Ref. Ares(2012)1311294 - 07/11/2012

7 November 2012

Professor Andrzej Dziech
AGH University of Science and Technology
Project Coordinator, INDECT
Al. Mickiewicza 30
30-059 Krakow

Dear Professor Dziech,

The Working Party 29, consisting of all European Data Protection Authorities, has followed with interest and also with some concern the partially published outcomes of the research done by INDECT in the last years. As any by the INDECT research project developed technology needs to be in line with the European data protection framework before it can be implemented in real life environments whenever that technology involves the processing of personal data, the Working Party 29 would like to enter into a dialogue with you in order to get a better understanding of the technology developed and its impact on the privacy of European citizens. To start that dialogue we would like to invite you to answer to the questions formulated below.

The following first set of questions is linked to the research itself as it is currently undertaken. The aim is to understand how research is done on a technology that needs to identify persons or select individuals out of a large number of persons. Such technology most likely needs to be developed and tested with real data in order to be working and effective at the end of the project. This could for example be data from people that participate in person in the project or data from biometric databases from various sources.

- What kind of personal data is being used and for what purpose?
- What data is being saved, where and for how long?
- What is (are) the legal basis for the processing of personal data in the research?
- When consent is that legal basis, how do you ensure that every person whose personal data you use (e.g. the students that have participated) has given his informed consent?
- In order to test the tools designed for data-matching what kind of data is being used?
- What databases do you have access to?
- Did you only do research with students in controlled environments or also in real life environments?
    - Do you test data-matching applications using face recognition tools for example in social networks? If yes, you might find personal data of a third person. What happens with this data? Who has access? Do you inform this third person?
    - How and where (in what surroundings) do you test applications?

- Did you establish performance statistics (false positive/negative statistics) for all different scenarios / technologies you have developed and are those included in the documentation.

The following second set of questions aims to understand what kind of research is done and what possible impacts on data protection can be expected.

- How "criminal behaviour" is defined as opposed to abnormal behaviour (flash mob, civil protests, etc.)? How is it possible to discriminate between these different types of events? Can this be done without identifying the persons present on the video material? Can you give us examples?
- Regarding Intelligent Systems of audio recognition and sound classification aimed at detecting threats, which measures are in place in order to discriminate between odd behaviour (for example the shouts for joy of children playing inside the monitored area) and dangerous events (screams, explosions, etc.)?
- Which is the effectiveness of Intelligent Systems operating on publicly available Web sources in analysing and detecting criminal activities in Internet world? Especially where no video analysis is being done. How is it taken into account that well organized criminals prefer to use confidential networks to perform their activities?
- With reference to the aforesaid systems installed in the network infrastructure of an Internet Service Provider, which measures are in place in order to discriminate between the traffic of the person under surveillance and the traffic of all other ISP clients? Thus to avoiding a generalized interception of communications of all users?
- Does INDECT develop technologies that analyse and gather information over longer periods on the internet. If yes, how are data protection rights respected, specifically the right to be forgotten? Does it also crawl pages that are marked as “private” in the robots.txt.
- What is the role / use of watermarking. How is it used. Does it include personal data. Is hidden information in the pictures?
- What mechanisms have been developed to blur and reverse the blurring in pictures and video footage. Is this technology implemented by default in technologies developed by INDECT?

Your cooperation in replying to these questions and providing further relevant information until 19 November, enabling the Working Party 29 to get an overview and ultimately assess the data protection relevant issues, would be highly appreciated.

Yours sincerely,

Jacob Kohnstamm
Chairman of the Article 29 Working Party