

# Managing personal data across the EU in the age of Big Data and Information Fusion

**Juan Gómez-Romero**

Visiting Researcher · Data Science Institute

Research Fellow · Universidad de Granada

# Motivation

*Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."*

Warren, S., Brandeis, L. The right to privacy. Harv Law Rev 1890; 193: 193–220.

HARVARD  
LAW REVIEW.  
VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in *Millar v. Taylor*, 4 Burr. 2302, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

# Motivation

## Energy in TIME project

Reduction of energy consumption by improved building operation

Data repository of energy consumption data

- User occupancy & behaviour
- Four demo sites: Faro, Bucharest, Helsinki, Levi



## ePOOLICE project

Organised crime prevention

Data repository of crime indicators and trends

- Data from social networks to detect opinion and events
- EU, national, and regional law enforcement agencies



## Motivation

What are the limitations of using personal data?

.

.

*What is 'personal data'?*

*Legal framework?*

*Ethical limits?*

*Technical implementation of measures?*

*Is anonymization enough?*

*What should I do in <my project>?*

.

.

# Personal Data & the Right to Privacy

## Personal data

Data that can lead to a univocal identification of a specific individual, and also can include additional information of interest attached to them.

## Big data analytics & privacy

### *A) Identification capability*

Even though in some cases sources alone do not include personal data, it may happen that further analysis or the combination of them may reveal the identity of individuals and characterize them.

... when datasets are combined to other sources (Sweeney 1997)

... when datasets measure traceable human behaviour (de Montjoye et al. 2015)

### *B) Interest*

Personal data can be the object of interest of an application.

## EU Legal Framework (1/4)

**Directive 95/46/EC** on the protection of individuals with regard to the processing of personal data and on the free movement of such data

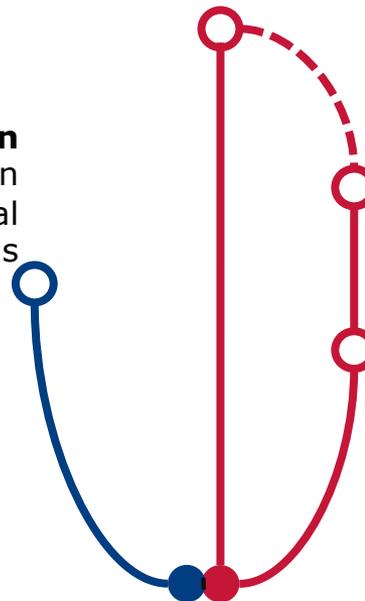
**Council Framework Decision 2008/977/JHA** on the protection of individuals and their personal data used in criminal investigations

**Directive 2002/58/EC** concerning the processing of personal data and the protection of privacy in the electronic communications sector

**Directive 2009/136/EC**

**Directive 2016/680** on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

**Regulation 2016/679** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data



## EU Legal Framework (2/4)

**Supervisory authority:** Public authorities responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to the Directive.

**Data controller:** Natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

**Privacy impact assessment (PIA):** Methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts

**Privacy by design:** System design paradigm that considers privacy since the very inception of a data processing system, and promotes the implementation of safeguards by means of a multi-level stack of technologies

## EU Legal Framework (3/4)

**Directive 2016/680** defines the requirements that must be followed by competent authorities of the Member States to process personal data for the purpose of security and criminal investigation

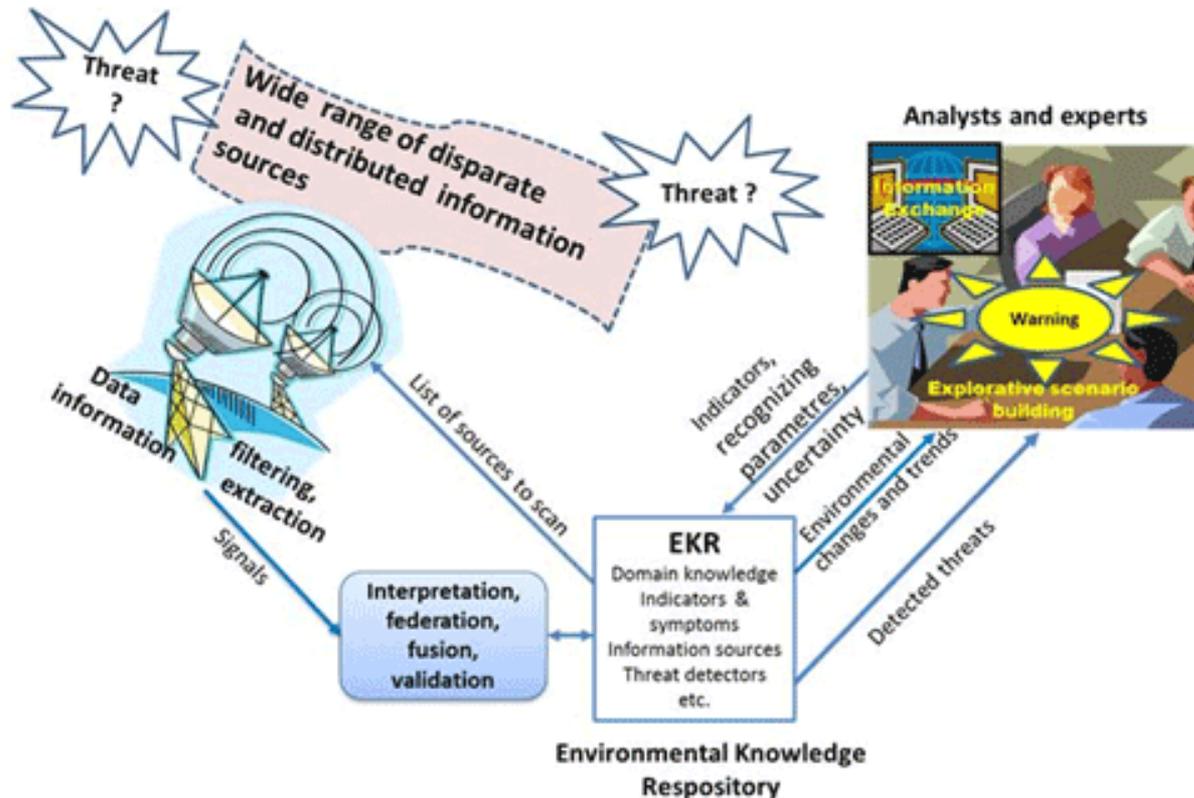
- Data collection and processing must be done for **specified, explicit, and legitimate purpose**
- **Other uses are allowed** if not incompatible with the purposes for which data were collected
- **No collecting excessive data**, no processing data excessively –particularly with the aim of *profiling* or *tracking*
- **No fully automated decision-making** based on data analysis –allow human users in the loop

## EU Legal Framework (4/4)

**Directive 2016/680** defines the requirements that must be followed by competent authorities of the Member States to process personal for the purpose of security and criminal investigation

- Guarantee the **right to access data** by the subjects; as well as **rectification, erasure, or blocking** –exceptions may apply depending on the national laws
- **Security** of data storage and transmission
- **PIA is compulsory** for activities potentially involving personal data
- Transfers to third countries are regulated by the **Privacy Shield** treaty

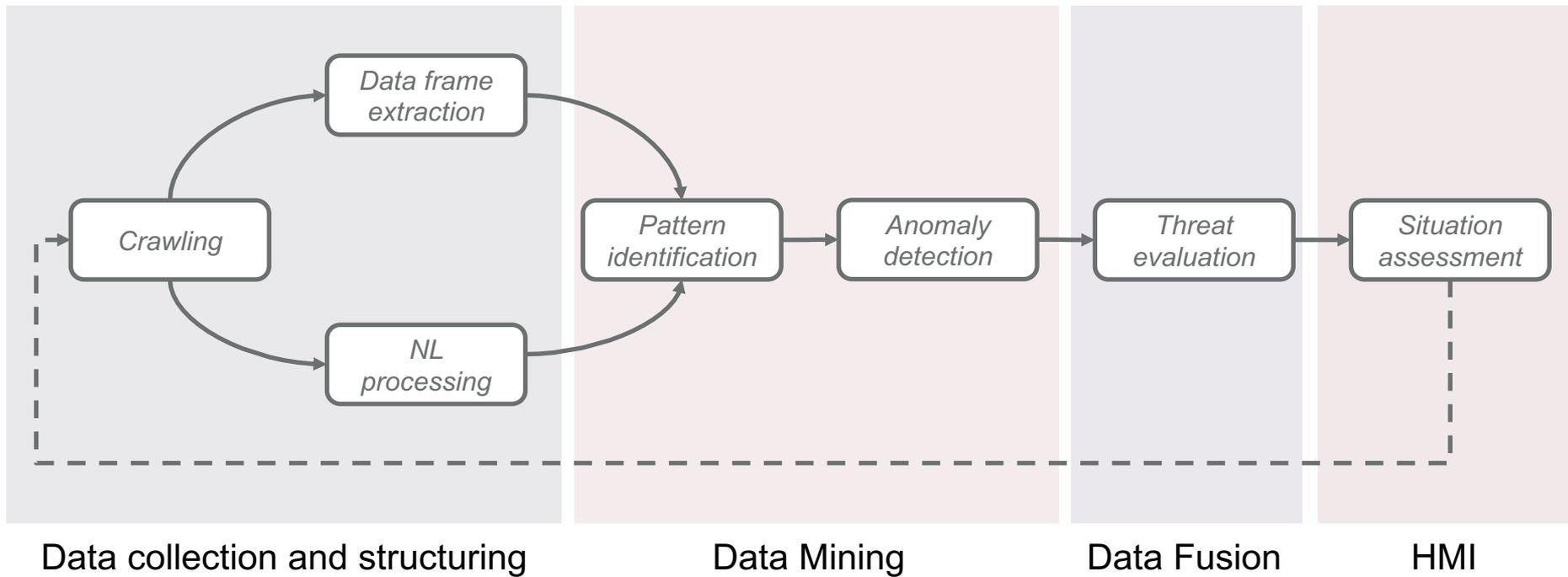
## A Practical Use Case: Environmental Scanning for OC Prevention (1/4)



© ePOOLICE Project Consortium

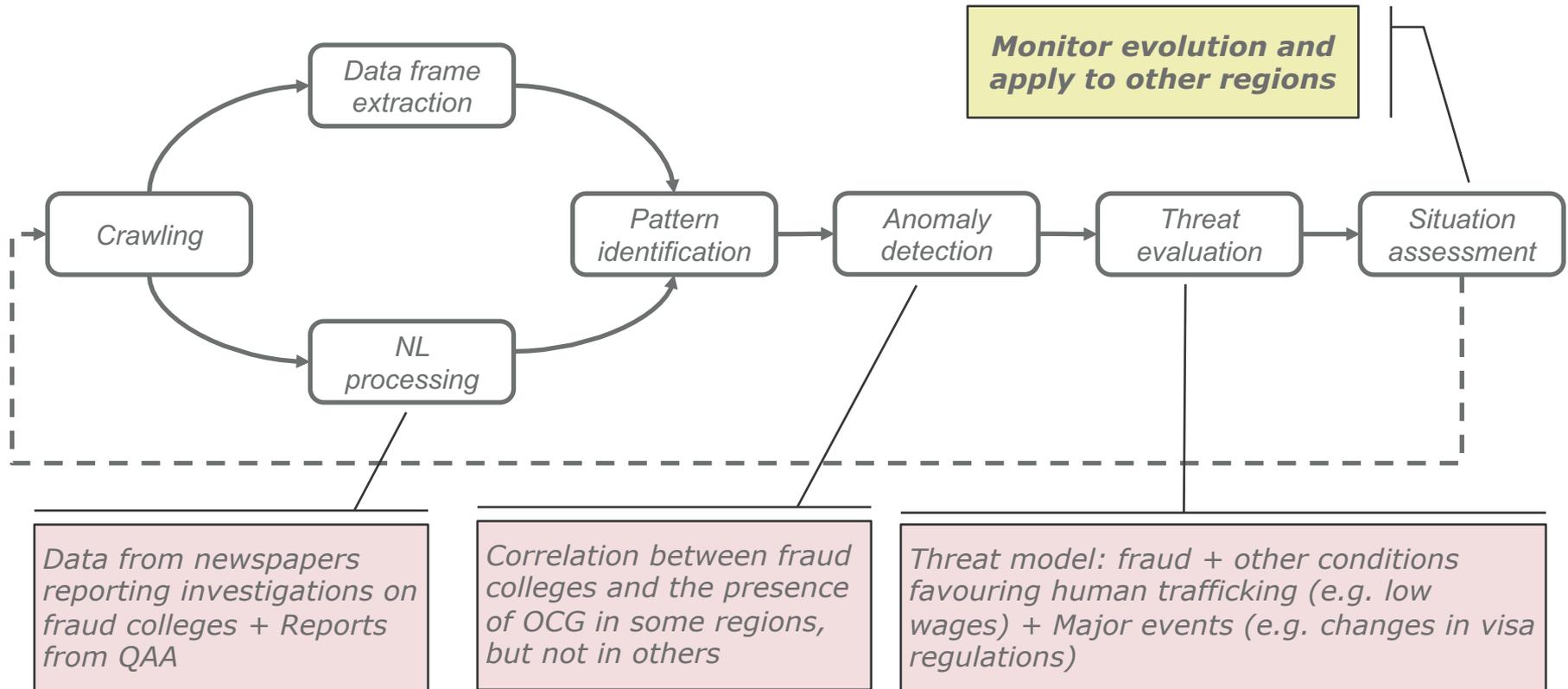
Identify and monitor indicators and facilitators of present and future development of organized crime activities

## A Practical Use Case: Environmental Scanning for OC Prevention (2/4)



## A Practical Use Case: Environmental Scanning for OC Prevention (3/4)

### Monitoring Human-Trafficking Indicators in the UK



# A Practical Use Case: Environmental Scanning for OC Prevention (4/4)

The screenshot displays the ePOOLICE Organised Crime Tool interface. On the left is a navigation menu with options: Overview, Layers, Threat Rules, Modelled Activity Threats, Modelled Threat Estimation, Corroborated Threats (highlighted in green), Combined Regional Threats, Regional Data, Sentiment, Analyse, Horizon, Documents, Categories, and Rules. The main area shows a map of Ireland with a date range of September 26, 2016 - September 27, 2016 and Categories (0). A pop-up window titled 'Corroborated Threat' is open, showing 5 attributes and 6 sources. The threat is located in Calne, with categories 'RentedHomeOrApartment' and 'VictimGeneral'. Attributes include 'country: england', 'city: calne', 'organization: independent press standards', and 'drug: cocaine'. Sources are listed as 'The Wiltshire Gazette and Herald | News' and 'The Wiltshire Gazette and Herald | Local'.

**ePOOLICE Organised Crime Tool** Alt C

September 26, 2016 - September 27, 2016 Categories (0)

**Corroborated Threat** 5 attributes 6 sources

**Around location** calne

**Categories**

- RentedHomeOrApartment
- VictimGeneral

**Attributes**

- country: england
- city: calne
- organization: independent press standards
- drug: cocaine

**Sources**

- The Wiltshire Gazette and Herald | News
- The Wiltshire Gazette and Herald | Local
- The Wiltshire Gazette and Herald | News
- The Wiltshire Gazette and Herald | News
- The Wiltshire Gazette and Herald | Local
- The Wiltshire Gazette and Herald | Local

## A Practical Use Case: Privacy Impact Assessment (1/2)

### Privacy Impact Assessment

- Personal data might be processed, but it is not the objective of the software –aims to analyse general trends, rather than to identify criminal acts and perpetrators
- Purpose is legitimate –OC is a major threat to society
- Only open data sources are used as input –no closed sources, no hacking into personal accounts
- **Open social networks are not used**
  - Open Closed parts are not part of the discussion
  - Not significant increase of the accuracy of macro-indicators
  - Not possible to delimit the situations in which big data analytics could lead to privacy interference
  - Ethical considerations –users' purpose for disclosed data is different

## A Practical Use Case: Privacy Impact Assessment (2/2)

### Privacy Impact Assessment

- Data storage
  - Characterization
    - Metadata (provenance, access-level)
    - Physical distribution
    - Pseudo-anonymization of named entities –not enabled in final version
  - Security
    - Password-based access
    - IP filtering
    - Access logging –at different levels
    - Encrypted data transmission between components
  - Data subject's rights
    - Query, modification, and erasure
- Comprehensive training programme

# Conclusions & Directions

## Conclusions

1. New EU legal framework for personal data processing
2. PIA is a key resource
3. Privacy by design to implement technical measures

## What's ahead?

1. Member States' translation into national laws
2. Transnational data processing (Privacy Shield)
3. Merger legislations and data reuse (Facebook & Whatsapp case)
4. Enforce personal data protection laws

Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, 23 September 2016 [[link](#)]

## **Acknowledgements**

This work has been funded by the University of Granada, under the Young Researchers Fellowships Programme; the Ministry of Education, Culture and Sport under the mobility program José Castillejo; and the EU 7<sup>th</sup> Framework Programme under grant agreement n° FP7-SEC-2012-312651.

Contributions and corrections by J. Valls, Lecturer at the Department of Criminal Law of the University of Granada.