelnstein, 2012). Here too, much information can be obtained about individuals, groups and their activities and connections. In the area of combating so-called political extremism, there are for example discussions and activities of different scenes and those involved can be followed using publicly accessible sources in order to identify and follow the dynamics and group structures of certain political scenes. Perhaps also information can be acquired that can be used in proceedings or to assess people or groups. One of the political activists interviewed could report that the police carried out internet searches in order to collect information about him. The information collected in the database went at times clearly beyond the connections with his political activities and were included in the assessment of how dangerous he is considered, in regard of possibly committing future crimes, as well as his classification in social networks, which resulted in further police measures. (AK2)

In addition to the new sources and types of information presented above, classical methods for collecting information, such as witness statements, information from the crime scene or the instrumentalities, fingerprint identification and further areas of the constantly growing area of forensics, still play a central role in police work. Their form and usefulness has also changed, as they can be digitised and used in new information systems, as will be described in the next section.

[2.2] Data exchange and structuring through databases

The information the police collect during preliminary proceedings or for the purpose of averting danger is recorded in police databases, which can be accessed by different authorities, departments and operators[4]. This also includes information originating from classical investigation work, such as witness statements, crime scene information, etc. The regional and federal police and their departments operate multiple databases to which specific information can be added. Installation orders (Errichtungsanordnungen EAO), which are present for each database, define the purpose each police database serves, which information is entered and in which form, who has access to the information, how long the information is stored and which specific regulations form the basis for storing and using the information. The principle of purpose binding applies when using the information or when providing it to other authorities. Reasons for use other than the intended purpose must be justified. These data protection requirements are also incorporated in the technical architecture of the databases. Data exchange and accessibility are also technically limited.

> *"The systems we use here [contain] up to 50% of code only for security mechanisms [...], to make sure that the data is deleted in a timely manner, when it needs to be deleted, and to define who should not see it and who can see it, etc." (SW2)*

4 The databases indicated below are a small fragment of the police databases used in Germany. The purposes, content and form of the collected information and possibilities of their use and networking vary considerably among the various databases. The databases indicated and described here have been selected as examples, as their purpose and structure represent in particular the possibilities that exist due to the new methods of data analysis, as they permit the future and structure oriented collection, networking and assessment of information. In that respect they indicate a trend that is expressed in the following sections. For a more complete overview of the databases available to the German police across the nation, see Deutscher Bundestag: 2011b.

In addition to the legal data protection regulations, a lack of technical interoperability of the databases and data formats hinders the possibility of exchange between different systems. (SW1) Therefore over the past years, there has been much effort to increase technical interoperability and to decrease the legal obstacles to the exchange of information between authorities and departments, for example by expanding upon the purposes of databases (see Monroy 2014) or by establishing new shared databases that can be operated collectively by multiple authorities[5]. In this way, more data from various fields and authorities is intended to be made available to the investigating authorities, to facilitate cross-entity case and structure analyses.

An important technical element for increasing the flow of information between State Criminal Police Offices (Landeskriminalämter, LKÄ) and the Federal Criminal Police Office (Bundeskriminalamt, BKA) in this context is represented by the so-called joint files. Joint files are databases that are centrally administered by an authority and filled and used by additional authorities. For the purpose of data exchange between state and federal police authorities, the BKA has created installation orders, according to the BKA law, that require the approval of the Federal Ministry of the Interior as well as the regional ministries of the interior (BKA-law §34). These orders are used to determine the purpose for which the data is collected, which data is collected and which authorities or departments can add and access them. The data in this type of joint files can be accessed and used by all the authorities involved (BKA-law §11), for example the LKÄ, the federal police and customs authorities. Joint files can also include other authorities, which happens for example in the case of the counter-terrorism file, in order to make it easier for the police and secret services to exchange information[6]. When transferring information into joint files, to some degree very large amounts of information from different origins and of different types must be brought into a standardised form in order to store the information so it can be accessed and analysed.

> *"In various special fields, that is in state security, in the area of organised criminality, in the area of drug-related crimes, in the area of fraud, economic lawsuits, there are always specialised bodies and these specialised bodies determine in what way this data exchange should take place and how it should take place. This is where standardisation takes place, so that everyone receives the same information as far as possible and [...] can properly assess the information." (POL1)*

The recontextualisation of the information during investigations or for purposes of prevention and averting danger takes place using data queries and/or with the use of data analysis tools. The purpose of these tools, above all, is to make the information available in a case and event specific manner and to determine and reflect complex relationships among

5 This includes, for example, counter-terrorism files or also right-wing extremism files, which are currently the object of public debate. (See Töpfer 2014)

6 As data can be entered in the counter-terrorism file not only by different police departments, but also by secret service agencies, this creates another problem. The close cooperation between the secret services and police threatens their constitutional institutional division, as was determined by the German Federal Constitutional Court within the scope of examining a constitutional complaint. Furthermore, the court determined that there was a deficiency regarding the guarantee of informational self-determination and criticised an absence of clarity of the guidelines about who can be recorded in the database. Furthermore, the recording of detailed data about people who are companions to people who are recorded in the database was also criticised. (See BVerfG 2013, Bundesministerium des Innern 2013, Töpfer 2014)

people, groups, objects, places or events, as further described in the following section. The software makes it possible to access different databases and data formats from different authorities and to include this information in the data analysis.

> *"The system [...] is very generic. It is possible to adapt it to the categories you want to investigate. Its purpose is to take information from all sources and in all possible formats and put it in a database in a standardised manner so it can then be analysed. (SW2)*

This makes it possible to carry out cross-institution, cross-region and cross-case analyses. The ability to make information always available in a decentralised manner and to permit it to be evaluated (partially) automatically makes a new object area visible in which a wide range of information can be connected together. Police can use knowledge to create assumptions within the scope of construction of suspiciousness including prosecution as well as avertion of danger and prevention, and for carrying out additional police measures. (JUR1/2, POL1/2, SW1/2)

In the area of state security, of great importance are the databases "Politically Motivated Crime" (PMK), which are divided into politically motivated crime left, politically motivated crime right and politically motivated crime by foreigners . In the case of politically motivated crime left, the file is used less for criminal proceedings and more for prevention and averting danger[7]. In this context, police work also focuses greatly on monitoring a political field, which is normally the task of secret services. (See Deutscher Bundestag, 2011). According to installation orders, the PMK database should help recognise "relevant people, groups of people, institutions, objects and articles", "interrelations/connections between people, groups of people, institutions, objects and articles" as well as "criminal organisations" and their structure. In addition, unimportant information and findings should be discarded. The databases can contain information regarding identification, companions, connections between a person and certain events, places, institutions or group structures, information about means of communication, account information and movements, information about court exhibits and similar that originates from telecommunication monitoring, information about offences, and much more. (See Bundeskriminalamt. Der Datenschutzbeauftragte 2008) Furthermore, it is possible to integrate free text fields, photos, results from (online) research or results from data analysis, for example in the form of diagrams of network structures. (AK2, SW1/2)
This example of only one database shows the multitude of the types of information and sources that are available for police investigation work and that, when entered into the databases and with the use of data analysis tools, can be made permanently and decentrally available.

---

7 It should be assumed that the various politically motivated crime databases have a similar structure. As for this case study, the installation order for the database "Politically Motivated Crime – left" was available as a document, the statements made here will be limited to this databases, unless otherwise indicated. The politically motivated crime databases are in no way the only police databases used in the area of "politically motivated crime", which are used above all for determining structures and for long-term oriented data collection. Rather it appears to be a trend to create databases with such an orientation of purpose, as can be assumed with the creation of new databases, such as the counter-terrorism files or right-wing extremism files. (see footnotes 6, 7). The politically motivated crime databases also do not represent the largest collection of politically oriented information. While the politically motivated crime left contains approx. 2,000 personal records, the "INPOL-Homeland Security" joint file already contains approx. 90,000 people. Overall, the latter contains approx. 1,500,000 data records. (See Deutscher Bundestag 2011b)

The exchange of data on a European and international level will also play a growing role in relation to decentralised and far-reaching availability (see ICF GHK 2013). Already today European countries exchange personal data that are collected in connection with political protests (AK1/2)[8]. This development is above all important in view of the development of critical European public protests, since thisdata can then possibly be used to risk assess persons and groups as potential offenders. These assessments can then in turn be used in order to declare an entry ban when protests on the occasion of certain events are expected (see ICF GHK, 2013; Monroy/ Jobst 2009.)

[2.3] Software supported data structuring and analysis: connecting the dots

The different police authorities use at times different data management and data analysis instruments, which are however very similar in their capabilities and range of application. (POL1, SW1) The software programs make it possible, depending on the case and access authority, to search various databases and query the data. When storing objects in databases, it is possible with the help of the software information management tool to fill them with properties and relations to other objects. It is also possible to query the databases, with the help of which information is selected and knowledge gaps are determined. Furthermore, complex networks and chain relationships, as well as relationship types between different objects can be determined, which are stored in different databases by different institutions. (POL1/2, SW1/2) Information that is scattered geographically and institutionally can be made accessible for individual operators as well as for decentralised teams or departments all over Germany. Furthermore, queries can be stored, so that when new information is entered to the database, certain facts relevant for the query can then be automatically assigned. Some products also allow the integration of external software, for example automated text analysis (POL1, SW1/2). Data analysis systems, as used by the police, make it possible to make larger amounts of information accessible and to analyse it in more complex ways than was possible with traditional filing systems. In addition, a larger variety of information sources and types can be included in the analysis than is possible in the case of paper files. The connection of information takes place as “connecting the dots”. Individual elements, which are taken out of their context to be stored in databases, are related to each other by database queries. The connections created in this manner can usually be visualised. It is possible however that the original context stays lost in this way and the relationships of some elements take on disproportional importance when linked to others (see Amoore 2008).

In addition to work on concrete cases, analysis software also simplifies the identification of certain modi operandi and their clustering, so that more specific measures can be found, for example regarding the relevant use of resources. In addition to operative prevention, also the strategic assessment of criminal developments, crime forecast and the monitoring of certain fields of crimes are simplified, so that medium-term resources and measures can be planned accordingly (POL1/2, SW2). In the area of politically motivated crime,

8 See also EC (2007), Monroy (2013), regarding exchange of data between police in the EU, for general information see Hempel et al. (2009).

also averting danger plays an important role that is closely connected with monitoring certain fields. The structurally-oriented focus of databases as well as the capabilities of the analysis software allow to make social structures and dynamics visible, to determine event and context related networks of relationships in data and to identify relevant individuals or groups. This information can be used to anticipate dangerous situations and to implement measures against individuals or groups that have been defined as dangerous. These measures can include increased surveillance, house searches or the declaration of obligations to register with the police or travel bans for a certain period of time, in order to prevent participation in an event defined as security-relevant.

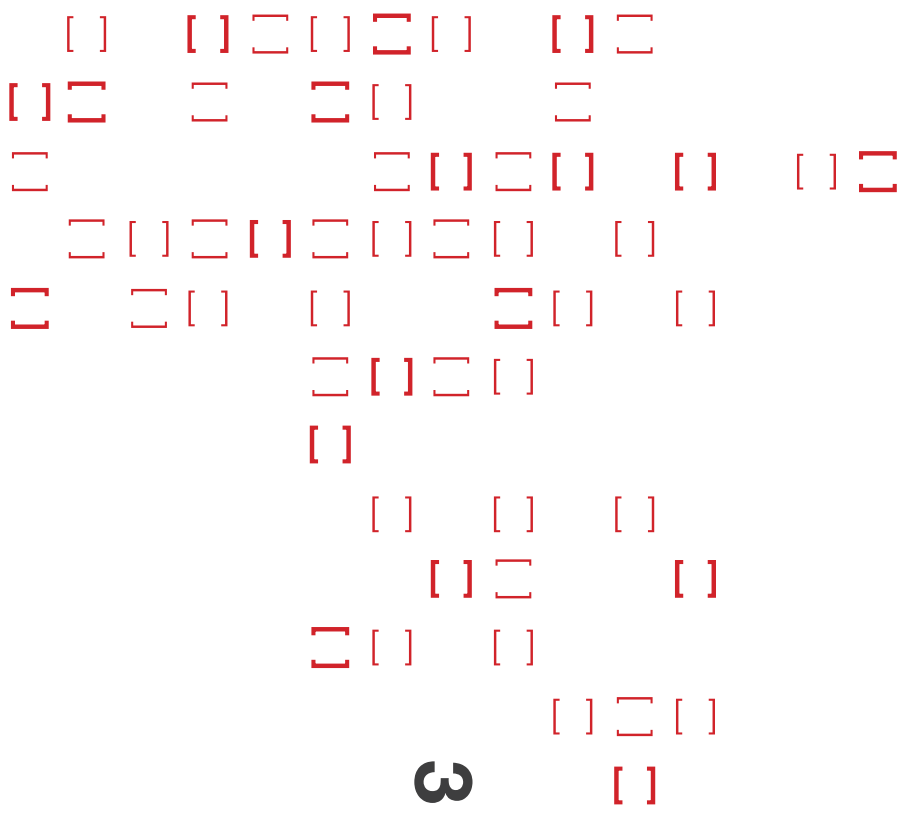
> *"Through this enormous exchange of data, an increasing amount of concrete measures [can be] implemented […], as it [the treatment, author's note] does not remain with the data track or the data image, but can result in very concrete house searches, identity verification, whatever police measures from the police spectrum can be yielded from the police laws." (AK2)*

The representation of new information sources and new methods of collection, storage, organisation and use of new information clearly show the changes to police work that have resulted from the digitisation of their daily work. This makes it possible for the police databases and the utilised analysis software to create suspect or offence profiles and to use them as a query in order to find suspects in databases. The profiles must be created manually as queries however. Therefore this is not yet a far-reaching automated process. The automated analysis of large amounts of data for the automated creation of risk or danger profiles for prevention, as can be found for example in the concept of predictive policing, (see Perry et al. 2013) is not carried out by law enforcement authorities[9], also because database queries only take place with respect to certain causes. This means there must be a reference to concrete investigations or prevention and/or danger averting measures. The actual event also defines then which databases can be accessed, as these have been created for a specific purpose. Additionally, there is no legal basis for the use of methods of automated pattern recognition in large datasets by police in Germany. Steps are being taken however to make this type of procedure possible in the future (see Monroy 2014). Furthermore, it is intended to make it easier for authorities to access databases across institutions (see Medick 2014, Töpfer 2014). The case study shows further that the restricting effect of cause relatedness has shown to be increasingly effective for the collection and storage of data in the context of preventive averting of danger, as is being done in the area of combating so-called political extremism. This trend is also favoured by the new technological possibilities, as they are available to the police, as will be described in the next section.

Up until now, the police have used databases and data analysis tools mainly as data management tools as well as for case and structure analysis. Even if this does not yet fully utilise the potential of the given technological possibilities, transformations are already taking place in police work with far reactive societal consequences. The following section analyses the effects of these developments. The focus here lies on the transformation of the police practices of constructing suspiciousness.

---

9 For example, the Ministry of local and urban affairs of North Rhein-Westphalia is currently examining to what extent it is possible to carry out pilot projects for the implementation of predictive policing strategies (see Landtag Nordrhein-Westfalen, 2014)



Changes in police knowledge and suspicion practices

The first federal police information system INPOL was introduced in 1972. “The purpose of this system is to make it possible to make information available across the nation to all concerned police authorities in an uncomplicated and quick manner.” (Lodde 1972, 25) The range of tasks for this information system was limited to manhunt queries and the comparison of crime information (see Schramm 1972). The quick and location-independent access to information about people and crimes was viewed as an advantage of this system with respect to previously used manhunt books (see Schramm 1972). In spite of these limited abilities of the INPOL information system at that time, there was already an indication that the initial computerisation of police work was clearly changing it. Wolfgang Rutschke, the former State Secretary for the Interior asked the following in his opening address at the autumn conference of the BKA in 1972 with regard to the topic of data processing:

> *“The BKA and other police offices will now hire [...] dumb and extremely diligent applicants, that is computers. Is there a risk of adaptation for man? Will everything be left to routine? Will the use of computers promote stereotypical thinking?” He continued: “A computer cannot replace the necessary fantasy, inventiveness, the intuitive comprehension of circumstances of police officers, [...]” and then concluded with the warning “[…] that the use of electronic data processing shall not be an end in itself, that the people who work in the criminal investigation department must not become machine operators, that there are people and fates hidden behind the stored data that the computer will never be able to comprehensively describe.” (Rutschke 1972: 11)*

These are questions that are still virulent today. Rutschke expected and feared a basic change to police work, that would encompass the role of officers, the handling of information and the police’s understanding of its subject, the population, and therefore the relationship of the police with the latter. Since the above statement was made, the technological possibilities of data use have expanded enormously. At the same time, the police have a large number of information sources and types available that can be used when working on combating and preventing crime. Below we will further examine and analyse Rutschkes’ questions, regarding the extent to which police work has been changed due to the increased computerisation and due to the digitisation of daily activities. The main interest of our research is on police activities combating so-called political extremism, which already formed the basis for earlier computerisation of the German police (see Weinhauer 2007).

[3.1] Changed requirements on investigation work

The access to a multitude of new information and types of information that result from the digitisation of daily activities was regarded as positive by the police experts who were interviewed. It opens up new possibilities for officers to pursue offences as well as for preventive work. Police and software experts also stated that these new possibilities also involve new challenges for the work of police officers. The new information sources, which result from the digitisation of daily activities as well as digital forensics, the possibility to make them available in digital form together with investigative results from classical police work and the possibility to analyse these information make the information selection by the officers more difficult. A police expert spoke of "data overflow", which on the one hand resulted from the amount of available information that the officer must handle, and on the other has caused quality issues concerning the information.

> *"In a large case, an investigator can experience a certain data overflow. He receives information from joint files, from his own files [...], data from special units [...], data from observation, for example. Then he receives data from telecommunication monitoring, […] internet monitoring. All of this data flows to him and in every case he must assess 'how is this relevant to my case? How legally valid is it? Do I have to edit it? Do I have to critically analyse it?'." (POL2)*

The new forms of information result in requirements for police work, which changes the role of officers in investigation processes. In addition to the classical qualities of investigators, such as intuition, power of deduction and experience, more abilities are requested that would be associated with computer analysts: As computer users, officers require a certain metaknowledge about technical processes (see Degele 2002, 167-169) to be able to evaluate the quality and validity of digital information as well as the results of database queries and data analyses, in order to suitably integrate them in their investigation work. If officers rely on the assessment of software for analysing the weighting of individual connections in social networks, they must be able to evaluate how this weighting materialises, for example by evaluating the communication frequency, the communication duration or the type of communication. This evaluation can have an impact on the construction of assumptios and grounds for suspicion. (SW2) Furthermore, a lack of knowledge regarding the structure of the database or query, on which a data analysis software produces query results, can lead to the creation of knowledge gaps that are not recognised as such, which can make the query results appear to be more reliable than they are. Results can emerge which do not match the intended query – e.g. inculpatory or exculpatory evidence could be neglected due to overcomplex data structures or inssufficient queries (SW1) The use of databases and data analysis tools and the handling of new types of information cause the necessity for new skills in handling information and change policing practices. This is also reflected in an institutional change, in which new professions, such as software experts, are integrated into police work and produce a new setting of priorities in the training and further education of officers. (POL1/2)

> *"When we work in the technical area, then the investigator, the classical investigator, who should then finally convict the suspect, needs someone who says to him "be careful, I used to be an investigator, I have continued my training and I can say to you, [...] that fact is valid in this way for you, this tells you this, and you should support this with these measures." (POL1)*

Police and software experts also agree that the requirements regarding the documentation of political activities have increased. As the entry of investigation results decontextualise them in the databases, information must be stored that makes a later logical recontextualisation possible by other officers. Unlike in a system with written files, there is no narrative context in the case of database queries. Database queries do however make it possible to access a larger pool of information than is possible with filing systems, and facilitate creating connections. although they create these connections in the form of "connecting the dots" – as a connection between individual elements whose context has been removed. This type of connection of individual elements reveals the risk that the represented connections appear as evident, but that – due to insufficient documentation regarding the information collection and use – are not sufficiently checked for the contextual consistency of the connections. It is also possible that the evidence for individual elements gains importance in a disproportional manner (see Amoore, 2008). This problem is accentuated especially in the case of staffing shortage and time pressure, when a thorough and critical checking of the results comes up short. In spite of this possible shortfall, information and information links obtained via database queries are included in the construction of suspicion and the creation of theories (AK2, SW1). In order to create valid investigation theories and to be able to initiate further measures, it is necessary to have reliable and comprehensible documentation regarding the recording, checking and modification as well as use of information in proceedings, which also permit a meaningful reconstruction of connections and work procedures and counteract the limited nature of "connecting the dots" and its persuasive visualisation. In particular, legal and software experts indicate considerable shortcomings in the practice of recording data.

> *"Previously records were kept in a classical manner. It started with a complaint that was received, then witnesses were heard, then there were the forensic investigation reports, which still exist today clearly, notes made in the file, etc. etc. etc., but this approach has been quietly replaced gradually so that only the information that is produced is entered in a system, but the actual notes to the file are no longer produced". (SW1)*

Police experts speak in this context of an increased vulnerability of police work, for example in criminal proceedings, which is a result from the more complex requirements regarding validation of evidence and construction of suspicion.

> *"Today with documentation, we must deal more intensively with the legally admissible adherence of this tool. Therefore from my point of view, this does not lead to a removal of load, rather to a higher and more scientific demand and in a certain way, to be honest, also to greater vulnerability. The possibility of errors is simply much higher". (POL2)*

According to statements made by legal and activism experts, insufficient documentation regarding police procedures for establishing suspicion, creating assumptions and investigations with the help of databases tends to shift the asymmetry of knowledge in favour of the police, as questioning of the police during criminal proceedings and therefore the traceability of certain theories is hindered. This also weakens the position of the defence in court proceedings (See Ziercke 2013). In addition, the possibilities of discovering incorrect or even potentially illegal procedures by law enforcement authorities during the preliminary proceedings are limited.

> *"This is an enormous problem, as the police have an enormous advantage in knowledge, […], that, so to speak, the information generation is not documented and above all, that these databases, these police information systems have an enormous advantage, selectively providing data or selectively processing data, so it becomes enormously difficult for the defence to fully reconstruct these steps and actually address those that were taken". (JUR2)*

The growing quantity of different types of information that the police can access makes it possible, with the help of data analysis tools, to derive more complex information and as a result to generate grounds for suspicion in a new manner, which can involve consequential actions. At the same time, the interviews show different perspectives that uncertainty regarding the derived information has increased and new procedures of knowledge formation and checking are required in the form of changed requirements regarding the validation of information and the documentation of information selection and creation of knowledge and theories. By decontextualising information when entering it into databases, the problem of the uncertainty of the knowledge to be acquired is increased, as context can be lost or misrepresented.At the same time, the information in a police database is considered as checked and therefore as valid, assessable knowledge that constitutes evidence for the construction of suspicion.

> *"With our own databases, there is […] data that has been checked for validity and reliability. And there are occasionally databases where we use soft data, but that also have a quality assessment from us. [...] Based on this evaluation I can therefore evaluate how I should treat these data". (POL1)*

In spite of efforts made to increase the interoperability of different databases, the lack of interoperability of various information systems still represents a problem. The ability of software to reliably involve various databases in data query and analysis can therefore have consequences on the query and analysis results, which find their way into the construction of suspicion. Also the ability to deal with unclear queries can change the results of the analysis. Functions, such as the possibility of using standardised queries or user-defined queries can influence work procedures and results, as they reinforce preconceptions so that the admission of aberrant possibilities, theories or assumptions is hindered (see Reichertz, 1994). Due to this growing role of computer technology in police practices, a police expert spoke of software developers as a part of the expanding field of investigation work (POL1). The architecture of databases, the capabilities of software tools or the results of automated text analysis for the preselection of information or the assessment of the intensity of social relationships with the help of the evaluation of communication behaviour within certain networks can also influence the police in their construction of suspicion and creation of theories, that is, even though they do not completely determine them (see Ziercke, 2013).

This increasing uncertainty regarding the assessment of information that is digitally collected and stored as well as of results of the (partially) automated analysis of this information and therefore the theories that were created using computer supported methods lead to new requirements on the process of collecting and processing information. At the same time, there are new requirements on police personnel and the field of relevant actors. In other words, the circle of the investigators now includes the figure of the investigator-analyst as well as the programmer-investigator. In this case it is necessary that in particular the software developers, who appear to be associated with the field of the investigation, must be made

aware of their role so they can adopt it consciously. As when the police, making use of software tools, distinguish in a field of political activism between legitimate and illegitimate political activities, the developer takes on a normatively charged role.

[3.2] Future and network orientation in the construction of suspiciousness

Police is obliged to only gather data for relevant causes. Data usage then takes place based on a specific purpose. In the case of politically motivated crime files, the relevant cause must not be in any case an offence and the purpose of the database does not only include the prosecution but also the prevention of offences. Within the scope of political activities, there can be various sub-crime occasions, for personal identification and storage of personal data in databases for politically motivated crime, for example encounters with the police at demonstrations. The requirement for keeping the data in the politically motivated crime left file, for example, can be having assessed a person as potentially dangerous. This means that there is an assumption that this person may take part in the future in serious offences (see Bundeskriminalamt, 2008, Deutscher Bundestag, 2011a, 2012a).

> *"When someone comes into the focus [of the police], then the probability that he has been stored in a corresponding file is relatively large. There is also unfortunately the problem that the police can maintain criminal proceeding and danger aversion files jointly, as mixed files". (JUR1)*

The definition of dangerousness can be amongst other conducted by allocating people to certain structural connections (AK2). Depending on the assessment of relevance of a person in certain personnel structures or political discussions, this may result in consequential actions, such as the collection of additional information about a person, his activities and environment (see Deutscher Bundestag 2011a). Analysis software makes it possible in this case to define relationships between objects (people, groups, things, events, locations, etc.) and to link them[10]. With the network orientation of databases, such as the "Politically Motivated Crime – left" or the counter-terrorism file, and the abilities of the analysis software to reconstruct networks with new quality and depth, these social network structures can be increasingly included in the assessment of how dangerous people are, insofar those are now visible and can be used as knowledge objects. This results in the danger of a growing abstraction and de-individualisation of the construction of suspiciousness, including dangerousness. The possibility of the long term collection and evaluation of information about people and groups, in which they are connected with each other, promotes a development in which police work becomes comparable with the secret service activities with the reconstruction of group structures, networks and scenes as well as their dynamics. Computer-supported assumptions about social networks are used for the construction of areas of suspiciousness and context-dependent identification of suspect groups and

10 The assignment of certain types of relationships can already represent an interpretation of the officer, which is reinforced by its reproduction in the analysis software. As the allocated types of relationships are incorporated in further queries that contribute towards the construction of suspicion or danger assessments, the implied preconceptions are reproduced.

risk groups in order to address them with police measures, which permit, for example, keeping potential offenders away from certain large political events (reporting obligations, travel bans, etc.) or make it possible to obtain information about certain people or groups, for example through the collection of information from publicly accessible sources. As this type of data analysis is subordinate to the clarification of a crime, as rather it is used for the creation of an overview of the situation or the preventive collection of information for possible future events, a validity of legitimacy check does not take place as a result of a criminal case. Only when an administrative check takes place, the legitimacy of the storage and use of the data will be checked.

> *"Sometimes we see diagrams that are generated in this manner, who has a bit of contact with whom, to visualise it. That is, when certain information, whether it comes from traffic data monitoring or direct telecommunication or other knowledge, if you are seen together with someone at a demonstration, which is then correlated, and then certain diagrams are developed, which in general lead, under certain circumstances, to the intensification of measures. When they [the law enforcement authorities, author's note] say, 'that is enough for us to include additional measures,' but that would not necessarily be enough for a conviction". (JUR2)*

Personal data may be entered in the police database due to violations that lie well below the threshold for a criminal offence. It is possible to be entered in police databases, such as the "Politically Motivated Crime-left"-database or counter-terrorism file also as a companion or contact person of others whose information are stored in those files. These entries create the possibility of being put into contact with people, groups or events that are also part of the database. Statements from activism and legal experts are in complete agreement that by already connecting people to political discussions and assuming that this person has a certain relevancy in certain networks could lead to increased monitoring measures. The purpose is not only to collect information about concrete offences, rather databases create an inventory of information that makes it possible in the case of future crimes or dangerous situations to be able to determine context-dependent grounds for suspiciousness and to be able to anticipate dangers and potential offenders. By querying certain properties, it becomes possible prior to large political events to identify people and groups as potential offenders and to prevent them from participating in the corresponding event, for example by means of addressing warnings to them, or making obligations to register with the police or travel bans. (Monroy/Jobst 2009) In this case there is the risk that political activities that are carried out on the basis of exercising fundamental civil rights will appear as illegitimate, as such police measures are not necessarily connected with past offences, but are carried out also their consideration as potentially dangerous – which is based on assessments of the political activities of subjects or their role in political group structures. Future-oriented structure reconstructions become much more important in this context (See ICF GHK, 2013).

> *" Well, what I learned from my case, first of all personal identification data is stored […] then you can link information about certain places to a person, in my case my home address. Then, as an event category, the registration of demonstrations was linked to my profile, date, type and name of the demonstration, meaning the political orientation. Then I was accused of being active in arelevant group, that was stored as an object, that is not a person, rather an institution, and then a connection was constructed". (AK2)*

Data storage and the resulting structure information between individuals, institutions, events and things, as is the case for the "Politically Motivated Crime-left"-database according to the corresponding installation order (EAO), creates a pool of information about a certain political field, which is used as a permanent space of possibility for generating situational knowledge, conceived necessary for concrete occasions. The database creates a space of persistent, potential suspiciousness that can be activated depending on the occasion by means of queries. The use of different cross-category databases makes it possible for the police to have context-dependent, situational access to those parts of the population, which are documented in databases accessible across Germany as a time-space network of continuous suspiciousness. The digitization of everyday life and the computer-aided analysis of information deriving from it allow to identify social networks and relations within data material, which would have remained hidden before. The structures identified are the basis of the assessment of persons and groups and thus constitute a matter of knowledge and a ground for activeness. As a result zones of suspiciousness emerge which describe a scope of action for the police depending on the subject's degree of suspiciousness. By that the application of databases and data analysis reconfigures the access to and assessment of parts of the population by the police. Beyond that the construction of zones of suspiciousness and the knowledge that is produced within this definition process influence which and whose political activities and positions are considered to be legitimate or illegitimate. For example, temporary travel bans or obligations to register with the police may be ordered within the context of political events, in order to prevent the participation of people and groups which are assessed as potential offenders. Possible addressees of these measures can be determined by querying certain criteria in databases which can include political activities, the allocation to certain political networks or former encounters with the police (SW1). Here, the assessment of persons or groups as potential dangers incorporates preconceptions regarding the legitimacy of political actions, which are obscured by the technological submission of the inquiry, as it is understood as a neutral result of querying validated knowledge (see Amoore 2008).

Averting danger has always been part of police work. The technological evolution of the digitisation of society and police work make it possible however to inspect social and political fields as well as their developments to new depths and at different levels of complexity, which gives this preventive orientation a new dynamic. This also encourages shifting the acquisition of knowledge for the prevention of concrete dangers towards the risk assessmentof people or groups of people, based on querying certain property categories, even though this practice is limited at the present time[11].

> *"The most important task of security agencies is to prevent criminal offences, not to solve them. [...] Consequently, there would be this idea or this wish, which is described in this "Minority Report", in this movie, already to be at the place of the crime prior to the suspect, which until recently has been left to Hollywood, but I think that with Big Data this is a possibility that we also have today. Also based on the considerable computing power that is possible, so that we can investigate data streams directly on-the-fly, there are great opportunities, apparently great opportu-*

11 However, it should be pointed out that the increase in importance of the preventive concept in police work cannot be fully explained only with the use of databases and data analysis tools. If technological developments also take on an important role in this "preventive turn" (see Koops: 2009), then a comprehensive analysis of the transformation of police actions must also include societal, cultural, political, organisational and legal factors and discourses.

nities for security agencies to improve themselves from a preventive policing point of view. But [...] Big Data also involves the fact that we always have a large amount of information that, in the end, we cannot assess". (POL1)

Regardless of these problems related to the assessment of information, computer supported identification of suspicion, danger and risk takes place in the form of queries and software based analysis. The results of those appear to be reliable and neutral, as preconceptions are hidden in their technological origin and submission. Furthermore information are perceived as significant even though their origin and meaning, also as a result of poor documentation, are at times difficult to comprehend and because the performative effects of databases and analysis software on query and analysis results are partially unknown.

"With the introduction of case processing systems, the classical method of record keeping is gradually no longer taking place, with everything now being kept electronically, [...] [and] as anyone can [enter data] with relatively no checks and there is absolutely no record of what took place. Then entire preliminary proceedings are based on this." (SW1)

The insufficient practice of documenting the construction of suspicion during preliminary proceedings and therefore the lack of a possibility to check the police practice also increases the non-transparency of processes for establishing suspicion, as can be seen below.

[3.3] Growing non-transparency of establishing suspiciousness

As the importance of preventive aspects increases policing activities are shifted to the field of pre-crime activities. In combination with new technological possibilities for data collection and data management, this shift favours the collection of information about citizens and makes situational access to political scenes possible for the police to combat "politically motivated crime". The police are not obliged to inform people automatically if and in which databases their information has been collected and stored. Consequently, citizens can only make a request to the police, during court proceedings or possibly in the case of objections against police measures of which they became aware, to learn about the information that is stored about them (see Deutscher Bundestag, 2012a). Consequently, controlling police activities is made more difficult since preventive measures usually do not lead to trials which imply a evaluation of legitimacy of the measures applied. This development is enhanced by the technically-caused increase in complexity of the construction of knowledge and the exchange of information between different authorities on different levels, as well as due to the increased use of clandestine measures in the acquisition of knowledge.

"In other words, they [state security] do not only want to pursue a person, and do not only want to explain a case, rather they also want to clarify the big picture and certain methods are more suitable for this, which are clandestine methods. [...] Here

data evaluation is naturally of great interest, if it is possible, for example, to reconstruct the social structure of people". (JUR1)

It is for this reason that the establishing of suspiciousness by police is becoming an increasingly non-transparent field in which the concrete forms of using knowledge for constructing fields of suspiciousness of various intensities, and therewith the processes of access to certain population groups, is becoming difficult to comprehend. In the area of combating so-called politically motivated crime, there is an increased risk of threatening fundamental democratic rights. As this unclear process of acquiring information and its use for the construction of suspiciousness and the thereby resulting measures create a situation in which politically active citizens perceive themselves as being constantly visible to police. The resulting uncertainty leads to a panoptic effect of adaptive behaviour. There is the risk that consequently, citizens will limit their political activities, cancel their political commitments or avoid cooperation with certain groups as they assume they are being subjected to greater police monitoring.

"On the one hand, these intimidation effects, stigmatization effects, so that suddenly, other people turn away and say: 'I will not have anything to do with those people or groups.' They have in some way now been stigmatized. It is exactly with these large alliances [...] from the FDP [German Liberal Party, author's note] to the left-wing parties, [...] that it is very clear that other people, who are rather citizen-rights oriented or also very liberal, that they[...] will then perhaps not want to have anything to do with anyone [who] has been placed in this situation. [...] The other effect, [...] is that there is an overall tendency that the assemblies will no longer be announced, [...] as there are always people who will end up in some stored data or [...] who fear repressive measures". (AK2)

The processes for data collection and storage that are almost impossible for the involved parties to comprehend and above all the unclear categories for the definition of suspicion and dangerousness that can involve consequential police actions, often represent a disproportionate limitation of the fundamental right to informational self-determination. Even though persons affected by police data storage have the right to request which information is stored about them, under certain circumstances, exercising this right ends in slow and expensive procedures that cannot be managed by many involved parties. One reason for this is a lack of cooperation by the authorities (AK2). Also statements from legal experts provide evidence for the fact that during investigations, the police try not to disclose much about their work methods. This assessment has been confirmed by a review of parliamentary requests regarding the use of data and databases by law enforcement authorities, as a great deal of information about the police working methods has been classified as secret (See for example Bundestag, 2012, 2012a). Although the concern of the police to not disclose their work methods is understandable from an institutional point of view, this practice involves risks for the exercising of fundamental rights.

Also social contacts with certain people and basic day to day activities, such as visiting certain websites, participating in events and similar can possibly contribute towards the generation of suspicion and therefore be perceived as suspicious when this information is present in databases and linked via queries (AK1/2, JUR2). Within the context of combating so-called political extremism, there is the risk that the legitimacy of certain activities that are connected with exercising fundamental democratic rights could be jeopardised, such as participation in demonstrations or working together with and in political groups.

A police expert shows his concern that by exaggerating the extent of investigative measures police work can be regarded as too negative and therefore argued for a critical yet factual discussion:

> *"For this reason, we always wish, on the side of the police, to have a very critical discussion, but that the discussion is based on facts. Simply in order to prevent citizens from being afraid to go to the police. They should not be afraid to make a complaint because they think, 'oh, if I now make a complaint, then perhaps I will quickly change from being a victim to being the suspect and become involved in something.' They should place their trust in the police, that they are a guarantee for their safety and do not have any interest in limiting their freedom". (POL1)*

These and other statements show growing awareness of the importance of the relationship between the police and the citizens. In view of the technical simplification of collecting information, increasing technical interoperability of information systems of different authorities and the current attempt to lighten the legal hurdles for data exchange between institutions, the problem of unclear processes of data use becomes more important. In addition, the agreements regarding the transnational exchange of information through European institutions puts the relationship between security agencies and citizens to the test. In particular, data protection and the right to informational self-determination are at stake here. As there is no joint European contact point where it is possible to discover which institutions in which countries hold data about involved parties, the right to informational self-determination can only be exercised by making individual requests according to the respective national procedures. For the parties involved, this is in actuality not enforceable (AK2).

Within the EU, there are active efforts to intensify the exchange of information regarding "travelling violent offenders". (See ICF GHK 2013) This information is intended to be used in order to assess the danger of people and groups in the run-up to political and other large events and to follow up with measures. This includes the practice of keeping people or groups defined as dangerous from protests in order to prevent possible disturbances in advance – at the cost of revoking the possibility of political participation. The difficult to verify assessment of people as a security risk within the context of political processes can lead to limiting the freedom to travel and limit the exercise of fundamental political rights. There is also the risk that through the cooperation of different national authorities, the responsibilities will be shifted and divided so that the possibility for citizens to object to certain measures is made more difficult. Under the security policy premise, the development of critical European public protests is weakened and the exercise of rights and fundamental rights is possibly hindered. European data exchange therefore creates new challenges for data-related fundamental rights, such as the right to informational self-determination and data protection. In addition, there is the risk of limiting fundamental rights as when the exchange of data about political activists is used for the non-transparent definition of suspicion or dangerousness and therefore the development of a critical and politically active European public is impeded.

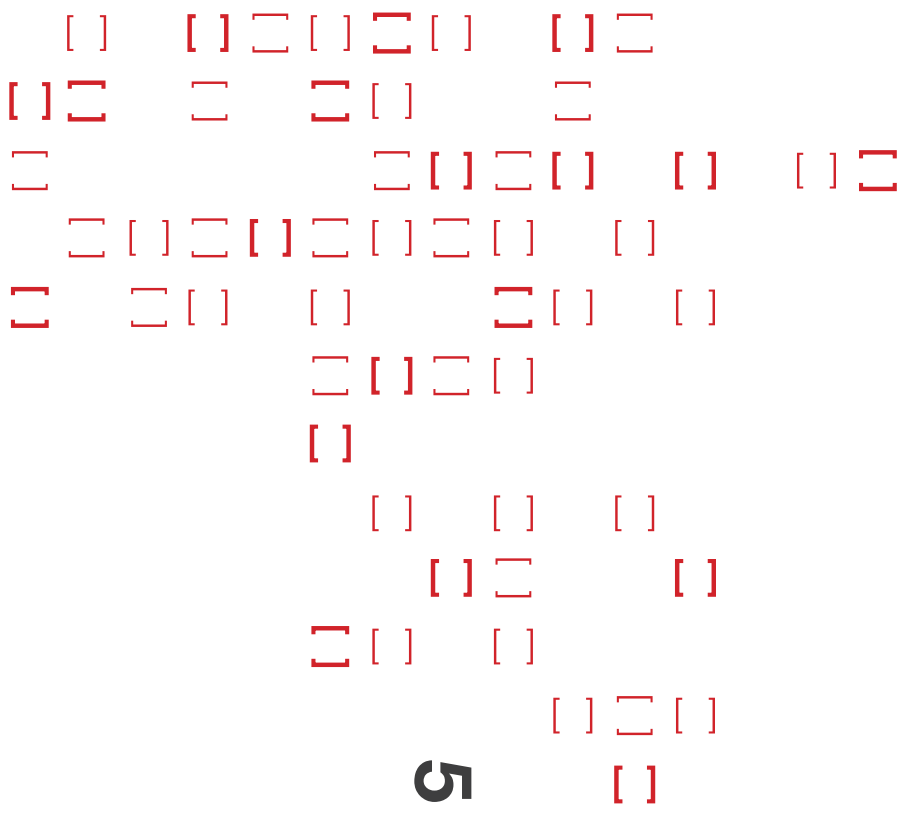
4

Conclusions

The term suspiciousness defines the limits for the scope of access of police measures. This scope can be described by zones of different levels of intensity of suspiciousness, which then permit certain methods for the police to gain access to parts of the population assigned to that zone. The construction of suspiciousness serves as a mechanism for the police to classify the population. Zones of suspiciousness classify the population either in relation to concrete acts or as risk or dangerous groups within the scope of prevention or averting danger. The establishment of suspicion and of zones of suspiciousness is also determined by the possibility of collecting and processing information, in order to derive grounds for suspicion. The digitisation of society has created new information sources that, with the use of data analysis tools, have created access to a wide range of information for the police. This knowledge about people, groups and social processes, in its form, is also established by the technicity of the data analysis tools. The technological possibilities of using knowledge in the long-term and in a mobile manner, favour a future-oriented approaches of police work, as they can rather operate to the concepts of danger and risk, for example for combacting so-called political extremism. In this context, the use of databases and data analysis tools causes an abstraction, and even a de-individualisation of suspicion, in a move away from concrete suspicion to the definition of dangerous structures. The use of multiple sources that require the mobility of information and its (partially) automated analysis in cooperations across institutional borders involves almost impenetrable processes regarding the construction of suspiciousness. If this takes place, such as in the context of averting or preventing danger, especially in a pre-trial phase of criminal proceedings, the comprehension of police measures is made more difficult, as often a check of legitimacy in court or in administrative proceedings possibly does not take place, and citizens can possibly not find out that they have been recorded or assessed as dangerous. In this way, suspiciousness or dangerousness, under the premise of averting danger, can lead to an abstract permanent condition that can be made context dependently by using data analysis tools.

The newly created uncertainties regarding the knowledge acquired using new sources and methods during preliminary proceedings and criminal cases refer to the necessity of creating work processes that permit valid forms of generating theories and exclude the unjust treatment of those involved in the proceedings. Therefore it is necessary to make the process of establishing suspiciousness transparent and understandable.

This case study has shown that the new possibilities available to the police to generate information, to make it available across agencies and to evaluate it using data analysis tools must lead to politics and society becoming concerned with how they can protect and expand upon the fundamental rights that are being threatened. This includes above all the protection of personal data, the protection of the core areas of private life and the right to informational self-determination. In addition, new non-transparent processes for the construction of suspicion and dangerousness can limit the exercise of fundamental rights by citizens. In this context, the transnational exchange of data represents a particular challenge, as it can affect the development of a European, critical political culture, which must be a central component of the formation of a democratic society.



References

[Amoore, L. (2008): Risk before Justice: When Law Contests Its Own Suspension, in: Leiden Journal of International Law, 21, 847-861.

[Amoore, L. (2011): Data Derivatives. On the Emergence of a Security Risk Calculus for Our Times, in: Theory, Culture & Society, 28(6), 24-43.

[Biermann, K. (2011): Dresdner Polizei fischte mit Datenschleppnetzen, http://www.zeit.de/digital/datenschutz/2011-06/polizei-dresden-vorratsdaten [30.07.2014].

[Bosco, F. et al. (in publication): Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities, in: Gutwirth, S. et al. (Eds.): Reforming data protection: The global perspective, Dordrecht: Springer.

[Bundesministerium des Innern (2013): Bericht des Bundesministeriums des Innern zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 24.04.2013, 1 BvR – 1215/07 (ATDG), auf die Zusammenarbeit und den Austausch von personenbezogenen Daten zwischen der Polizei und den Nachrichtendiensten (Stand: 24.10.2013). http://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/13-12-06/Anlage4.pdf?__blob=publicationFile&v=3 [8.8.2014]

[Bundeskriminalamt (Eds.) (1982): BKA-Vortragsreihe Bd. 28: Polizeiliche Datenverarbeitung, Wiesbaden: Self-published.

[Bundeskriminalamt. Der Datenschutzbeauftragte (2008): Errichtungsanordnung: PMK-links-Z, https://fragdenstaat.de/files/foi/603/ifg_bka_pmk-links_eao.pdf [20.05.2014].

[Bundesrat (2014): Drucksache 153/14: Gesetzesentwurf der Bundesregierung. Entwurf eines Gesetzes zur Änderung des Antiterrordateigesetzes und anderer Gesetze, http://www.bundesrat.de/SharedDocs/drucksachen/2014/0101-0200/153-14.pdf?__blob=publicationFile&v=1 [20.05.2014].

[Busch, H. et al. (1988): Die Polizei in der Bundesrepublik, Frankfurt a.M.: Campus Verlag.

[BverfG (2013): 1 BvR 1215/07 vom 24.4.2013, Absatz-Nr. (1 - 233), http://www.bverfg.de/entscheidungen/rs20130424_1bvr121507.html [01.08.2014].

[Chan, J. et al. (2001): E-policing. The Impact of Information Technology on Police Practices, Brisbane: Criminal Justice Commission.

[Cope, N. (2004): Inteligence Led Policing Or Policing Led Intelligence? Integratin Volume Crime Analysis into Policing, in: Brit. J. Criminol., 44, 188-203.

[Degele, N. (2002): Einführung in die Techniksoziologie, Stuttgart: UTB.

[Deutscher Bundestag (2011): Drucksache 17/8089: Antwort der Bundesregierung auf die kleine Anfrage „Umfang der zum Zwecke der Prävention geführten polizeilichen Dateien“, http://www.bundesrat.de/SharedDocs/drucksachen/2014/0101-0200/153-14.pdf?__blob=publicationFile&v=1 [20.05.2014].

[Deutscher Bundestag (2011a): Drucksache 17/5136: Antwort der Bundesregierung auf die Kleine Anfrage „Maßnahmen gegen ‘gewaltorientierten Linksextremismus’“ .. http://dip21.bundestag.de/dip21/btd/17/051/1705136.pdf [22.08.2014]

[Deutscher Bundestag (2011b): Drucksache 17/7307: Antwort der Bundesregierung auf die Kleine Anfrage „ Umfang der zum Zwecke der Prävention geführten polizeilichen Dateien“,http://dip21.bundestag.de/dip21/btd/17/073/1707307.pdf[27.08.2014]

[Deutscher Bundestag (2012): Drucksache 17/11582: Antwort der Bundesregierung auf die kleine Anfrage „Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen“, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf [31.07.2014].

[Deutscher Bundestag (2012a): Drucksache 17/8089: Antwort der Bundesregierung auf die kleine Anfrage „Computergestützte Kriminaltechnik bei Polizeibehörden“, http://dipbt.bundestag.de/dip21/btd/17/085/1708544.pdf [31.07.2014].

[Dix, A. (2013): “Funkzellenabfragen auf dem Prüfstand,” in: Datenschutz und Datensicherheit - DuD 37 (1), 6.

[EC (2007): Council recommendation of concerning a handbook for police and security authorities concerning cooperation at major events with an international dimension, ENFOPOL 171, http://www.statewatch.org/news/2009/dec/eu-troublemakers--handbook-2007.pdf [21.10.2014]

[Ericson, R.V./Haggerty, K. (1997): Policing the Risk Society, Oxford: Oxford University Press.

[Ferraris, V. et al. (2013a); Defining Profiling. Available at SSRN: http://ssrn.com/abstract=2366564 or http://dx.doi.org/10.2139/ssrn.2366564

[Ferraris, Valeria et al. (2013b): The Impact of Profiling on Fundamental Rights. Available at SSRN: http://ssrn.com/abstract=2366753 or http://dx.doi.org/10.2139/ssrn.2366753

[Gläser, J./Laudel, G. (2008): Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen. 3., überarb. Aufl. Wiesbaden: VS Verlag.

[Guagnin, D. et al. (2013): Evolution of technologies in profiling (Working Paper), http://profiling-project.eu/wp-content/uploads/2013/08/Evolution-of-Technologies-in-Profiling-08_08.pdf [18.06.2014].

[Harcourt, B.E. (2014): Governing, Exchanging, Securing: Big Data and the Production of Digital Knowledge, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2443515 [29.08.2014]

[Harnisch, S./Pohlmann, M. (2009): Strafprozessuale Maßnahmen bei Mobilfunkendgeräten – die Befugnis zum Einsatz des sog. IMSI-Catchers, in: Online-Zeitschrift für höchstrichterliche Rechtsprechung 5/2009, 202-217.

[Hempel, L. et al. (2009): Exchange of information and data between law enforcement agencies within the European Union. Discussion paper Nr. 29/09 des Zentrum Technik und Gesellschaft. http://www.ztg.tu-berlin.de/pdf/Nr_29_Hempel_Carius_Ilten.pdf [08.08.2014]

[Heinrich, S. (2007): Innere Sicherheit und neue Informations- und Kommunkationstechnologien. Veränderungen des Politikfeldes zwischen institutionellen Faktoren, Akteursorientierungen und technologischen Entwicklungen, Berlin: LIT-Verlag.

[ICF GHK (2013): Study on possible ways to improve the exchange of information on travelling violent offenders including those attending sporting events or large public gatherings, https://netzpolitik.org/wp-upload/travelling_violent_offenders_study_1.pdf [30.07.2014].

[Koops, B.-J. (2009): Technology and the Crime Society: Rethinking Legal Protection, in: Law, Innovation & Technology, 1, 1, 93-124.

[Landgericht Dresden (2013): Beschluss vom 17. April 2013, Az. 15 Qs 34/12; Amtsgericht Dresden, Beschlüsse vom 25. Februar 2011; Az. 270 Gs 711/11 und 270 Gs 729/11; Pressemitteilung vom 24.04.2013, http://www.justiz.sachsen.de/lgdd/content/1029.php [22.08.2014]

[Landtag Nordrhein-Westfalen (2014): Drucksache 16/6453: Antwort der Landesregierung auf die Anfrage: “Verfügt die Polizei in NRW künftig über ein Einbruchsorakel?”, http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD16-6453.pdf [29.08.2014]

[Laufer, B.: Ausreiseverbote für Nato-Gegner mit teils “haarsträubenden” Begründungen, in Telepolis, http://www.heise.de/tp/artikel/30/30064/1.html [27.08.2014]

[Lianos, M./ Mary, D. (2000): Dangerization and the End of Deviance: The Institutional , in: British Journal of Criminology 40, 2, 261-278.

[Lodde, R. (1972): Datenfernverarbeitung, in: Bundeskriminalamt (Eds.): Datenverarbeitung. Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 13. März bis 17. März 1972, Wiesbaden: Self-published, 25-37.

[Loven, H. (2011): Unbescholten im Fadenkreuz der Terrorfahnder. Als Linksextremist observiert und verhaftet, in: Deutschlandfunk, http://www.deutschlandfunk.de/unbescholten-im-fadenkreuz-der-terrorfahnder.862.de.html?dram:article_id=123852 [27.08.2014]

[Lyon, D. (2003): Surveillance Technology and Surveillance Society, in: Misa, T.J. (Eds.): Modernity and Technology, Cambridge: Massachusetts Institute of Technology, 161-184.

[Manning, P.K. (2008): The Technology of Policing. Crime Mapping, Information Technology, and the Rationality of Crime Control, New York: New York University Press.

[Mayring, P. (2008): Qualitative Inhaltsanalyse. Grundlagen und Techniken, Weinheim und Basel.

[Medick, V. (2014): „Neufassung des Antiterrordateigesetzes: Gesetzgeber muss Menschenrechtsschutz ernst nehmen“, http://www.spiegel.de/politik/deutschland/anti-terror-datei-bundesdatenschuetzerin-vosshoff-kritisiert-gesetz-a-982330.html [08.08.2014]

[Monroy, M., Jobst, H. (2009): ““Troublemaker” im Visier”, in: Telepolis, http://www.hei se.de/tp/artikel/29/29880/1.html [22.08.2014]

[Monroy, M. (2013): „Deutschland setzt sich durch: EU will “reisende Gewalttäter” überwachen und speichern“. Telepolis. http://www.heise.de/tp/artikel/39/39747/3.html [08.08.2014]

[Monroy, M. (2014): „Kleine Rasterfahndung“ bald alltäglich? Data Mining von Polizei und Geheimdiensten soll erstmals Rechtsgrundlage erhalten, https://netzpolitik.org/2014/kleine-rasterfahndung-bald-alltaeglich-data-mining-von-polizei-und-geheimdiensten-soll-erstmals-rechtsgrundlage-erhalten/ [20.05.2014].

[Monroy, M. (2014a): „Stille SMS“: Behörden verschicken immer mehr heimliche Ortungsimpulse, http://www.heise.de/tp/artikel/41/41664/1.html [30.07.2014].

[Oevermann, U. et al. (1994): Kriminalistische Datenerschließung. Zur Refoprm des kriminalsitischen Meldedienstes, in: Bundesriminalamt Wiesbaden (Eds.): Sonderband der BKA-Forschungsreihe, Wiesbaden: Self-published, 121-310.

[Perry, W.L. et al. (2013): Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations, https://www.ncjrs.gov/pdffiles1/nij/grants/243830.pdf [27.08.2014]

[Rose, N. (1991): Governing by Numbers: Figuring Out Democracy, in Accounting, Organzations and Society. Vol. 16, No. 7, 673-692.

[Reichertz, J. (1994): Polizeiliche Expertensysteme: Illusion oder Verheißung, in: Hitzler, R.: Expertenwissen: Die institutionalisierte Kompetenz zur Konstruktion von Wirklichkeit, Opladen: Westdeutscher Verlag, 193-213.

[Rutschke, W. (1972): Eröffnungsansprache, in: Bundeskriminalamt (Eds.): Datenverarbeitung. Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 13. März bis 17. März 1972, Wiesbaden: Self-published, 9-13.

[Scharff, T. (2008): Erfassen und Erschrecken. Funktionen des Prozeßschriftguts der kirchlichen Inquisition in Italien im 13. Und frühen 14. Jahrhundert, in: Lepsius, S.; Wetzstein, T. (Eds.): Als die Welt in die Akten kam. Prozeßschriftgut im europäischen Mittelalter, Frankfurt a.M.: Verlag Vittorio Klostermann, 255-274.

[Schramm, H. (1972): Zielvorstellungen des Bundeskriminalamtes zur Einführung der Datenverarbeitung, in: Bundeskriminalamt (Eds.): Datenverarbeitung. Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 13. März bis 17. März 1972, Wiesbaden: Self-published, 13-25.

[Schulz, L. (2001): Normiertes Misstrauen. Der Verdacht im Strafverfahren, Frankfurt a.M.: Verlag Vittorio Klostermann.

[Stuff, H.-G. (1982): Die Veränderung der Arbeitswelt des polizeilichen Sachbearbeiters, in: Bundeskriminalamt (Eds.): BKA-Vortragsreihe Bd. 28: Polizeiliche Datenverarbeitung, Wiesbaden: Self-published, 221-227.

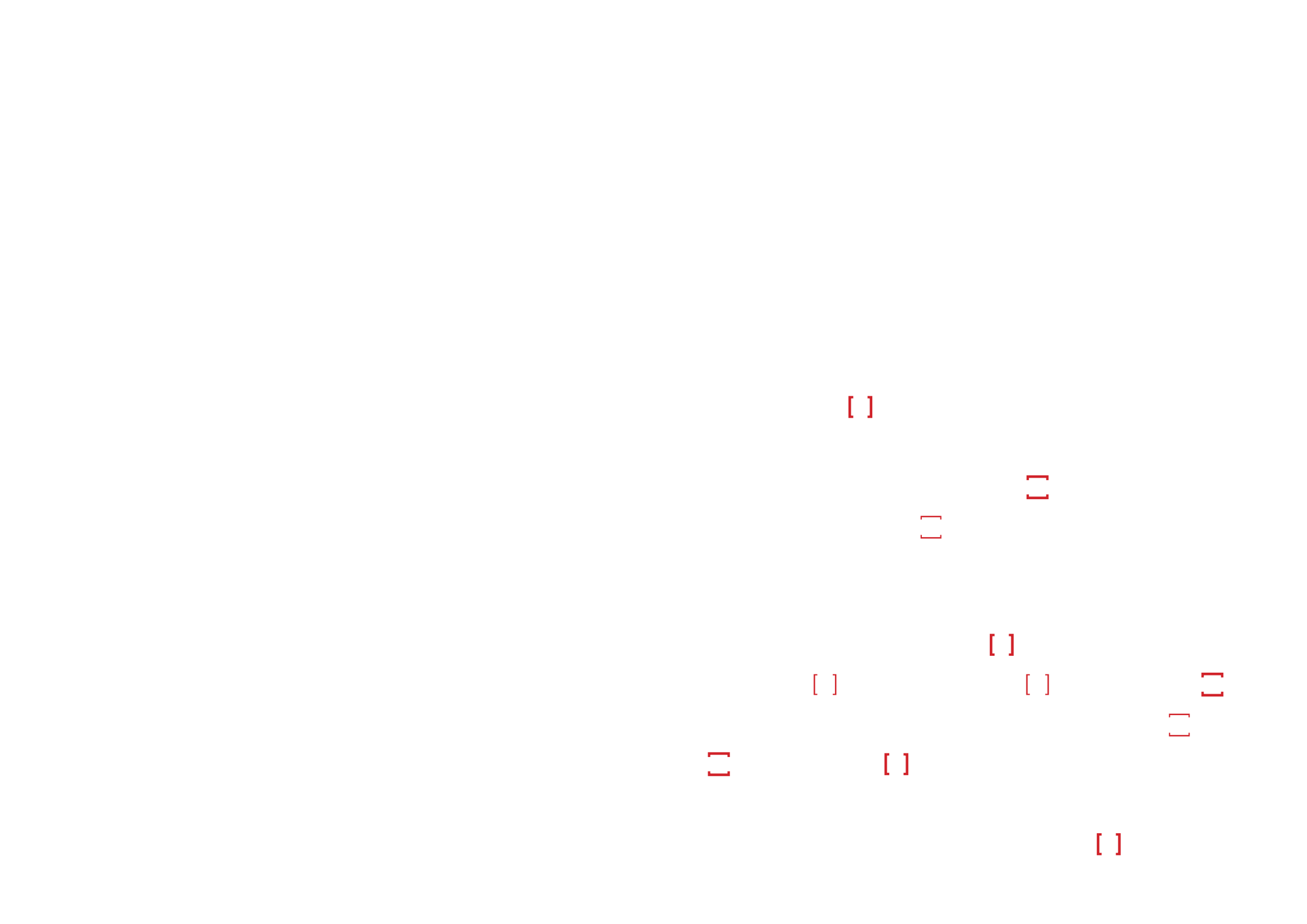
[Singelnstein, T. (2012): Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, in: Neue Zeitschrift für Strafrecht, 31, 11, 593-606.

[Töpfer, E. (2014): "Neufassung Des Antiterrordateigesetzes: Gesetzgeber Muss Menschenrechtsschutz Ernst Nehmen," Institut Für Menschenrechte, aktuell, 02/2014.U.S. Customs and Border Protection, U.S. Department of Homeland Security (2013): U.S. Customs and Border Protection Passenger Name Record Privacy Policy, http://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf, [30.07.2014].

[van Brakel, R/de Hirt, P (2011): Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, in: Cahier Politiestudies 2011-3 no.20, 163-192.

[Weinhauer, K. (2007): Staatsmacht ohne Grenzen? Innere Sicherheit, "Terrorismus"-Bekämpfung und die bundesdeutsche Gesellschaft der 1970er Jahre, in: Krasmann, S./Martschukat. J. (Eds.): Rationalitäten der Gewalt. Staatliche Neuordnungen vom 19. bis zum 21. Jahrhundert. Bielefeld: transcript Verlag, 239-265.

[Ziercke, J. (2013): Kriminalistik 2.0 – effektive Strafverfolgung im Zeitalter des Internets aus Sicht des BKA, http://www.bka.de/nn_243818/DE/Publikationen/Herbsttagungen/2013/Redebeitraege/herbsttagung2013Redebeitraege__node.html?__nnn=true, [29.08.2014]



Appendix: the questionnaire

DEFINITION and LEGISLATION

General questions

1. What is your understanding of automated profiling? Please consider as broad as possible a definition, as profiling done by machines, linking information stored in large or different databases.
2. Do you think that a definition of automated profiling by law is needed? If yes, why do you think it is needed? Do you have an existing or proposed definition?
3. According to your experience, which are the main technologies used in profiling contexts?
4. Could you please list the most important risk and the most important benefit of profiling techniques?
5. Is, in your opinion/experience, profiling a challenging area to be regulated? If yes, why?
6. The Council of Europe offers a definition of profiling that divides the profiling process into three stages[1]: 1) collection and storage of data, 2) correlation and analysis of data; 3) practical application of profiles. In your opinion, which of these steps need to be subject to a stricter regulation both at EU and national level?

Questions related to national legislation

7. Has Article 15 of Directive 95/46/EC[2] been transposed into your national legislation?
    a. If YES, please provide details of the national law and the text in the original and, if available, in English.
    b. If NOT, which provisions in national data protection law are relevant in relation to profiling?
8. As a Council of Europe member state, has your government implemented Recommendation (2010)13 on Profiling, or does it intend to do so? Which measures have so far been taken at the national level towards its implementation?
9. Art. 7 of the Council Framework Decision 2008/977/JHA[3] further addresses individual automated decisions, where data are processed within the context of police and judicial cooperation in criminal matters.

---

1 Application of Convention 108 to the profiling mechanism (2008): http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profiling_2008_en.pdf

2 Article 15 of DPD states: (1). Member states shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
(2): Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view, or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

3 Art. 7 of the Council Framework Decision 2008/977/JHA titled "Automated individual decisions" states: "A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests."

a. How has this provision been transposed into corresponding provision(s) in national measures?

b. Can you please share your opinion on possible limitations, from the data protection perspective, of this provision and/or its national implementation?

10. Apart from national provision(s) transposing Art. 15 of Directive 95/46/EC, are there any specific legal provisions or other rules or regulations on automated profiling in your legal framework?

a. If YES, please add the available documentation and provide a brief explanation of the definition used and of the main provisions. a(I). Which are in your opinion the main challenges of this provision, if any?

b. If NOT, are there other ways in which citizens are legally protected against profiling?

11. Is there any policy written by the DPA on the implementation of Article 15 and 12[4] of Directive 95/46/EC with regard to automated decision based on profiling?

If YES,- is this an internal guiding policy for the employees of the DPA, or a public policy addressing data controllers?

12. Are you entitled, as a data protection supervisory authority, to comment and advise on government proposals which interfere with citizens' right to data protection? For example to carry out audits or to scrutinize the pre-legislative phase? If so, please specify the form and legal basis.

Questions related to the General Data Protection Regulation (GDPR)

13. Please, list the main aspects regarding profiling that in your opinion are important to be included in the proposed General Data Protection Regulation (GDPR) under discussion.

14. That is your opinion on the present draft Article 20 of GDPR[5] (version January 2012)?

---

4 Article 12 of the DPD states: Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1); (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

5 Article 20 GDPR states: (1). Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.
(2). Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.
(3). Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.
(4). In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include

15. Which are the main weaknesses and strengths that you see in this provision?

16. The European Parliament has produced a report[6] on GDPR. What is your position on the proposals contained therein on profiling?

17. As you know European Data Protection Supervisor (EDPS) supports the article 20 provision with 3 main arguments[7]. What is your opinion on these arguments, especially on those related to your national context?

18. In the "Advice paper on essential elements of a definition and a provision on profiling within the EU GDPR" [8], the Article 29 Working Party has proposed a definition[9] and several suggestions on how to improve the article 20 GDPR[10]. What is your opinion on these arguments, with particular reference to your national context?

19. Where profiling in the police and criminal justice sector is concerned, what is your opinion on Article 9[11] of the proposed Directive on Data Protection in the law enforcement sector (COM(2012) 10 final)?

---

information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.
(5). The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

6 The full report is attached to this questionnaire as ANNEX I.

7 Here link to the EDPS opinion: http://www.europarl.europa.eu/document/activities/cont/201205/20120524ATT45776/20120524ATT45776EN.pdf The three main arguments are summarized below (see full text in Ferraris, Bosco, D'Angelo, Cafiero, Suloyeva (2013), "Defining Profiling", p.15, online at http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_definition_0208.pdf) "The EDPS supports the clarification provided by the Proposal on its scope of application and the development of the list of definitions (EDPS, 2012). With regard to the measures based on profiling, the EDPS supports the provisions of article 20 of the proposed Regulation. The article builds upon the existing Article 15 of Directive 95/46/EC on automated individual decisions, and extends its scope to all types of measures which produce legal effects on a natural person, not only to decisions. Firstly, the positive aspect is that it would apply not only to processing intended to evaluate certain personal aspects but also to those activities carried out to analyse or predict these aspects, therefore encompassing a broader category of processing. Secondly, it introduces a number of categories of personal aspects, which would fall under the scope of this provision, such as processing concerning an individual's economic situation, location, health and personal preferences. Thirdly, article 20(2) sets forth the conditions under which this type of processing may take place by way of derogation and it provides data subjects with the right to have human intervention but not with the right to submit their point of view, as is currently provided for in Article 15 of Directive 95/46/EC".

8 The full "Advice Paper" is attached as ANNEX II.

9 The definition proposed states that: "Profiling" means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements".

10 Main proposals for improvement concern the scope: "It […] welcomes Rapporteur Albrecht's proposal to broaden the scope of Article 20 covering processing of personal data for the purpose of profiling or measures based on profiling. The Working Party regards this as a necessary step towards more legal certainty and more protection for individuals with respect to data processing in the context of profiling"; a greater transparency and control for data subjects; more responsibility and accountability of data controllers; a balanced approach to profiling and the role of EDPB.

11 Article 9, "Measures based on profiling and automated processing" (1). Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests. (2). Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.

DOMAINS of APPLICATION

In the remainder of this questionnaire, we apply the following working definition of profiling – as elaborated in the framework of the PROFILING project:

"Profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (human or non-human, individual or group) subject. Constructing profiles is the process of discovering unexpected patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific subject or to identify a subject as a member of a specific group or category and taking some form of decision based on this identification and representation".

20. As far as you know, in which of the following domains is profiling applied in your country, at the national level?
    a. intelligence, national security, counter-terrorism
    b. criminal investigation
    c. border control
    d. finance (credit rating, anti-money laundering)
    e. healthcare domain (including insurance)
    f. employment
    g. education
    h. marketing
    i. social media and web
    j. behavioural advertising
    k. other, namely …
21. Can you list, for each of the previous domains, at least one potential risk and one potential benefit brought about by the application of automated profiling?
22. As regards profiling, which of the above mentioned domains is more challenging in your country?
23. How is the exchange of data between public bodies and private actors at national/regional level regulated?
24. Is there any law/regulation in your country on the collection of personal data and on the use of such databases? If YES, are there specific sectors involved (e.g. banking, telecommunications, etc.)?

COMPLAINTS AND REMEDIES

25. What is the procedure for data subjects' direct complaints for data protection violation to the DPA?
26. Do you also receive data subjects' complaints through associations/other bodies or entities?
27. How do you deal with the complaints received? What is the procedure followed?
28. Which are the most common reasons for complaining?

29. Have you ever received a complaint on automated profiling?

30. Do you investigate data processing practices at your own initiative? If so, have you ever investigated cases or processed of automated profiling?]

31. Are there compensation mechanisms (or similar practices) envisaged for data subjects whose rights have been infringed by profiling?

32. Are you aware of any other legal procedure for data subjects to be compensated in case their rights are harmed by automated profiling, e.g., civil liability or administrative complaint procedures?

33. Are there any relevant court cases on automated profiling in your country?

34. Is there a specific national training, instruction or guidance, on profiling for the DPA officials?

35. In your view, the number of complaints the DPA receives on profiling which percentage represent of the actual number of infringements?

FUNDAMENTAL RIGHTS: HOW FUNDAMENTAL RIGHTS/ PRINCIPLES RELATE TO PROFILING

36. In your opinion, which are the main fundamental rights and principles challenged by profiling?

37. Article 20 of Directive 95/46/EC envisages "prior checking"[12]. Does your DPA envisage any specific check procedure to be carried out to assess possible cases of infringements of fundamental rights and freedoms in profiling processes?

38. In which of the above listed domains of application of profiling (see question no. 19 Domains of application) is there a considerable risk of infringement of citizens' right of the protection of their personal data?

39. Can you provide concrete examples of infringements of fundamental rights/principles in the context of profiling? Have you ever processed a concrete case?

40. Thinking about concrete cases of infringements, can you rank the following fundamental rights/principles in terms of how they are challenged by profiling (1=the most challenged, 7=the least challenged)? Please include the rights/principles you mentioned in question 34 if they are not already mentioned.

- Autonomy and self-determination
- Due process
- Right to data protection
- Right to non-discrimination
- Right to privacy
- Transparency
- ...

41. Are you as DPA part of a network of bodies/institutions involved in human rights protection? If YES, please list the names of such bodies or institutions and your role within them.

12 Article 20 of Directive 95/46/EC, titled "Prior checking" states that:
1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

CITIZEN AWARENESS

42. In your view, which of the below points could have a major effect on data subjects' decisions to submit a complaint in case of automated profiling that significantly affects them? (more than one answer possible)

- awareness of their fundamental rights (e.g. data protection)
- transparency of the profiling process
- being informed that a certain decision is (partly) based on profiling
- knowledge of the logic involved in the processing
- compliance with the profiling authorization in change of services (e.g. on the web)
- awareness of the legal effects of individual measures based on profiling
- financial compensation to the data subject for breach of rights
- substantial fines for data processors being found to violate data protection rules

43. In your experience, which are the main limitations for data subjects' understanding of profiling risks and implications?

STRATEGIES FOR AWARENESS

44. How do you inform the general public about the right of data subject as regards data collected or used for profiling purposes? Do you face any significant technical or practical challenge in providing this information?

45. Do or did you produce any report/study/website on data protection, especially on profiling, to increase data subjects' awareness of such issues in your country?

46. Should data subjects' awareness of automated profiling and its possible implications be increased, and if so, how?

RELEVANCE OF THE QUESTIONNAIRE

47. Do you find the topic of the questionnaire relevant to your everyday activity or to the current policy debate on data protection?

- Yes, completely
- Yes, more or less
- No, not sufficiently
- No, not at all (Why?)

48. Do you have any additional information or comment you wish to share?

With financial support from the
“Fundamental Rights and Citizenship Programme”
of the European Union

---

unicri
United Nations
Interregional Crime and Justice
Research Institute

AMAPOLA
PROGETTI PER LA SICUREZZA DELLE PERSONE E DELLE COMUNITÀ

CENTRUL ROMÂN DE POLITICI EUROPENE
CRPE
DEBATING EUROPE
PROVIDING EXPERTISE

Tilt
Tilburg Institute
for Law, Technology,
and Society

TU berlin
