

INTELLECTUAL PROPERTY & TECHNOLOGY

Artificial Intelligence & Law

A journey through the main legal issues raised by AI

Introduction

Is AI the new oil?	3
Overview of the AI Act	4
AI around the world: Perspectives from the US, UK and China	6
AI in the EU	8

AI & Intellectual Property

AI & Copyright

Generative AI and prompt protection	12
Can generative AI rely on the text and data mining (TDM) exception for its training?	14
'New' music created by AI: Who is the author?	16
The US Copyright Office denies registration of AI-generated images	18
The protection of the output generated by AI systems	20

AI & Patents

AI as inventor: Legal challenges and implications for patent law	22
--	----

AI & Trademarks

Advantages and limitations of using AI in intellectual property management before Trade-mark Offices	24
Generative design and product protection	26

AI & Technology

AI & Privacy

Deep fake and deep nude	30
Cognitive biases and discrimination of the algorithm	32
AI nudging in e-commerce: Privacy implications of algorithmic neuromarketing	34
Synthetic data: A safeguard or a threat to privacy?	36

AI & Cybersecurity

Risks and opportunities of the diffusion of AI	38
--	----

AI & Outsourcing

AI and outsourcing agreements	40
-------------------------------	----

AI & Liability

Liability for damages caused by AI	42
------------------------------------	----

Sector-based AI

AI and Food & Beverage

Applications of AI in crucial sectors of the agri-food industry	46
---	----

AI & Fintech

AI in the financial sector: Risks, regulatory obligations, and investor privacy protection	48
--	----

AI & Gambling

The use of AI in the regulated gambling sector	50
--	----

AI & Life Sciences

AI impact on medical devices	52
------------------------------	----

AI & Fashion

AI & Fashion: Between creativity and innovation	54
---	----

AI & Antitrust

'Algorithmic collusion'	58
-------------------------	----

Is AI the new oil?

When, in 2006, the English mathematician Clive Humby coined the famous slogan “data is the new oil,” which has proven to be increasingly true over time, perhaps it was not yet anticipated that this “oil” would be one of the essential propellants for the development of one of the most fascinating and potentially revolutionary technologies of our time: Artificial Intelligence (AI).

Although still a young technology in many respects, AI is already transforming the sectors in which it is applied, from manufacturing to medicine, from marketing to finance, from chemistry to e-commerce, thanks to its ability to learn and analyze complex data. AI-based technologies are expected to play an increasingly decisive role in these sectors.

Despite the challenging international context, 2022 was a record-breaking year for AI, thanks to the continuous evolution of hardware and the exploits of DALL-E 2 and ChatGPT, which quickly gained millions of users and showcased the potential of this technology to the general public.

In Italy, the AI market reached a volume of around EUR 422 million (+21.9%) in 2022, and between 2022 and 2025, it is expected to reach EUR 700 million with an average annual growth rate of 22%. These figures were reported by Anitec-Assinform, the association of Confindustria that represents companies in the information and communication technology sector. AI, along with other market enablers such as cybersecurity, big data, and cloud computing, will be a driving force for the development of the Italian digital market. Moreover, these numbers are even more remarkable considering that there are no obligations or public incentives linked to this market, and all this is happening in a context of great economic and geopolitical uncertainty.

According to the research results of the [Artificial Intelligence Observatory at the Polytechnic University of Milan](#), presented in early 2023, 61% of large Italian companies have already initiated at least one AI project, with 42% of them having more than one project in operation. Among SMEs, 15% have at least one ongoing AI project (compared to 6% in 2021), usually only one, but one in three plans to start new projects in the next two years.

The most significant share of the Italian AI market is related to Intelligent Data Processing solutions that analyze and extract information from data, especially for forecasting purposes in areas such as business planning, investment management, and budgeting activities. Applications in the field of language interpretation (both written and spoken) are also important. For example, there are Generative AI applications that automatically extract and process information from documents or analyze internal or external communications (such as emails, social networks, and the web). Recommendation Systems, which suggest content to customers based on their preferences, are also noteworthy, as well as Computer Vision initiatives that analyze the content of an image in contexts such as public surveillance or production line monitoring. Intelligent Robotic Process Automation solutions automate certain activities of a project and oversee its various stages.

In this scenario, it's inevitable that AI raises important legal and non-legal issues. This explains the attention that institutions are devoting to this technology. Around the world, guidelines or legislative proposals regarding the development and use of AI have been published or are being adopted. In Europe, discussions are underway regarding the proposal for a regulation on artificial intelligence (AI Act), a process that will result in a common regulatory framework among all EU Member States and will [require companies to undertake significant compliance programs related to both the production and use of AI-based systems](#).

In this publication, we will guide you through the main legal challenges and issues raised by AI, also from a comparative perspective. We'll address topics such as the relationship between AI and copyright, trademarks, and patents. We'll discuss implications related to the protection of personal data, as well as contractual aspects and liability regimes. And we'll delve into the peculiarities of this technology in specific industries such as Food & Beverage, Fintech, Gambling, Life Sciences, and Fashion.

Alessandro Ferrari

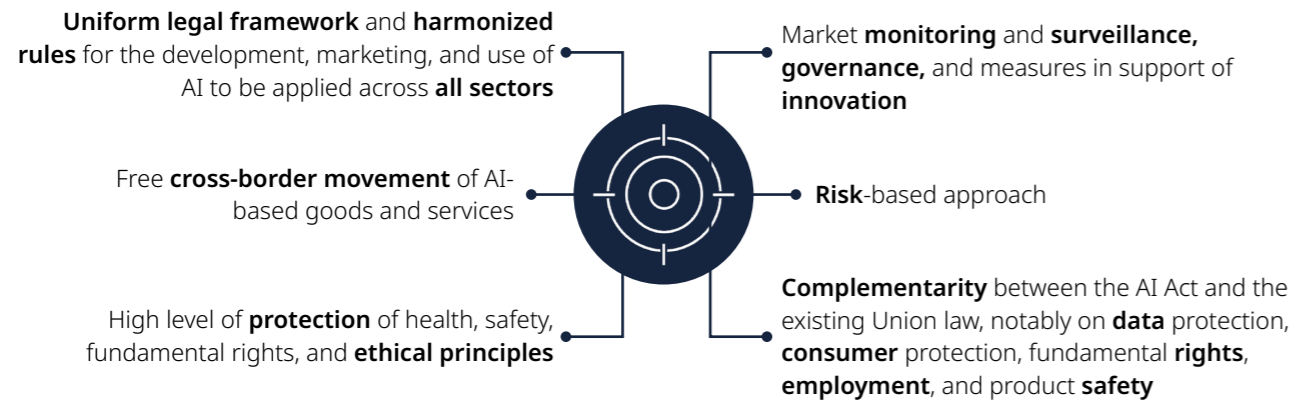
Partner
Head of Technology Sector, Italy

Overview of the AI Act

by ARIANNA ANGILLETTA

Considering that the AI Act proposal is still under discussion and undergoing continuous evolution, the following overview focuses on the most recent official positions adopted by the Council of the EU and the Parliament (as of the publication date of this booklet) regarding the draft AI Act presented by the Commission in 2021.

Objectives



Objective scope of application



The definition of “AI system” should be based on **key functional characteristics** of AI: its **learning, reasoning, or modelling** capabilities to distinguish AI systems from simpler software systems and programming approaches.

AI systems should be designed to operate with **varying levels of autonomy** and be used on a stand-alone basis or as components of a product. The concept of autonomy relates to the degree to which such systems **function** without human involvement.

These are AI systems that are intended to perform **generally applicable** functions in a plurality of contexts (eg image and speech recognition, audio and video generation, pattern detection, question answering, translation, and others).

They may be used either as **high-risk AI systems** by themselves or as **components** of other high-risk AI systems.

A highly debated topic in the negotiations of the AI Act proposal concerns how to treat large-scale **language models**, like **ChatGPT**, that can adapt to various tasks and are trained on huge amounts of different sets of data to clarify the **responsibility** along the AI value chain.

Subjective scope of application



The AI Act applies to:

- ✓ **Providers** placing on the market or putting into service AI systems in the EU.
- ✓ **Users** who are physically present or established in the EU.
- ✓ **Providers** and **users** who are physically present or established in a third country, where the output produced by the system is used in the EU.
- ✓ **Importers** and **distributors**.
- ✓ **Product manufacturers** placing on the market or putting into service an AI system together with their product and under their own name or trademark.
- ✓ **Authorized representatives** of providers, which are established in the EU.



Exclusions:

- ✗ AI systems if placed on the market, put into service, or used for the purpose of activities concerning **military, defense, national security**, or solely for the purpose of **scientific research** and **development**.
- ✗ **Research** and **development** activities regarding AI systems.
- ✗ Obligations of **users** who are **natural persons** using AI systems during purely personal non-professional activities, subject to certain transparency obligations.

Risk-based approach



Prohibited AI practices

↓
unacceptable risk

High-risk systems

↓
specific **requirements** and **obligations** are envisaged for the respective providers, users, authorized representatives, importers, and distributors.

Certain AI systems

↓
providers and users are subject to specific **transparency** obligations.

Requirements

on risk management, data, technical documentation, record-keeping, transparency, and provision of information to users, human oversight, accuracy, robustness, and cybersecurity.

Providers' obligations

establishment of a quality management system, documentation keeping, conformity assessment, and corrective actions.

Transparency obligations

- **Systems intended to interact with natural persons:** natural persons must be informed that they are interacting with an AI system.
- **Biometric categorization and emotion recognition systems:** natural persons must be informed if they are exposed to such systems.
- **Deepfake:** it must be disclosed that the content has been artificially generated or manipulated.

AI around the world: Perspectives from the US, UK and China

by MARIA CHIARA MENEGHETTI



US

The US' approach to AI regulation has been fragmented, cautious at the federal level, and more active at state and local levels.

At the **federal level**:

- **January 1, 2021** - The **National AI Initiative Act** came into effect, aiming to strengthen and coordinate AI research, development, and training across all departments and agencies of the US.
- **February 3, 2022** - The **Algorithmic Accountability Act** was presented to Congress, assigning the Federal Trade Commission (FTC) the task of creating regulations to govern automated decision-making processes (including those derived from AI and machine learning).
- **October 4, 2022** - The White House introduced the "**Blueprint for an AI Bill of Rights**," a non-binding document that provides some guiding principles and outlines the current administration's vision for how government agencies and companies should approach and use AI.

The AI initiatives brought before Congress have generated little interest.

In **2023** there is an expectation of increased regulatory activity by the **Federal Trade Commission** (FTC) and the **National Institute for Standards and Technology** (NIST):

- **August 11, 2022** - The FTC proposed legislation on commercial surveillance and data security, aimed at regulating the issue of automated decision-making.
- **January 26, 2023** - NIST released the **AI Risk Management Framework** (AI RMF) for managing and standardizing AI-related risks.
- **February 17, 2023** - The FTC announced the creation of an **Office of Technology** that will support the FTC in enforcing competition and consumer protection laws in technology-innovative areas such as AI and automated decision-making.

More extensive production has taken place at the local level. Many states have already introduced or are discussing the introduction of sector-specific regulations to govern specific issues, including:

- In **2019** several states (including Alabama, California, New York, and Vermont) passed **resolutions** for the establishment of **task forces and specific studies on AI**.
- In **2020 proposals for AI legislation** were put forward in 13 states, with most of them being rejected, except for the proposal to create a deep technology initiative in high schools, which was adopted in Utah.
- In **2021**, Alabama, Colorado, Illinois, and Mississippi enacted specific laws to regulate the use of **predictive and decision-making systems** in the workplace and the insurance sector.
- In **2022**, among the proposals advanced in 17 states, specific provisions were adopted in Colorado, Illinois, Vermont, and Washington, either for the creation of **ad hoc commissions** to study AI or for the amendment of existing regulations.

Throughout **2023 several state privacy laws** (in California, Connecticut, Colorado, and Virginia) will also become applicable, introducing specific requirements for those using automated decision-making systems, covering AI systems that use personal data.



UK

- **September 22, 2021** - The government published its **National AI strategy**, outlining a decade-long plan to make the UK a global AI powerhouse, focusing on **three key pillars**: 1) investing and planning for the long term, 2) promoting AI adoption across all economic sectors, and 3) developing a favorable regulatory and governance framework for innovation.
- **July 18, 2022** - The government presented the **AI Action Plan**, which proposes a less centralized and more risk-based approach to regulating AI compared to the European AI Act. For instance, the UK approach does not include a closed categorization of "high-risk" AI systems or the establishment of a dedicated authority (such as the AI Board), but rather leaves the implementation of the regulatory framework to existing regulatory bodies.
- **July 18, 2022** - A new **Data Protection and Digital Information Bill**, including specific provisions for responsible AI use, was introduced in Parliament.
- **March 29, 2023** - The **White Paper** titled "A **pro-innovation approach to AI regulation**" was published, outlining the UK's plans for implementing an innovation-friendly approach to AI regulation. The White Paper defines five key principles that regulators should consider to facilitate the safe and innovative use of AI: 1) security, safety, and robustness, 2) transparency and explainability, 3) fairness, 4) responsibility and governance, and 5) contestability and redress.



China

China has been among the first countries to take a leading role in defining AI rules.

In particular:

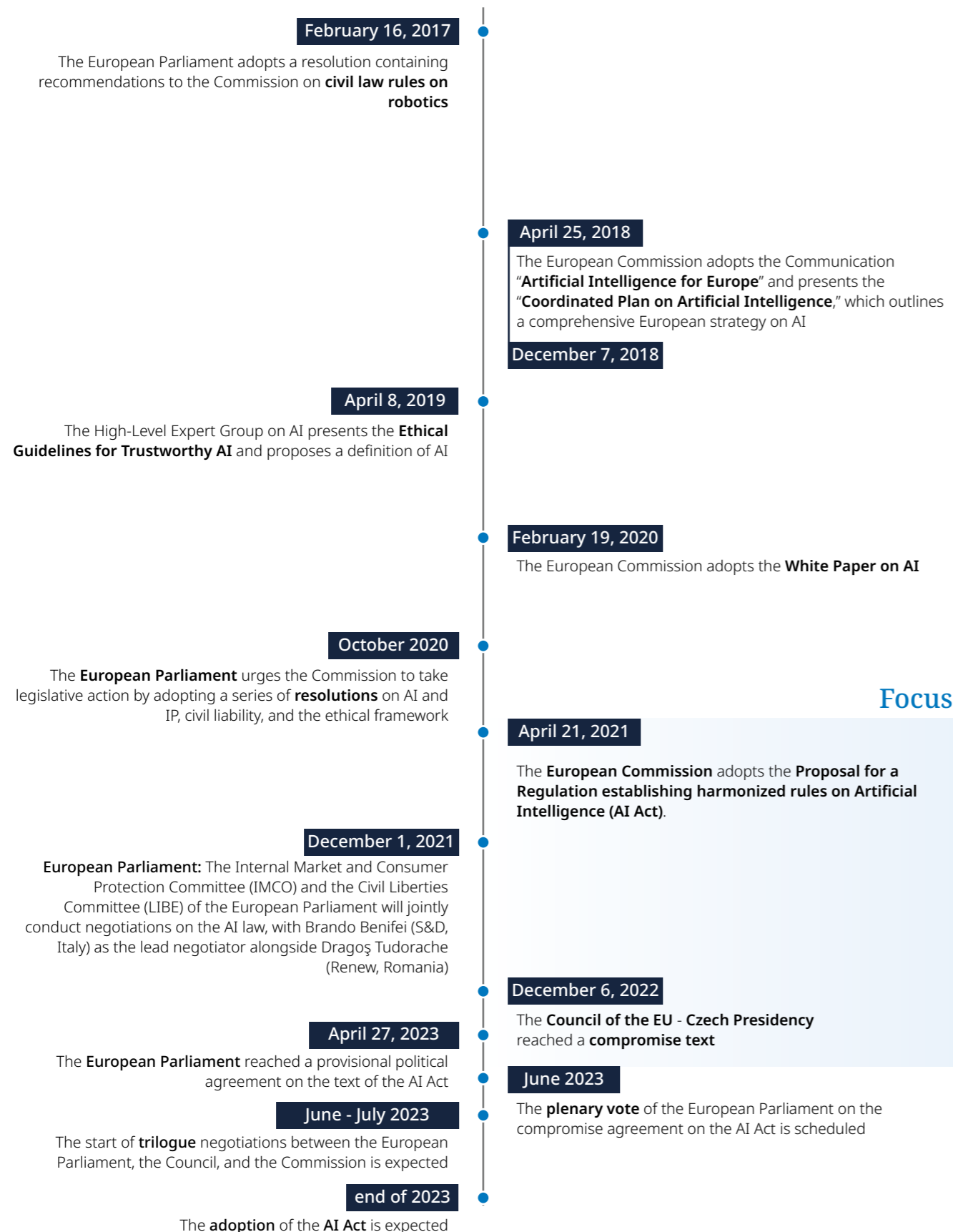
- **July 20, 2017** - The Chinese government established a strategic plan for AI development called the "**Next Generation Artificial Intelligence Plan**," which outlines the country's approach to technological advancement and sets specific goals until 2030.
- **July 1, 2021** - The Chinese Academy of Information and Communication Technology adopted the "**Reliable AI White Paper**," emphasizing the importance of improving the reliability of AI systems and advocating for the adoption of specific standards.
- **September 26, 2021** - The Ministry of Science and Technology adopted the "**Ethical Code for Next-Generation Artificial Intelligence**," which establishes ethical standards for the use of AI in China, focusing on the protection of personal information, AI responsibility, and prevention of AI-related monopolies.
- **January 4, 2022** - The Cyberspace Administration of China (CAC), the Chinese government agency responsible for internet oversight, introduced the "**Regulation on the Management of Algorithmic Recommendation Services of Internet Information**" (effective from March 2022). This regulation governs the use of algorithms in online recommendation systems, requiring that such services be moral, ethical, responsible, transparent, and promote "positive energy." The regulation includes obligations towards end-users in terms of information disclosure and prohibits price discrimination based on user profiling. In September 2021, the same authority issued recommendations aimed at strengthening the governance of algorithms used in internet information services.
- **January 10, 2023** - Measures came into effect to **regulate the use of "deep synthesis" technologies**, with the aim of governing AI-generated services and content (such as deepfakes), including the introduction of specific distinguishing marks (eg watermarks).

These interventions should be considered in the context of a complex national regulatory framework. Sector-specific AI provisions coexist with cross-cutting regulations on privacy, **cybersecurity**, and **data security** adopted in the past five years.

Additionally, there are also some **local measures**, such as the regulations on the promotion and development of AI in Shenzhen and Shanghai, approved in September 2022.

AI in the EU

by MARIA CHIARA MENEGHETTI



Focus

The journey of the AI Act

April 2021

European Parliament

The European Parliament has received thousands of amendments to the current draft of the AI Act, and a compromise text has not yet been reached.

Among the recent discussed changes are:

1. **Definition:** Aligning the definition of AI with the one proposed by the OECD.
2. **Scope:** Open-source AI models are excluded from the regulation unless they integrate a high-risk system, a prohibited system, or deepfakes.
3. **Obligations:** Stronger obligations for general-purpose AI systems that approach those of high-risk systems.
3. **Prohibited systems:** Prohibited practices include AI systems for social scoring and biometric classification.
4. **High-risk:** Significant exemptions for high-risk systems and a notification procedure for developers who believe their system is not high-risk.
5. **Governance:** Reducing the role of the AI Office.
6. **EU database:** Extending the obligation to register high-risk AI systems in the centralized European database to AI distributors who are gatekeepers under the Digital Markets Act

Feb-Mar 2023

April 27, 2023

European Parliament

The European Parliament reaches a provisional political agreement (to be validated in the plenary vote in mid-June 2023) on the AI Act, which includes the following points:

1. **Scope:** The imposition of stricter obligations for "general-purpose" AI models is confirmed, and generative AI must be designed in compliance with EU law.
2. **Prohibited systems:** The ban on biometric identification software is extended (with post-processing use only allowed for serious crimes and with prior judicial authorization), as well as the ban on emotion recognition systems in certain sectors (such as employment and justice) and expanded to include predictive policing (from criminal offenses to administrative offenses).
3. **High-risk:** An additional filter has been added. The categories listed in Annex III are considered high-risk only if they pose a "significant risk" to health, safety, or fundamental rights. Large-scale online platform recommendation systems (defined by the Digital Services Act) are also included in the high-risk systems category.
4. **Bias:** Stricter measures for the handling of sensitive data by providers of high-risk AI systems.

April 21, 2021

The **European Commission** adopts the **Proposal for a Regulation establishing harmonized rules on Artificial Intelligence (AI Act)**.

July 2021

Council of the EU - Slovenian Presidency.

Discussions have focused particularly on: scope and definitions; social scoring practices and biometric recognition; list of high-risk systems.

November 2021

November 29, 2021

Council of the EU - Slovenian Presidency. Shares the initial compromise text, which focuses on Articles 1-7 of the AI Act.

January 2022

Council of the EU - French Presidency. The main topics of discussion have revolved around: the definition of "AI for general purposes" and the diversification of transparency obligations for high-risk systems; the proportionality of penalties for SMEs; the new structure for the AI Board and increased flexibility for regulatory sandboxes.

June 2022

June 15, 2022

Council of the EU - French Presidency. Agrees on the final compromise text (which focuses on Articles 4, 16-29, 40-52 of the AI Act).

July 2022

Council of the EU - Czech Presidency. Reaches a compromise text that includes the following points:

1. **Scope:** AI "for general purposes" is included in the AI Act with specific obligations.
2. **Prohibited systems:** Prohibited AI systems also include the use of subliminal techniques, exploitation of vulnerabilities, and social scoring.
3. **High-risk:** The criterion of "decisive and not incidental weight in the decision-making process" is added, and the power to update the list of such systems is left to the EU Commission.
4. **Governance:** The AI Board is strengthened, and the regulatory sandbox regime is made more flexible.
5. **Transparency:** Transparency obligations are strengthened, particularly concerning deepfake systems.

December 6, 2022

AI & Intellectual Property

AI & Copyright

Generative AI and prompt protection

Can generative AI rely on the text and data mining (TDM) exception for its training?

'New' music created by AI: Who is the author?

The US Copyright Office denies registration of AI-generated images

The protection of the output generated by AI systems

AI & Patents

AI as inventor: Legal challenges and implications for patent law

AI & Trademarks

Advantages and limitations of using AI in intellectual property management before Trademark Offices

Generative design and the protection of products



AI & Copyright

Generative AI and prompt protection

by GUALTIERO DRAGOTTI

Key issues

- ☑ The spread of generative AI systems suggests investigating the possibility of granting **copyright protection** to prompts.
- ☑ Granting copyright protection to prompts entails some important corollaries regarding the level of **creativity** of the work and the **scope** of protection.
- ☑ Transactions involving prompts will likely be governed in terms of **assignment or licensing**.
- ☑ In the absence of legislative, regulatory and jurisprudential support, it's appropriate to rely on **past experiences and contractual arrangements**.

Even those who are accustomed to closely following the world of technology and innovation have been amazed by the overwhelming acceleration in the development of **generative AI technologies** and systems. Among them, the most popular today, especially for textual content, is [ChatGPT](#) and, more generally, models belonging to the GPT-x family, developed by the same entity also at the forefront of AI systems dedicated to the creation of images from textual data with the [Dall-E 2](#) model. Equally well known platforms have been recently made available to the general public.

The spread of these increasingly improved systems raises several interesting questions for those concerned with intellectual property, including the nature of **works** created using such tools, the attribution of any **rights** to them, the **relationship** between these rights and those on the works used to train AI systems, which have already been subject to [disputes](#), particularly in the US.

The nature and protection of prompts

One topic that – for the time being – has been less explored, at least by jurists, relates to the nature and protection of **instructions** given to AI systems to generate a specific result. These instructions are known as **prompts**.

For example, an image can be created by providing a system employing the Stable Diffusion model with the prompt “a female lawyer in court, in front of the judge’s bench, explaining a complex case, sepia drawing style.” If you try it by yourself, you will see that the AI will propose a number of images; you will be then in the position to select the preferred one and iterate until you are happy with the result. If you give ChatGPT the prompt “Compose a concise story about a lawyer trying to explain a difficult technical issue in court, resorting to an unexpected solution,” after a few passes, it comes up

with: “*The lawyer stood nervously before the jury, trying to explain the intricacies of a computer programming issue at the heart of the case. The technical language and jargon left the jury confused and disengaged. To make the jury understand the issue, the lawyer comes up with an unexpected solution of using a simple, childlike computer drawing with a big red button labeled ‘run program’ to explain the problem. This simple illustration helps the jury understand the technical issue, and the lawyer was able to make his point.*”

Whatever the assessments and conclusions regarding the possibility for images and text created with the aid of AI systems to access **copyright protection**, we have to analyze the possibility of **protecting the relevant prompts**.

Several elements should be taken into account in this evaluation:

1. The formulation of prompts must (also) meet **technical requirements**. Each platform has prepared and publishes manuals indicating the parameters and commands that can be used to create prompts.
2. The relationship between prompt and result is not necessarily unambiguous; in fact, the AI system usually has an **opacity coefficient** that prevents the establishment of a direct and deterministic link between prompt and work.
3. Most models return multiple results for each prompt, leaving the user with the option of selecting the preferred one or ones and processing them further, if appropriate, through an actual **dialog** (which is the hallmark of ChatGPT).

4. **Collections** of prompts are already available, and the authors – assuming we can use this term – sell for a fee directly or through appropriate platforms, such as [PromptBase](#).

These circumstances might make it seem possible to grant protection to a prompt used in AI systems under intellectual property law. This is because they’re works that can be traced back to the **creativity** and **personality** of their author, have **economic value**, and are **easily reproduced**.

Admitting prompts to copyright protection has some significant ancillary consequences in our system. The first relates to the level of **creativity** of the work, which must exceed a minimum threshold, however low. The second relates to the **extent** of protection, which can never allow the author to monopolize solutions and technical devices, which must remain available to all. Protection must be similar to that provided for **computer programs**, which have as their object the **outward form** of the work and not the ideas and technical solutions that determine its operation.

Assuming there’s a space for prompt protection, it’s helpful to reflect on the relationship between that **work** and the **one generated through the AI system**, which is likely to be posed in terms of elaboration and **derivative work**. Equally valuable is reconstructing – again in terms of derivation and elaboration – the relationship between prompts and **pre-existing works** of art employed as prompts or used to prepare prompts (think of the lyrics of a musical work or poem used to prepare a prompt to create images or videos).

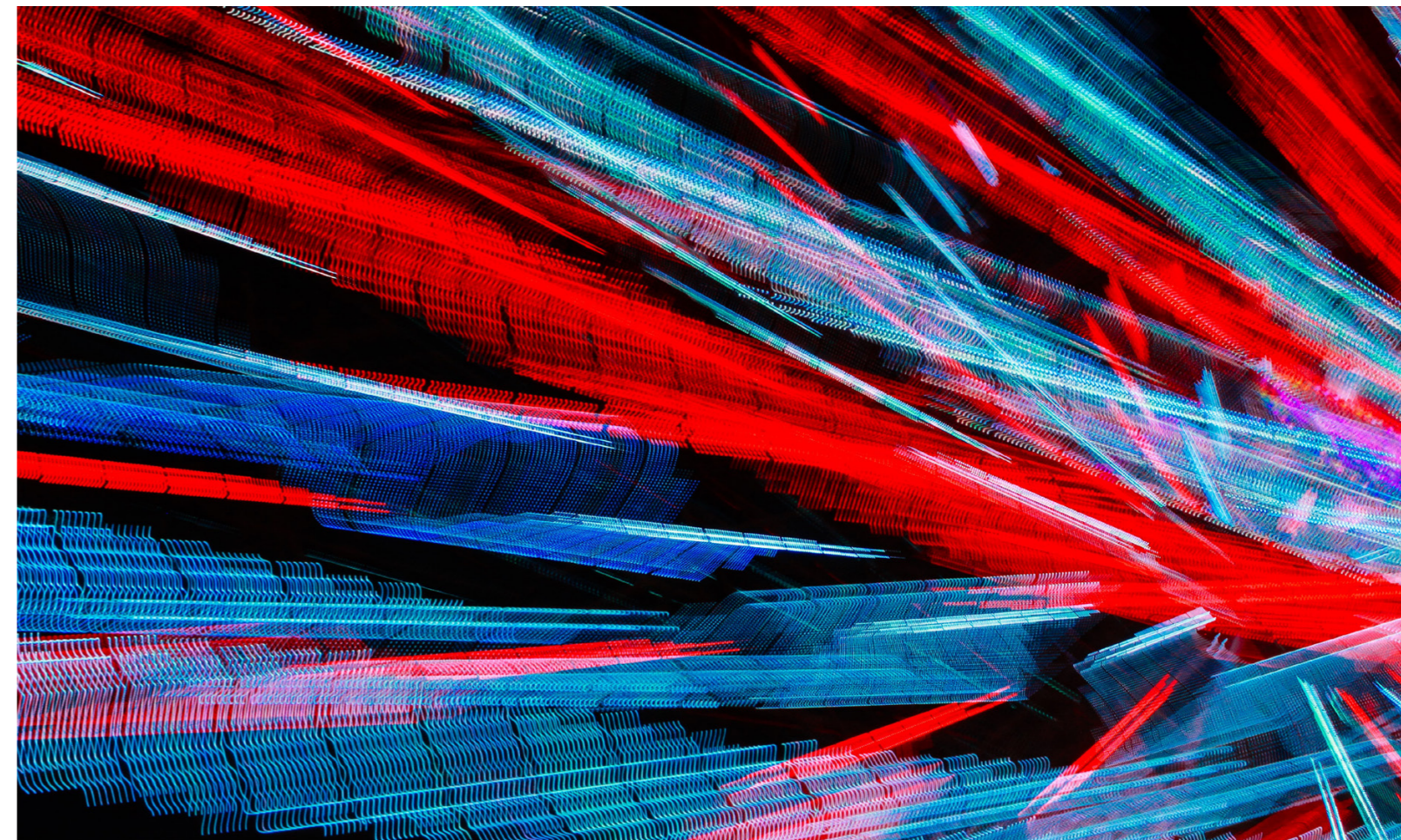
The regulation of transactions, past experiences, and contractual agreements

Once these relationships are brought into focus, it will also be possible to regulate the transactions, likely in terms of **assignment** or **licensing**. The use of a work of authorship as a prompt for an AI system was not among the foreseeable uses until recently, and permission to use a prompt to generate specific works or on certain platforms does not necessarily extend to works of a different nature or other platforms (and perhaps not even to different versions of the same platform).

These questions, and the many others that generative AI systems pose, open up scenarios that are, for the most part, unexplored. In the absence of reliable **normative and jurisprudential support**, it’s a good idea to move cautiously, using past experience – hence the reference to the principles elaborated on the protection of database software and more generally of [useful creations](#). And we should look at **contractual agreements**, clarifying the rights and obligations of all parties involved in the generation (creation?) of works through AI systems from prompts.

Glossary

Prompt: Instructions provided to AI systems to generate a specific outcome.



AI & Copyright

Can generative AI rely on the text and data mining (TDM) exception for its training?

by ELENA VARESE and CAROLINA BATTISTELLA

Key issues

- ✓ In the process of data processing, the absence of **permission** from the author of the work from which the data is extracted may constitute copyright infringement.
- ✓ The TDM exception allows AI systems to access large amounts of **data** used by generative AI to create **new content**.
- ✓ Article **70-quarter** Copyright Law exempts any TDM activity carried out on the intellectual work provided that (i) the person exercising it has had **legitimate access** to the content and (ii) the owner has not made a **reservation** statement.
- ✓ Reproductions and extractions may be **kept only as long as necessary** for the purpose of text and data extraction.

Can generative artificial intelligence systems' use of data, images and content for their own training rely on the new dedicated **text and data mining (TDM) exception** introduced by the **Copyright Directive**?

The self-training of generative AI systems and the coordination with copyright

Generative AI systems "**self-train**" using machine learning algorithms that analyze massive amounts of data, images and content and learn to use that information to create new content similar to existing content.

Such analysis, however, could be considered as a **reproduction**, even if only temporary, of the data and sources used, including any **protected works** or entire portions of the **databases** employed. Therefore, problems of coordination with the regulations protecting copyright and related rights - in particular, the **exclusive right of reproduction** under Article 13 of Law No. 633/1941 (Copyright Law) - may arise from the automated **extraction** of such content. But not only that. It could also conflict with the **right of the creator of a database** to prohibit the extraction or reuse of all or a substantial part of it.

In the context of **copyright law**, the doctrine has questioned whether **creative processing** of the protected information and/or work can be carried out. On this point the European legislator has already

provided that in the process of data processing, the absence of **authorization** from the author of the work from which they are extracted may constitute copyright infringement. However, it's clear that making the activity of data and content extraction subject to the prior obtaining of authorization from the owner of the copyrights involved would entail high transactional **costs** and also **timeframes** incompatible with those of developing AI systems. It's precisely for these reasons that the European legislator intervened by reforming this subject through the introduction of certain **exceptions** and **limitations** to copyright that are mandatory for each Member State.

TDM's exceptions

Specifically, with regard to **data mining**, the Copyright Directive 2019/790/EU introduced the **text and data mining (TDM) exceptions**, which are regulated in Articles 3 (Text and data mining for the purposes of scientific research) and 4 (Exception or limitation for text and data mining). TDM is defined in Article 2 of the Copyright Directive as "*any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations.*" At the national level, these articles have been transposed, respectively, with the introduction into the Copyright Law of Articles 70-ter - which deals only with extraction

for **scientific purposes** by research organizations and cultural heritage protection institutions - and 70-quarter - which allows the extraction of text and data in general, by anyone, even for mere **profit**.

Given the large amounts of data that AI systems use to generate new content, the close relationship between generative AI and the TDM exception is evident: the text and data mining exception allows AI systems to access **large amounts of data**, which are used by generative AI to create **new content**. Should these systems not be **allowed** to access such data, their ability to generate content would undoubtedly be limited.

The admissibility of text and data mining for commercial purposes: Legitimate access and reservation

Among the two TDM exceptions regulated by the European directive, the second one, which allows mining also for **profit**, deserves particular attention. Article **70-quarter** of the Copyright Law **exempts** any text and data mining activity that is carried out on the intellectual work, including software or database protected by a related right, regardless of the purpose or the qualification of the person performing it.

This, however, provided that:

- a. the person had **legitimate access** to the content for the purpose of text and data mining; and
- b. the owner of the copyright and related rights and/or the owner of the database have not expressly **reserved** the extraction of text and data (**opt out** mechanism), thus bringing TDM's activities under its exclusive control.

However, the liberalizing scope of the **opt-out** mechanism granted by Article 70-quarter depends on the **manner** in which the **reservation is made** by the rights holder. It is Article 4, para. 3 of the Copyright Directive itself that requires that the reservation be expressed "*in an appropriate manner, such as machine-readable means in the case of content made publicly available online.*" This provision seems to require that the reservation statement be **readable** in an automated manner when the work to which it relates is made available to the public on the **internet**. Actually, the effects of opting out can also result from the inclusion of an appropriate **clause** in a contract, an assumption moreover confirmed by the Copyright Directive itself, which does not include Article 4 among the mandatory rules.

In addition, the qualification of the reservation statement is **independent** of any assessment regarding whether there are **computer mechanisms** to prevent data extraction. This interpretation is based on the merely **informative function** of the reservation. Thus, it will be sufficient to include the reservation in the R&D of the website, even if it lacks protective measures.

Therefore, the **reservation**:

1. may be a "**digital**" statement without computer protection mechanisms, such as the exclusion protocols contained in robots.txt files; or
2. may be achieved through the affixing of a **digital rights management system** that not only has a computer protection function but also incorporates an automatically detectable computer declaration; and

3. on the other hand, it **cannot** consist of the mere affixing of **technical protection measures** that do not include any declaration, and which therefore turn out to be mere tacit manifestations of will. Thus, the presence of technical measures does not have the effect of making any TDM activity per se unlawful, but it does, however, make extractions incompatible with the technical measure adopted prohibited, since Article 174-ter prohibits circumventing technological protection measures.

Retention of copies after the conclusion of data mining

A further problematic issue concerns the **retention** of copies after data mining has concluded. With respect to this, para. 2 of Art. 70-quarter provides that reproductions and extractions "*may be retained for as long as necessary for the purposes of text and data mining,*" this is because the functionality of a copy to text or data mining ceases at the time it is **accomplished**. Therefore, copies may **not be** retained for **purposes beyond** that of TDM, such as to verify and demonstrate achievements.

There is, however, part of the doctrine that argues that reproductions for data mining can also be kept for as long as it takes to **train** AI systems. In this respect, it would actually need to be checked on a **case-by-case basis** whether AI training constitutes text and data **mining** or whether, instead, it constitutes an **activity subsequent to it**. Only in the former case copies could be retained even during the AI training phase.

Article **70-quarter**, however, omits to regulate the reproductions and any further uses necessary for the use of the text and data extracted as a result of their computational analysis, namely the use that AI systems could potentially make of them. On this point, some scholars have noted that the **use of the result** of data mining could be conditioned on the **permission** of the owner of the rights to the analyzed content.

When only the **form** or a **portion of it** is extracted with data mining, it must be verified whether the extracted and reused fragments constitute independently creative and therefore protected portions. With respect to this question, someone believe that the use of **creative fragments** does not interfere with copyright when their original meaning imprinted by the author is no longer understandable, for example, because in the new context such fragments are unrecognizable.

Therefore, **developers** who intend to use copyrighted works to train a generative AI system will need to follow three steps:

1. obtain **legitimate access** to the data;
2. verify that the rights holders have not **reserved** the right to make **reproductions** for TDM purposes;
3. keep the copies made only **as long as necessary** for TDM purposes.

Clearly, it is important to monitor future case law to understand how these requirements will be applied in practice.

AI & Copyright

‘New’ music created by AI: Who is the author?

by CAROLINA BATTISTELLA and REBECCA ROSSI

Key issues

- ☑ The use of AI systems in music raises questions about whether music **generated** by or with the **help of AI** can access **copyright protection**.
- ☑ Legal protection of works is subject to the requirement of **human contribution**. In addition, to enjoy ownership of a right, it is necessary to possess **legal capacity**.
- ☑ Through **related rights**, legal protection can be granted to those who intervene on the work, including performers, executors and phonogram producers.
- ☑ Copyright protection applies to works created by AI in cases where such technology is used as a tool to **assist** an author (human) in the creative process.

The increasing use of AI systems in the **music** industry raises question marks about copyright protection.

In this article, we will analyze the opportunities and legal issues in terms of **copyright law** related to **music generated by** or with the **help of** AI systems, tools and techniques - namely, the ability of a machine to reproduce part of the creative capabilities of the human brain - that are increasingly used in the creation of music, videos and lyrics.

The rapid and unstoppable development of AI raises numerous questions in the field of intellectual property law. The processes of making and developing creative works is governed by copyright law and is closely linked to technological and commercial transformations. It is therefore not surprising that advances related to AI technologies and their use in the creative sector give rise to new development and **business** opportunities, but also to new **legal issues**, especially related to the identification of the **author of** the work and the attribution of related **rights**.

One of the reasons for this success is that AI systems offer the most diverse application possibilities, simplifying and speeding up time-consuming processes: from music **composition** to **mastering**, from song **identification** tools to the creation of highly personalized **playlists**. This new technology is changing the way music is created by artists and heard by audiences.

There are already numerous applications and platforms capable of creating **music online**. Some of these would even seem to be able to produce music of any genre from a simple textual description. Others, however, enable the creation of **high fidelity** (HiFi), ie high-resolution (with sounds generated at 24KHz) songs and melodies. These algorithms are also capable of

generating music with **complex composition**, having been trained with data from more than 280,000 hours of music, and are even able to rely on existing sounds, melodies and songs, regardless of how they are played, ie even if they are whistled, sung or played on an instrument, potentially being able to replace most soundtrack composers.

Copyright protection on musical works generated by AI

The main problem of AI systems capable of creating music lies in the fact that the **data** with which such systems were **trained** could contain **copyrighted material**, resulting in copyright infringement of such musical works. In any case, even when the music created by AI does not infringe other copyrighted materials and is itself new, there is a debate about the level of **protection** that can be afforded to these works.

From a legal point of view, it is necessary to understand whether national, European and international copyright law subordinates the legal protection of a work to the requirement of **human input** in its creation.

For example, in the **Berne Convention for the Protection of Literary and Artistic Works** of 1886, reference is made several times to the concept of **“author,”** although without ever providing for its human nature. Therefore, theoretically, it would seem possible to protect a work created by an artificial author. On the other hand, other international and European legislations focus on the **subject matter of copyright protection**, not including any reference to the creator of the work. Similarly, **Article 1 of Law No. 633/1941** (the Italian Copyright Law) provides that *“intellectual works of a creative character belonging to literature, music,*

figurative arts, architecture, theater and cinematography, whatever the mode or form of expression, are protected under this law.” Again, the provision lacks any reference to the possible requirement of human contribution for the purpose of protection.

Nonetheless, it's important to remember that at the national level, as well as at the EU and international level, to enjoy **ownership** of a right it's necessary to have **legal capacity**; hence it is complex to recognize a protection for works created by **“machines”** which, although capable of creating musical pieces independently, would for obvious reasons be incapable of exercising or claiming their rights, should they be granted. Moreover, in our legal system, **Article 6 of the Copyright Law** provides that the original title to the acquisition of copyright is constituted only by the creation of the work *“as a particular expression of intellectual work,”* and it is precisely the explicit reference to the concept of **“intellectual work”** that is emphasized by many to argue that the author must be a human person.

So, if music tracks are generated by AI software, a distinction must be made between music tracks obtained by AI with **human assistance** and tracks generated **independently** by AI.

In the former case, the work implies a **human creative effort**, so the natural person - ie the author - who originated such compositions will be entitled to the **legal protection** granted by copyright law. More critical issues emerge, however, in the latter scenario because the rules on copyright provide that human **intervention** is necessary to give rise to a protectable creative work.

As for the **content** made by AI, to assess whether it qualifies as a **“work”** under EU law and, therefore, whether it is protectable by copyright, several studies and publications on the subject have identified - also in accordance with the case law of the Court of Justice of the EU - a **test** divided into four steps and criteria. In the field of music, a song made through AI should be (i) a **“production in the literary, scientific or artistic field”**; (ii) the product of **human intellectual effort**; (iii) the result of **creative choices**; and (iv) an **output** that expresses the choices provided for under point (iii).

Related rights

Another interesting topic when it comes to music tracks generated with the help of AI software is that of **related rights**. There are a number of rights that, alongside the category of copyright, grant legal protection to those who intervene in the work itself through their own **entrepreneurial activity** or **creativity**. In the field of music, related rights are granted, for example, to **performers** of songs, regardless of whether they are also authors of the musical work.

In light of the analysis elaborated above, then, original **improvisation** by performers using AI tools and techniques, as with traditional instruments, could be protected as a copyrighted work if it meets the requirements of **originality** and complies with the conditions of **fixation** required by national law. Similarly, **phonogram producers** could benefit from legal protection regardless of whether the underlying sound was created by a human being or generated by AI, there being no threshold for protection except that the object must qualify as a phonogram, namely it must be

a fixation of sound. On the contrary, with respect to a **performance**, the mere act of activating the AI-enabled sound or word generation (eg pressing the **“generate”** button) without further action could not constitute performance in the sense intended by the international conventions, given that an artistic performance requires some **active involvement** on the part of the performer to grant related rights protection.

Case-by-case assessment: assisting the (human) author in the creative process

It's necessary to use a **case-by-case assessment** to determine who is the author of the work and to demonstrate the presence of the level of **originality** and **human intellectual effort** required to obtain protection under copyright law. This can also be done through **reverse engineering** operations that manage to qualify the human interventions or contributions in the use of the AI system that led to obtaining that particular content.

Copyright protection rules may be applied to works created by AI in cases where such technology is employed as a tool to **assist** an author in the creative process. When human input is totally absent, or at any rate very limited, and the result of an intellectual effort derives exclusively from AI, it still seems that the application of copyright law should be ruled out by virtue of the well-established law principles that identify a **natural person with legal capacity** as an **“author.”**

Although the idea of some recognized legal protection even for works created independently by AI is still a long way off, the proposed AI Regulation bodes well. With the **AI Act**, we aim to fill the current regulatory gaps created by the unstoppable technological development by promoting **investment** and innovation in AI, improving **governance** and effective enforcement of existing fundamental **rights** and **security** legislation, and facilitating the development of a single market for AI applications.

AI & Copyright

The US Copyright Office denies registration of AI-generated images

by REBECCA ROSSI

Key issues

- ☑ The use of AI systems for **image creation** raises **questions** regarding the possibility of granting **legal protection** to works generated by graphic generation software.
- ☑ The US Copyright Office **has denied the registration** of AI-generated images as it considered them works created **without any human intervention**.
- ☑ There is **no human creativity** when the instructions provided by the user to the AI **do not allow for predicting and achieving a particular expressive outcome**.
- ☑ The legal protection of works generated with AI should be subject to **specific legislative intervention**, as currently it seems no one can claim ownership of such works.

The continuous development of AI has made using this innovative tool for **image creation** increasingly common. However, it has also brought about a series of issues worldwide regarding the possibility of granting **legal protection** to such works, raising questions about the **role of the artist** and **their creative autonomy**.

In this article, we will discuss the recent decision of the US Copyright Office (**USCO**) regarding **registering** a work created using **derivative graphic generation software**.

It is essential to specify that, just like in Italy, US copyright law does not require the deposit of a work to obtain the protection provided by **copyright**. Such protection is automatically granted when the work is created and fixed for the first time in a tangible form or recorded in a sound medium. However, it is possible – and advisable – **to register** original works with the USCO to obtain a **certificate of registration** and **proof** of the work's creation date.

The 'Kashtanova Case' and the legal principles underlying the registration of a work through copyright

The case's protagonist is Kristina Kashtanova, the author of the **graphic novel** Zarya of the Dawn. With the decision dated February 21, 2023, the USCO expressed its position by **denying** the registration of the images in the comic book because AI generated them so they were not eligible for protection under the US legislation stipulated in the **Copyright Act**.

On September 15, 2022, the author had already applied with the USCO to register her work without specifying in that request the use of **generative AI software** to create the panels in her work.

The registration certificate was initially issued. Only after approving the application did the USCO learn - through statements made on social media - that Ms. Kashtanova had used generative AI software to create her graphic novel.

In light of this new information, the USCO deemed it necessary to seek further clarification from the author regarding the **extent of human intervention** in creating the images in her book.

As reiterated in the decision by the USCO, the **registration** of an **original work** is granted only if a human being has created it. The Copyright Act protects only the **"fruits of intellectual labor"** that **"draw on the creative powers of the mind."** Since this discipline is limited to protecting the **"original intellectual conceptions of the author,"** registration cannot be granted if the USCO determines that the work - in our case, the images - was not created by a human being but rather by a generative AI tool.

Under relevant case law (Feist Publ'ns, Inc. v. Rural Tel. Serv.; Burrow-Giles Lithographic Co. v. Saroni) and statutory provisions (see 17 U.S.C. § 102(a) and (b)), the USCO stated that registration **cannot be granted** to works **created by a machine** or a **mechanical process** that operates **randomly** or **automatically** without **sufficient creative input** or intervention from a **human author**.

The examination of the elements of the graphic novel

Based on the principles outlined above, the USOC's second examination focused on four fundamental elements of the work: (1) the **text**, (2) the **structure**, (3) the **AI-generated images**, and (4) the AI-generated images **subsequently modified** by the author using **Photoshop**.

Firstly, it was recognized that Kristina Kashtanova was the **author of the text** of the work as it was written by her without the aid of other sources or technological tools, acknowledging its protection under the Copyright Act. Similarly, protection was recognized for the **"compilation"** of the **selection and arrangement** of images and text comprising the work and for the **placement and disposition** of these elements on each of the pages.

Regarding the individual images generated by AI, the USCO stated that they **were not the product of the author's human creativity** so they were not eligible for protection under US copyright law.

An intriguing aspect of the decision is that it dedicates ample space to the **technical analysis** of the generative AI software's functionality.

As highlighted by the USCO, the software used by Ms. Kashtanova autonomously generates the obtained results. This system employs AI technology to generate images in response to **text prompts** provided by the user. However, the software **does not interpret** these prompts as **specific instructions** to create a **particular expressive outcome**. From the initial user prompt, **four different images** are generated based on the software's training data. Although additional prompts applied to one of these initial images may influence subsequent images, the process is **never controlled by the user** because it is **impossible to anticipate** what the mechanical process will create in advance.

Moreover, such software **cannot understand** grammar, sentence structure, or words like humans do. In practice, what happens is that the AI system **converts** the words and phrases from the user's prompt into **tokens**, which are compared to the software's training data and then used to generate the image.

In this context, the USCO sought to emphasize that the **instructions** given by the user to the AI **do not pertain** to the **creation** of a **particular expressive outcome** but indicate, in **broad terms**, the goal the user intends to achieve. Therefore, a prompt is **not guaranteed** to generate a particular expressive result.

On this point, Ms. Kashtanova highlighted that she had invested significant time and energy working with the software to achieve a final result. However, the USCO observed that these efforts were **insufficient** to consider her the "author" of the images for which protection was sought, as such elements are **not relevant** for assessing whether *"a work possesses the minimal creativity required by Copyright law and the Constitution."* According to the Office, the process by which a user of generative AI software obtains a final image that satisfies them **cannot** be considered the **same creative process** as that of a human artist, writer, or photographer who **envisions** and **progressively develops** their work.

Finally, it was also determined that some of the images generated by the AI, although subsequently modified by the author using Photoshop, were unsuitable for constituting an original creation because the **changes** made to those images were too minor to provide the necessary creativity required for legal protection.

The new certificate of registration issued by the USCO

In light of the above, the USCO has decided to cancel the original certificate of registration for the graphic novel Zarya of the Dawn - as the initial application contained "inaccurate and incomplete information" - and issue a new certificate only for the material created by the author, Kristina Kashtanova. Therefore, The US Office has **excluded** the images generated by AI from the **registration**, considering them **works created without human intervention**.

However, it is essential to note that this **decision is not final**. In cases of registration refusal, the USCO regulations allow the alleged author to challenge the unfavorable decision and request a "Reconsideration." Additionally, if there are no further developments, it should be remembered that the examined decision represents an **administrative decision non-binding on US federal courts**. The **theoretical assessments** provided by the USCO serve as **mere guidance** for judges.

The unresolved issue of ownership of creations made by generative AI software and the need for legislative intervention

This decision leaves **unresolved** the **issue** of the **actual ownership** of the **analyzed images** by the USCO and, in general, images created through generative AI software, which currently **appear** to have **no claimant**.

The generation of works using AI systems is an exciting innovation that inevitably raises many questions regarding protecting intellectual property rights. The Kashtanova Case is undoubtedly one of the numerous and very recent examples demonstrating how digital art requires, even in Italy, **increasingly profound considerations**, if not **specific legislative intervention**, regarding the legal protection of AI-generated works.

In light of these challenges, a broader debate is necessary on how copyright should be **applied** and **safeguarded** in an era where AI is **becoming increasingly ubiquitous in artistic creation**.

AI & Copyright

The protection of the output generated by AI systems

by LARA MASTRANGELO and CHIARA D'ONOFRIO

Key issues

- ☑ The deployment of generative AI systems raises the problem of **protectability of the output** produced by AI and the **liability** if such works infringe the rights of third parties.
- ☑ Most national laws, including those outside the EU, **do not recognize** copyright protection to works of authorship made by **machines**.
- ☑ Early decisions on copyright protection of work created through AI systems have shown a **contrast** between the position of the Copyright Office in the **US** and the one taken by the Supreme Court in **Italy**.
- ☑ A **derivative work** enjoys independent protection as a **creative elaboration** when it's authorized by the author of the original work. The question arises, however, as to whether the creativity of a machine can qualify as "creative elaboration" in the absence of any **human contribution**.

The extraordinary deployment of the **generative AI** systems raises several legal issues, including the twofold problem of the **protectability** of the output produced by AI systems and the **liability** in the event that these works infringe the rights of third parties.

These issues challenge our society with essential **ethical** questions before even considering the legal ones. And the choices that will be made by national legislators in this area will profoundly affect the economic and social framework of the next few decades.

First, it should be noted that the output generated by AI systems can take the most disparate **forms**: images can be created from simple text descriptions, but also sounds, videos or graphics can be produced just from data sets. Moreover, such outputs are frequently the result of an **autonomous** work created by AI, without any human participation. Recently, works generated by AI systems have even received prestigious **awards**: for instance, the short film *The Crow* won the Jury Prize at the Cannes Short Film Festival and, according to a report in the New York Times, an AI-generated artwork won the Colorado State Fair's annual art competition.

Copyright ownership of works made by AI: Italian and non-EU legislation

However, from a legal standpoint, the issue is much more intricate than just awarding a prize. Given this complexity, we can briefly point out that to this day - with a few exceptions - most national legislations, including non-European ones, tend **not to** recognize **copyright ownership** of intellectual works created by **machines**.

The only jurisdictions that expressly provide protection for computer-generated works are Hong Kong, India, Ireland, New Zealand, South Africa and the UK. In particular, in the UK, the Copyright Designs and Patent Act 1988 provides that copyright of a work created by an AI machine is vested in the **person who** has **organized** the machine's **functions** in such a way as to enable the machine to generate the work.

One of the main arguments in favor of recognizing protection for content generated by AI systems is the **investment** of economic **resources**, and other types of resources in the **development** and **training** of the **algorithms** that underlie such systems. In other words, granting protection to AI-generated content produced would also indirectly protect the significant investments made by market players.

Some commentators have, however, observed that such an approach would be more akin to the recognition of **related rights**, such as those of phonogram producers, instead of a proper copyright protection. On the other hand, to have protection under copyright law, many national legislations require human contribution (in Italy, Law no. 633/1941 - the Copyright Law - expressly refers to "**intellectual work**"; the US copyright law is limited to the protection of the "**author's original intellectual conceptions**," and so on). However, since these legal frameworks were devised before the development of today's sophisticated AI systems, there are many **grey areas** and difficulties related to their interpretation, which are likely to lead to possible litigation.

The US and Italy: Two conflicting approaches on copyright protection of AI-generated works

In the first months of 2023, two cases, one in the US and the other one in Italy, provided conflicting approaches on the topic of copyright protection of works created using AI tools.

On one hand, the **US Copyright Office** cancelled a certificate of registration previously granted to the **graphic novel** *Zarya of the Dawn* on the grounds that the author of the comic strip, Kristina Kashtanova, had used well-known image-generating software to create the sequence of drawings that made up the comic strip.

The **communication** sent by the US Copyright Office clarified that Kristina Kashtanova "*author of the work's text as well as the selection, coordination, and arrangement of the Work's written and visual elements. That authorship is protected by copyright. However, as discussed below, the images in the Work that were generated by the [...] technology are not the product of human authorship*". Under US law only certain elements of the work are susceptible to copyright protection, which covers just "**the fruits of intellectual labor**." Therefore, the Office cancelled the original registration certificate and issued a new one covering only the **material** effectively created by **the author**.

In Italy, a recent **decision** of the Italian **Supreme Court** dealt, albeit incidentally, with the issue of the **protectability** of a work created with the aid of **software**. The dispute arose from RAI's use of the image of a **digital flower**, which was retrieved online, as the centerpiece of the set design of the Italian Music Festival (Sanremo) in 2016, without the author's authorization. The broadcaster brought proceedings before the Italian Supreme Court claiming that the second-instance decision of the Court of Appeal had erroneously qualified as intellectual work an image generated by a software and not attributable to a creative idea of its supposed author.

Contrary to the conclusions of the US Copyright Office, the Italian Supreme Court clarified that the use of software is compatible with the processing of a work of art, specifying that in such cases the creativity element should be rigorously scrutinized to verify on a case-by-case basis the extent to which the use of the tool absorbs or replaces the creative elaboration of the artist. In other words, the Italian Supreme Court does not exclude that works generated through software or other computer mechanisms may be awarded copyright protection. Therefore, if the AI system is considered a **mere tool** through which a human subject creates works, according to this approach, the content could still be considered an expression of the intellectual creativity and personality of its author.

Plagiarism and infringement: The protectability of AI-generated works inspired by or derived from pre-existing works

In light of the above, another aspect to be evaluated is the possibility that an original work created by AI could be considered the result of **plagiarism** or **infringement** of another pre-existing work.

A similar issue has already been brought before the US courts. In particular, in January 2023, the artists Sarah Andersen, Kelly McKernan and Karla Ortiz filed a **class action** aimed at challenging the legitimacy of a certain image generator software. According to their claim, these AI systems would have drawn on billions of images and photographs, including their own, for their "**training**," without first obtaining the **consent** of the legitimate owners. The artists' claims of unlawfulness are not limited to the AI learning modalities, but also extend to the **outputs** generated by them, which reflect the **style** and **characteristics** of their works.

On this note, the question of **protectability** for works **inspired by** or **derived from** others and their relationship with the original work becomes relevant. This issue is certainly not new and - especially in the field of art - can present significant margins of uncertainty.

The Italian legal system covers this type of works under **Art. 4 of the Italian Copyright Law**, which protects **elaborations** of works without affecting the rights of the original work. Under **Art. 7 para. 2** of the same law, the author of the elaborated work is considered to be the author within the limits of their own work. Furthermore, **art. 18** of the Italian Copyright Law provides for the author's **exclusive elaboration right**, which includes all forms of modification, development and transformation of the work provided for under Art. 4, implying the need to obtain the artist's **consent** for any subsequent creative elaboration.

It follows that a derivative work enjoys independent protection under copyright as a **creative elaboration**, provided that it has been **authorized** by the author of the original work. On the contrary, no authorization is required if the new work is a **parody**, which is to be understood in a broad sense. Italian case-law has clarified that parodic, humorous or ironic works, and in general works that **revisit** another person's work, are parodic to the extent that they change the **meaning** of the original work, so as to rise to the role of independent work of art and as such worthy of autonomous protection. To achieve this result, it is therefore necessary to consider the derivative work as a whole and assess whether, although inspired by the original, it diverges from it to convey a different **message**.

When a transforming activity is carried out by AI systems, the question becomes even more complicated. On one hand, the issue of copyright protection of an AI-generated work becomes once more relevant, which then raises the question on whether the activity of a machine can effectively qualify as "**creative elaboration**," especially when any human contribution is missing. On the other hand, as a general principle, it would be difficult to imagine a parody work realized by an AI system, since one would have to admit that they are capable - on their own - of **changing the meaning** of a pre-existing work. If this was the case, we would then be faced with AI systems equipped with critical-thinking ability, which could be defined for all intents and purposes as sentient.

AI & Patents

AI as inventor: Legal challenges and implications for patent law

by LAURA GASTALDI, MASSIMILIANO TIBERIO and CAMILA FRANCESCA CRISCI

Key issues

- ☑ Currently, there are no **unanimous settled case-law** on whether AI can be qualified as an inventor.
- ☑ Particularly debated are the aspects of the **ownership of moral and economic rights** to the inventions generated by AI.
- ☑ The **extension of patent protection** to AI creations may require a partial rethinking of **legal requirements for patentability**.
- ☑ Denying patent protection to AI creations could entail the risk of **people unrelated to the invention** take credit for it or a **reduced sharing of knowledge**.

In the rapidly evolving landscape of our world, AI has progressively taken on a central role, with its capacity to facilitate **inventions** becoming undisputed.

This fascinating development necessitates some critical legal considerations, especially concerning the **patent system**. This article explores some of the most contentious issues, including recognizing AI as an **inventor**, owning **moral and economic rights** resulting from AI-related inventions, and the potential challenges and advantages of **extending patent protection** to inventions autonomously generated by AI.

Case law on the qualification of AI as an inventor

Regarding the qualification of AI as an inventor, the European Patent Office (**EPO**) recently ruled on the issue, **rejecting** two patent applications designating an AI system called DABUS (Device for Autonomous Bootstrapping of Unified Sentience) as an inventor. These applications were filed by DABUS creator, Steven Thaler, as part of the Artificial Inventor Project initiative, which aims to claim intellectual economic rights for inventions generated by AI in the absence of **human creative input**.

In particular, EPO considered that the designation of DABUS as an inventor was contrary to the **European Patent Convention**, which in its opinion would presuppose that the inventor is a natural person. The Office also considered that the applicant could not even be considered as the successor in title of the machine, since the latter has no **legal personality** and cannot transfer any rights.

Similar conclusions have been reached by other Offices, notably the US Patent Office (**USPTO**) and the UK Patent Office (**UKIPO**), while DABUS patent applications have succeeded in South Africa and Australia, where the possibility of recognizing AI as an inventor has become a reality.

The ownership of the moral and economic rights on the invention generated by AI

It's clear that to date there are **no unanimous decisions** on the matter, and there are many aspects particularly debated, starting with the **ownership** of moral and economic rights on the invention generated by the AI.

As for **moral rights**, considering that they traditionally belong to the **inventor**, they should be, by default, owned by the machine. However, it is not self-evident that an AI system can claim moral rights in the absence of **legal personality**. At the same time, it would be necessary to determine who is entitled to the **economic rights** arising from the patent; to this end, the candidates could include the **owner** of the machine, its **user**, the **programmer** or, again, the person who developed the **algorithm**.

The effects of extending patent protection to AI-generated inventions

The idea of extending patent protection to AI-generated inventions carries numerous implications.

For instance, satisfying the **legal requirements for patentability**, particularly **novelty** and **inventive step**, may become more challenging. Novelty, as defined by the law, refers to an invention that does not already form part of the state of the art **when the application is filed**.

With AI having access to an ever-increasing amount of information and thereby broadening **the scope of the state of the art**, assessing an invention's novelty could be more difficult. At the same time, however, it could be argued that mere access to more information does not automatically imply a greater state of the art, since it is also necessary for the recipient to be able to **understand such disclosed knowledge**.

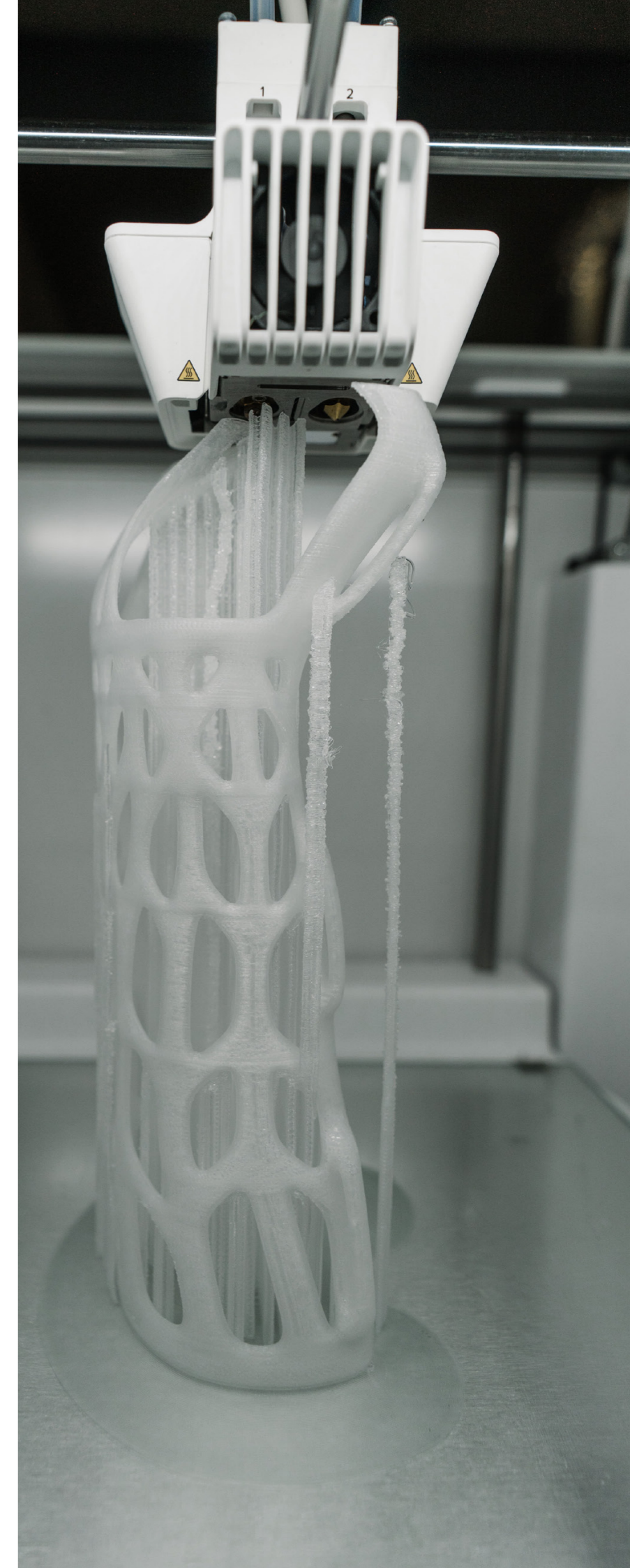
With regard to the inventive step requirement, according to which an invention does not have to be obvious from the state of the art to a **person skilled in the art**, in view of the greater breadth of information available at the time of filing the application, it may be necessary to rethink **the person skilled in the art parameter** in the case of inventions generated by the AI, commensurate with the **AI's skill**.

Equally challenging would be the assessment of the **sufficiency of disclosure**. In fact, the patent system relies on a sort of **agreement** between the **inventor** and **society**: the possibility to exclude competitors must be balanced by the benefit that people derive from the **clear and complete disclosure** of the features of the invention, to enrich the **common scientific heritage** and, once the patent monopoly has expired, allow the exploitation of the invention. However, AI creations may represent the epilogue of an **inventive process** that is not necessarily **intelligible** to human beings, with the consequence that their sufficiently clear and complete disclosure may not prove to be a particularly easy task.

The risks of not recognizing the patentability of AI creations

On the other hand, not recognizing the patentability of AI-generated creations could have **drawbacks**. For example, there could be a risk that the invention is nonetheless generated by AI, but that this is **not declared**, and people not involved in the inventive process take credit for it. In addition, denying patent protection to inventions created by AI could lead to greater recourse to the protection provided by **trade secret rules** and, therefore, less sharing of knowledge with the broader community.

In conclusion, there is certainly a question as to whether **patent law** is currently adequately equipped to answer the many questions that this issue raises. The hope is that the important implications that technological development brings with it will be taken into consideration, also in the context of a political debate, so they can find an adequate regulatory response.



AI & Trademarks

Advantages and limitations of using AI in intellectual property management before Trademark Offices

by GINEVRA RIGHINI and MARIA RITA CORMACI

Key issues

- ✓ AI systems enable trademark offices to enhance their **efficiency**, enhance the quality of their services and registration process, and shorten the timeframe for granting protection.
- ✓ Several analytical procedures still rely on human intervention and discretion, notably the evaluation of a mark's **distinctiveness** and **reputation**, as well as the examination of the **likelihood of confusion** between two marks.
- ✓ **WIPO** and **EUIPO** are among the most extensively used technological tools in this field.

The advantages and limitations of AI systems related to the trademark registration context

We're witnessing an increasing use of AI in multiple fields, including **trademark registration**. Trademark offices are actively embracing AI tools to enhance the quality and **efficiency** of their services. AI offers a wide range of **tools** and **functionalities** that can streamline the day-to-day activities of trademark offices, improving trademark registration **processes** and reducing the **timeframe** for granting protection.

Through the use of AI, **trademark offices** can swiftly and accurately analyze large volumes of data, identify **irregularities** in trademark applications, and gather data for search **reports** when this is requested by the applicant of a new application. The implementation of AI tools primarily enhances the **efficiency** of trademark offices.

However, there are **limits** to the effectiveness of AI tools. Indeed, even though AI tools are increasingly employed by trademark offices to streamline and automate certain tasks in the management of IP rights registration, there are still certain types of analysis that require subjective **evaluation** and human **judgment**. Evaluating the distinctiveness or reputation of a trademark, as well as determining the likelihood of confusion, all rely on circumstances which relate to an individual case. These circumstances cannot be understood and analyzed by AI tools alone. Human intervention is still very much required.

Currently, the application of AI tools is primarily focused on facilitating human work in areas where objective parameters exist, such as the classification of goods and services, conducting preliminary examinations for mark descriptiveness, and ensuring compliance with principles of morality and similarity between the signs. However, these tasks must still be paired with human participation.

The instruments made available by WIPO and EUIPO

An example of an AI tool that enhances the efficiency of trademark search and evaluation is the **WIPO's Global Brand Database**. This well-known tool offers users various search strategies to choose from, such as assessing the similarity of word marks based on different criteria including exact identity matches; fuzzy or phonetic matches; embedded matches, which happen when the results contain the searched term or are based on stemming, which means there is a match with the root or ending of the searched term. Additionally, the database uses AI to identify conceptual, shape, and color similarity among figurative marks, employing a composite analysis based on cross-color and edge information. With this tool, potentially conflicting signs can be identified more efficiently, allowing users to focus on the most relevant results.

WIPO's tools also offer suggestions regarding the relevant classes of the Nice Classification. When users input their desired goods and services, the tools indicate the appropriate classes for identical or related goods



and services. For example, if someone is searching for a software or hardware, the tool might recommend classes 9, 42, and 45.

Similarly, the EU Intellectual Property Office (**EUIPO**) has recently implemented AI-based tools to simplify the trademark **registration process**. These tools include: automatic **translation** of decisions; **image** search in eSearch and TMview; and an AI-powered application for goods and services classification. The latter enables a **semantic comparison** of terms, helping with the selection of the most appropriate protection for the trademark at issue.

The EUIPO is continuously advancing the implementation and enhancement of its tools, leading to a faster and more precise sign **comparison** and accurate predictions of dispute outcomes, with an accuracy rate of over 90%. The increasing accuracy of AI results empowers users to make more informed decisions. Moreover, the EUIPO offers the convenience of a virtual assistant through **chatbots** in the Easy Filing section, further simplifying and streamlining the trademark filing process. Overall, the integration of AI-based tools is a significant stride for the EUIPO in delivering a more efficient and effective service.

Although the use of AI tools in trademark offices revolutionizes intellectual property management, it is important to recognize that these tools expedite the trademark search and evaluation process, enhance

office **efficiency**, and reduce backlogs. Nevertheless, **human intervention** is still necessary to make legal decisions and interpreting data derived from AI tools. While AI can **simplify** certain aspects of trademark examination, it cannot entirely replace **human sensitivity, experience**, and understanding of the legal context in which these tools are employed.

AI & Trademarks

Generative design and the protection of products

by TAMARA D'ANGELI

Key issues

- ✓ The **advantages** of generative design include reduced research and development times, the consolidation of complex structures and versatility.
- ✓ Generative design solutions can be protected through registration as **designs or models**, irrespective of the specific product sector they belong to.
- ✓ To obtain protection as a design or model, the requirements of **novelty** and **individual character** must be fulfilled.
- ✓ **Examples** of potentially protectable generative designs include the “Generative Vase” “Generative Shoes” and “Generative Scarves.”
- ✓ Issues for protection may arise with reference to the **requirements for access to protection and graphic representation**.

What is generative design?

Generative design is an iterative design **exploration** process that uses AI software to generate a range of design solutions that satisfy a set of **constraints**. Unlike traditional design, which typically starts with a model based on an engineer's knowledge, generative design begins with design parameters, or rather, the initial identification of **rules** and **parameters** that define the **characteristics** and **properties** of the design. These include shape, structure, color, texture, and so on, and subsequently, it uses **shape-generating** AI software to automatically create a series of design variations that adhere to those rules and parameters.

Therefore, generative design is a **technique** based on the use of algorithms that allow for the generation of complex and organic **shapes** and **models**, resulting in **unique** and **distinct** forms that are difficult to achieve using traditional design methods. Compared to such methods, the fundamental change lies in the fact that the parties no longer have to create their own products by themselves. Generative design can be seen as a form of “**collaboration**” between the designer and the software, where the designer defines the design rules and parameters and the software automatically generates a series of design solutions based on those parameters.

Among the **advantages** of generative design are: i) the opportunity to perform simultaneous exploration, validation and comparison of hundreds or thousands of design **options**; ii) the reduction of research and development **times** for new products and, consequently, the acquisition of a significant competitive advantage in accelerating product market launches; iii) the opportunity to build and consolidate **complex structures**, such as organic details and internal lattice structures, to leverage the maximum design **freedom**

allowed by additive manufacturing technologies. A single complex geometry created by a generative algorithm and 3D printed can replace assemblies composed of dozens of separate parts.

Another crucial aspect to consider is the **versatility** of generative design. The algorithms employed in generative design can be effectively applied across various **industrial sectors**, enabling customization of shapes and models according to specific project requirements. While generative design initially gained traction in industries like aerospace and aviation due to their heightened technological performance needs, it has gradually expanded to disciplines such as architecture, product design, lighting design, automotive, packaging, fashion design (jewelry, accessories, footwear) and more. Sectors in which the potential for **fractal, cellular, randomizing formalization** inherent to generative design appears congenial to the main lines of **aesthetic research** and necessary to explore a wide range of innovative design solutions that would otherwise be difficult or impossible to obtain.

Finally, worth mentioning is the combination of generative design and **additive manufacturing (AM)**, namely **3D printing**, a production technology that enables the creation of three-dimensional objects by sequentially adding materials layer by layer, instead of subtracting material from a solid block as in conventional manufacturing processes. In brief, it is a process that starts with the creation of a virtual 3D model of the product, which is then divided into thin sections called “**slices**.” These slices are then used to generate a printing program that guides the machine in the physical creation of the object. All of this with a significant freedom of choice in the **materials** that can be used, including plastic, metal, ceramic, and even biological materials.

Generative design and 3D printing are renewing and revolutionizing the **manufacturing industry** and product design. In fact, by combining these two technologies, it becomes possible to optimize both **performance** and **production**, resulting in more efficient, lighter, stronger and higher-quality products.

Forms of protection for generative design: Registration as a design or model

Registration as a **design** or **model** is one of the useful tools for protection, as long as specific requirements are met. It allows for the protection of the **entire appearance** of a product or **part** of it. This includes the characteristics of lines, contours, colors, shape, surface structure, materials of the product itself, or its ornamentation. Therefore, it is one of the legal protection institutions that can be used to safeguard the external appearance of a product from **unlawful imitation**, which goes beyond mere similarity and does not require specific aesthetic appeal. It's worth noting that a design has a **two-dimensional** character and can pertain to the **lines** and **colors** of a product or a two-dimensional **graphical** pattern. On the other hand, a model has a **three-dimensional** character and pertains to the shape of a product.

The **field of activity** is not relevant for the purpose of protection. The tool of designs and models can be used for any product, provided that the **requirements**, which we will now see, are met and verified by entities such as the EU Intellectual Property Office (**EUIPO**). The EUIPO is responsible for the registration of intellectual property rights within the territory of the EU and for verifying the specific **conditions for accessing** protection.

When is it possible to protect the appearance of a product through registration as a design or model?

As previously mentioned, to obtain protection as a design or model, certain requirements must be met: **novelty** and **individual character**.

A design or model is considered new if it has **not** been made **available** to the public before the date of filing of the application for registration, except in cases of non-destructive pre-disclosure. This includes, for example, the case of disclosure made by the same author within the 12 months preceding the registration date.

Moving forward, a design or model has individual character if the overall **impression** it produces on an informed user differs from the overall impression produced on such user by any design or model that has been made available to the public before the date of filing of the application for registration. The **informed user** will perceive differences that may overlook the **average consumer**.

The protection granted by registration has a duration of five years, which can be renewed for additional five-year periods, up to a maximum of twenty-five years.

Examples of generative design that could potentially be protected through registration as a design or model

- “**Generative Vase**”: it is an example of generative design applied to the **furniture** sector. It was created by a design and technology studio based in Barcelona, Spain, which focuses on designing **objects** and **environments** generated algorithmically.

It is a product created through the use of computer algorithms that have generated organic and intricate shapes, which were then transformed into a physical object through 3D printing. The shape of the vase was generated using a series of predefined rules and parameters, resulting in an organic and fluid form composed of interconnected cells.

- “**Generative Shoes**”: they represent an example of **applying** generative design to the **footwear industry**. They originate from an **algorithm** created by the designer himself, who is an American designer and engineer dedicated to experimenting with new design and production techniques using generative design software and 3D printing. Specifically, a **machine learning** algorithm was used to analyze data on the user's **foot** dimensions and shape.

The new collection of 3D-printed **shoes** and **accessories**, inspired by speculation on consumerism, emerges from a collaboration with a company specializing in 3D printers and graphics software. More specifically, the collection consists of many unique pieces with a 3D-printed, gold-plated heel. The shoes were produced using the aforementioned printing technique, starting from **nylon powder**, which was fused and layered to create a final shoe form that perfectly adapts to the foot. Celebrities such as Dita Von Teese and Katy Perry have appreciated the design by wearing these iconic shoes.

- “**Generative Scarves**”: they originate from the idea of an English designer and scientist and are an example of the application of generative design in the **fashion** industry. More specifically, they were generated through software that uses **data** collected from the **human body**. The designer created a collection of generative scarves that change color in response to variations in the human body, such as **temperature** and **perspiration**.

Those mentioned are just a few examples of generative designs. What is of significance is that, when the mentioned requirements for registration are met, the appearance of such products may be protected through **registration** as a **design** or **model**. The output of investments related to these technologies and the production of such products could therefore receive **protection**.

The issues related to the protection of generative design through registration as a design or model

In conclusion, it's essential to mention the pertinent **issues** associated with the protection of generative design through registration as a design or model that may arise.

One of the notable issues is linked to the requirements for **obtaining protection**. Due to the algorithmic nature of generative design, there is a possibility for the generated outcomes to be similar or identical to those produced by other algorithms. This situation may impede the demonstration of the design's novelty and individual character, affecting its eligibility for registration.

Lastly, the **graphical representation** is another critical aspect to take into account. Registering generative design requires the presentation of suitable 2D or 3D images or drawings that represent the appearance of the product to be protected. This might not fully capture the complexity and organic nature of the design and its features, which can be highly intricate.

AI & Technology

AI & Privacy

Deep fake and deep nude
Cognitive biases and discrimination of the algorithm
AI nudging in e-commerce: Privacy implications of algorithmic neuromarketing
Synthetic data: A safeguard or a threat to privacy?

AI & Cybersecurity

Risks and opportunities of the diffusion of AI

AI & Outsourcing

AI and outsourcing agreements

AI & Liability

Liability for damages caused by AI



AI & Privacy

Deep fake and deep nude

by GIORGIA CARNERI

Key issues

- ☑ Deepfake and deepnude are AI applications that raise concerns about the malicious and manipulative purposes they pursue with increasing frequency.
- ☑ Deep fakes can give rise to serious forms of **identity theft**, leading to manipulation of victims' physical representation and reputational damage.
- ☑ Deep nude content is used as acts of **cyberbullying** or **revenge porn**, in some cases even fueling the practice of illegal pornography and child pornography.
- ☑ The exercise of the **right to be forgotten** as a protection for the data subject may encounter serious **enforcement challenges** due to content sharing on multiple online platforms and the difficulty in identifying the origin of the manipulated image.

AI is an ever-evolving technology that is having a significant impact on the way we live and interact with the world around us, bringing several innovations in many fields while at the same time bringing new challenges for privacy and personal data protection.

Among these challenges, deep **fakes** and **deep nude** is a topic of increasing prevalence and relevance, entailing a number of **risks** and **critical issues**. In this article we'll explore the main issues and possible negative consequences of these technologies with particular reference to identity theft, cyberbullying and revenge porn, and the right to be forgotten.

What are deep fakes and deep nudes?

Deep fakes are videos or images created using AI to replace one person's face with another's. Often it's so realistic that they are almost indistinguishable from reality. The word deep fake is a neologism created by merging the terms "**fake**" and "**deep learning**," a particular AI technology. The starting point is always the real **faces**, real **bodies**, and real voices of people (all "**personal data**" under the **GDPR**), but transformed into digital "**fakes**." Unfortunately, deep fakes are not created for purely goliardic purposes, but can also be used for illicit purposes, such as spreading fake news or compromising a person's reputation.

Deep nudes, on the other hand, are a **subcategory** of deep fakes, consisting of images manipulated by AI for the purpose of removing a person's clothing, creating fake, sexually explicit images. This technology has been used to make **pornographic** images of celebrities and other people without their **consent**, and it seems clear that deep nudes can also be used for **extortion** or **defamatory purposes**.

The main risks and critical issues: From identity theft to difficulties in exercising the right to be forgotten

The ease with which sensitive attributes of an individual's personal sphere can be manipulated using technologies such as deep fakes is evident. The situation is further complicated by the increasing availability of **apps** and **software** that enable the creation of highly sophisticated deep fakes with common devices such as smartphones, which are now within the reach of everyone, including **minors**.

Identity theft

As also pointed out in the [Vademecum of the Italian Data Protection Authority](#), the phenomenon of deep fakes can give rise to particularly serious forms of **identity theft**, as the people involved completely lose control over their own image and public representation of themselves. Not only the **physical representation** of the people involved in the deep fake can be manipulated, but also the **context in which** they are placed, the **people** around them, and the situations they represent. Moreover, the possible negative consequences can extend beyond the victim's personal sphere, for example, by damaging the **reputation** of a company or organization with which the person is associated.

Cyberbullying and revenge porn

Deep fake videos can be created with the intent to engage in actual acts of **cyberbullying** or even **revenge porn**, that is the online sharing – for the purpose of **blackmail**, **denigration**, or **revenge**, by former partners, lovers, or rejected admirers – of photos and videos with **sexual** or even **pornographic** content, which, in the case of deep nude, are obviously fake.

In the specific case of deep nudes, the faces of people (including minors) can be "**grafted**," using special software, onto the **bodies** of other subjects, either naked or engaged in poses or acts of an explicitly sexual nature. It is also possible to take images of clothed bodies and "**undress**" them, reconstructing what the body would look like under clothing and creating highly realistic images.

Initially, the phenomenon mainly involved **famous** people for the purpose of discrediting or blackmailing them. But in recent times, with the increasing spread of software using this technology, the risk also involves "**ordinary**" people, who can become the object of psychologically and socially very damaging actions. Deep nude videos can also be used, without the complete **knowledge** of the subjects depicted in the images, to fuel the practice of illegal **pornography** and, unfortunately, even very serious crimes such as **child pornography**.

Right to be forgotten

The right to be forgotten is a key provision of the **GDPR**: this right aims to ensure that data subjects can have their personal **data deleted** under certain circumstances, such as when such data is no longer needed for the purposes for which it was collected or when the data subject withdraws their consent for it to be processed.

However, the right to be forgotten may encounter **difficulties** in practical **application** in certain cases. Since images and videos created through deep fakes

can be shared on multiple online platforms and quickly go **viral**, the data subject who wishes to enforce this right (and the data controller who has to follow up on the relevant request) may not see their claim fully satisfied. Nevertheless, there are also great difficulties in identifying the origin of the manipulated image. This can make it difficult to determine who created the image and with what intent, making it difficult to identify those responsible and take appropriate legal action.

These issues are just some of the significant challenges arising from the spread and exploitation of deep fakes and deep nudes.

It's important, therefore, that **data controllers**, **data protection authorities**, and **companies** implementing AI technologies work together to develop effective **solutions** to address the risks associated with the use of deep fakes and deep nudes to ensure the **protection** of data subjects' **personal data** and guarantee the exercise of the rights recognized by the **GDPR**. Only through concerted and coordinated action will it be possible to successfully address these challenges and protect the rights of individuals in the digital society in which we live.



Glossary

Deep fakes: videos or images created using AI to replace one person's **face** with another's, often so realistic as to be almost indistinguishable from reality.

Deep nudes: images manipulated by AI for the purpose of removing a person's **clothing**, creating fake, sexually explicit images.

Revenge Porn: online sharing - for the purpose of **blackmail**, **denigration** or **revenge**, by former partners, lovers or rejected admirers - of photos and videos with **sexual** or even **pornographic** content, which, in the case of deep nude, are fake.

Cognitive biases and discrimination of the algorithm

by ENILA ELEZI

Key issues

- ✓ Based on **machine learning algorithms**, it's possible to "teach" the algorithm to produce predefined and even non-predefined outputs, if the algorithm is not supervised by a human.
- ✓ Through the **datasets** provided to the algorithm for its training, it can reproduce **cognitive biases** derived from the set of (unbiased) information provided.
- ✓ Examples of risks generated by cognitive biases can be found in the field of **personnel selection** and **insurance risk assessment**.
- ✓ These risks can be reduced or avoided through **technical actions** (eg diversified and representative datasets) and **regulatory measures** (eg risk management systems, transparency obligations, human supervision).

Although the importance of AI is increasingly becoming an integral part of our daily lives, the increased use of AI systems raises concerns about "**biases**," which are prejudices and resulting **discriminations** that can arise from their use.

Machine learning algorithms

AI can be defined as the ability of a machine to exhibit **human-like capabilities** such as reasoning, learning, planning, and creativity, and it is composed of various algorithms that learn through machine learning. Based on machine learning algorithms, it's possible to guide and "**teach**" the algorithm what results to generate, similar to teaching a child the letters of the alphabet through illustrated books. In this case, AI can "learn" from a dataset and produce a predefined output (in the case of **supervised machine learning**).

In other cases, starting from a dataset, the algorithm learns to identify complex processes and patterns without the careful guidance of a human mind (unsupervised machine learning). It's as if we always wanted to teach a child the letters of the alphabet through illustrated books, and the child will be able to produce their "own reasoning" by generating words and phrases that are not predefined outputs.

Cognitive biases

It's in these scenarios that we find AI models like ChatGPT where **cognitive biases** can be produced. Algorithms are nothing more than mathematical models that are "**trained**" using datasets provided by humans. Returning to our illustrative example involving a child, when the letter "A" consistently correlates with the color red, it increases the likelihood of the child using the color red when reproducing the letter on a blank sheet of paper.

At the same time, through the initial datasets provided to the algorithm, it's possible for the algorithm to reproduce "**biases**" that are simply derived from the set of **information provided**. Bias can infiltrate in various ways, and in this context, we will focus on biases related to prejudices, opinions and ethnic, cultural, social issues.

Personnel selection and insurance risk assessment using ML algorithms

One area where the use of AI can create great efficiency on one hand, and raise concerns on the other, is the workplace, specifically **personnel selection** using machine learning algorithms. When the personnel selection algorithm is trained using historical datasets of candidates who have demonstrated greater success in a specific role, it may perceive the shared attributes among these candidates as more significant for that role. This is what happened to a **well-known multinational company** in search of new resources for an IT role: the algorithm automatically rejected female candidates because it relied on a dataset collected over the past ten years where the majority of tech hires were male. The algorithms identified and highlighted the biases of their own creators, demonstrating that training automated systems on **biased data** leads to future non-neutral decisions.

In addition to the above, in the insurance landscape, AI systems are being increasingly used to provide **personalized products** and **services** at more competitive prices, ranging from health and life protection to underwriting and claims assessment. If not properly developed, even in this perspective, AI systems can pose significant risks to people's lives, including **discrimination**. For example, an insurance **risk assessment** algorithm

could use customer data such as age, gender, income, profession, and health status to determine the insurance price and the level of risk associated with the customer, excluding certain individuals.

Technical and regulatory remedies for biases and discrimination

The risks generated by these cognitive biases can be reduced or even avoided through **actions** both from a **technical** and **regulatory** standpoint. First and foremost, it's necessary to act on the algorithm itself. Training algorithms on the most **diverse** and **representative dataset** possible is essential, constantly monitoring the produced outputs to identify and correct biases at the source. Additionally, in the selection process, it may be relevant to involve not only technical experts but also a variety of **professionals** to prevent unintentional discrimination.

On the other hand, clear regulatory provisions are also crucial. It should be noted that the described AI systems already fall within the scope of the **AI Act** draft. The AI Act adopts a risk-based approach (similar to the **GDPR**), identifying three levels of risk (unacceptable, high, and limited). These systems are listed in **Annex III** of the proposed Regulation and include systems that fall within the **context of work and employment**, including the selection and hiring of personnel.

For these systems, a series of **obligations** (eg risk management systems, transparency, human oversight) are foreseen, which **suppliers** must comply with from the design and development phase, and **compliance** with these obligations must be carefully evaluated before the commercialization of the system itself.

However, the application of these rules will only concern the near future. For the time being, it is necessary to rely on the combined provisions of other regulations that impose **transparency obligations** or the **right to opt-out** regarding the processing carried out by these systems, as well as the right to request **human intervention** in the processing of this data. These provisions can be found in Article 22 of the GDPR and the new transparency provisions incorporated by Legislative Decree no. 104/2022 (the **Transparency Decree**), which introduce significant regulatory obligations when "automated decision-making or monitoring systems" are used concerning **workers**.

Using AI in personnel selection processes, the creation of personalized offers, and access to certain services can lead to significant improvements in **efficiency** and **accuracy**. But it's important to pay attention to the risks of **discrimination** and **cognitive biases** associated with the use of these algorithms. Only through a combination of **transparency**, **fairness** and **clear** regulatory provisions that impose specific obligations on the users of AI systems can we ensure that AI is used in a more responsible and equitable manner.



AI & Privacy

AI nudging in e-commerce: Privacy implications of algorithmic neuromarketing

by NOEMI MAURO

Key issues

- ✓ Algorithmic marketing has **privacy** implications related to algorithms' collection of users' personal data and user **profiling**.
- ✓ With neuromarketing 2.0, the concept of the "**average consumer**" is dropped and transformed into that of the "**profiled consumer**."
- ✓ Through an artificially profiled shopping experience, companies can carry out more effective **advertising**, while consumers can obtain products/services more **quickly** and **easily**.
- ✓ Neuromarketing based on AI systems, by grafting itself into consumer **decision-making processes**, can go so far as to undermine their **free will/free consent formation** in violation of the GDPR and consumer law.

It's not surprising that companies can influence the **consumer decision-making process** through strategic **marketing** choices, but the issue is where to draw the line between the benefits both parties get from a personalized buying process and the **modeling** of consumer preferences and trends to increase capitalization. Moreover, what role does AI play in analyzing consumer buying **preferences** and **trends**?

Neuromarketing and nudge marketing

The AI boost in **e-commerce** is becoming increasingly relevant as it offers a way to influence customers' decisions without them realizing it. This new type of marketing, called "**neuromarketing**," uses AI algorithms to analyze customers' behavior and target them with personalized communications. However, "**algorithmic marketing**" also raises some **privacy** issues. Algorithms used in neuromarketing can collect **personal data** from users and generate detailed **profiles**. Understanding the implications of algorithmic marketing on user privacy is essential for companies that are interested in using this technology but without facing challenges brought by data protection authorities.

The **Nudge Theory**, first formulated by Richard Thaler and Cass Sustein, is based on the principle of **choice architecture**, according to which it is possible to **influence** the human mind to take certain actions or make choices under the belief that they have acted in total autonomy. By contrast, the decision has been conditioned by a "**deus ex-machina**" from the outside. **Nudge marketing** takes advantage of the human brain's inclination to save energy through the automation of choices and behaviors. Accordingly, it's based on the idea of influencing the "**decision shortcuts**" that guide the consumer when making a purchase.

Neuromarketing 2.0

By amending the Consumer Code (Legislative Decree 206/2005, as subsequently amended), the legislator has recently taken steps to protect the **weaker** party in the buying and selling relationship from situations such as aggressive marketing or misleading advertising. However, commercial practices that are excessively intrusive into the individual's personal sphere are increasing in online commerce.

Neuromarketing 2.0 relies on the power of **neuroscience** to identify and leverage consumer buying preferences, while increasing the efficiency of computational algorithms through the use of AI, which allows for more accurate and factual information. Thus, the concept of the "**average consumer**" on which classical economic theory is based is replaced with the "**profiled consumer**." The profiled consumer is exposed to advertisements and offers that use specific **psychological aspects** obtained through a study of the individual based both on the **chrono story** of previous purchases and on elements of biometrics that make it possible to identify, for example, a buyer's peaks of interest to refine the user experience ("**feel data**").

E-commerce: The benefits of a profiled shopping experience through AI

AI has already been used to support online marketing for some time, so this is not a revolution in the way we think about e-commerce. The benefits of an artificially profiled shopping experience are significant, both from the perspective of companies and consumers. The former can increase the number of successful sales, thanks to advertising that is effective in meeting more or less induced desires of the customer. The latter, on the other hand, will enjoy greater satisfaction in quickly and easily obtaining the desired products or services.

Algorithmic marketing grounded in neuroscience principles permeates the typical shopping experience on online sites. Consumers have become used to chatbots and virtual assistants available 24/7, and to suggestion lists that are constantly updated through self-learning fueled by the profiled individual's purchase choices ("loop in retro-feedback").

Under these terms, "nudge-tech" (ie the application of Nudge Theory to digital technology) has made it possible to use hardware and software systems to change the behaviors of a marketing platform automatically, based on the data collected and analysis conducted.

Privacy implications of AI marketing

What then are the **privacy implications** of AI marketing? The information collected and processed to create end-user consumption profiles is often arbitrary, unbiased, and obtained through bias-fueled correlations. Via the **back-feedback loop mechanism**, what's missing is the **variety** of upstream options to be presented to the consumer for them to make the final choice, leading to an **alteration** of the will formation process.

We no longer really know whether we **like what we see**, or whether **we see it because we like it**. Perhaps the two concepts have now overlapped? The creation of environments in which the self-fulfilling prophecies limit incoming input, creating gray areas in which only certain information passes the selective assessment of the algorithm to reach the consumer - which already seems to be satisfied in the first instance - invoke the urgency of addressing issues such as that of "**neuro-privacy**."

Neuromarketing based on AI systems that make it even more accurate, engenders concern as it is embedded in decision-making processes. It heavily affects the preferences and habits of life, the personal identity of the consumer, going so far as to undermine the free will of the customer who, especially in e-commerce, is in a physical and mental position disadvantaged compared to the marketer. The implications are not only inherent in the free formation of consent, but also lead to a clear violation of the Consumer Code which, in Art. 2, c. 2, states how consumers have the right "*to the exercise of commercial practices according to principles of **good faith, fairness and loyalty***."

In short, it's a short step from **suggestion** to **submission**, and the profiling that numerous online platforms and social media operate nowadays to build customer loyalty is likely to result in enslavement.

While the above may still seem like a dystopian and distant future, it's wise to keep in mind the exponential speed with which AI technologies are developing. In a world where digital capitalism runs the show, it will be increasingly important to remember a quote from Stefano Rodotà (first president of the Italian Data Protection Authority): "Not everything that is technically possible is legally legitimate and ethically permissible."

Glossary

Neuromarketing or algorithmic marketing: a form of marketing that uses AI algorithms to analyze consumer **behavior** and influence consumer **choices**.

Nudge-marketing: a form of marketing that, by exploiting the human brain's predisposition for "**energy conservation**," leads consumers to make choices in the belief that they have acted completely autonomously, when in fact the decision has been conditioned by an external "**deus ex-machina**."

Neuromarketing 2.0: relies on the aid of **neuroscience** to identify and exploit consumer buying **preferences** by increasing the **efficiency** of computational algorithms through the use of AI.

Loop in back-feedback: a self-learning mechanism of AI systems fueled by the profiled subject's **purchase** choices that results in the loss of the variety of upstream options that must be submitted to the consumer for them to make the final choice, leading to an **alteration** of the will formation process.



Synthetic data: A safeguard or a threat to privacy?

by CRISTINA CRISCUOLI

Key issues

- ✓ Synthetic data can help **minimize** the amount of **personal data** processed by AI applications and overcome the obstacles set by data protection law.
- ✓ Thanks to synthetic data, it's possible to overcome the **inconveniences** arising from the use of **anonymized data**.
- ✓ Synthetic data can be an extremely useful tool, but it has to be used in compliance with applicable laws, particularly those **protecting personal data**.

The spread of AI and its use in any market sector make it urgent to find **solutions** to protect fundamental rights and freedoms, particularly concerning the **right to privacy** and **data protection**.

The exploitation of vast amounts of personal data for **training** AI systems, the difficulty of verifying their **accuracy** and **relevance**, the loss of **control** by individuals over their information, and the existence of many issues in verifying the accuracy of decisions made by AI are just some of the privacy-related risks associated with the use of AI systems.

Synthetic data as a tool for data minimization

As outlined by the [Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data \(Convention 108\)](#), responsible innovation in the field of AI requires an **approach** focused on **avoiding** and **mitigating** the potential risks of processing personal data.

Using **synthetic data** can be a solution to **minimize** the **amount** of **personal data** processed by AI applications, prevent **retrieving** this information back to the relevant individuals (ensuring the non-reversibility of de-identification), and overcome the obstacles to technological evolution posed by data protection laws.

Synthetic data – which is so defined since it is obtained through a **synthesizing** process – is **fictitious information** derived from actual data, thanks to the use of generative **machine learning algorithms**. The algorithm is trained to reproduce the characteristics and structure of the original dataset, allowing us to obtain statistically accurate results.

The synthesizing process – which can be implemented through various techniques – starts from a **real dataset**, which can include any kind of information (including

images), to obtain an **artificial dataset** that mirrors the features of the original dataset. This process allows the characteristics and structure of the source information to be replicated without the need to replicate or trace the identifying elements of the source information (ie reveal any personal data).

Synthetic data enables us to overcome the limits of anonymization

The above features represent a significant step forward for using personal data because they **overcome** the **inconveniences** associated with **anonymized data**. Data protection legislation does not apply to anonymized data because it does not fall under the definition of “personal data.”

However, to refer to anonymized data, it must be **impossible** to **retrieve** the **identity** of the individual to whom it relates. This represents a limitation to the use of the information, either because technological progress has made it very difficult to guarantee the absolute **irreversibility** of the data obtained or because the removal of any identifying element to ensure complete anonymization often results in the reduction of the usefulness of the data obtained.

Such inconveniences can be overcome thanks to the **synthesizing** process described above.

Moreover, the fact that **synthetic data** – such as anonymous data – is **not** considered “**personal data**” makes **legislation** on protecting such data **inapplicable** to their use, which provides many obstacles to using such information. The draft of the AI Act puts synthetic and anonymized data on an equal footing when **Article 54** regulates the conditions for using personal data for development in the AI regulatory **testing space**.

This explains the reasons why the use of synthetic data is increasingly common in the field of **machine learning**, whose algorithms need a massive amount of data to be “**trained**.”

Privacy concerns arising from the use of synthetic data

No **risk** for **privacy**, then? Unfortunately, **this is not the case**.

Although synthetic data has an artificial nature, it's **obtained** from **real information**, which must be processed following data protection laws.

Firstly, this must be considered when **collecting** the information to be used in the synthesizing process. Compliance with data protection laws must be ensured when selecting or obtaining the information to be synthesized by the algorithm. In particular, it's necessary to ensure that **individuals** are adequately **informed** about the **purpose** of processing their data, that they have the chance to maintain **control** over its use, and that such use is based on an appropriate **legal basis**.

The above is particularly important considering that, according to **Article 2-decies** of the Italian Privacy Code (Legislative Decree No. 196/2003 as subsequently amended), personal data processed in breach of the personal data protection laws cannot be used.

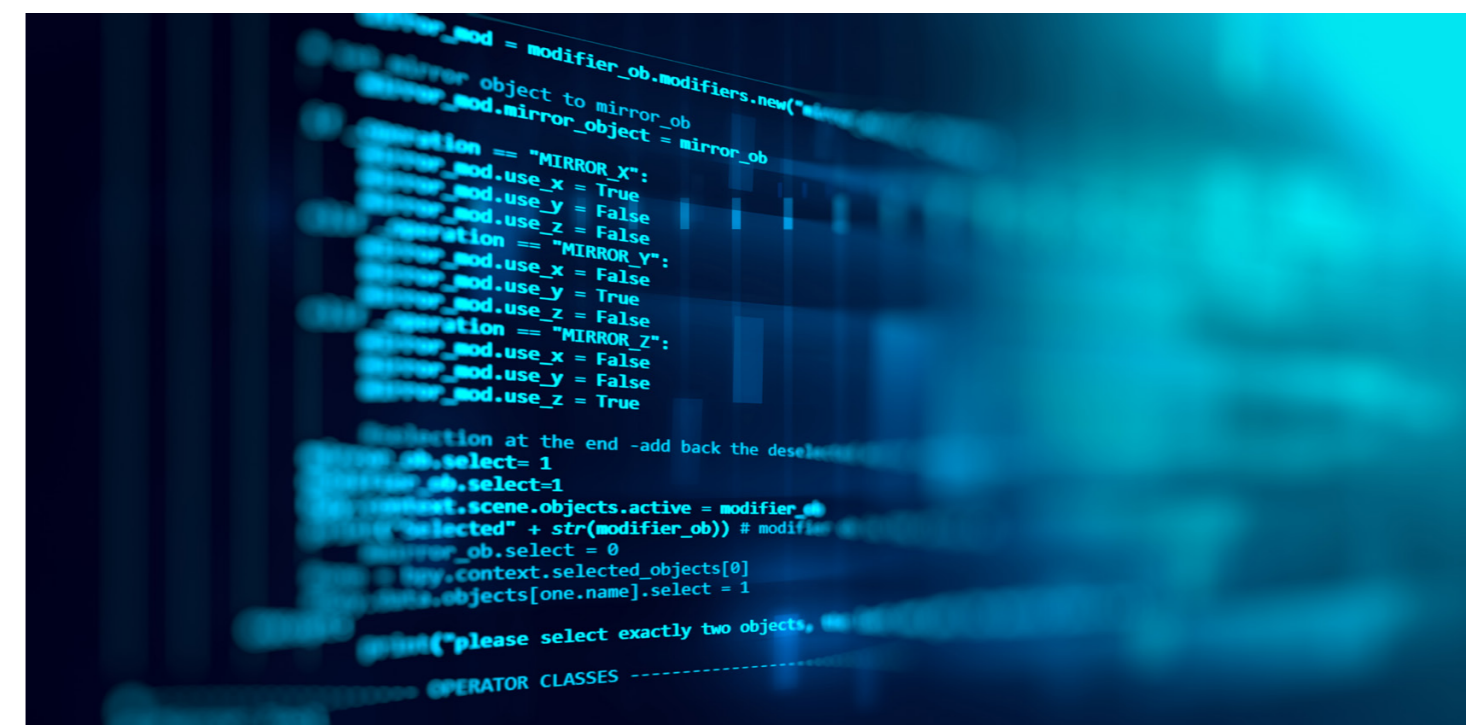
Furthermore, appropriate criteria should be defined to verify that the synthesizing algorithm is not biased by **deficits** in reprocessing the original dataset, such that the **identity** of the data subjects can be traced.

Measures must be taken to prevent the possibility of tracing back to the original dataset. According to EDPS, a “**privacy assurance assessment**” should be conducted to assess how data subjects could be re-**identified** and what information would be revealed about them in such a case.

By contrast, appropriate cautions should be taken to ensure **the transparent use** of synthetic data, avoiding the risk of potentially harmful distortions (eg identity theft or the “deep fake” technique allows the creation of synthetic multimedia content that can generate distorting effects on public opinion).

Lastly, it is necessary to avoid the **risk** of **discrimination** that could result from using synthetic data that is not adequately representative of the phenomena it addresses. The **quality** of **synthetic data** is closely related to the quality of the original information and the data generation model. Synthetic data may reflect **biases** present in the source dataset. This risk is exacerbated by the difficulty of verifying algorithm outputs, especially when dealing with particularly complex datasets.

The above reflections highlight how synthetic data – like many other innovations introduced by AI – can be a precious tool that could benefit society as a whole. However, its use must be controlled and carried out in compliance with applicable laws, particularly **data protection laws**. With this in mind, we hope that the **AI Act** will provide unambiguous answers and to ensure responsible use of the technology under discussion.



AI & Cybersecurity

Risks and opportunities of the diffusion of AI

by TOMMASO RICCI

Key issues

- ✓ The rapid advances in the field of AI entail its exponential application to all economic sectors, necessitating **caution** in assessing the risks and opportunities for cybersecurity.
- ✓ AI can pose **cyber risks** related to vulnerabilities, data manipulation, automation, and lack of transparency, which can compromise the security of corporate systems.
- ✓ AI in cybersecurity offers opportunities for improvement in **prevention, detection, and response**, by automating processes and enhancing defense capabilities.
- ✓ It's crucial for businesses to develop a robust **cybersecurity strategy** that takes into account the regulatory requirements applicable to the specific case.

The enthusiasm linked to AI tools experienced a rapid acceleration in the early months of 2023, owing to the launch of publically accessible solutions like ChatGPT and DALL-E 2. These solutions quickly went viral due to their ability to generate original textual or visual content that captivated public attention.

As businesses endeavor to enhance their own processes and products by integrating third-party AI solutions through the use of Application Programming Interfaces (APIs), or by developing their own, it's essential to navigate cautiously. The potential risks associated with the use of these technologies need to be thoroughly assessed, as do the opportunities arising from the application of AI in reinforcing cybersecurity.

AI cyber risks

AI developments have led to significant progress in various fields, but they have also introduced new cyber risks. The **"dual" nature of AI** allows for both harmless and harmful applications, peaceful and military, making it essential to pay attention to the risks associated with the use of these technologies.

Firstly, **AI systems have known vulnerabilities**, such as the potential for corruption or manipulation of input datasets. Such interference can result in distorted and unrepresentative results. Secondly, AI systems are generally designed to infer and perform actions in an automated fashion, without the need for consistent human involvement. This scenario lowers the capacity to identify potential vulnerabilities that could be exploited by unscrupulous competitors or cybercriminals to compromise business systems.

In addition, **the decision-making process of machine learning or AI programs isn't always immediately**

apparent to those tasked with their supervision. Both decision-making models and the underlying data may not be transparent or easily interpretable, although efforts are being made to enhance the transparency of these tools. This situation can complicate the tracing of a breach's cause or purpose, even when a breach is detected.

It's worth noting that as of recent data, **83% of web traffic is now API traffic**, suggesting a significant area of potential vulnerability if not properly secured.

Moreover, there are risks associated with the misuse of technology itself. With the advent of large language models, attackers now find it easier to create highly sophisticated and convincing phishing emails, capable of deceiving even the most tech-savvy users.

AI opportunities in cybersecurity

However, from another perspective, organizations can rely on AI's capabilities both to update their practices in terms of cybersecurity and to protect their AI-equipped systems. AI enhances the ability to detect and respond to existing threats, and allows for the development of new preventative defense capabilities. Thanks to the use of AI, for example, companies can streamline and improve the operational model of security by reducing lengthy and complex manual inspection and intervention processes, and redirect human efforts towards oversight and problem-solving tasks. Specifically, AI can enhance current systems and practices of cybersecurity in three main directions:

1. Prevention and Protection: AI provides a way to automate the threat detection process - enhancing, rather than replacing - the human analyst through machine learning and deep learning techniques. Many of AI's applications for threat detection and prevention

use a version of machine learning called "unsupervised learning," where collected data sets are used to find patterns, which are in turn used to detect anomalies, such as unusual file movements or changes.

- 2. Detection:** AI allows a transition from static detection methods (Signature Based Intrusion Detection System) that detect cybersecurity breaches through system analysis in search of characteristic signs of computer breaches, to more dynamic and continuously improving methods. AI algorithms can detect any change that appears abnormal, without needing a predefined definition of what is abnormal. In this way, AI represents a powerful tool for threat qualification and investigation, proving particularly useful for monitoring high-risk investigations, such as those in the high finance sector. AI can recognize significant changes in user behaviors that may pose a security risk.
- 3. Response:** Thanks to AI, it's possible to reduce the workload for cybersecurity analysts. For instance, by intelligently automating ordinary repetitive manual activities, such as searching for signs of compromise within log files, human resources can focus on higher-value activities and prioritize risk areas. Furthermore, response systems equipped with AI can proactively intervene and dynamically segregate networks to isolate valuable information in secure places or redirect attackers away from vulnerabilities or important data.

For instance, in March a renowned technology company announced the launch of **Security Copilot**, an AI system that simplifies and enhances the capabilities of security experts by summarizing and rationalizing threat information, and helping to identify harmful activities amid the noise of web traffic. The software supports security teams by providing important details, correlating and summarizing attack data, prioritizing incidents, and suggesting the best course of action.

Designing and applying AI in cybersecurity

According to a recent report published by a cybersecurity solutions provider, there are **1,287 password attacks per second** while according to ENISA's [Threat Landscape report 2022](#) the¹ proliferation of bots that create virtual characters can easily compromise the process of creating regulations, as well as interaction between communities, flooding government agencies with false content and comments.

In such a hostile environment, **it's critical for businesses of all sizes to develop a cybersecurity strategy** with solid foundations that take into account the specific requirements depending on the operational sector. For instance, the Italian Legislative Decree no. 65/2018 implementing the NIS Directive 1 requires companies within its scope to adopt appropriate and proportionate technical and organizational measures for managing cyber risks, and to prevent and minimize the impact of any security incidents suffered.

Designing effective corporate security solutions involves the development of governance, management, and IT security legal compliance processes based on a structured and systematic acquisition and analysis of information both on applicable regulatory requirements and on possible cyber threats. This is to guide, design, verify, and monitor the appropriate countermeasures. Cyber Threat Intelligence activities must also continue throughout the life cycle of corporate information systems, as they are essential drivers for their correct evolution and an enabling factor for the implementation of effective defense and prevention measures.

1. The ENISA Threat Landscape (ETL) report is the annual report of the European Union Agency for Cybersecurity, ENISA, on the state of the cybersecurity threat landscape.

AI & Outsourcing

AI and outsourcing agreements

by ALESSANDRO FERRARI and FILIPPO GRONDONA

Key issues

- ✓ **Outsourcing** AI solutions presents both **opportunities** and specific **risks** that need to be addressed in the outsourcing agreement.
- ✓ AI outsourcing agreements should clearly define the **purposes** and **methods** by which providers can access and use client **data** to ensure **confidentiality, security, and integrity**.
- ✓ The **liability regime** plays a crucial role in AI outsourcing agreements, especially in the **absence** of specific regulations.
- ✓ It's important to carefully regulate **information security** and **incident management** in AI outsourcing agreements to foster **cooperation** between the parties.
- ✓ AI outsourcing agreements should consider the regulatory landscape and comply with relevant **sector regulations**.

AI has made a significant impact globally, highlighted by the groundbreaking launch of ChatGPT, which captured widespread public attention. AI-based solutions have become prevalent across various sectors, revolutionizing industries such as finance, transportation and healthcare. With an abundance of data now at their fingertips, companies are capitalizing on AI to automate processes, reduce repetitive tasks, facilitate decision-making, and gain a competitive edge on the market. The advantages of implementing AI technologies are evident, driving **process** optimization and **cost** reduction.

However, developing and implementing AI solutions is no easy feat. It demands specialized expertise, substantial infrastructure investments, and continuous updates and maintenance. Consequently, many companies are turning to **outsourcing** as a strategic solution for AI development and implementation.

Outsourcing offers a multitude of **opportunities**, enabling businesses to tap into the technical skills of expert suppliers, ensuring top-notch maintenance, support, and upgrades throughout the agreement. It also enables tailoring AI solutions to specific business needs while keeping a watchful eye on cost control.

Nevertheless, as the realm of AI expands, so do the legal considerations. When drafting AI outsourcing agreements, companies must address crucial **legal risks**, particularly when internal functions and processes are outsourced.

Data management in outsourcing agreements

One of these concerns revolves around the use of data by the supplier for the AI solution development and enhancement. AI technologies, particularly machine learning, rely heavily on data to generate valuable insights. Therefore, it's crucial to establish clear definitions within the AI outsourcing agreement regarding the supplier's **access** to and use of the client's data, including the purposes of solution development and improvement. In cases involving confidential information, the client should establish boundaries and require measures such as segregated environments to maintain confidentiality.

Moreover, the supplier must commit to adopting robust **security measures** to guarantee the integrity, security, and confidentiality of the customer's data and information, especially when using cloud-based AI solutions.

If **personal data** is processed as part of the AI outsourcing agreement, the parties should align their processing activities to the General Data Protection Regulation No. 679/2016 (GDPR). For instance, when transferring data outside the EU/EEA, the parties must verify the existence of **appropriate safeguards**, such as an adequacy decision by the European Commission or the execution of Standard Contract Clauses (SCCs), before any transfers occur.

Establishing AI liability framework

The issue of **liability** takes center stage in AI outsourcing negotiations. When discussing AI-based technologies, liability discussions become multifaceted. As with any contractual negotiation, the liability regime underscores the conflicting interests of the parties involved. The supplier will seek to limit liability, particularly when it arises from events beyond its control, such as the use of customer data and information.

However, liability takes on a new dimension in the **realm of AI**. It is widely recognized that AI-generated outputs, even in the case of weak AI (ie algorithms lacking self-determination and the ability to comprehend processed information), can have significant real-world consequences. This raises questions of accountability for damages. In the absence of specific legislation, experts have proposed various hypotheses regarding AI-generated liability, assigning it alternately to the manufacturer, developers, or the owner/user of the AI solution. Clearly allocating liability in the outsourcing contract is vital to provide legal certainty between the parties.

Incident management

Another critical topic in AI outsourcing agreements revolves around incident management, especially when the solution is based on cloud infrastructure. **System failures** or **data loss**, whether accidental or intentional (eg cyberattacks), can have far-reaching effects, impacting not only the affected systems but also the services provided to the end customers.

It's important to note that **data breaches** also fall under the scope of the GDPR, which sets out specific communication obligations for data controllers vis-à-vis the relevant authorities and data subjects. If system failures or data loss affect an operator of essential services or a company within the **national cybersecurity framework**, the communication obligations outlined in personal data processing regulations may come up beside the additional obligations set forth in Legislative Decree No. 65/2018, which implemented the EU Directive 2016/1148 (NIS Directive), and Decree-Law No. 105/2019, enacted into law as Law No. 133/2019, which introduced the national cybersecurity framework.

Close partnership between the provider and the user of the AI solution is essential for ensuring compliance with such regulations. Therefore, the AI outsourcing agreement should include clear obligations of **cooperation** and **assistance** in the event of incidents that disrupt the AI solution or lead to data loss, while still allowing the customer to seek recourse against the supplier if the incident is the result of inadequate security measures.

Compliance with sector regulations

Compliance with **industry sector regulations** is crucial and should not be overlooked. European and national authorities have taken significant steps in recent years to regulate outsourcing in critical sectors such as **banking** and **insurance**. The European Banking Authority (**EBA**) and the European Insurance and Pension Authority (**EIOPA**) adopted guidelines on outsourcing which require to explicitly address

specific topics in outsourcing agreements. One such relevant topic concerns the sub-outsourcing of critical and important functions by banking and insurance companies, which is permitted only under strict conditions, along with the information and audit rights of supervisory authorities.

The Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA) has recently come into effect. This new regulation mandates that contracts between financial entities, including insurance and reinsurance companies, and IT service providers, regardless of whether they qualify as outsourcing, must envisage certain provisions. For example, suppliers should commit to post-termination obligations to improve the parties' ability to manage IT risks in the financial sector.

Furthermore, financial entities are now required to conduct periodic testing, including threat-led penetration testing, to assess incident management preparedness, identify vulnerabilities and deficiencies in digital operational resilience, and promptly implement necessary corrective measures. Fulfilling these regulatory obligations requires the introduction of **ad hoc provisions** within the outsourcing agreements to ensure effective cooperation with technology service providers.

Liability for damages caused by AI

by MARCO DIMOLA and GIACOMO LUSARDI

Key issues

- ✓ The **current legal framework** may not be adequate to regulate liability for damages caused by AI-based products and services.
- ✓ The European Commission has submitted a proposal for a **directive** to harmonize Member States' laws on **tortious liability** for damages caused by AI systems.
- ✓ The **AI Act** focuses mainly on **monitoring** and **preventing damages**, while the AI Directive focuses on the applicable tort liability if damage occurs.

The unstoppable **development** of digital technologies and the **exponential spread** of AI systems pose delicate issues in the area of **civil liability**, for two main reasons.

First, because the Italian general civil liability rules date back to the **1942 Civil Code**, and, second, because the applicable rule may depend on multiple **factors**: status of the injured party, type of product/service in which the AI system is incorporated, type of damage caused.

The potential uncertainties in the event of litigation have prompted the EU to intervene with **legislative proposals** which are still under discussion. Before analyzing the proposals, we will give an overview of the **protection and remedies** that the current system makes available to persons harmed by an AI system.

The current legal framework, between contractual and tortious liability

In the AI environment, **damages** are often the consequence of the **breach** of a certain obligation between the damaging party and the **injured party**. In such a case, the latter will be entitled to exercise the **remedies** available per the specific **contract** in place, which will mostly be a contract of sale or services, an employment contract, a contract in the insurance or banking sector, or a contract for financial intermediation. Where there is no contractual relationship, the injured party may invoke **tortious liability**.

If AI systems can be traced back to products, any **defects** will fall under the **product liability rules** set forth in Directive 85/374/EC, now transposed in Italy into the Consumer Code. However, this protection is mostly **addressed to consumers** and only allows for the compensation for damage for **death, personal injury, and destruction or deterioration** of goods other than the defective product.

Other legal provisions that may be invoked in Italy in case of damages caused by AI systems are Article **2050** of the Italian Civil Code (performance dangerous activities), Article **2051** of the Italian Civil Code (damages caused by things in custody), Article **2054** of the Civil Code (circulation of vehicles), and Article **2043** of the Civil Code (general tort liability).

The proposed Directive on AI and tortious liability

To **avoid fragmentation** resulting from inconsistent legislative measures across Member States and to **reduce legal uncertainty** for businesses developing or using AI in the internal market, the European Commission announced on September 28, 2022, the adoption of **two proposals** aimed at adapting tort rules to the digital age, the circular economy, and the impact of global value chains.

One of the two proposals aims to **revise** the existing **product liability law**. The other consists of a new directive on liability for Artificial Intelligence (**AI Directive**), which is aimed at **facilitating compensation** for damage for those who have suffered damages resulting from the use of AI systems.

In the Commission's view, **existing national liability laws**, particularly for **fault**, are **not suitable** for regulating liability actions for damages caused by AI-based products and services. The main limitations of these regulations could be inherent in the characteristics of AI, including its **complexity, autonomy and opacity** (the "black box" effect), which could make it **difficult** or **unduly burdensome** for the injured parties to identify the responsible subjects and prove to have met the requirements of tortious liability. In addition, the AI supply chain involves several **players**, making the attribution of liability even more complex.

The AI Directive is part of a coordinated **European approach** to address the rise of AI and digital technologies: the **AI Act** proposed by the Commission in April 2021, focuses primarily on **monitoring** and **preventing** damages, while the AI Directive aims at **harmonizing** the liability regime where AI systems cause damage. In summary, the AI Directive aims to ease the injured party's **burden of proof** through two main tools: **rebuttable presumption** and **disclosure of evidence**.

Rebuttable presumption is intended to make it easier for injured parties to **prove** the **causal link** between the fault of the defendant-injurer and the output produced by the AI system, or the failure of the AI system to produce the output that gave rise to the damage. The AI Directive does not, therefore, go so far as to provide for a **shift of the burden of proof** on the defendant (e.g. suppliers or manufacturers of the AI system), as this is considered too burdensome (and may in fact stifle innovation and adoption of AI-based products and services).

In addition to the rebuttable presumption, with respect to **high-risk** AI systems, the AI Directive gives national courts the power to order the **disclosure** of evidence by the provider or another person bound by its obligations where the provider refused to comply with the same request made by the injured party-claimant (or any other person entitled to do so). In addition, the claimant may request the **preservation** of the evidence.

The AI Directive: Next steps

Five years after the AI Directive was transposed in the Member States, the Commission will submit a **report** to Parliament, the Council, and the Economic and Social Committee, in which it will assess the achievement of its intended **objectives**.

In the same context, the Commission will also consider whether it is appropriate to provide for a **strict liability regime** for damages caused by specific AI systems and for **compulsory insurance coverage**.

Sector-based AI

AI and Food & Beverage

Applications of AI in crucial sectors of the agri-food industry

AI & Fintech

AI in the financial sector: Risks, regulatory obligations, and investor privacy protection

AI & Gambling

The use of AI in the regulated gambling sector

AI & Life Sciences

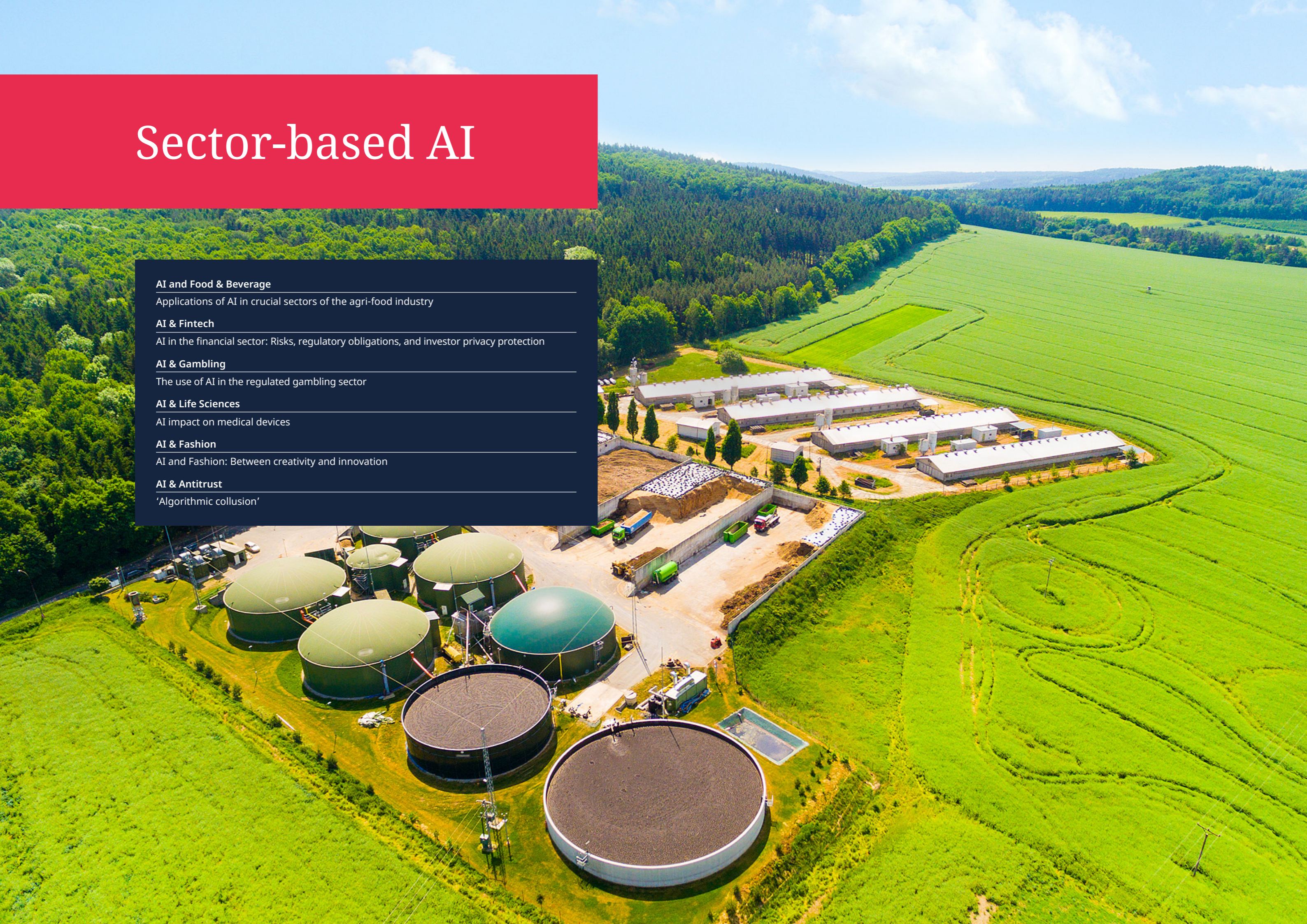
AI impact on medical devices

AI & Fashion

AI and Fashion: Between creativity and innovation

AI & Antitrust

'Algorithmic collusion'



AI and Food & Beverage

Applications of AI in crucial sectors of the agri-food industry

by FEDERICO MARIA DI VIZIO

Key issues

- ☑ In the agri-food sector, one of the main advantages of AI is its ability to **optimize production processes**, improving the quality and safety of products while reducing waste.
- ☑ In the **logistics** field, AI enables the streamlining of delivery routes, reducing transit times and costs, as well as monitoring food transportation.
- ☑ AI applications that allow for the analysis of **large amounts of data** not only enable the prediction of consumer trends and the personalization of marketing strategies but also facilitate the discovery of new ingredients and the refinement of existing production systems.

AI is revolutionizing the **agri-food sector**. Thanks to its ability to process and analyze large amounts of **data**, AI can be used to improve product **quality**, reduce **waste**, increase **efficiency**, and enhance the customer **experience** when interacting with companies. In light of this, there are multiple applications of AI that can be of interest to Food and Beverage companies, such as its impact on production processes, logistics, data analysis, research and development, food safety, marketing, and advertising.

Optimization of production processes

One of the main advantages of using AI in the food industry is the ability to optimize **production processes**, improving product quality and reducing waste. AI can be used, for example, to predict the **demand** and **consumption** of certain agricultural products, ensuring greater production efficiency and reducing environmental impacts.

Furthermore, companies can use AI to monitor **food production** and processing, identifying any **issues** or **errors** in the processing process and reducing **risks** **crop** issues much faster and more efficiently than humans alone, analyze **soil** conditions, and enable operators to reduce the spread of **plant** diseases, for example. AI can also monitor the health status of **livestock**, quickly identifying potential unusual animal behaviors.

Evolution of logistics

Another sector in which AI represents a significant factor for growth and evolution is **logistics**, which has become a central theme for all economic operators in recent years, from international giants to smaller

entities. By using AI, **delivery routes** can be planned and optimized, transit **times** and transportation **costs** can be reduced, and the transportation of both plant-based and animal-based food can be monitored. This can reduce waste and ensure timely product delivery.

Data analysis for marketing purposes and new product development

Data analysis is another area where AI can make a difference. AI enables the analysis of **vast amounts of data** from multiple sources, such as sensors, monitoring systems, and customer feedback, to identify **trends** and patterns and obtain useful information for making informed decisions on **marketing strategies**, **demand** forecasting, and product development. For example, companies can use AI to analyze customer **taste** data and suggest related or personalized products to meet their needs. This can help companies improve their product offerings and better satisfy customer needs.

Furthermore, AI can be used to discover new **ingredients**, refine existing **recipes** or **production systems**, and develop new products based on consumer **preferences**. AI can also be employed for **advertising** and communication initiatives with **consumers**, as the technology enables the analysis of customer tastes and preferences, allowing for personalized and targeted advertising campaigns.

Customer-company relationship: Personalized services, planning, and investments

AI has many "internal" applications for Food and Beverage companies, including those mentioned above. However, the importance it could have in customer-company relationships should not be underestimated.

The use of **chatbots** and other conversational interfaces, which are essentially AI applications, allows for **personalized customer service** and improves the overall consumer-producer experience.

However, the adoption of AI in the agri-food sector, like many other economic sectors, requires adequate **planning and investment**, as well as advanced training and knowledge of AI systems. Therefore, it is advisable that companies, before embarking on the digitalization of some or all of the mentioned activities, and during the implementation of AI solutions, are supported by **technical** and **legal experts** in the Food and Beverage and digital sectors. This will help identify any production or legal challenges associated with the AI revolution.

The role of **legal professionals** is increasingly in demand in this field, as they play a key role in ensuring that companies can use AI **ethically** and **to their advantage**, in compliance with applicable regulations. Additionally, seeking assistance from such professionals can enable companies to safely **negotiate** contracts with AI technology providers, such as software and robotics, and ensure that such contracts align with the real interests of the business.



AI & Fintech

AI in the financial sector: Risks, regulatory obligations, and investor privacy protection

by EMANUELE GAMBULA

Key issues

- ✓ AI is a resource that can improve the efficiency concerning the operations related to portfolio management and the optimization of financial return predictions.
- ✓ Despite its ability to bring various benefits, AI is also a source of numerous risks, such as cyber-attacks and possible discrimination on credit access systems used by financial institutions.
- ✓ The regulatory obligations arising from the AI Act imply the pursuit of the principle of transparency. This principle may overlap the information obligations already provided by the applicable privacy laws.

With fast technological advancements, AI has emerged as an indispensable tool, particularly in **the financial sector**. AI possesses the remarkable capability to analyze vast **volumes of data**, including Big Data and Alternative Data, unveiling patterns and models that would be virtually impossible for humans to discern. Such unrivaled potential makes AI an invaluable resource in **financial markets and portfolio management**.

AI in the financial sector: Benefits and risks

According to the Chartered Financial Analyst (CFA), the **AI technologies** most commonly used in the financial sector include Natural Language Processing (NLP) techniques, artificial neural networks, decision trees, random forests, and many others. All these technologies have in common the use of **Machine Learning**, which allows computers to learn without being explicitly programmed for a specific task. In particular, large amounts of **historical data** are analyzed and patterns are identified, which are then fed to AI. This enables AI to make increasingly accurate **predictions** based on an initial dataset.

When evaluating the implementation of AI in financial markets, it's feasible to **train** the software using historical and prospective data, enabling optimized **predictions such as stock returns**. The European Securities and Markets Authority (ESMA), in its report on AI and the securities market, emphasizes the versatile application of AI across various stages of **trading** financial instruments. Hedge funds, for instance, have developed Machine Learning models that effectively divide and execute orders across multiple venues and trading hours, aiming to minimize market impact on brokers and transaction costs, as highlighted in recent findings.

To the potential benefits arising from AI, numerous **risks** are added, some of which relate to the **quality** of the data on which AI is trained. If AI were trained on low-quality data affected by statistical distortions, it would result in indirect **discrimination** of investors in accessing the market. Specifically, this risk could arise in **credit access systems** where characteristics of individual individuals are penalized. Furthermore, risks can stem from **cyber-attacks** aimed at compromising the quality of data analyzed by AI through "**data poisoning**." Finally, another issue related to the risks associated with the use of AI, especially in the financial domain, is the **concentration** of AI in the hands of a few providers. This could lead to distorting effects on **competition** in unregulated markets where requirements are less stringent than those provided by the applicable legislation for traditional intermediaries.

Regulatory obligations and safeguards of investors' privacy

With reference to the European regulatory proposal, AI tools used in the financial sector would fall within the definition of the "high-risk systems." From a legal standpoint, AI systems used for **creditworthiness assessment** would potentially entail **joint liability** with the developers of the AI. The developers would have the task of monitoring their activity, including the selection and analysis of data acquired by the AI, as well as the **retention of log data** provided the applicable legislation of financial services.

Furthermore, AI offers the possibility to meet the **suitability and appropriateness assessment** outlined by the Article 25(2) of Directive 2014/65/EU (MiFID II) by analyzing significantly larger datasets compared to



traditional methods. The **know your customer rule** involves not only additional information beyond what investors provide during profiling, which may still be influenced by cognitive and behavioral limitations, but also **cross-references** with data provided by autonomous third parties providers. This approach enables the delivery of more tailored customer service with the goal of ensuring **consistency** in an investor's behavior over time.

The activity described above encompasses the processing of a substantial amount of **personal data** belonging to the investor. Such processing would be deemed lawful as it is necessary for the execution of **the contractual agreement** between the investor and brokers. Moreover, the investor's objection to automated processing, as outlined in Article 22 of the GDPR, could potentially **be exempted** if the AI-driven profiling of the investor is "*is necessary for entering into, or performance of, a contract between the data subject and a data controller.*"

Regardless, in compliance with the provisions of Article 22 of the GDPR, taking into account the **informational obligations** stated in Article 13, the data controller must also furnish meaningful information about the underlying logic of the AI. The latter aligns with

the principles advocated by the recent European regulatory proposal on AI, particularly in terms of **transparency**. **Extensive informational obligations** would be imposed on the AI producer, and a portion of this information would understandably have to be made accessible to the data subject as well. However, uncertainties may arise regarding whether clear and comprehensible **information** for the data subject necessitates a technical and detailed explanation of the AI's "**logic**." Therefore, the information provided to the data subject should not unnecessarily be excessively technical, as it may undermine comprehension for users who lack adequate technical knowledge. In other words, striking a balance between transparency and **clarity of technical information** is crucial.

AI & Gambling

The use of AI in the regulated gambling sector

by VINCENZO GIUFFRÈ

Key issues

- ✓ Given the countless and diverse factors to consider in the **odds determination process**, AI enables the analysis of a vast amount of **data** to establish accurate probabilities for event outcomes.
- ✓ By monitoring player behavior, identifying anomalous gameplay patterns, analyzing financial transaction data, personalizing gaming offers, and providing support and information, AI can help prevent **gambling problems** and **promote responsible gaming**.
- ✓ In recent years, the gaming sector has experienced an increase in **fraudulent activities**, which has led to the need for AI to detect fraud.

Betting is an activity that involves the prediction of an **uncertain future event**, and the money you bet is based on the probability that you think that event will or will not happen. The area of regulated gambling is an ideal testing ground for AI. AI works by collecting data, which allows to analyze **statistics** and **events** to continuously improve its accuracy.

The gaming industry relies heavily on the exploitation of **historical data** to anticipate future outcomes and behavior. It's therefore a fundamental skill and necessary for game design, odds setting, risk management, customer profiling, optimization of bonus programmes and fraud detection.

The correct identification of the probability of the occurrence of an event

Following the increasing national **regulation**, at European and non-European levels of the gambling sector, analysts working in this sector and who define the probability of the occurrence of an event – from which it is then possible to set the odds to be offered on the market - need to equip themselves with tools that allow the analysis of a large amount of data.

In this regard, reference is not exclusively to the classic cases of probability that a team win a certain competition or event. But, for instance, in the context of real-time betting, it could prove particularly useful to calculate the **speed** and **trajectories** of the players on the field to predict in real time and in advance the occurrence of a goal, so as to correctly update the live odds during an event.

The most innovative data analyzed by the sports betting industry includes the fitness and past performance of a player, the **weather conditions** before a given event,

the **environmental factors** of the venue and the event and the growth prospects of a club.

This data-driven approach allows bookmakers to identify **trends** and **game statistics** of the game that can be used to establish the **odds** of each possible outcome and, therefore, the odds that will be offered to customers.

This allows bookmakers to establish the most accurate odds and to offer more competitive odds to their customers.

Responsible gaming and the identification of fraud

Just as AI facilitates the creation of new products for gambling, it can act as a safeguard to counteract the negative effects of the industry. In the context of responsible gaming legislation, there are rather traditional practices to prevent the risks of players. They are in fact based on the gaming behavior of **players** who have **cancelled** and **self-excluded**. AI can play an important role in the interaction with customers, in particular in maximizing the **experience** of the players in areas such as customer service, which is very useful in detecting, but especially preventing, problem gambling.

The rationale behind this is that new technologies go a step further in tracking and assessing each customer, accumulating a large amount of behavioral data. Through AI trained with the behavioral data of known problem gamblers, companies can automatically identify and indicate a customer with a risk of problem gambling, even if still at an early stage, so it can monitor patterns and intervene promptly stopping their operations before the gaming activity becomes problematic. Players who receive **personalized feedback** on their gaming **behavior** measured in

terms of time spent and money spent, are more likely to modify their gaming behavior, compared to those who do not receive personalized feedback and who individually decide to self-suspend or limit themselves.

In a different respect, AI can use machine learning techniques to analyze **historical data** for betting histories, odds information, and players' gaming patterns to categorize anomalous abnormal betting patterns and irregularities that could indicate the presence of **fraud**. For instance, AI may be able to detect a betting pattern that seems irrational or suspicious, such as a large number of bets on an unlikely outcome or a large volume of bets on a match in an unknown league.

The use of AI to detect fraud in betting can also improve the reputation of the sports betting industry. When players know that the industry uses advanced technologies to prevent fraud, they are more likely to bet safely and confidently.

Therefore, the real revolution in the world of betting involves using predictive AI tools to promote **responsible gaming**, limit fraud, prevent **money-laundering** phenomena and **match-fixing** cases. While such tools have already been in use for bookmakers for a couple of years to identify odds and develop new products and services, it will be up to national regulatory authorities to work in concert with operators to ensure the lawfulness and supervision of betting events.



AI & Life sciences

AI impact on medical devices

by NICOLA LANDOLFI and CARLOTTA BUSANI

Key issues

- ✓ In recent years, **medical devices** incorporating **AI-based software** have exponentially increased to enhance diagnosis and treatment effectiveness, reduce human error, and improve access to care.
- ✓ AI has found numerous **applications** in healthcare, not only in diagnosis and surgery but also in everyday patient care and treatment recommendation.
- ✓ With the introduction of the **AI Act**, medical devices could be subject to a **dual regulatory regime** with heightened **regulatory obligations**.

AI is revolutionizing the **Life Sciences** sector by offering technological solutions that can significantly affect new **product** development, **patient care**, and the **efficiency** and **sustainability** of national healthcare systems.

The qualification of AI-based software as medical devices

From a regulatory standpoint, products containing AI-based software can be classified as **medical devices** depending on the specific **intended use** identified by the manufacturer. Generally, only software with a **medical purpose** — such as diagnosis, monitoring, or disease prevention — qualifies as a medical device. Conversely, software with a “generic” and non-medical diagnostic intended use does not fall under this category, even if intended for use in a healthcare context.

For instance, software that collects, archives, stores, or transmits data acquired through specific **electromedical equipment** creates a database that can be accessed when providing healthcare services. However, since it lacks a specific medical purpose, it typically does not qualify as a medical device. The classification of software as a medical device is essential as it entails applying **specific requirements** to ensure the **health and safety** of patients and users.

Undoubtedly, the medical device sector has witnessed a substantial increase in the use of AI software in recent years. These systems and solutions improve **diagnostic** accuracy, reduce human **error** by identifying pathologies more precisely, and provide therapeutic options that enhance the chances of recovery, positively affecting treatment effectiveness. The improved efficiency of available tools leads to shorter access times and treatment durations, benefiting patients and healthcare systems.

Examples of medical devices using AI

Numerous examples of medical devices use AI, ranging from software that helps doctors in disease **diagnosis** to those suggesting personalized **treatment options** based on specific patient data, such as genetic profiles. AI has also found applications in **radiology**, where various software currently available on the market analyze image data and detect anomalies. Additionally, AI increasingly helps **surgeons** in performing delicate **operations** through sophisticated devices.

However, medical devices using AI need not necessarily be complex products accessible only to healthcare professionals. On the contrary, several solutions have been specifically designed to be available to **patients** for the **daily management** and **monitoring** of various conditions. A notable example includes products for patients with **diabetes** that continuously monitor blood sugar levels and automatically adjust insulin administration.

The impact of the AI Act on medical devices

While AI software for medical purposes is currently considered a medical device from a regulatory perspective, it's essential to consider a potential **regulatory innovation** that could affect the entire sector. The EU is discussing the proposed **AI Act**, which may significantly affect medical devices incorporating AI software. According to the provisions outlined in the proposal, these products could be subject to a **dual regulatory regime** encompassing both medical devices and AI-containing products, resulting in increased regulatory obligations for all stakeholders in the supply chain.



In conclusion, AI in medical devices already requires adherence to specific **requirements** to ensure patient **health and safety**. In the coming years, forthcoming regulations might intensify the number of applicable regulatory obligations. This topic is under intense debate in the industry, with many voices emphasizing the importance of avoiding the **proliferation of obligations** for stakeholders in the supply chain. Despite a rapidly evolving regulatory framework that leaves some room for interpretation, the use of AI systems undoubtedly presents significant opportunities to improve **patient** health and enhance the **efficiency** of healthcare systems. Therefore, developments in technological innovation and the regulatory framework in the Life Sciences sector are eagerly awaited.

AI & Fashion

AI and Fashion: Between creativity and innovation

by VALENTINA MAZZA and DEBORAH PARACCHINI

Key issues

- ✓ Algorithmic works of art are eligible for **copyright protection** as long as **human choices** are involved.
- ✓ In the case of an entirely AI-designed collection, the **software developer** could enjoy **copyright protection** for the software and for the work created with it and be held **liable** in the event of infringement of third-party's IP rights.
- ✓ **Big data** enables fashion brands to profile customers and users through using predictive AI systems to create targeted marketing campaigns and offer personalized services. However, this processing has to comply with GDPR rules.
- ✓ In the fashion sector, AI can come to life through **virtual influencers** (ie digitally created robots resembling humans capable of interacting with real people). But using virtual influencers does not exempt fashion brands from **transparency obligations**.

Recently, **retail** giants have embraced an algorithmic approach to fashion. From **apps** that provide feedback or advice on outfits to interactive **fitting rooms** with mirrors that recognize the clothes you are wearing and suggest other matching options based on style, color and mood, AI seems to be the latest trend in the **fashion industry**.

The creation of AI-based fashion items takes the relationship between **innovation** and **creativity** to a new level and raises a series of questions, some of which are still unanswered. Who is the **owner** of the creations made by AI? Can AI infringe upon the intellectual property **rights** of others? What kind of personal **data** is collected by AI? Is the resulting data **processing** subject to data protection regulations? Will AI enhance or diminish creativity in the fashion industry?

Copyright protection for works created by AI

Under Italian law, **creative works** must be **original** to obtain copyright protection, and traditionally the requirement of originality has been linked to the **natural person** of the author. In fact, according to **Article 6** of Law No. 633/1941 (Copyright Law), "the original legitimacy for the acquisition of copyright consists in the creation of the work, as a particular expression of the intellectual work" of the author. Therefore, machines and AI seem to be excluded from the notion of authorship.

This position was reiterated in a very recent decision by the **US Copyright Office**, which denied **registration** of AI-generated **images** on the grounds that they were

considered unprotectable under US copyright law. The Office noted that registration of an original work is only possible if it was created by a **human being** since copyright law protects only "*the fruits of intellectual labor*" that are "*based on the creative powers of the mind*," and such discipline is limited to the protection of the author's "*original intellectual conceptions*."

In accordance with case-law (Feist Publ'ns, Inc. v. Rural Tel. Serv.; Burrow-Giles Lithographic Co. v. Sarony) and legislation (see 17 U.S.C. § 102(a) and (b)) on copyright law, the US Copyright Office held that copyright protection cannot be granted to works made by a machine or mechanical process that operates randomly or automatically without sufficient **creative input** or **intervention** by a human author.

Similar conclusions were also reached at the national level with a recent Italian Supreme Court ruling on the recognition of copyright protection on a digital work depicting a **flower**, created through the use of **software**, that was used in a past edition of the Sanremo Festival.

In 2016, RAI used a digital work depicting a flower found on the web as a set design for the famous song festival without seeking **permission** from the author, who had created it some time earlier through the use of software. For this reason, two years later, the author sued RAI before the Court of Genoa, claiming infringement of her copyright on the work.

Confirming the decision of the judges at first instance and on appeal, the Supreme Court dwelt on the legal concept

of **creativity**, holding that it does not coincide with that of creation, originality and absolute novelty. According to this interpretation, the creativity protected by Italian law is given by the personal and individual expression of an objective content belonging to the categories listed in **Article 1** of Copyright Law. Therefore, an intellectual work can be protected provided that a **creative act**, albeit minimal, susceptible of **manifestation** in the **outside world** can be found in it.

In the case at hand, the digital image used in the set design of the Sanremo Festival did not simply represent a **reproduction** of a flower, but was a true reworking, deserving of protection under copyright law, since it was an original and creative idea coming from its author. Therefore, the Supreme Court rejected RAI's defense that the author's process was limited to choosing an algorithm and approving the result generated by the software, pointing out that the use of software does not exclude the elaboration of an intellectual work protectable by copyright, but only requires scrutinizing its **rate of creativity** more rigorously.

Therefore, algorithmic works of art are eligible for copyright protection as long as **human choices** are involved. In the case of an entirely AI-designed **fashion collection**, the **person who developed the software** could enjoy copyright protection for both the software itself and the work created through its use, and presumably be held liable in the event of infringement of third parties' intellectual property rights.

AI in big data analysis

In such **data-driven** system, **fashion brands** are increasingly investing in **AI** to offer their customers innovative products and services. In fact, fashion houses are not only focusing on the use of algorithmic works that we have just analyzed, but they are also reinventing their websites and e-commerce channels by hiring **virtual sales assistants**, **e-concierges**, and **chatbots** capable of interacting with customers to help them choose and try out their favorite outfits, even from the comfort of their homes, while providing them with a new and exclusive shopping experience.

In this new reality, a crucial role is undoubtedly played by the **data** collected through **websites**, online **applications**, and **social networks**, which allow brands to understand which clothing items are trending and predict new trends. The fuel of the fashion industry can be found precisely in the use of **big data** and **predictive AI systems**. When AI is integrated into digital properties, brands can profile their customers and users to understand their interests and preferences, create targeted marketing campaigns, and provide personalized services based on their needs.

However, **targeting** users and customers of brands through big data analysis and the use of algorithms is considered processing of personal data. For this reason, fashion houses that decide to operate online and offer innovative services to their customers must comply with the requirements provided by data protection regulations, particularly with the obligations and responsibilities established by the GDPR.

For example, fashion brands must collect and process only the personal data that is strictly necessary for as long as it is needed, in compliance with the principle of **minimization** set out in **Article 5** of the GDPR.

Moreover, to lawfully collect and process personal data, brands have to identify the appropriate legal basis, which, in the case of optimized profiling using AI systems, must be obtained through the **consent** of the data subject. The GDPR also introduces specific information and transparency obligations: **Article 13** of the GDPR requires the data controller to provide information about the processing activities, its purposes and methods, the existence of automated decision-making (including profiling), the underlying logic, and the potential consequences for the data subjects. Lastly, the performance of a Data Protection Impact Assessment (**DPIA**) according to **Article 35** of the GDPR is also crucial, as this type of processing can be invasive and entail a high risk to the rights and freedoms of the data subjects.

Monitoring and **profiling** activities of online users through algorithms and other big data analysis tools can also be optimized by **combining** data collected directly from users with those inferred from their behavior (eg **custom audience matching** and **look-alike** activities), including through **cookies** and other tracking technologies. These mechanisms are not only used to monitor users on the web but also to **influence** their behavior and **choices**, particularly regarding consumers' purchasing decisions, sometimes undermining individual autonomy and freedom.

Brands must take specific **precautions** when intending to adopt user tracking mechanisms. The Italian Data Protection Authority (*Garante per la protezione dei dati personali*) has also intervened on this point. With its **Guidelines on cookies and other tracking tools** issued on June 10, 2021, it reiterated the circumstances in which the installation and use of cookies (or other tracking tools) can occur on users' devices and the rules for analyzing data collected through such technologies. In particular, to lawfully install cookies or other tracking technologies, brands operating online must: (i) inform users with a short privacy information notice (the **cookie banner**) that redirects to an extended privacy information notice (the **Cookie Policy**) outlining the purposes and methods of data processing through these technologies, and (ii) obtain a **specific consent**, which means a clear positive action from the user consciously consenting to the installation of cookies.

When AI becomes real, CGI is born

Thanks to the use of AI, brands can not only profile users and analyze large amounts of data, but they can also offer users renewed and innovative shopping experiences. In fact, AI enables the generation — and bringing to life — of different real-world personalities in the **virtual world**. These personalities are **digital robots** that simulate hyper-realistic human appearances, qualities, expressions, behaviors, and characteristics, going beyond common stereotypes. A brilliant example of this is virtual influencers, known as **CGI** (computer-generated imagery), who, in their virtual form, promote renowned brands, endorse their products and services, and act as ambassadors for principles and rights.

Virtual influencers are the latest trend on **social media**. Currently, social networks host over 200 virtual influencers, with the most followed ones including Nefele, the first Italian virtual influencer and advocate for inclusion and diversity values, the twins Eli and Sofi, Shudu, Lil Miquela, Noonnoori, Rozy, and the popular virtual streamer CodeMiko on Twitch. Many fashion brands are already turning to these CGI influencers for promoting their products. For instance, Rihanna chose Shudu to promote her cosmetics brand Fenty Beauty, while Prada, Chanel, and Fendi have been collaborating with the famous Lil Miquela for years.

This demonstrates that robots can also set new fashion trends. Sometimes, collaborating with **virtual influencers** rather than real people even brings **advantages** to fashion brands. In the real world, there is always an element of uncertainty due to human free will. In the virtual world, brands can exercise complete **control** over influencers, determining how they should present themselves to their followers both **aesthetically** and **communicatively**. This control helps minimize **reputational damages** resulting from behaviors or initiatives unrelated to brand endorsement.

Even though they are virtual, influencers still need to comply with the regulations of the real world. For this reason, **transparency obligations** in advertising also apply to these new forms of virtual life. Furthermore, it is necessary to **explicitly** disclose the non-real **identity** of these characters on the platforms through which they convey advertising messages. Users should be aware that they are interacting with an **avatar** and not a human. This idea stems from the belief that the development of **reliable** technologies, both ethically and morally, should serve as useful tools for society and be aligned with human needs.

Moreover, it's interesting to note how avatars and AI systems can be linked to forms of "**abuse**" of images, as in the case of **deep fakes**. This can result in more serious violations of personality rights, such as potential **damage** to **one's image, reputation, and digital identity**, non-consensual **dissemination** of private images, potential risks of phishing and vishing **attacks**, identity theft, and breaches of security measures based on biometric recognition.

In this context, it's essential that the systems used are **cyber resilient**, and the importance of adopting incident response schemes to remedy negative impacts on the business and protect the virtual influencer's and brand's reputation becomes apparent. This includes developing a post-attack **remediation plan** to mitigate potential claims for damages or other forms of liability.

It's evident that the development of these new technologies requires a **regulatory intervention** to prevent abuses. Meta, for example, has started working with its developers and experts on an **Ethical Framework** to establish clearer boundaries for the use of avatars and virtual influencers, considering both potential harms and benefits. Currently, Meta's primary aim is **transparency** and the importance of always providing the possibility to distinguish between what is real and what is not.



‘Algorithmic Collusion’

by ALESSANDRO BOSO CARETTA and MASSIMO D’ANDREA

Key issues

- ✓ Algorithms can facilitate **collusive behaviors** between competing undertakings and give rise to new forms of anticompetitive coordination.
- ✓ Four “**algorithmic collusion**” scenarios can be identified: (i) monitoring algorithms, (ii) parallel algorithms, (iii) signalling algorithms and (iv) self-learning algorithms.
- ✓ There is the risk that **self-learning algorithms**, programmed to determine an undertaking’s best pricing strategy, will autonomously **learn**, without any human intervention, that in certain market contexts, the most effective way to maximize profits is to **coordinate** business conducts with those of competitors.
- ✓ The widespread use of such algorithms could lead to a **collusive outcome** even if the undertaking using them doesn’t explicitly intend to collude.

One of the most interesting aspects in the relationship between AI and antitrust law is the risk that algorithms – and, in particular, **pricing algorithms**, increasingly used by undertakings to determine the best pricing strategy in real time – may facilitate **collusive behaviors** between competing undertakings and give rise to new forms of **anticompetitive coordination**.

Explicit collusion and tacit collusion

The term “**collusion**” refers to any form of **coordination** among competing undertakings with the objective of raising or maintaining **profits** above the level they would reach in a competitive scenario, i.e. in the absence of the collusive behavior.

It is common to distinguish in economic science between “**explicit collusion**” and “**tacit collusion**.” The former term refers to collusive behaviors that are the result of **agreements** or **concerted practices** between undertakings, ie the conscious and voluntary coordination. The second term refers to forms of coordination based on **parallelism** of behaviors by competing undertakings that, although conscious (**conscious parallelism**), is the result not of agreements but rather of **autonomous choices**.

In principle, antitrust law does not prohibit parallelism of behaviors between competing undertakings (**tacit collusion**), but prohibits anticompetitive agreements (**explicit collusion**), which are prohibited at EU level by Art. 101 TFEU and at national level by Art. 2 of Law No. 287/1990.

The risk of collusion generated or facilitated by the use of algorithms

The main risk from an antitrust point of view connected to the use of algorithms is that they are capable of facilitating **collusive behaviors** between competing undertakings or making new forms of **coordination** possible; in some cases, even in the absence of the prior programming of the algorithm to achieve the collusive outcome.

It is therefore usually made reference to “**algorithmic collusion**” and the economic and legal literature has identified four scenarios: (i) monitoring algorithms, (ii) parallel algorithms (iii) signalling algorithms and (iv) self-learning algorithms.

Four possible scenarios of algorithmic collusion

Monitoring algorithms

In this scenario, the case is that each undertaking participating to a price **cartel** can verify, through the use of an algorithm duly programmed to monitor the prices applied on the market, that the cartel has been **effectively implemented** by the other participants (ie verify that other undertakings participating to the cartel actually apply the **agreed price**) and detect possible deviations. In this case the algorithm would act as an instrument facilitating the **stability** of an anticompetitive cartel.

Parallel algorithms

It is noted in economics that one of the difficulties in implementing an anticompetitive cartel in highly dynamic markets is the fact that continuous and sudden changes of the market conditions require similar

frequent adjustments of the price agreed within a cartel and thus continuous **communications** between the cartel participants to agree on new **prices**. Such communications increase the risk that the cartel may be detected (and thus investigated) by the competent **authorities**. In this scenario it is deemed that undertakings may use pricing algorithms with the aim of determining **simultaneous** and **parallel reactions** to changes of the market conditions, reproducing a scenario of conscious parallelism of behaviors. In this context, competitive concerns may arise if undertakings agree to programme price algorithms not with the purpose of competing with each other, but to set their prices in a coordinated manner at a supra-competitive level.

Signalling algorithms

Competing undertakings can reach a common understanding to coordinate their conducts without explicit communications, by means of **unilateral signals** and **announcements** concerning the commercial terms they intend to apply and by aligning their conducts on the basis of such announcements. But undertakings might not observe the signals sent by competitors or voluntarily decide not to align their behavior with the competitors’ announcements.

In this scenario, it is deemed that appropriately programmed algorithms could favor an **automatic alignment** of the behavior of the undertakings with the announcements of competitors. Each undertaking could transmit in this way – through signalling algorithms – continuous **signals** concerning, for example, the **price** it intends to apply. When all undertakings concerned send the signal announcing the same price, each firm’s algorithms process the competitors’ signals and ensure that the firms apply the price of the message concerned. This corresponds to an **agreement** between the undertakings to apply that price.

Self-learning algorithms

Finally, it may be the case that using machine learning and deep learning technologies, a highly sophisticated algorithm can itself make **autonomous business decisions**, based on the analysis and processing of market data.

This is the case of **self-learning algorithms**, programmed to maximize companies’ profits, learning autonomously, without any human intervention, that, at least in certain market contexts, the most effective way to achieve this goal is to coordinate business conducts with those of competitors.

The use of this kind of self-learning algorithm could lead to a **collusive outcome** that occurs without the algorithm having been programmed to implement a restrictive cartel or facilitate its implementation.

Self-learning algorithms and antitrust law

The Fact-finding Survey on Big Data jointly carried out by the Italian Competition Authority, the Italian Communications Authority and the Personal Data Protection Authority noted that “*the spread of pro-collusive pricing algorithms can facilitate the stability of cartels and the creation of market contexts leading to collusive equilibrium.*”

The Fact-finding Survey points out that, in presence of sophisticated algorithms, characterized by machine learning mechanisms, it’s very difficult to identify the “*decisive ingredient for an infringement of Article 101*

TFEU” – ie the “*exchange of wills*” between competitors aimed at agreeing and coordinating a given commercial practice, although it highlights that the investigation of anticompetitive agreements facilitated by the development of sophisticated algorithms “*is one of the priorities of the Italian Competition Authority’s activity.*”

The first three algorithmic collusion scenarios above can be more easily brought within the perimeter of application of the anticompetitive agreements’ prohibition, since in such cases the algorithms help implement or facilitate an anticompetitive cartel. Greater doubts arise with reference to the collusive outcome achieved through the self-learning algorithms, since it does not constitute the result of an “*exchange of wills.*”

It is the latter case that gives rise to the most relevant competition concerns.

A self-learning algorithm programmed to define the best pricing strategies to maximize the firm’s profit – which is per se a legitimate goal – may learn that one of the ways, if not the most effective way, to achieve this goal is to **align its price** with that of its competitors on **supra-competitive values**.

The widespread use of self-learning algorithms could lead to **collusive outcomes** even in markets not particularly concentrated, taking into consideration the high capacity of AI systems to quickly process market information (such as possible price deviations of competitors from the supra-competitive price) and the ability of the algorithms to determine in real time the best pricing strategy (ie one that maximizes the undertaking’s profits) on the basis of this information.

In the absence (for the time being) of explicit provisions expressly regulating the use of algorithms and sanctioning algorithmic collusion, the main issue at stake is: (i) whether the competition rules suffice to detect and prevent algorithmic collusion conducts detrimental to competition, eg by interpreting extensively the concepts of “agreement” and “concerted practice” or applying the provisions on the collective dominance and its abuse; (ii) whether it is necessary to adopt new provisions and, if so, what type of provisions (eg provisions which expressly identify algorithmic collusion capable of constituting a competition infringement or provisions which set forth certain requirements and conditions for the use of the algorithms and appropriate controls to prevent collusion).

Contacts



Alessandro Ferrari
Partner
Head of Technology Sector, Italy

alessandro.ferrari@dlapiper.com
02.80618646



Elena Varese
Partner
Co-Head of Consumer Goods, Food
and Retail Sector, Italy

elena.varese@dlapiper.com
02.80618602



Giulio Coraggio
Partner
Head of Intellectual Property
& Technology, Italy

giulio.coraggio@dlapiper.com
02.80618619



Roberto Valenti
Partner
Head of Life Sciences Sector, Italy

roberto.valenti@dlapiper.com
02.80618518



Gualtiero Dragotti
Partner
Global Co-Chair, Patent Group

gualtiero.dragotti@dlapiper.com
02.80618514



Marco De Morpurgo
Partner
Global Co-Chair, Life Sciences

marco.demorpurgo@dlapiper.com
06.68880520



Alessandro Boso Caretta
Partner

alessandro.bosocaretta@dlapiper.com
06.68880502

