

1. What is the current status of the project?

INDECT started the 3rd year of work. Almost 3 years are ahead of the project. All project tasks are realized according to the schedule.

Current status of the work can be also reflected in numbers:

- Research activities of INDECT resulted in over 75 publications in 2010
- 25 project meetings were organized last year (2010)
- An international conference: "Multimedia Communications and Security Services 2010" organized by the project was attended by over 100 participants and almost 50 scientific papers (<http://mcss2010.indect-project.eu/>)
- Another edition of the conference will be held in June 2011 (<http://mcss2011.indect-project.eu/>)

New techniques related to watermarking, semantic analysis and image processing have been developed.

2. The project INDECT been criticized from many sides. It appears mainly from the fear of total surveillance of the EU population.

According to all existing technologies such as video surveillance, data retention, telecommunications, face recognition, websites, discussion forums, Usenet groups, data servers, P2P networks and individual computer systems and existing databases, such as names, addresses, biometric data, Internet messages, police, intelligence, military, forensic and civilian databases, data of air-and sea-based platforms and satellites linked together logically and can be evaluated and managed in real time. Is that correct?

It is not correct at all.

INDECT complies with all requirements concerning research project within the scope Security Call of the 7th Research Program. The Program is run by European Commission and agreed by European Parliament.

More information about the objectives of the Call can be found at:

ftp://ftp.cordis.europa.eu/pub/fp7/docs/wp/cooperation/security/k_wp_200801_en.pdf

Security is one of the main priorities of European Union what was confirmed at European Security Research Conference in Stockholm in 2009.

INDECT is only one of over 60 projects realised in the scope of the Security Call.

No surveillance of the EU population is done by INDECT and certainly no "total surveillance" takes place.

The project concerns development of advanced technologies to be applied for detecting threats related to terrorism and serious criminal activities.

In each case final decision regarding the degree and the source of threat is taken by an authorised person (not the system which only supports the decision making process).

In particular INDECT is absolutely *not* involved in the surveillance of:

- Personal data,
- The content of telecommunications voice connections,
- Public data servers,
- Individual computer systems (unless a writ is issued and the personal computer is physically “arrested”)
- Public databases with names, addresses, biometric data
- Police, intelligence, military, forensic or any other such kind of data bases
- Exchange of mails
- Data of air- and sea-based platforms and satellites (linked or not)

The project does not intend to perform automatic linking between different categories of information.

All personal data that is processed at the experimental part of the research is related to persons who were informed about the scope of the research and agreed to take part in the project tests.

Quite often INDECT researchers are surprised by the news coming from media and other sources informing about the areas of research and objectives of the research. Just to give one example: one of the speakers at an event organised by Chaos Communications (Berlin, December 2010) claimed that INDECT technology gathers information from, and fills up central data bases such as Schengen Information System (SIS), border control system, “dangerous people” data bases, movement databases (flight information records, toll, rail tickets), social security data, customer databases, financial transactions, RFID sensors, banking information and VISA Information System (VIS), etc.

According to the same source “INDECT technically and organizationally supports the EU border protection agency FRONTEX.”

Such kind of misleading and untrue information is sometimes broadcasted to the public giving rise to misunderstandings about the project.

3. Or could you differentiate which of these measures are definitely intended?

INDECT solutions are introducing some kind of ‘intelligent analysis’ into the existing monitoring systems.

This will allow for detecting such threats as for example a weapon in a hand of potential criminal.

The project also performs research on tools for detecting threats related to internet, such as for example: human organs trafficking, child pornography, etc.

A simplified example of usage scenario could look as follows:

- At the first step INDECT tool detects a potential threat through analysis of camera image, (for example a gun in a hand of a person in a bank or an unattended luggage).
- The second step is to indicate the threat to a person responsible for security (e.g. police officer).
- Subsequently the person in charge analyses the information, judges if it is not just a false alarm, assesses the level of threat.
- Finally, if there are justified reasons, decision of relevant security action is undertaken.

Furthermore, new methods for privacy protection are elaborated, e.g. hiding faces of persons being in the recorded video sequences. The methods are mainly based on digital watermarking.

New cryptographic algorithms are developed in the project for more efficient protection of stored and transferred data.

4. How do you respond to criticism?

We regret that incorrect or simply false information about INDECT can be found in media.

We publish project results at scientific journals and at conferences.

Project web page is continuously updated.

Project is present at main events related to security research, ethical issues and societal impact of the research.

We present the project scope and results to media and to politicians (in particular to MEPs).

We clarify misunderstandings and untrue information about the project objectives and work done in the project.

As written above, INDECT organised an international conference: “Multimedia Communications and Security Systems – 2010” which, obviously, was open to public. Results of all INDECT working groups were presented at the conference. The audience could ask any question related to the research.

Besides, methods used by some opponents of the project put in question credibility of such persons or groups. An example:

We have noticed a 'curious' page on the Internet. Its address is very similar to our real address: <http://www.indect-project.eu/>.

From the information about who registered the domain, one may read that the site was registered in Cologne, Germany. The content is very similar to the original as well. In practice, it has been copied from the contents of our site, but with the modification (to our detriment) of certain facts. For example, the fake site is unreasonably suggesting that the INDECT research is based on investigation of all people or worldwide unified watching of humanity! In our opinion, this type of illegal, misleading action is a typical example of defamation.

5. How do you view the tension between the INDECT project and the informational self-determination?

We do not see any contradiction between the project and informational self-determination. INDECT tools have for objective to search for threats (like acts of terrorism, serious crime, child pornography, human organs trafficking, etc.) and support defining sources of threats. The project does not (and would not be technically capable) to perform surveillance of the society as a whole and/or individual computers of all citizens (as it is sometimes claimed).

What is done is supporting of ‘traditional’ methods of police work with intelligent analysis of information that is already available to police services.

The definition of privacy to which you referred: “The right of the individual to decide what information about himself should be communicated to others and under what circumstances” is not violated in our research. Current, manual methods will be replaced by innovative, semi-automatic technologies – still being in line with all national and EU legal regulations.

INDECT Project was a subject to scrutiny carried out by Polish General Inspector of Personal Data Protection (pol. Główny Inspektor Ochrony Danych Osobowych – GIODO). Following the scrutiny a letter was issued by the Office of GIODO signed by The Director of Inspection Department. The letter states that the scrutiny had for the scope the compliance with regulations concerning protection of personal data (law from 29th August 1997 on Protection of Personal Data) and regulation of the Minister of Interior Affairs and Administration, with respect to processing of personal data and technical and organisational conditions that equipment and information systems used to process personal data should be conformant to.

The audit has shown that the project fulfils all the requirements relevant to personal data protection regulations.

As all the projects realised in the domain of security research of EU 7th Framework Program INDECT was a subject to reviews done by independent experts, in particular Ethical Review.

INDECT Ethics Board is a body which is responsible for overseeing ethical issues in the research process and with respect to tools developed by the project. The body is composed of members representing different areas (human rights lawyer, police, ethicist, academia, industry). Every project report is subject to review of the Ethics Board.

Ethics Board assures that privacy and data protection rules are obeyed in the project.

6. What about the right of presumption of innocence?

As stated above INDECT does not 'spy' on citizens. INDECT tools anonymously detect potential threats (e.g. appearance of dangerous tools in the video recording). After the source of threat is detected regular policing and legal procedures are applied.

7. Is there an independent review of suspicion?

The question was answered at the question 5 (if we do understand the question correctly).

8. How to prevent misuse by an implementation of the project?

INDECT is a research project aimed at development of technologies and security research. Some of the results could be implemented as prototypes only.

What is done within project is developments of procedures and methods for securing access to some of INDECT tools. In particular authentication and authorisation methods are considered.

Additionally logging of all activities of police officers using these tools is planned. Logging system would record such information as: who accessed what information at what time, from which pc, where the information was sent to, etc.).

There are measures that are recommended for end-users of INDECT tools (police departments). These measures comprise proper selection and training of persons having access to the tools.

The implementation of technologies being developed into operational systems is not covered by the INDECT Project. We are researchers, we create the program and technologies. How it will be used depends on the end-user and EU regulations. The system will probably grow, but there will be more and better protection of personal data.

The protection of personal data is also one of the most important topics of INDECT.

It's like with cars. They are getting faster, but they are safer with airbags, ABS. People want security but also privacy. One does not exclude the other.

9. What mechanisms / bodies / institutions to ensure this?

The question was answered at the question 5 (if we do understand the question correctly).