

BIG DATA

DATA MINING E PROTEZIONE DEI DATI PERSONALI

Elementi di informatica giuridica
SSPL I anno
Prof. Angela Busacca



DATA MINING PROCESS

quali rischi per la privacy?

- identificazione dell'origine dei dati
- corrispondenza dei dati con l'identità dei singoli soggetti interessati

Quali rischi per i big player?

- perdita del valore economico dei dati
- mancata tutela del valore giuridico dei dati



Variety

- Structured
- Unstructured
- Semi-structured
- All the above

3 Vs of Big Data

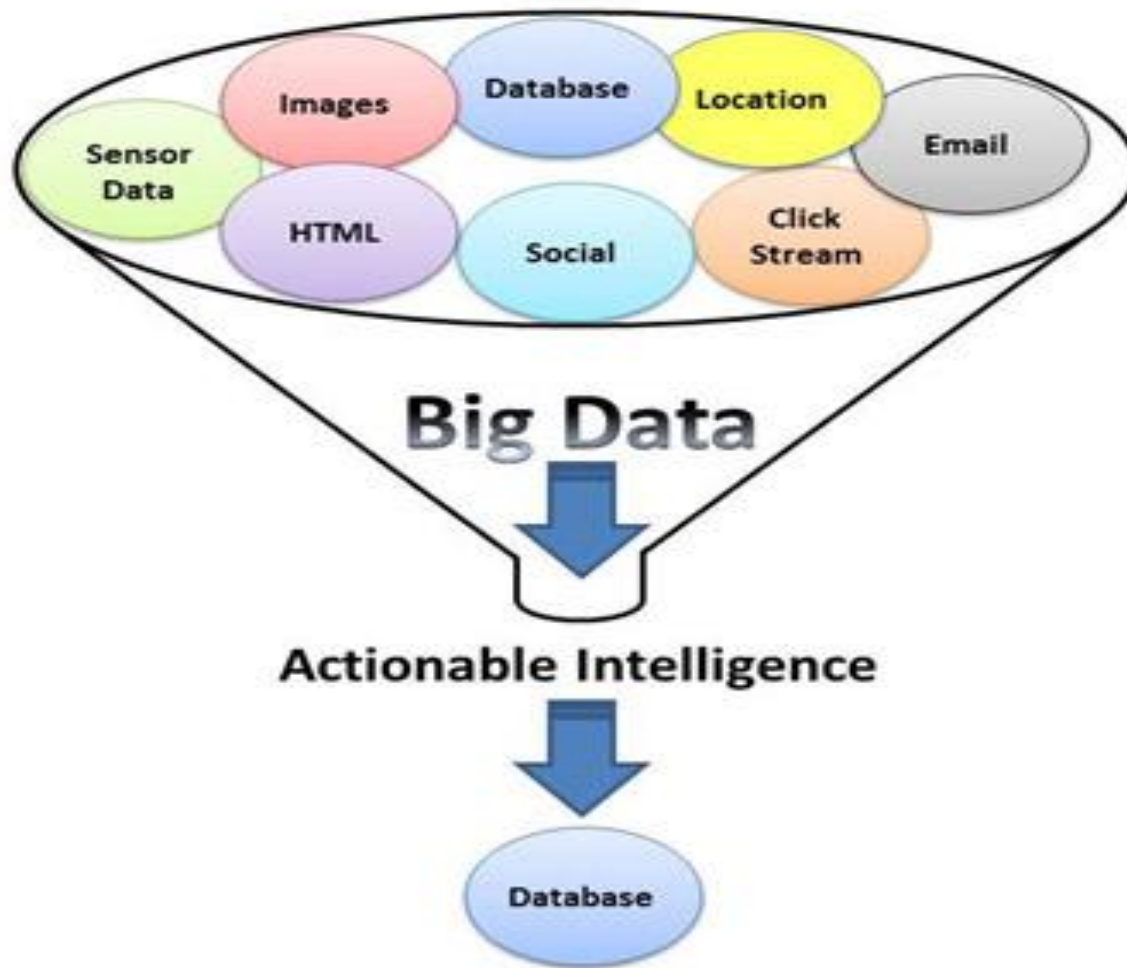
Volume

- Terabytes
- Records
- Transactions
- Tables, files

Velocity

- Batch
- Real-time
- Streams
- Near-time





PRINCIPALI PROFILI DI INTERESSE :

- Regolamentazione applicabile
- Identificazione corretta delle situazioni di titolarità/appartenenza dei dati
- Diritto all'esportazione di dati
- Possibilità di utilizzare metodi automatici per la catalogazione
- Criteri e Modelli per la protezione dei dati personali

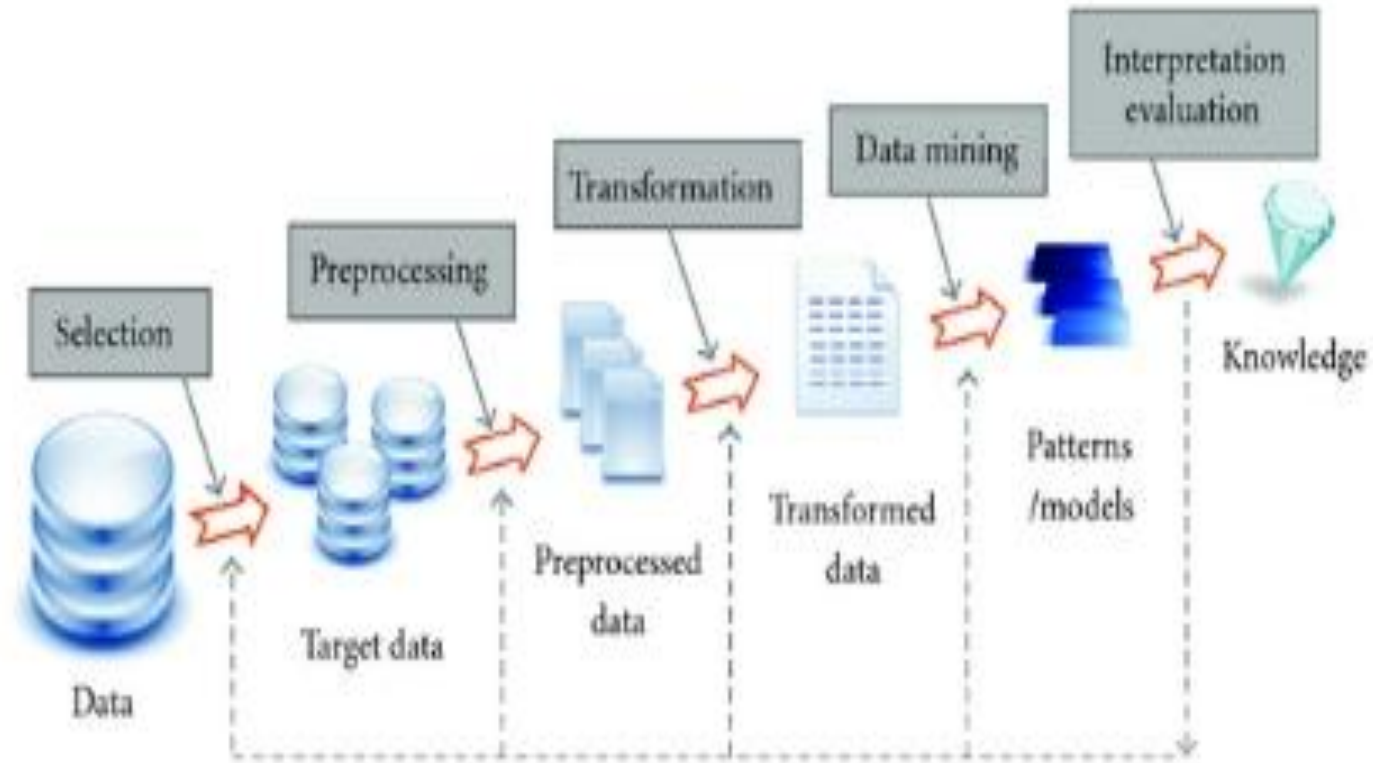


INTERNET OF THE THINGS

- Dispositivi indossabili (Smart-watch // cardio frequenziometri)
- Domotica
- Sensori intelligenti (in spazio aperto)
- Sensori intelligenti (per servizi pubblici)



KNOWLEDGE DATA DISCOVERY PROCESS



*Indici
con quasi-identifiers*

	ETA'	CAP	SESS O	Esito
1	21	98122	M	Positivo
2	23	98124	F	Negativo
3	29	98124	M	Positivo
4	28	98123	F	Positivo
5	27	98121	F	Negativo
6	22	98123	F	Negativo

*Indici
con criteri più generali*

	ETA'	CAP	SESSO	Esito
1	20-25	98100	M	Positivo
2	20-25	98100	F	Negativo
3	26-30	98100	M	Positivo
4	26-30	98100	F	Positivo
5	26-30	98100	F	Negativo
6	20-25	98100	F	Negativo



GDPR ART. 25

PRIVACY BY DESIGN // PRIVACY BY DEFAULT

- 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
- 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

MODALITÀ DI TUTELA DELLA PRIVACY NELLE OPERAZIONI DI SOCIAL DATA MINING

- *Distributed Privacy Preserving Data Mining*
- *Knowledge Hiding*
- *Privacy-aware Knowledge Sharing*
- *Data perturbation and Data Obfuscation*

