AI vs. the GDPR

Alessandro Guarino
StudioAG

Bruxelles 7/11/2018

The Speaker

18+ Years in Information/Cyber Security Consultancy

StudioAG
Consulting & Engineering

Speaker Author

Digital Forensics Alumni — 2011

CyCon International Conference on Cyber Conflict — 2013

2016 ISSE — 2013-2017

E-PRIVACY XX — 2016 →

IET Events The Institution of Engineering and Technology

pirate security conference psc

Università di Roma Tor Vergata — 2017

NATO OTAN — 2018

Standards

UNINFO

CS·CG CEN/CENELEC/ETSI Cyber Security Coordination Group

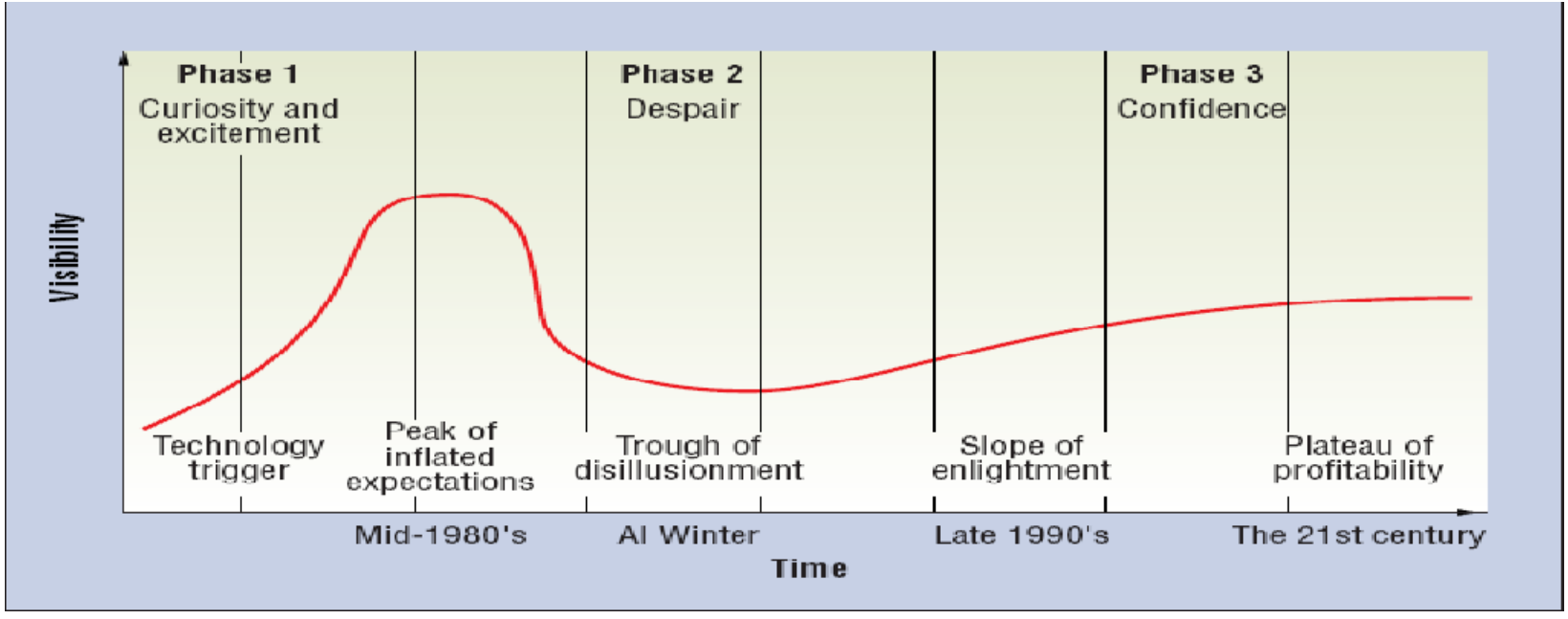
ETSI

cen CENELEC — 2011 →

Artificial Intellingence?

The machines taking over? Not so fast…

A bit of history and the highs and lows of AI



From "The history of Artificial Intelligence" – Huang, Smith, 2006

The reality…

Several algorithms and techniques, generally catalogued under the label of "Artificial Intelligence", have come of age in the last decade and have left the realm of academia for the real world.

They are however mostly domain- and task-specific:
Recommender systems, natural language interfaces for virtual assistants, prediction systems and image classifiers are nowadays almost taken for granted and incorporated into consumer products.

Profiling

Anticipating the GDPR definition:

Any form of **automated** processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a **natural per**son, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Machine lerning models used for instance in Marketing fall into this definition…

AI-enabled services can generate value for the customer as well as for the supplier, if done correctly

Machine Learning

«Practical AI»

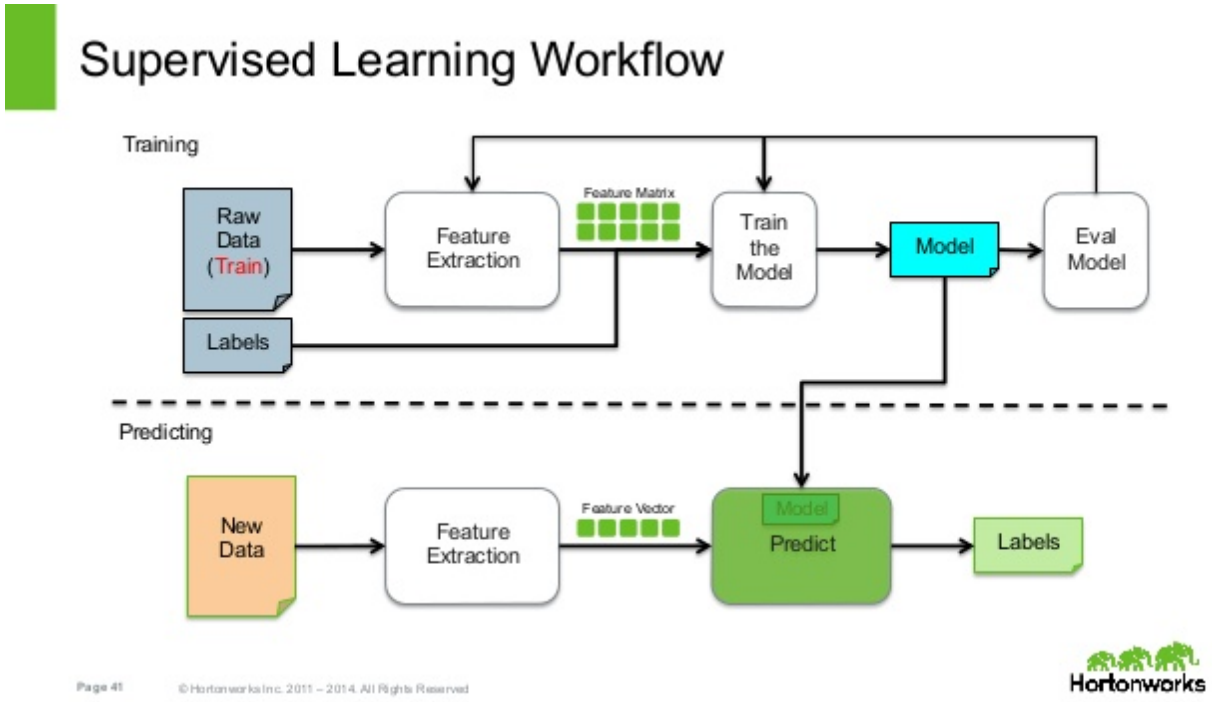
The tools actually used to do profiling

Supervised vs Unsupervised Machine Learning

Data is the fuel!

Black box problem (vs. old style rule based expert systems)

The process



Source: Hortonworks

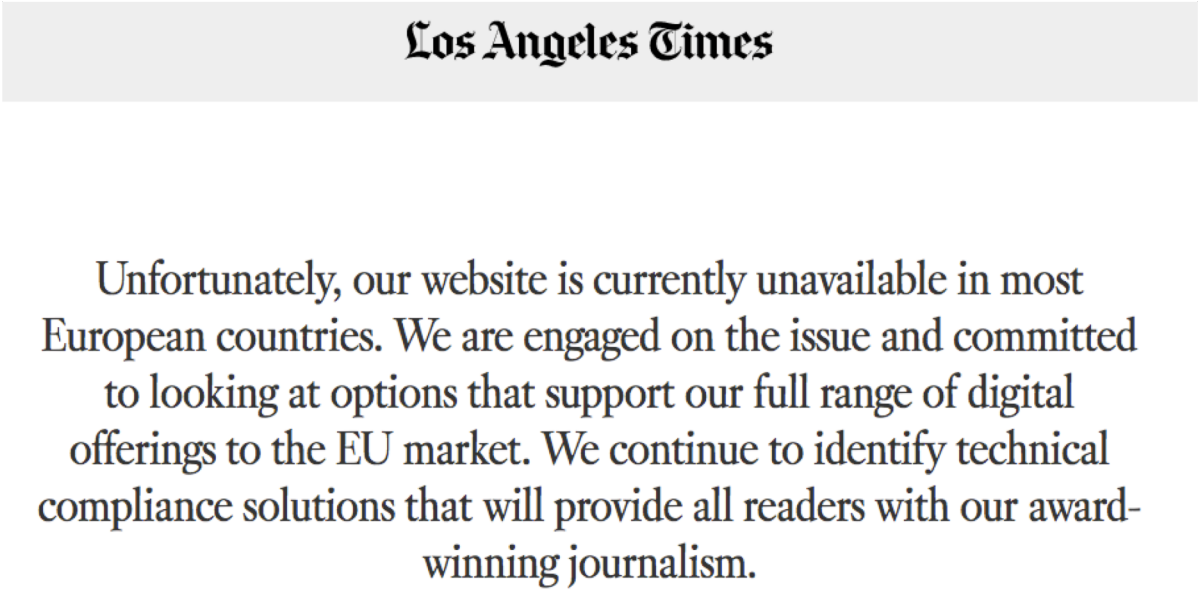
Data Economy

The »currency of the twenty-first century " and postulate that

We have been paying for services on the internet by sharing information.

No more?

Apparently some actors are not able to cope with big data withdrawal…



Risks for Privacy

Marketing, surveillance, and profiling need big datasets to function correctly, and when these data are personal data a wholly new set of problems and considerations arise.

- Potential for intrusive surveillance (behavioral predictions)
- Potential for discrimation in automated decisions
- Lack of control over personal data
- Accountability of the models
- Reuse of data (and results) with other parties, even governmental ones

How the GDPR works

How the GDPR tackles this risks

- The Fundamental Charter and the two rights
- Geographical scope…

The Regulation define strict limits on what can be done and how can it be done with individuals' personal data, including by controllers not based inside the Union but processing Europeans' personal data.

Risk-based approach

Data belongs to the (interested) subject

EU vs. USA (& UK?)

Rights of the data subjects

The GDPR provides the following rights for individuals:

The right to be informed
The right of access
The right to rectification
The right to erasure
The right to restrict processing
The right to data portability
The right to object
Rights in relation to automated decision making and profiling.

The Problem with Principles

Accountability

Transparency

Lawfulness -> Consent

Adequacy and minimization

Accuracy

Privacy by design

Source: Huffington Post

GDPR

Automated decision-making is allowed only where the decision is:

- necessary for the entry into or performance of a contract;
- authorised by Union or Member state law applicable to the controller
- based on the individual's explicit consent.

You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:

- give individuals information about the processing
- introduce simple ways for them to request human intervention or challenge a decision
- carry out regular checks to make sure that your systems are working as intended

The challenge

Developing and deployng GDPR-compliant systems

(especially predictive and decision-supporting ones)

Most applications *will* have to be re-engineered or re-designed to fulfill GDPR principles – privacy by design included

AI systems that operate as black boxes even for their own creators, will have to stand a scrutiny for transparency and accountability - not an easy task.

Fairness of algorithms

The challenges emphasize the importance of work that ensures that algorithms are not merely efficient, but transparent and fair.

On the other hand… it is a higher bar then human decisions in many cases.

Could skew the market into non-adoption of innovative systems or adoption of «weakened AI»

Conclusions

It can be done rightly (as in GDPR-compliant) but it’s not straightforward

It implies a change in the way of thinking about Big Data and Machine Learning

Cross-disciplany competences are needed

It will be interesting to see how far the GDPR can reach…

Thanks for Your Time
What are your questions?

Contacts:

a.guarino@studioag.eu

 **@alexsib17**

Slides online on:
www.studioag.pro

StudioAG – Consulting & Engineering
www.studioag.eu