FuturICT.hu

„Infocommunication technologies and the society of the future (FuturICT.hu)” project

TÁMOP-4.2.2.C-11/1/KONV-2012-0013

ÚJ SZÉCHENYI TERV

How Hungarian data protection framework is used for crime prevention

Dr. Zoltán Alexin, PhD.
University of Szeged,
Department of Software Engineering
H-6720 Szeged Árpád tér 2.
e-mail: alexin@inf.u-szeged.hu
http://www.inf.u-szeged.hu/~alexin

OPENSUR-2013 Workshop, 2-3th July, 2013. Ljubljana, Slovenia

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

http://www.futureict.eu

Who am I

- Mathematician, PhD. on application of machine learning algorithms to natural language problems
- Created and supervised several R&D projects on this topic
- Since 2004, I began studying privacy issues
- Member of a regional medical ethics committee
- Contributed in the Association on Fair Data Processing
- Member of the presidential board of the Hungarian Data Protection Society
- Common research project with Joseph Cannataci
- Blogger
- Proceedings before Civil Courts, Constitutional Court, European Commission, ECtHR
- Achievement: excluding data from the National Health Insurance Fund database connected with unsubsidized care events, ethics approval of medical research projects without intervention, some minor results

Content

- Uniqueness of the Hungarian data protection legislation
- An introduction to Hungarian data protection legislation
- The bipolar nature of Hungarian data protection and its general consequences
- How this data protection framework is used for crime prevention and law enforcement
- Policy recommendations
- Conclusions

Unique feature of Hungarian data protection legislation

- EU 95/46/EC Data protection directive Article 7.
- Member States shall provide that personal data may be processed only if:
  - (a) the data subject has given his consent; or
  - (b) processing is necessary for the performance of a contract to which the data subject is party; or
  - (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
  - (d) processing is necessary in order to protect the vital interests of the data subject; or
  - (e) processing is necessary for the performance of a task carried out in the public interest; or
  - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party.
- **The red points are not implemented.**

New legislation framework

- New Basic Law (Constitution) from 1st January 2012.
- New Law on Constitutional Court 1st from January 2012.
- New Data Protection Law from 1st January 2012.
- New Law on Misdemeanors from 15th April 2012.
- New Labor Code from 1st July 2012.
- New Law on Public Transportation Services 1st July 2012.
- New Penal Code from 1st July 2013.
- New Higher Education Law from 1st July 2013.
- New Civil Code from 15th March 2014.
- etc.

New Data Protection Law

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
- (1) Personal data may be processed under the following circumstances:
  - a) when the data subject has given his consent, or
  - b) when processing is necessary as decreed by law or by a local authority (hereinafter referred to as "mandatory processing").
- (2) Special categories of personal data may be processed according to Section 6, and under the following circumstances:
  - a) when the data subject has given his consent in writing, or
  - b) when processing is necessary for the implementation of an international agreement, or
  - c) when processing is provided for by a law because it is necessary for the performance of a task carried out in the public interest concerning the data under Point 3.b) of Section 3.

Cases C-468/10 and C-469/10

- European Court of Justice 24 November 2011
- (Directive 95/46/EC – Article 7(f) – Direct effect) in Joined Cases C-468/10 and C-469/10
  - 1. Article 7(f) of 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 must be interpreted as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources, thereby excluding, in a categorical and generalized way, any processing of data not appearing in such sources.
  - **2. Article 7(f) of Directive 95/46 has direct effect.**

Bipolarity of the DPA

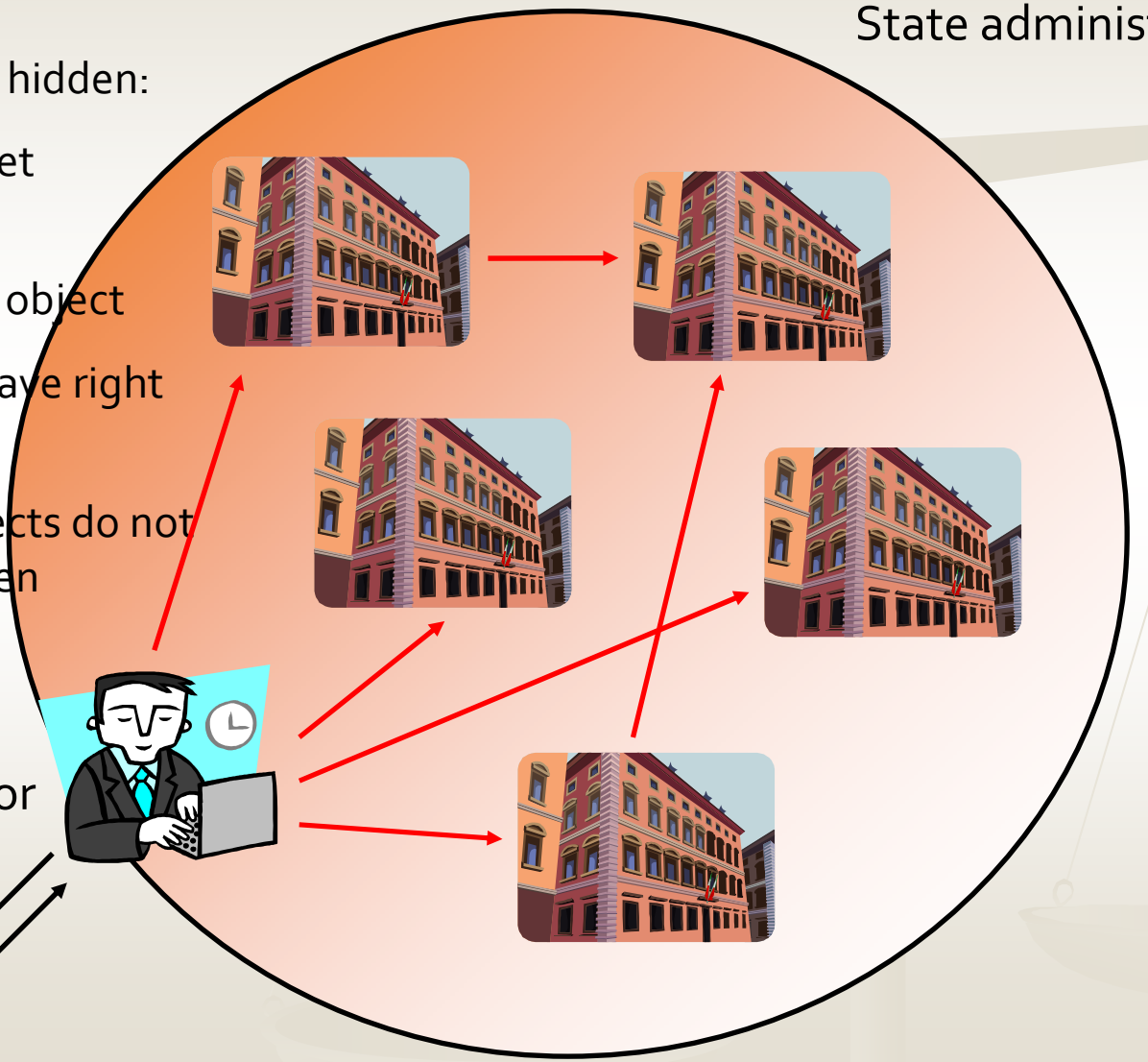
- There are two cases when personal data can be processed:
  - Data subject give consent
  - The law provides for the data processing (legal obligation)
  - (In fact, data can be processed in the life interests of the data subject.)
- A novelty of the new DPA is that data can be processed in the legitimate interests of the data controller or third party, *but only when obtaining consent is impossible or requires disproportionate efforts (Google Street View).*

Paternalistic legislation

State administration

State Administration is hidden:

- data subjects do not get preliminary information
- data subjects may not object
- data subjects do not have right to get legal remedy
- many times data subjects do not have right to be forgotten



primary data processor

data subject

Paternalistic data processing

- Tremendous number of secondary data processing laws and decrees (3-400 laws and 3-400 decrees)
- The task of the data protection authority is to check whether data is processed by legal authorization
- When a public body processes personal data without authorization – then the government will amend the regulation so as it would be legal (tug of war)
- The data protection authority has not the necessary influence on regulation and data protection practice

Centralized databases

- Contain data about all Hungarian citizens, and sometimes about foreigners:
- Population registry, resident address registry, social security database (employment and medical history), taxation registry, business companies register, transportation databases (handicapped parking permits, driving licenses, toll road entry/exit), car register (damage history, mileage, insurance, owner), misdemeanor registry, criminal history registry, personal bank credit history, *medical prescription registry* etc.
- From the service providers: medical data, telecommunication data, PNR (passenger's personal data).

How the police acquires data

- Act XXXIV. of 1994 on the police
  - Police may request any types of personal data from the centralized registries, and from service providers whenever it is need for crime prevention
- Act XIX. of 1998 on prosecution procedure
  - Investigation authority (police) is allowed to order seizure of evidences if those are supposed to be connected with a criminal act
  - Computers or data media can also be seized (introduced explicitly in the law in 2012)
  - Seizure of medical or lawyer's documents shall be approved by a judge

CCTV cameras

- Act XXXIV. of 1994 on the police
  - Surveillance of public places can only be done by the police
  - The inside of public transportation vehicles are public places, therefore the surveillance is done by the police (8-30 days).
- Act I of 2012 the labor code
  - It allows proportionate data processing if the employees are informed beforehand
- Act CXXXIII of 2003 on condominiums
  - Allows to install cameras if at least the 80% of the owners agreed (15 days, operated by a security guard)
- Recommendation of the National Data Protection and Freedom of Information Authority
  - 2013 January

Telecommunication data

- Act C. of 2003 on the electronic communication
- Implementation of the Data Retention Directive 2006/24/EC
- The case before the Constitutional Court ceased because of the new law, the Ombudsman of Hungary was asked but did not afford to the Constitutional Court according to the new law
- Telephone metadata is stored for 1 year, web logs are stored for half year by the service providers
- The police may request data from the database in connection with any kinds of investigation
- Telecoms are retaining data for 7 years for accounting purposes and the police requires personal data back to 7 years threatening the telecom with seizure of their computers

Road misdemeanors

- Act II of 2012 on misdemeanors (minor offences)
- First it was against speedsters (who are disobeying the speed limits) but later many minor offences were included like soil pollution, fishing and hunting without permission, providing false statistical data, disobeying regulation on staying on ice etc.
- Three strikes (for the third offence within 6 months the penalty will be more serious)
- Objective responsibility of the owner: if they (he and the driver) do not want to name the actual driver – the owner of the car will pay the fine
- Automatic fining, police radars installed on highways and automatically send photos to the owner
- The central database of misdemeanors is keeping records for 3 years

Policy recommendations

- Data protection law is maintained by the Ministry of State Administration and Justice, secondary data protection laws and decrees are maintained by many stakeholders (ministries) having different interests.
- The amount of legal text (700 rulings) prevents harmonizing the regulation, even functioning the state of law.
- Deregulation is needed as well as the state has to give more rights to data subjects (e.g. afford to the Court).
- Only the deletion can prevent personal data being used further. (Peter Schaar)
- I would allow the police to access special categories of personal data (medical) in the life interests of somebody.

Thanks for the attention!