Ref. Ares(2013)721102 - 18/04/2013

ARTICLE 29 Data Protection Working Party

Brussels, 18 April 2013

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

Dear Professor Dziech,

On behalf of the Article 29 Working Party I would like to thank you for your letter of 29 November 2013. I would like to share with you some concerns with regard to the replies to the questions sent on 7 November 2012.

Video footage must be considered in many cases as personal data because of its special nature. In its Opinion on the Processing of Personal Data by means of Video Surveillance (Opinion 4/2004 – WP 89) the Working Party stated that "image and sound data that relate to identified or identifiable natural persons is personal data:

a. even if the images are used within the framework of a closed circuit system, even if they are not associated with a person's particulars,
b. even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers,
c. irrespective of the media used for the processing – e.g., fixed and/or mobile video systems such as portable video receivers, colour and/or BW images -, the technique used – cabled or fibre optic devices -, the type of equipment – stationary, rotating, mobile -, the features applying to image acquisition – i.e. continuous as opposed to discontinuous, which may be the case if image acquisition only occurs in case a speed limit is not respected and has nothing to do with video shootings performed in a wholly casual, piecemeal fashion – and the communication tools used, e.g. the connection with a "centre" and/or the circulation of images to remote terminals, etc…

Identificability within the meaning of the Directive may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices."

It is understood that research needs space to discover new or better technological means or enhance the performance of existing tools. Indeed, the Article 29 WP acknowledges that the INDECT project sought for the consent of all involved persons and carried out experiments in

controlled areas. Nevertheless it is to be taken into account that when the research project involves the processing of personal data and it is likely to affect the privacy of European citizens not only the research itself and the way in which it is undertaken, but also the results of the research need to be in line with the fundamental rights, and in particular with the right of privacy and data protection, preferably before these results are implemented in practice.

The principles of "privacy by design" and "data minimisation" are of paramount importance when it comes to the implementation of the technologies the INDECT project aims to deliver. In this context a more substantial approach is required which combines the compliance with data protection regulatory framework of all data processing carried out with the proactive consideration of the implementation of "data minimisation", "privacy by design" and "data protection by default" principles in the development of new technologies and solutions.

The Article 29 WP appreciates that many of the described technologies aiming at detecting potential threats seem to be designed to focus the attention of security or surveillance operators to possible dangerous events, like for example abandoning a luggage, through "innovative human decision support algorithms" that do not need to identify the persons on the video footage.

However it would be desirable to develop technologies and solutions that do not require and do not foresee the storage of the video images processed or retrieved data of alleged online criminal activities, because also blurred pictures that carry the unblurred information in an encrypted form or any other technology allowing to hide information (as the watermarking technology described in your letter), entail privacy and data security risks that can only be entirely mitigated by not saving them in the first place. Moreover, it is not compatible with the original purpose to keep or store information that could include personal data (even if indirectly identifiable) that is only "potentially useful in the future".

The Working Party will continue to closely monitor the developments regarding the further developments in the research and implementation of INDECT technologies and invites you to continue the dialogue.

Yours sincerely

Jacob Kohnstamm
Chairman