Artificial Intelligence, Algorithmic systems, profiling & data protection

2019

Luca Bolognini

President, Istituto Italiano per la Privacy e la Valorizzazione dei Dati – Italian Institute for Privacy and Data Valorisation

Founding Partner, ICTLC - ICT Legal Consulting law firm

l.bolognini@istitutoprivacy.it

WHAT WE TALK ABOUT WHEN WE TALK ABOUT ~~LOVE~~ A.I.

BIG DATA (user/non-user generated)

IoT – Smart environments

Artificial Intelligence & Robotics

Blockchains

Profiling, Machine Learning

Cloud computing

Edge computing

Ethics

Privacy

Data Protection

Contract Laws

Competition & Consumer Law

IT and IP Law

Sectoral Laws (i.e. fintech, 5G)

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

WORDS ARE SOMETHING IMPORTANT

Etymology, past meanings

Current meanings

Actual meanings

Sounds, tones, shapes, colors, time, space of words are relevant

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

PROFILING: SHAPING INDIVIDUALS

Art. 4(4) - GDPR
‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, 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 -> like “creating dossier”

Definition of “profiling” (Merriam-Webster): to draw “the line that bounds and gives form to something”, “to shape the outline of by passing a cutter around“

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

SMART: SHARP PAIN IN OUR FUTURE?

Origin of the word «SMART» (source: Oxford Dictionaries)
Old English smeortan (verb), of West Germanic origin; related to German schmerzen; the adjective is related to the verb, the original sense (late Old English) being '**causing sharp pain**'; from this arose 'keen, brisk', whence the current senses of 'mentally sharp' and 'neat in a brisk, sharp style'.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

ARTIFICIAL INTELLIGENCE

“Artificial intelligence (AI) systems are software (and possibly also hardware) systems **designed by humans** that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.
As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).”

A definition of AI: Main capabilities and scientific disciplines

High-Level Expert Group on Artificial Intelligence - European Commission (April, 2019)

In short, AI = human-designed expert knowledge-based deciding systems

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

ARTIFICIAL ROBOTS, HUMAN ALL TOO HUMAN?

Origin of the word «ARTIFICIAL» (source: Oxford Dictionaries)
Late Middle English: from Old French artificiel or Latin artificialis, from artificium: ‘handicraft’. Artifice: a clever expedient. Often, deceptive.
Artificial as hyper-rational?

The term “ROBOT” comes from a Czech word, robota, meaning "forced labor"; the word 'robot' was first used to denote a fictional humanoid in a 1920 play R.U.R. (Rossumovi Univerzální Roboti - Rossum's Universal Robots) by the Czech writer, Karel Čapek but it was Karel's brother Josef Čapek who was the word's true inventor.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

BIG DATA: KEY DIMENSIONS

3 Vs: Volume, Variety, Velocity

+ s? sssss… silence.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

IoT, Internet of Things

The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment (Gartner)

5G «explosion» in the near future, powerful enabler

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Big changes for privacy in a smart environment: interactivity and accountability are transforming

BEFORE IOT -> Data subject n.1 = **active – interactive** – in principle, the GDPR (and also Directives 95/46/EC and 2002/58/EC) identifies an «interactive» data subject

AFTER -> Data subject n. 2 as a NON-USER = the IoT implies the involvement of **passive subjects** which are out of reach (in terms of information to be given and of consent to be collected)

BEFORE IOT -> Controlling/processing actors = data **controller** and data **processor** that are **active subjects**

AFTER -> NON-SUBJECTS as controlling/processing actors = data controllers and processors are also, merely, objects

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

FUTURE WORST-BEST CASE SCENARIO: AN INTELLIGENT IOTIZED WORLD CITY

Smart Cities are made of: User Generated Contents, Profiling, On Premise, Cloud & Edge computing, Augmented Reality/Humanity, Internet of Things, Artificial Intelligence, Robots, Blockchains, Public-Private strategic Alliances, etc…

Everything is going to be tracked AND analysed AND physically/virtually/juridically data driven

Everybody is going to be tracked AND analysed AND physically/virtually /juridically data driven

I.E. a smarter city necessarily implies a higher risk for private and family life, and for personal data protection.

How could we protect natural persons (not only citizens) from this new Smart Big Brother, without renouncing to facilities and useful services and tools?

Both technological and legal safeguards can be adopted.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

SO WHAT, IN TERMS OF LEGAL ISSUES?

?

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Legal Accountability/Liability of Things?

Compulsory insurance systems?

Product liability approach?

Zoological model (pet owners-like)?

Strict/objective liability, for whom?

Who can be considered as (joint) controller/processor in the chain?

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Legal Personality to A.I.?

Social humanoid robot “Sofia” – from its birth in Hong Kong (2016) to Honorary Citizenship in Saudi Arabia (2017). Bullshit? Big mistake?

How could we make and consider as accountable, liable a non-human entity, which is not able to consciously suffer?

The poet is a faker
Who’s so good at his act
He even fakes the pain
Of pain he feels in fact.

Fernando Pessoa, 1932

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

BIG DATA/AI PROCESSING versus ART. 5 GDPR

- **Transparency and Fairness** (5.1.a): what about deep learning and, more generally, algorithm IP/secrecy, newborn data & digital subconscious?
- **Data minimisation** (5.1.c): what about massive volume?
- **Storage limitation** (5.1.e): what about machine learning?
- **Purpose limitation** (5.1.b): what about variety of sources/data?
- **Accuracy** (5.1.d): what about super-velocity of processing and results?
- **Accountability** (5.2): what about objects/things/expert algorithms autonomous coding and decisions?

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Big changes for privacy in a smart environment: from data protection & privacy to “personal effects protection”

Reconsideration of the concepts of privacy and data protection, merging them together – as the continuous processing of personal data (protected according to art. 8 of the Charter of Fundamental Rights of the European Union, “CFREU”) is also by default accompanied in IoT by the invasion of what, according to art. 7 of the “CFREU”, we define as private and family life. The concept of “personal sphere” has changed. It has lost its classic features, opening its doors to the first inanimate objects which now are able to act independently in terms of the information they reveal and can even talk to each other, exchange data that they have acquired. Smart “things” are objects which are precisely part of the “personal sphere” which carry risks of “interference” with respect to the individual’s privacy. Thanks to the intrinsic characteristics of the IoT, we have witnessed the reunification of the rights that Articles 7 and 8 of the CFREU had divided: the Internet of things requires that data protection and privacy are fused together in order to protect the individual from the activities of connected and interconnected intelligent objects that invade the private sphere (even the human body) while processing personal data.

Privacy+Data Protection=“Personal Effects Protection”

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Is new AI & Big Data driven business unlawful?

- Are thousands of startups and spin-offs in our incubators and universities outlaws?

- Recital 4, GDPR: **The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality**. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, **freedom of thought**, conscience and religion, **freedom of expression and information**, **freedom to conduct a business**, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Big changes for privacy in a smart environment: DPIAs to consider also physical threatens to rights and freedoms

A good Data Protection Impact Assessment (art. 35 GDPR, art. 23 Dir. 2016/680/UE) should not only focus on data/information security

It is paramount to assess the possibile risks to freedom and rights of natural persons: **some processing activities could be perfectly lawful, legitimate, secure but, still, not safe because of some intrinsic risks implied by that specific data processing, for its very nature**

Moreover, a robust DPIA should consider also material/physical impacts on natural persons, caused by a virtual elaboration of data

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 1. 3D privacy

Often we cannot choose not to be a data subject and to remain invisible to sensors of the smart object.

The protection of the personal sphere and its “material data” is becoming three-dimensional

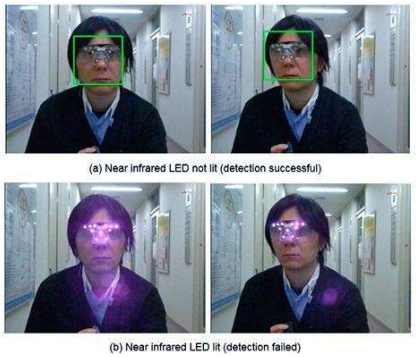
3D privacy consists in adopting also physical security measures, empowering users and non-users as data subjects with material tools in order to self-control over their information and to self-defend from data collection in IoT open environments. It is the use of other objects or other physical elements in order to avoid capture of personal information, shielding the individual from such collection,

restoring the privacy of the individual sphere and keeping the data protect.

3D privacy = a type of data protecy self-enforcement

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

3D privacy: examples



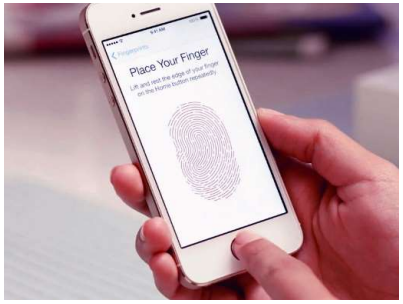
Privacy visors

Anti-paparazzi foulard

Personal antiradar

Privacy screen

Biometric passwords



iPhone press-code

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 2. Crowd-privacy

Privacy Flag H2020 Project: to enable users in order to exchange information/awareness and to organize self-defense measures from cyber/privacy threats on line and in IoT environments

UNITY MAKES STRENGHT

Crowdsourced tools to monitor and check Smart and IoT systems in terms of security and privacy

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 3. A “Food&Drug approach” and ADS/targeting labelling

Thinking about the impacts -> Disclosing what data processing was behind a targeted conten

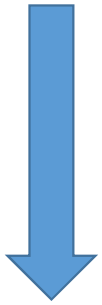
Like food&drug labelling, detailing ingredients and preservatives, users should be enabled to discover and understand why they are receiving a specific ads

Online users deserve the max possible **transparency** when receiving online "food for thoughts", such as ADS and other contents. Users shall know what they are taking and why, understanding criteria which are behind a digital content targeting. It would be possible to adopt a **code of conduct** according to Article 40 of the GDPR, combining it with a web-based **label-add-on**, to improve both the **accountability** of the digital content-providers and the **users’ awareness over IoT Big Data-driven impact** on their life.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 4. Blockchains for objects-accountability

Blockchain can help tracking – in a trustless way – all data processing transactions between things. Tampering of material objects (typically off-chain) could be detected and tracked through IoTized seals

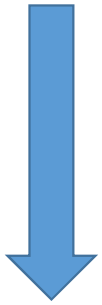


Possibility to make smart objects and non-human automated algorithms more accountable from a GDPR perspective

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 5. Automated GDPR audits and certifications for smart environments

Art. 42 GDPR will allow new kinds of certification models and schemes, adopting «automated probes» to audit in real time privacy and security compliance levels in smart deployments



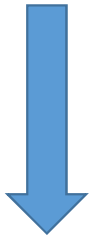
Possibility to make Smart Cities and other intelligent applications more accountable and trustable

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 6. Ethics & Data protection + Rule of Law by Design

It will be paramount to comply with Data Protection By Design principle according to art. 25 GDPR

and to carry out Ethics & Data Protection Impact Assessments (EDPIAs) during design phases



Good guidance from European Commission's Ethics Guidelines for Trustworthy Artificial Intelligence (AI) - A document prepared by the High-Level Expert Group on Artificial Intelligence (April, 2019)

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Possible solutions - 6. Ethics & Data protection + Rule of Law by Design – EC Ethics Guidelines for Trustworthy Artificial Intelligence (AI)

Based on fundamental rights and ethical principles, the Guidelines list seven key requirements that AI systems should meet in order to be trustworthy:

- Human agency and oversight
- Technical robustness and safety
- Privacy and Data governance
- Transparency
- Diversity, non-discrimination and fairness
- Societal and environmental well-being
- Accountability

Aiming to operationalise these requirements, the Guidelines present an assessment list that offers guidance on each requirement's practical implementation. This assessment list will undergo a piloting process to which all interested stakeholders can participate, in order to gather feedback for its improvement. In addition, a forum to exchange best practices for the implementation of Trustworthy AI was created.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

AGAIN, THE MEANING OF WORDS IS KEY

Asimov's Laws (1942) – What meaning for **orange words** below?

First Law - A robot may not **injure** a human being or, through inaction, allow a human being to come to **harm**.

Second Law - A robot must obey the orders given it by human beings except where such orders would **conflict** with the First Law.

Third Law - A robot must **protect** its own **existence** as long as such protection does not **conflict** with the First or Second Laws.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

BE CAREFUL WITH SUPERFLUOUS SUPERSTRUCTURES

- RULE OF LAW BY DESIGN, OK.
- BUT… WHAT IF LAWS WILL BE NON-HUMAN GENERATED AND INTERPRETED/APPLIED?
- ARE BOT-JUDGES, BOT-MEMBERS OF PARLIAMENTS, BOT-CITIZENS, BOT-VOTERS ONLY SCIENCE-FICTION?

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

PLAYING WITH FIRE IN TRIALS?

The Estonian Ministry of Justice has officially asked Estonia's Chief Data Officer to design a "robot judge" to take care of small claims court disputes. The AI-based "judge" should analyze legal documents and other relevant information and come to a decision. Anyway, a human judge will have an opportunity to revise those decisions.
(March, 2019)

Supreme Court of the US - Case Loomis v. Wisconsin Petition for certiorari denied on June 26, 2017 - Legitimate: to rely on the risk assessment results provided by a proprietary risk assessment instrument such as the Correctional Offender Management Profiling for Alternative Sanctions at sentencing because the proprietary nature of COMPAS prevents a defendant from challenging the accuracy and scientific validity of the risk assessment; and to rely on such risk assessment results at sentencing because COMPAS assessments take gender and race into account in formulating the risk assessment.

ALGORITHMIC ENTITIES: COMPANIES WITHOUT A BOARD OF NATURAL PERSONS

In Hong Kong a robot appointed as Director of the venture capital fund Deep Knowledge (2014). Its name was Vital (Validating Investment Tool for Advancing Life Sciences).

In Delaware, it could be possible to establish a company without human directors nor human shareholders. See: *LoPucki, Lynn M., Algorithmic Entities (April 17, 2017). 95 Washington University Law Review (Forthcoming).; UCLA School of Law, Law-Econ Research Paper No. 17-09. Available at SSRN:* *https://ssrn.com/abstract=2954173*

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

More in general: how to protect fundamental rights in a smart world?

"**Rule of law by design**" risks to become obsolete and weak against "***autonorms.exe***"

Today, that democracy-defending formula would need to be expanded upon and better specified: "**rule of human law by default**". We should in no way accept the idea of subjecting ourselves to rules, regulations, laws, decisions and codes that are automated and artificially created. No public law should ever be generated from an inhuman algorithm. No robot and no other form of artificial intelligence should be designed without an ON/OFF button that can be controlled only by humans and not by other machines – meaning that for each robot or form of artificial intelligence there should be at least one human super-admin and definitely no artificial super-admin. Also the robots, like the kings (and the mayors), have to be held accountable to human law. And each super-admin, or remote-Commander-in-Chief, in turn, should also be subject to the rule of human law.

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Thank you!

Luca Bolognini

President, Istituto Italiano per la Privacy e la Valorizzazione dei Dati –

Italian Institute for Privacy and Data Valorisation

Founding Partner, ICTLC - ICT Legal Consulting law firm

l.bolognini@istitutoprivacy.it