Artificial Intelligence and privacy rights

Gaetana Natale*

Today is it possible to compromise rule of technology with the rule of law to protect fundamental rights?

Artificial Intelligence has the immense potential to benefit our way of living, but it's already undeniable it creates new risks of extensive and serious damages. Damages creates by AI can arise in the context of contractual relationships or regardless of any previous relationship with the injured party.

It is arguable conventional tort law and contractual liability system can always ensure adequate distribution of risks and fair compensation of damages. These new challenges have pushed European Institution to undertake several initiatives aimed for the harmonization of the rules on AI including an civil liability.

Three steps are important:

1) Raise awareness on how AI operates and the challenges it presents to conventional tort law and contractual liability system;

2) Analyze and compare national and EU rules already in place pertaining to the matter;

3) Provide Knowledge of EU legislation being prepared.

In the first stage it is important to understand how algorithm operate in machine learning to compromise, trade off rule of technology with rule of law. What is an algorithm?

If this than that: a process or set of rules to be followed in calculations or other problem-solving operations, or performing **computation** especially by a computer "a basic algorithm for division", a step by step procedure for solving a problem or accomplishing some end.

Etimology: alteration of middle English *algorisme*, from Old French & Medieval Latin *algorismus*, from Arabic *al.khwarizmi flourished* a.d. 825 Islamic mathematician.

The basic concept to understand is: *The inference*. Algorithm operates with "***inference***" and not on the base of principle of causality. The perception of mind is a rational act of the mind and it is simply application of the principle

---

(*) Avvocato dello Stato, Professore di Sistemi Giuridici Comparati, Consigliere giuridico del Garante per la tutela dei dati personali.

Relazione presentata dall'Autrice nel corso del seminario organizzato dalla Rete Europea di Formazione Giudiziaria (REFG) che opera con il sostegno finanziario del programma Giustizia dell'Unione europea. Il seminario sul tema "Civil liability due to artificial intelligence" rientra nell'ambito del "Progetto di giustizia civile". L'evento si è svolto il 25 e 26 maggio 2023 presso la sede di Roma dell'EJTN.

of causality with the methods of induction. Here, there is even some kind of vague relevance to our everyday life, but once more the crucial point regards the conception of the world, the applicability of the principle of causality, the idea of knowableness. Rather, one can characterize the true state of the thing a lot better in this way, since all experiments are subject to the law of quantum mechanics from this matter follows that, by quantum mechanics is established permanently the invalidity of the principle of causality.

In the *Cambridge Dictionary* we found this definition of *Artificial Intelligence*:

"*the study of how to produce machines that have some of the qualities that the human mind has, such as the ability to understand language, NPL Natural Processing Language, recognize pictures, solve problems and learn*". Indeed AI is a result in global level of high performance computing, machine learning, deep learning, Internet of thing, blockchain dapps, blockchain protocols, the **technology stack** as a connection of users, content, data, app, services, criptocarrency, open internet/platforms, logical layer, infrastructure connectivity, nanotechnology, according to scheme input/output/response prediction. Data Mining, in others words data is value, data driven economy an information, feature extraction, annotation, validation, information became Knowledge and knowledge became prediction.

To understand IA is important to study some mathematics theories as Bayesian statistics, Markov Chain, Turing Test, Asimov Law, Moore Law, theory of Shannon, Logical Complex of Godel, theory of Arrow, Gray Code.

Entranglement or a spooky action at distance as A. Einstein writed are concepts that AI can not understand.

"*One day the machines will be able to solve all problems, but none of them can deliver us one*" (Albert Einstein).

"*The measure of intelligence is the ability to change*".

Can we compromise this mathematical concept, trade off the rule of technology with the rule of law to protect human rights?

Yes. It is possible if the algorithm are created without bias and discrimination (*Loomis case, Compass case, Cambridge Analytica, Conseil of State 25 november 2021 n. 7891*) according to some important principles or model rule, general clauses as *accountability and privacy by design and default* art. 25 GDPR to avoid black box (Zuboff *surveillance capitalism*, *micro-targeting*, *social scoring*) and to create AI trustworthy based **on transparency, no discrimination, right to explanation pursuant to 22 GDPR**, or **explainibility of algoritms logic**, *human in the loop*, human in command, control in rolling review.

Article 22 GDPR: "**Automated individual decision-making, including profiling**"

"*1. The data subject shall have the right not to be subject to a decision*

based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedom and legitimate interests; or

c) is based on the data subjec's explicit consent".

Mumford: "*The technology is a form of order*".

Article 25 GDPR "**Data protection by design and by default**"

"*1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likehood, and severity for rights and freedoms of natural persons by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular , such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article".

The first problem is: Who must certificate the security of AI devices? Independent Authority or the same producer?

The liability, strict liability, product liability and *pre-emption doctrine* is regulated with the **risk assessment. Today he have in progress a lot of European Regulations: Data Act, Digital Service Act, Digital Market Act (with a combination Antritrust rule of Abuse of Dominant position), Digital Governance Act.**

In Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence of 21

April 2021, approved the last May 11 (including AI generative, before not inserted), the Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following specific objectives:

1) Ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;

2) Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;

3) Facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

The legal basis for the proposal is in the first place Article 114 of the Treaty on the Functioning of the European Union (TFUE), which provides for the adoption of measures to ensure the establishment and functioning of the internal market, **subsidiarity (for non-exclusive competence) and proportionality.**

It is crucial that strict liability became "accountability", as a preemptive remedy. Not only rules, but "Digital due procedure" as well to avoid data tracing and data scraping.

It is crucial the time of regulations: the technology is faster than law.

The regulation follows a risk-base approach differentiating between uses of AI that create:

a) An unacceptable risk;

b) A high risk;

c) Low or minimal risk.

The list of prohibited practices in Title II comprises all those AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights. The prohibitions covers practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or person with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. The brain enhancement, neurolaw, because in this case algorithm is not a mere tool, but can change human behavior. Other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by existing data protection, consumer protection and digital service legislation that guarantee that natural person are properly informed and have free choise not to be subject to profiling or other practices that might affect their behavoiur. The proposal also prohibits Ai-based social scoring for general purposes done by public authorities. Finally, the use of "real time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply.

Fundamental rights

The use of AI with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ("The Charter"). This proposal seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach.

With a set of requirements for trustworthy AI and proportionate obligations on all value chain participants, the proposal will enhance and promote the protection of the rights protected by the Charter: the right to human dignity (Article 1), respect for private life and protection of personal data (Article 7 and 8), non-discrimination (Art. 21) and equality between women and men (Art. 23). It aims to prevent a chilling effect on the rights to freedom of expression (Art. 11) and freedom of assembly (Art. 12) to ensure protection pf the right to an effective remedy and to a fair trial, the rights of defence and the presumption of innocence (Artt. 47 and 48) as well as the general principle of good administration.

Furthermore, as applicable in certain domains, the proposal will positively affect the rights of a number of special groups, such as the workers'rights to fair and just working conditions (Art. 31), a high level of consumer protection (Art. 28), the rights of the child (Art. 24) and the integration of persons with disabilities (Art. 26). The right to a high level of environmental protection and the improvement of the quality of the environment (Art. 37) is also relevant, including in relation to the health and safety of people.

The obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. In case infringements of fundamental rights still happen, effective redress for affected persons will be made possible by ensuring transparency and traceability of the AI systems coupled with strong ex post controls.

This proposal imposes some restrictions on the freedom to conduct business (Art. 16) and the freedom of art and science (Art. 13) to ensure compliance with overriding reasons of public interest such as health, safety, consumer protection and the protection of other fundamental rights ("responsible innovation") when high-risk AI technology is developed and used. Those restrictions are proportionate and limited to the minimum necessary to prevent and mitigate serious safety risks and likely infringements of fundamental rights. The increased transparency obligations will also not disproportionately affect the right to protection of intellectual property (Art. 17), since they will be limited only to the minimum necessary information for individuals to exer-

cise their right to an effective remedy and to the necessary transparency towards supervision and enforcement authorities, in line with their mandates. Any disclosure of information will be carried out in compliance with relevant legislation in the field, including Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. When public authorities and notified bodies need to be given access to confidential information or source code to examine compliance with substantial obligations, they are placed under binding confidentiality obligations.

What exactly are the dangers posed by AI?

Italian case of Chat GPT: on March 31 Italian Authority has stopped it to not respect privacy law and GDPR, after there is a agreement for implementation of precautional measures to protect personal data.

Italy'data regulator issued a temporary emercency decision, demanding OpenAI stop using the personal information of millions of Italians that's included in its training data. According to regulator, OpenAI doesn't have the legal right to use people's personal information in ChatGpt. In response, OpenAI has stopped people in Italy from accessing its chatbot while it provides responses to the officials, who are investigating further.

The action is the first taken against ChatGPT by a western regulator and highlights privacy tensions around the creation of giant generative AI models, which are often trained on vast swathes of internet data. Just as artists and media companies have complained that generative AI developers have used their work without permission, the data regulator is now saying the same for people's personal information.

Similar decisions could follow all across Europe. In the days since Italy announced its probe, data regulators in France, Germany and Ireland have contacted the Garante to ask for more information on its findings.

"If the business model has just been to scrape the internet for whatever you could find, then there might be a really significant issue here", says Tobias Judin, the head of international at Norway's data protection authority, which is monitoring developments. Judin adds that if a model is built on data that may be unlawfully collected, it raises questions about whether anyone can use the tools legally.

Europe's GDPR rules, which cover the way organizations collect, store and use people's personal data, protect the data of more than 400 million people across the continent. This personal data can be anything from a person's name to their IP address - if it can be used to identify someone, it can count as their personal information.

Unlike the patchwork of state-level privacy rules in the United States, GDPR's protections apply if people's information is freely available online.

In short: Just because someone's information is public doesn't mean you can vacuum it up and do anything you want with it.

Italy's Garante believes ChatGPT has four problems under GDPR: 1) OpenAI doesn't have age controls to stop people of 13 from using the text generation system; 2) it can provide information about people that isn't accurate; 3) and people haven't been told their data was collected. Perhaps most importantly, its fourth argument claims there is "*no legal basis*" for collecting people's personal information in the massive swells of data used to train ChatGPT.

"The Italians have called their bluff", says Lilian Edwards, a professor of law, innovation and society at a Newcastle University in the UK. "It did seem pretty evident in the EU that was a breach of data protection law".

Broadly speaking, for a company to collect and use peple's information under GDPR, they must rely on one of six legal justifications, ranging from someone giving their permission to the information being required as a part of a contract. In this instance , there are essentially two options: getting people's consent - which OpenAI didn't do - or arguing it has "**legitimate interests**" to use people's data, which is very hard to do. This defense is "inadequate".

OpenAI's privacy policy doesn't directly mention its legal reasons for using people's personal information in training data, but says it relies upon "legitimate interests" when it "develops" its services.

The Federal Trade Commission should open an investigation and order OpenAI to halt the release of GPT models until necessary safeguards are established. These safeguards should be based on the guidance for AI products the FTC has previously established and emerging norms for the governance of AI.

Marc Rorenberg and Merve Hickok reminded the Commission that they previously declared that AI products should be **"transparent, explainable, fair and empirically sound while fostering accountability".**

On April 4, 2023 President Biden, meeting with his top science advisors, explained the need to address the potential risks of AI to society, economy and national security. He called for **"responsible innovation and appropriate guardrails to protect America's rights and safety, and protecting their privacy, and to address the bias and disinformation".** He said **"tech companies have a responsibility to make sure their products are safe before making them public"**.

A recent letter calling for a moratorium on AI development blends real threats with speculation. But concern is growing among experts. In late March, more than 1,000 technology leaders, researchers and other pundits working in and around artificial intelligence signed an open letter warning that AI technologies present "profound risks to society and humanity".

The group, which included Elon Musk, Tesla's chief executive and the owner of Twitter, urged AI labs to halt development of their most powerful systems for six months so that they could better understand the dangers behind the technology.

"Powerful AI systems should be developed only once we are confident that their effects will be positive and their risks will be manageable", the letter said. The letter, with now has over 27,000 signatures, was brief. Its language was broad. The letter represented a growing concern among AI experts that the latest systems, most notably GPT-4, the technology introduced by the San Francisco start-up Open AI, could cause harm to society. They believed future systems will be even more dangerous.

Some of the risks have arrived. Others will not for months or years. Still others are purely hypothetical.

"Our ability to understand what could go wrong with very powerful AI systems is very weak", said Yoshua Bengio, a professor and AI researcher at the University of Montreal . "So we need to be very careful".

Why are they worried?

Dr. Bengio is perhaps the most important person to have signed the letter. Working with two other academics - Geoffrey Hinton, until recently a researcher at Google and Yann LeCun, now chief AI scientist at Meta, the owner of Facebook - Dr. Bengio spent the past four decades developing the technology that drives systems like GPT-4. In 2018, the researchers received the Turing Award, often called "the Nobel Prize of computing", for their work on *neural networks* (*brain imaging and brain enhancement*) .

A neural network is a mathematical system that learns skills analyzing data. About five years ago, companies like Google, Microsoft and Open AI began building neural networks that learned from huge amounts of digital text called **large language models** or L.L.M.s.

By pinpointing patterns in that text, L.L.M.s. learn to generate text on their own, including blog posts, poems and computer programs. They can even carry on a conversation.

This technology can help computer programmers, writers and other workers generate ideas and do things more quickly. But Dr. Bengio and other experts also warned that L.L.M.s can learn unwanted and unexpected behavoiurs. These systems can generate **untruthful, biased and otherwise toxic information.**

Systems like GPT-4 get fact wrong and make up information, pollution information , "filter bubbles" a phenomenon called "*hallucination*".

Companies are working on these problems. But experts like Dr. Bengio worry that as researchers make these systems more powerful, they will introduce new risks.

Short-Term Risk: Disinformation

Because these systems deliver information with what seems like complete confidence, it can be a struggle to separate truth from fiction when using them. Experts are concerned that people will rely on these systems for medical advice, emotional support and the raw information they use to make decisions.

"*There is no guarantee that these systems will be correct on any task you give them*", said Subbarao Kambhampati, a professor of computer science at Arizona State University. Experts are also worried that people will misuse these systems to spread disinformation. Because they can converse in human-like ways, they can be surprisingly persuasive.

"*We now have systems that can interact with us through natural language processing and we can't distinguish the real from the fake*", dr. Bengio said.

Medium-Term Risk; Job loss.

Experts are worried that the new AI could be job killers. Right now, technologies like GPT-4 tend to complement human workers. But Open AI acknowledges that they could replace some workers, including people who moderate content on the internet.

They cannot yet duplicate the work of lawyers, accountants or doctors. But they could replace paralegals, personal assistant and traslators.

A paper written by Open AI researchers estimated that 80 percent of the US work force could have at least 10 percent of their work tasks affected by LLMs and that 19 percent of workers might see at least 50 percent of their tasks impacted.

Long-Term Risk: Loss of Control

Some people who signed the letter also believe artificial intelligence could slip outside our control or destroy humanity. But many experts say that is wildly overblown.

The letter was written by a group from the Future of Life Institute, an organization dedicated to exploring existential risk to humanity. They warn that because AI systems **often learn unexpected behaboiur from the vast amounts of data they analyze, they could pose serious , unexpected problems.**

They worry that as companies plug LLMs into other internet services, these systems could gain unanticipated powers, because they could write their own computer code. They say developers will create new risks if they allow powerful AI systems to run their own code.

"*If you look at a straightforward extrapolation of where we are now to three years from now, things are pretty weird*", said Anthony Aguirre, a theoretical cosmologist and physicist at the University of California, Santa Cruz and co-founder of the Future of Life Institute.

"*If you take a less probable scenario-where things really take off, where*

there is no real governance, where these systems turn out to be more powerful than we thought they would be-then things get really, really crazy" he said.

Dr. Etzioni said talk of existential risk was hypothetical. But he said other risks-most notably disinformation- were no longer speculation.

"*Now we have some real problems*", he said. "*They are bona fide.* They require some responsible reaction. They may require **regulation and legislation.**

This is the problem: which type of regulation? Self-regulation, co-regulation, etero-regulation with a strong public control? Functional or structural regulation based on the purpose of benefit? GDPR is not enough today to regulate the complexity of AI, "spontanesus intelligence" out of human control. It is important to introduce sandbox method regulation with empiric approach to achieve flexible regulation called "future proof". Not stopping technologic progress, but it is important to introduce adequate regulation.

On 18th April in Spain it is created ECAT European Centre Alghoritm Transparency to control enforcement of rules Digital Services Act. But there are others important problems that needs a solution:

1) The problem of relation between Europe and USA: *Shrems Case.*

2) The problem of governance, compliance, execution, inspection and public-private enforcement.

3) The problem of One Stop Shop and consistency cooperation and amicable settlement.

4) The problems of liability of gatekeepers and "notice and take down" in three different activities: mere conduit, caching, hosting.

5) The problem of validation and certification of AI devices.

The Proposal for a Directive of the European Parliament and of Council an adapting non-contractual civil liability rules to artificial intelligence **(AI Liability Directive) Brussels, 28 september 2022** is important to consider the impact assessment on the initiative on civil liability for damages caused by AI.

Although AI-enabled products/services are expected to be safer than traditional ones, accident will still occur. Current liability rules, in particular national rules based on fault, are not adapted to handle compensation claims for harm caused by AI-enabled product/services. Under such rules, victims need to prove a wrongful action/omission of a person that caused the damage. The specific characteristics of AI , including autonomy and opacity (the so-called "black box" effect) make it difficult or prohibitively expensive to identify the liable person and prove the requirements for a successful liability claim. The Commission wants to avoid that victims of harm caused by AI, eg citizens,

business, are less protected than victims of traditional technologies. Such lack of compensation can affect their trust in AI and ultimately the uptake of AI - enabled products/services. It is uncertain how national liability rules can be applied to the specificities of AI. In addition, faced with a result, which is unjust for the victim, courts may apply existing rules on an ad hoc basis in a way to come to a just result. This will cause legal uncertainty. As a result, business will have difficulties to predict how the existing liability rules will be applied in case damage occurs. They will thus have difficulties to assess and insure their liability exposure. This impact is magnified in case of businesses active across borders as the uncertainty will cover different jurisdictions. It is also expected that, if the EU does not act, Member States will adapt their national liability rules to the challenges of AI. This will result in further fragmentation and increase costs for businesses active across borders.

The initiative delivers on the Commission's priority for the digital transition. The overarching objective is to promote the rollout of trustworthy AI to harvest the full benefits of AI. Therefore the AI White Paper aims at creating an ecosystem of trust to promote the uptake of AI.

The liability initiative is the necessary corollary of safety rules adapted to AI and complements thus the AI Act.

The AI initiative will:

- Ensure that victims of AI - enabled product/services are equally protected as victims of traditional technologies.
- Reduce legal uncertainty regarding the liability exposure of business developing or using AI.
- Prevent the emergence of fragmented AI-specific adaptations of national civil liability-rules.

The proposal has three important items:

1) To alleviate the burden of proof;
2) Minimum harmonisation of strict liability;
3) Mandatory insurance is needed as well.