



ISSUE N.5 | JANUARY 2025

Diritto Intelligente

In this issue

- *EDPB opinion on AI model Training: How to address GDPR compliance?*
- *New directive on product liability applies to artificial intelligence and is now in place*
- *Landmark decision of the Garante against and AI-powered chatbot*
- *AI and Copyright: The European Commission's opinion on the Italian draft law*

Contents

Editorial.....3

EDPB opinion on AI model Training: How to address GDPR compliance?4

New directive on product liability applies to artificial intelligence and is now in place10

Landmark decision of the Garante against and AI-powered chatbot13

AI and Copyright: The European Commission’s opinion on the Italian draft law.....15

UK: Government begins consultation on copyright and AI18

Legal design tricks20

Legal tech bytes.....22



Editorial

December 2024 was a year of monumental progress in relation to AI regulation within the European Union.

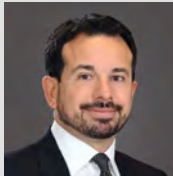
We witnessed two pivotal milestones that are set to shape the future of AI compliance. The European Data Protection Board (EDPB) issued its groundbreaking Opinion on AI training. Meanwhile, the Italian Data Protection Authority (Garante) made a landmark decision against an AI-powered chatbot.

The EDPB's Opinion offers invaluable insights into crucial concepts like anonymity, legitimate interest, and the handling of unlawfully processed data in the context of artificial intelligence systems, setting an exceptionally high bar for AI compliance.

In a striking move, the Garante's groundbreaking decision against a major AI-powered chatbot, resulting in a major EUR15 million fine, serves as a cautionary tale. This ruling shines a spotlight on major aspects like transparency, legal bases, and the protection of minors, emphasizing the crucial need for companies to align their AI systems with GDPR principles and prepare for the upcoming AI Act.

This edition is also packed with insights from diverse perspectives on other pressing issues in the AI legal landscape. We dive into the new EU Product Liability Directive and its implications for AI, highlighting the expanded scope of liability to include software and AI systems. We also cover the European Commission's feedback on Italy's draft AI law, particularly its stance on copyright and how it aligns with EU regulations. We also have the latest updates on the UK government's copyright and AI consultation, offering valuable insights into potential reforms post-Brexit.

And that's not all—this issue also offers a practical piece on leveraging legal design techniques to tackle complex legal challenges, focusing on problem definition and solution development. It's clear that companies are going to have to change their approach to compliance of AI systems in the light of last month's regulatory developments. This issue also includes our commentary on the transformative potential of AI in legal tech, showcasing innovative tools designed to enhance efficiency and compliance.



Giulio Coraggio

Location Head of the Italian Intellectual Property and Technology Department at DLA Piper

EDPB opinion on AI model Training: How to address GDPR compliance?

Authors: *Giulio Coraggio and Tommaso Ricci*

The European Data Protection Board's [Opinion 28/2024](#) represents a landmark effort by the EDPB to clarify how the GDPR applies to AI models.

With organizations increasingly turning to Artificial Intelligence for decision-making, customer service, fraud detection, and personalization, the question of how to reconcile these technologies with stringent data protection laws has never been more pressing.

Previously, companies struggled to fit fast-evolving AI capabilities into a regulatory framework designed before widespread AI adoption. Opinion 28/2024 responds to a request from the Irish Supervisory Authority, addressing four key areas:

- Conditions for considering AI models “anonymous”
- Using legitimate interest as a legal basis

- Handling the aftermath of unlawful data processing during model development
- Emphasizing documentation, accountability, and continuous risk management

This guidance is not limited to Large Language Models or generative AI. Any AI model that is trained on personal data, regardless of complexity or purpose, falls within its scope.

You can watch below episode of our podcast on the opinion of the EDPB on AI training on the [YouTube Channel Diritto al Digitale](#), and you can also listen the episode on Diritto al Digitale podcast on [Apple Podcasts](#), [Google Podcasts](#), [Spotify](#) and [Audible](#). Also, you can read the article below:

AI models and anonymity: Meeting a high standard

A significant point in the EDPB's opinion concerns the criteria under which AI models can be considered truly anonymous. Merely stripping out direct identifiers no longer suffices. The EDPB raises the bar, insisting on a case-by-case analysis and warning that even aggregated data may be susceptible to re-identification attacks like model inversion or membership inference.

Key takeaways:

- Case-by-case Analysis: Each AI model is unique, and organizations must demonstrate that re-identification risks are not "reasonably likely."

- High Threshold for Anonymity: Techniques like differential privacy can help inject "noise" to prevent extracting personal data, but pseudonymization alone is insufficient.
- ICO's Pragmatic Angle: The UK ICO's position is slightly more pragmatic, urging organizations to implement realistic safeguards and justify potentially risky approaches, such as web scraping, with robust data minimization strategies.

By understanding these requirements, businesses can better align their data-handling practices with the EDPB's strict standards on anonymity.

Relying on legitimate interest: A strict balancing test

The EDPB's opinion clarifies that legitimate interest (Article 6(1)(f) GDPR) is not a "quick fix" for justifying data processing in AI models. Instead, it imposes a three-step test:

1. Identify a Legitimate Interest: The interest must be concrete, lawful, and clearly defined.
2. Assess Necessity: Is the personal data essential to achieve the stated goal? Could the same result be achieved with less intrusive methods?
3. Balancing Test: The rights and freedoms of data subjects must not be overridden. Consider data sensitivity, transparency, and potential discrimination risks.

ICO's Perspective on Legitimate Interest: The ICO encourages specificity. By clearly defining the interest behind training an AI model, controllers can strengthen their case when balancing organizational goals against individual rights. Detailed documentation, possibly in the form of Data Protection Impact Assessments (DPIAs), is crucial.



Dealing with unlawfully processed data in AI development

What happens if personal data used to train an AI model was originally obtained unlawfully? The EDPB's opinion outlines several scenarios:

- **Same Controller, Tainted Data:** If the controller that unlawfully processed data continues to deploy the model, they must re-examine the model's compliance and may need to halt use, retrain it, or apply remedial measures.
- **Third-Party Acquisition of the Model:** A company purchasing a pre-trained AI model must conduct due diligence. Ignorance of unlawful origins is no defense.
- **Anonymization Before Deployment:** If the model's personal data are truly anonymized before deployment, the GDPR may cease to apply—provided this anonymization meets the high threshold set by the EDPB.

This framework stresses accountability across the AI supply chain. Every party involved must ensure data legality, not just the initial data collector.

Documentation and accountability: The cornerstones of compliance

Throughout its opinion, the EDPB underscores the importance of documentation and accountability. Robust records are essential to demonstrate compliance at every stage of AI model development.

Documentation essentials:

- **DPIAs:** Particularly for high-risk processing scenarios, DPIAs should identify risks, propose mitigations, and highlight safeguards.
- **Records of Processing Activities (Article 30 GDPR):** Keep detailed logs of data sources, purposes, and protective measures.
- **Technical Reports & Vulnerability Assessments:** If using differential privacy or other controls, maintain evidence to back up these claims.

A transparent record-keeping strategy not only helps in regulatory audits but also builds trust with users, clients, and partners.





Risk management and privacy-enhancing techniques for AI models

A proactive risk management approach lies at the heart of EDPB-compliant AI development. This begins with privacy-by-design principles:

Core strategies:

- **Data Minimization:** Only collect what the AI model truly needs.
- **Pseudonymization and Differential Privacy:** Consider injecting noise, encrypting data, or limiting access to reduce re-identification risks.
- **Regular Testing and Updates:** Continuously test the model against known attacks and update controls as technology evolves.

Supervisory authorities will likely want to see tangible evidence that organizations actively mitigate risks. Adopting state-of-the-art techniques and regularly assessing vulnerabilities demonstrates a firm commitment to privacy and security.

Special categories of data and automated decision-making

If an AI model processes special categories of data (e.g., health, biometrics), the GDPR imposes even stricter rules. Valid exemptions or explicit consent become critical. The potential harm to individuals is higher, and so are the stakes for compliance.

Automated Decisions Under Article 22 GDPR: For systems that significantly affect individuals—such as those determining credit eligibility—transparency and human oversight are non-negotiable. Controllers must provide understandable explanations of how the AI model makes decisions and offer meaningful avenues for individuals to challenge or request human intervention.

Meeting these standards may require close collaboration between legal and technical teams to translate complex decision-making logic into clear, intelligible information for data subjects.

Harmonization and contextual application of the EDPB opinion

The EDPB's opinion promotes harmonization across EU/EEA jurisdictions, but it also acknowledges that no two AI models are identical. Each AI model demands a tailored approach, factoring in data types, processing methods, and intended uses.

For businesses, this means there is no one-size-fits-all template. Expect to adjust your compliance strategy model by model, remaining agile as new guidance and regulations (like the upcoming EU AI Act) emerge.

Real-world example: The GEDI case

A recent case involving GEDI, a major Italian media group, and its arrangement with OpenAI offers a practical illustration of the EDPB's opinion in action. GEDI intended to share large news archives—containing personal data—with OpenAI for AI model training.

The Italian Data Protection Authority (Garante) raised red flags, showing that even well-established companies must rigorously justify data usage. The GEDI case underscores that vast datasets of seemingly “public” information can still be personal data under the GDPR.

Regulatory concerns:

- Legal Basis: Was legitimate interest or another legal basis clearly established?
- Transparency: Could individuals reasonably know their data might be used to train AI?
- Data Subjects' Rights: Were there mechanisms for data subjects to object or understand how their data was processed?

Practical steps from the EDPB opinion for businesses implementing AI models

To navigate these complex requirements set out by the EDPB opinion, businesses willing to exploit AI can adopt a robust, proactive approach:

1. Perform DPIAs Early and Often: Identify high-risk areas and revisit assessments as models evolve.
2. Choose and Document Your Legal Basis Carefully: Legitimate interest requires a thorough balancing test; consent demands transparency and meaningful choice.
3. Implement Privacy-Enhancing Techniques: Differential privacy, anonymization, and pseudonymization can reduce re-identification risks.
4. Maintain Detailed Documentation: Keep rigorous records of processing activities, justifications, and risk assessments to satisfy EDPB standards.
5. Test for Vulnerabilities: Regularly evaluate your AI model against membership inference attacks, model inversion, and other potential exploits.
6. Ensure Transparency: Make sure data subjects know how their data is used and what rights they have.
7. Stay Informed: Track regulatory updates and evolving guidance to remain compliant and competitive.

Lessons from the opinion of the EDPB on AI models

The EDPB's opinion on AI model compliance sets the stage for a future where innovation and data protection must walk hand-in-hand. By understanding the high bar set for anonymity, the conditions for using legitimate interest, the ramifications of unlawful data processing, and the need for rigorous documentation and risk management, businesses can navigate a complex landscape with confidence.

As AI technologies advance, so will regulatory expectations. Organizations that invest in privacy-by-design, ongoing audits, and clear communication will be better positioned to maintain trust, avoid enforcement actions, and remain at the forefront of responsible AI innovation.



New directive on product liability applies to artificial intelligence and is now in place

Author: *Federico Toscani*

The new product liability directive (the “**Directive**”), published in the Official Journal on November 18, 2024, is expected to have a significant impact on companies involved in the production and commercialization of Artificial Intelligence (“**AI**”) systems. The key point is the extension of the scope of the Directive to software, in order to allow injured parties to seek compensation for damages caused by AI systems.

After a long wait, the Directive was approved by the EU Council and published in the Official Journal on November 18, 2024. The Directive will apply to products placed on the market after December 9, 2026.

Until the publication of the Directive, it was unclear whether the original 1985 version – dated 1985 – covered intangible products, including software. With the progressive development of technology – and the related risks – the legal doctrine argued for an interpretative extension of


product liability to include software. This was based on the assumption that differentiating liability between tangible and intangible products was unjustifiable.

However, there had never been a definitive clarification by the European Court of Justice on this issue. Therefore, the matter was – up to the publication of the Directive – uncertain. The Directive seeks to fill this gap by explicitly extending the regime to software, ensuring robust protection even in cases where the damage is caused by an intangible product.

The product liability directive applies to Artificial Intelligence

The Directive establishes joint and several liability among various economic operators involved in the production chain of an AI system. Specifically, Article 8 of the Directive identifies the following liable parties:

- **The manufacturer of a defective product**, defined as:
 - Any party that develops, produces, or manufactures a product. If the product is composed of multiple components, this includes the party responsible for the final assembly. This provision is relevant where an artificial intelligence system is embedded in a physical product, making the final assembler liable even if it did not directly develop the AI system.
 - Any party that markets a product under their own name or brand, even if it did not manufacture the product. In the context of the AI Act, this would be the provider of the AI system.
 - Any party that develops, produces, or manufactures a product for its own use.
- **The manufacturer of a defective component**, if that component is integrated into a product or interconnected with a product under the control of the manufacturer. This is particularly relevant when an AI system embedded in a physical product causes a malfunction (e.g., software controlling a robot malfunctions and injures a person).
- **Any party that significantly modifies a product already placed on the market**. This provision aligns with the AI Act’s concept of reclassification as a provider when a deployer significantly alters a system. For instance, liability may arise if a user modifies or integrates AI software, thereby altering its functionality.
- **The importer of a defective product or component**, or the authorized representative of the manufacturer. If there is no importer or authorized representative established in the EU, the liability extends to the logistics service provider.



Definition of product

Article 4(1) of the Directive broadens the definition of product. According to the Directive, products are not only tangible goods but also electricity, files for digital manufacturing, raw materials, and software, including artificial intelligence.

The only exclusion applies to open-source software, provided that it is developed or supplied as part of a non-commercial activity.

Damages

Article 6 of the Directive limits compensable damages to the following:

- **Death or personal injuries**, including medically recognized psychological harm. This is particularly significant as it allows for compensation for psychological harm potentially caused by chatbots or algorithms displaying harmful content to users.
- **Damage to or destruction of property.**
- **Destruction or corruption of non-professional data.** This covers cases where software causes data breaches impacting data integrity (e.g., corruption of data) or availability (e.g., deletion of data). However, this applies only if the affected data is not used for professional purposes.

Further, under Article 5 of the Directive, the right to compensation is no longer limited to consumers but extends to any individual harmed by a defective product.

Definition of defective product

According to Article 7 of the Directive, a product is considered defective when it fails to offer the safety that a consumer can reasonably expect. This concept is particularly challenging to apply to AI systems, as their complexity and advanced learning capabilities (e.g., through machine learning techniques) create a “black box” effect, making it difficult – even for the developers – to understand why the system produced a certain output.

Nevertheless, under Article 10 of the Directive, a product’s defectiveness is presumed when:

- The claimant demonstrates that the product fails to meet mandatory safety requirements set by EU or national law aimed at preventing the specific harm suffered; or
- The claimant demonstrates that the damage was caused by an obvious malfunction.

These presumptions underscore the importance of compliance with the obligations set out in the AI Act in determining a product’s defectiveness, since the lack of compliance trigger the presumption of defectiveness. As a result, in addition to the penalties imposed under the AI Act, companies face the risk that non-compliance may provide grounds for third-party compensation claims. This position of the Directive seems reasonable, since adherence to standards set by sectoral regulations – including those on cybersecurity – remains the most effective way to facilitate the assessment of a product’s defectiveness.

Burden of proof

The Directive confirms a strict liability system, meaning that it does not require the injured party to prove fault or negligence. However, under Article 9 of the Directive, claimants must still prove:

- The defectiveness of the product;
- The damage suffered; and
- The causal link between the defect and the damage.

Proving defectiveness and causation is particularly complex due to the technical nature of AI systems and the “black box” effect, as injured parties typically lack access to the necessary technical information.

To address this, the Directive introduces a disclosure mechanism. In particular, Member States must ensure that, upon request from a claimant presenting sufficient facts and evidence to establish a plausible claim, the defendant is required to **disclose relevant evidence** in their possession. If the defendant refuses to disclose, it triggers the presumption of defectiveness. This measure is designed to help injured parties meet their burden of proof.

However, the Directive stops short of reversing the burden of proof, a measure that would have had a significant impact on liable companies.

Exemptions from liability

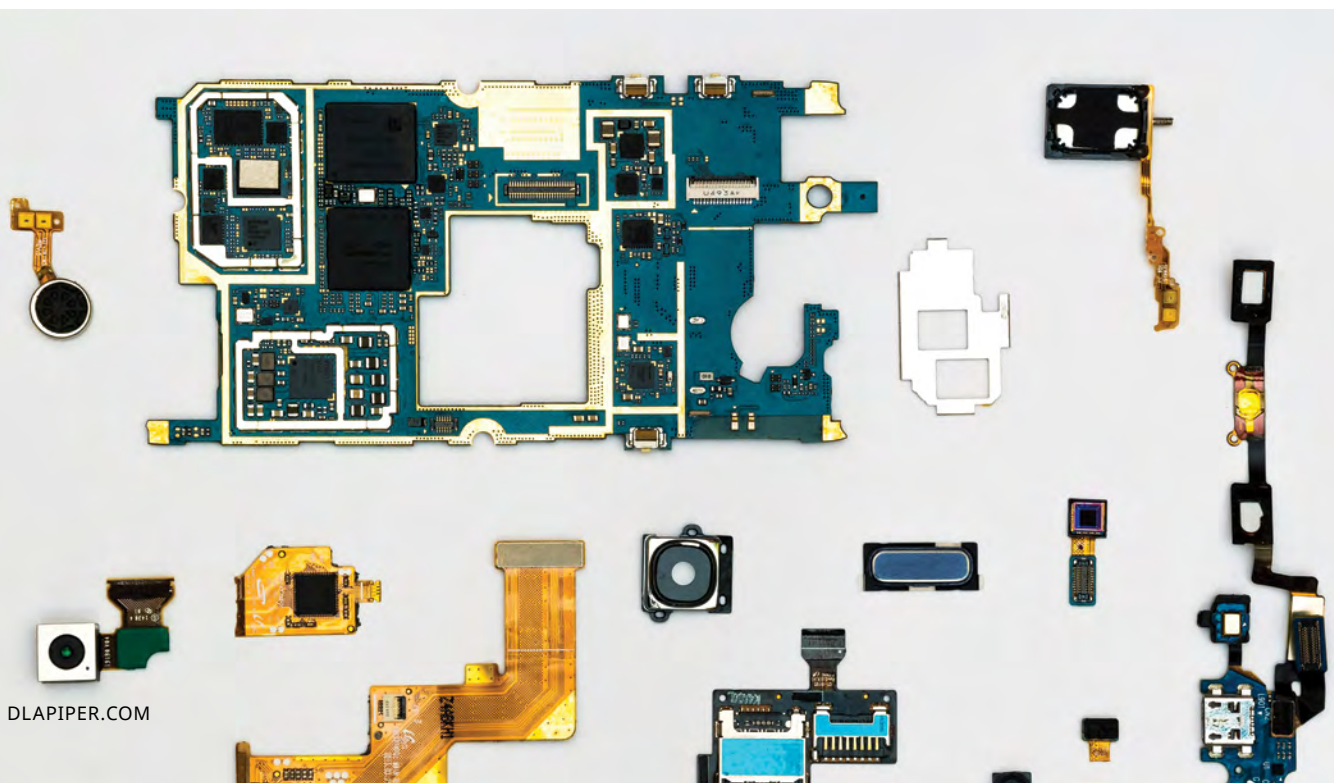
The Directive retains and introduces several grounds for exemption from liability. Particularly relevant for AI systems are:

- Proof that the defect did not exist at the time the product was placed on the market. However, Article 11(2) specifies that this exemption does not apply if the damage was caused by software embedded in a physical device under the manufacturer’s control (e.g., failure to update software). In such a case, the manufacturer shall ensure the security of the software throughout the entire period in which the product is under its control.
- Proof that the defectiveness resulted from compliance with legal requirements.
- Proof that the state of scientific and technical knowledge at the time the product was placed on the market or while under the manufacturer’s control did not allow for the discovery of the defect. This is especially relevant in cases where an AI system produces completely unpredictable outputs that cannot be traced back to errors in training or other development stages.
- Proof that the defect was unrelated to any modifications made to the product.

Conclusions

The Directive significantly expands the scope for obtaining compensation for damages caused by defective products, now explicitly including AI software. This represents an additional layer of regulation for the artificial intelligence

ecosystem, where coordination with other legislation – particularly the AI Act – will play a crucial role in defining liability cases.



Landmark decision of the Garante against and AI-powered chatbot

Author: *Roxana Smeria*

The Italian Data Protection Authority (the Garante) recently issued a significant [ruling](#) addressing breaches of the GDPR by an AI-powered chatbot.

More specifically, the investigations by the Garante have been triggered following a data breach on March 20, 2023 suffered by the chatbot. Following such event, the

investigation revealed that the company breached additional obligations of the GDPR, leading to a fine of EUR15,000,000.

We outline below the main violations found by the Garante.

Lack of data breach notification to the Garante

The Italian data protection authority noted that the company failed to notify the Garante about the breach in a timely manner, as required under Article 33 of the GDPR, despite the breach's potential to cause significant risks to affected individuals.

In this respect, it highlighted that since, at the time of the events, the company had no establishment within the European Union, it had to notify the data breach to all the EU data protection authorities whose residents had been impacted as it had no lead supervisory authority at that time.

Lack of legal basis for the processing by the generative AI model

The Garante found the company in violation of Articles 5(2) and 6 of the GDPR for failing to identify a valid legal basis for processing personal data for training its AI model before launching the service.

The company claimed that the processing for providing the artificial intelligence service was based on the performance of a contract and that algorithm training relied on legitimate interest. However, the Garante determined that the company had not formalized these legal bases before the service's

launch. Moreover, the documentation submitted later, such as a Data Protection Impact Assessment (DPIA) and a Legitimate Interest Assessment (LIA), were drafted months after the service went live.

Given company's establishment in Ireland, the Italian authority referred the matter to the Irish Data Protection Commission as the lead supervisory authority under GDPR Article 56 for further evaluation and action regarding the use of legitimate interest as a legal basis.

Lack of transparency due to the unclear privacy notice

The Garante found that the company violated Articles 5(1) (a), 12, and 13 of the GDPR due to significant deficiencies in its privacy policy. The issues primarily related to a lack of transparency, accessibility, and completeness in the information provided about how personal data was processed, especially for training AI models.

The investigation revealed that the privacy policy was only available in English and not easily accessible. Users were unable to review the privacy policy before providing their data, as it was poorly positioned on the registration page. Furthermore, the privacy policy only addressed the data collected for using the chatbot service, without providing any information about how personal data, including publicly available data from non-users, was processed during the training of AI models.

The language in the privacy policy was found to be vague and unclear. Terms used like "improving services," failed to communicate the specific purpose of training artificial intelligence models, such as fine-tuning or advanced AI research. This lack of clarity made it difficult for individuals to understand the nature and scope of the data processing activities, which included the innovative and complex use of AI technology.

The company argued that it had taken steps to provide transparency through privacy policies, pop-ups, and publications, including research documents and technical notes made available since 2019. However, the Garante concluded that these efforts were insufficient. The privacy policy did not provide critical information, such as the legal

basis for data processing or the potential impacts of training activities on individuals' data. The use of supplementary documents did not fulfill GDPR requirements, as users and

non-users were not reasonably expected to seek out or review such materials independently.

Lack of age verification for minors

Another critical issue addressed by the Garante was the protection of minors' data. The investigation revealed violations of GDPR Articles 24 and 25(1) for failing to implement adequate systems to verify the age of users registering for the chatbot.

More specifically, the terms of service stated that minors between 13 and 18 years old required parental consent to use the service, but no mechanisms were in place to enforce

this requirement. This omission allowed all users, including minors, to access the service without age verification or parental involvement.

The Garante noted that a lack of common European standards for age verification does not exempt data controllers from their responsibility to verify the contractual capacity of users, as required by GDPR.

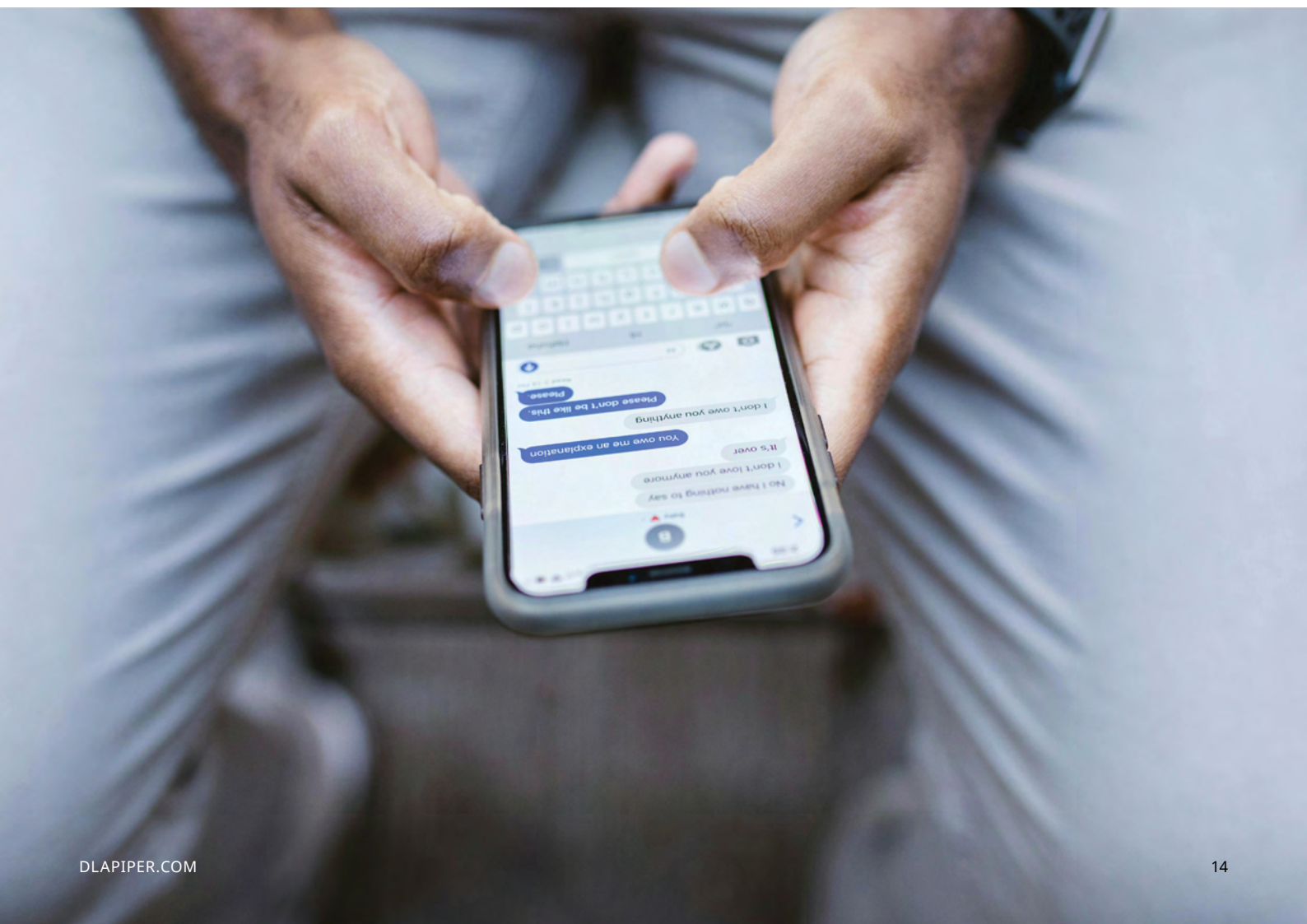
Conclusions

With this decision one of the first proceedings by the Garante against a company offering AI-driven services directly to end-users comes to an end.

This decision highlights the restrictive vision of the Garante on artificial intelligence technology, specifically with reference to accountability and transparency principles. Moreover, companies providing AI-powered services directly to end-users shall carefully consider the adoption of appropriate measures to verify the age of the users.

The decision sets an important precedent, signaling that regulatory authorities will closely scrutinize the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate compliance into the core design and functionality of their AI systems.

It will be interesting to see how the scenario will change after the EDPB's opinion on AI training on which you can read the article [HERE](#).



AI and copyright: The European Commission's opinion on the Italian draft law

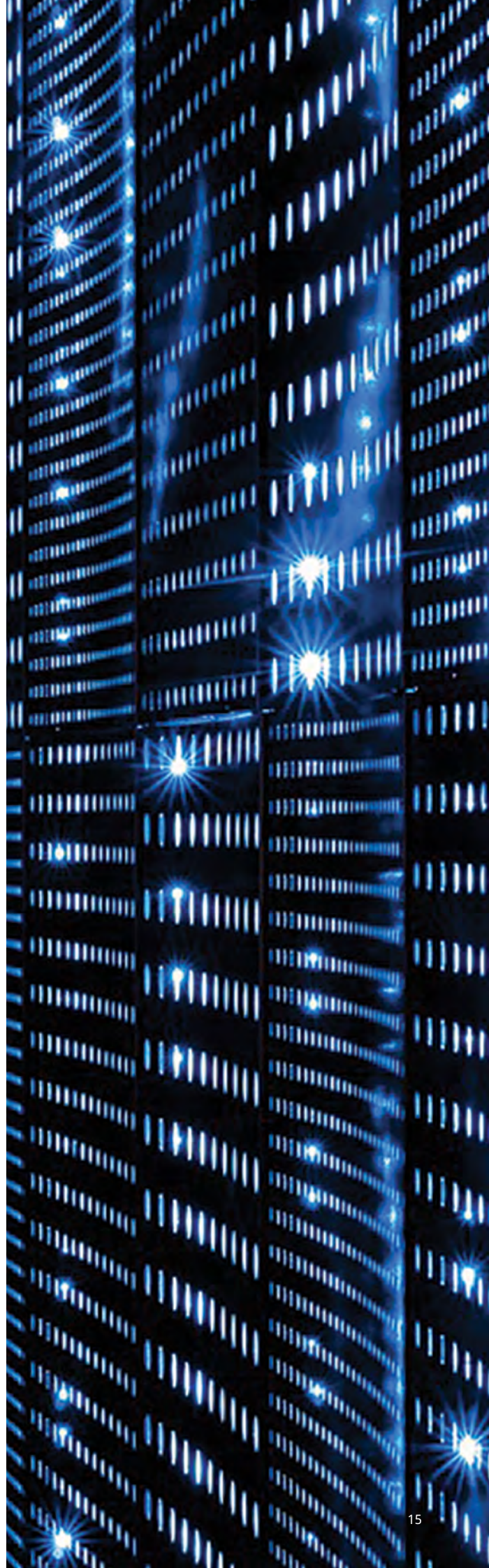
Author: *Maria Vittoria Pessina*

On November 5, 2024, the European Commission issued a detailed opinion (C (2024) 7814) addressing Italy's draft law on Artificial Intelligence (AI), criticizing several aspects almost article by article. Concerns were raised over multiple provisions, including those related to the interaction between AI and copyright.

In April 2024, Italy approved a draft law introducing measures to regulate the use of AI, aiming to comply with the European regulatory framework and protect fundamental rights, including copyright. The draft law establishes regulatory criteria to balance the opportunities offered by new technologies with the risks associated with their improper use, underutilization, or harmful deployment. It includes specific provisions to ensure transparency, safety, and user rights protection concerning AI-generated or modified content. However, the European Commission identified issues in some provisions, requesting changes to prevent overlaps with the EU AI Regulation. Among the targeted provisions are those addressing the relationship between AI and copyright.

The draft law approaches the issue of copyright and AI primarily through two measures:

- 1. Identifying AI-generated content (Article 23)**
- 2. Protecting copyright for works created with AI assistance (Article 24)**



Key provisions

Article 23

This article introduces the requirement to identify AI-produced or AI-modified content with a visible marker, such as a watermark with the acronym "IA" or an audio announcement for sound content. The identification must appear at the beginning and end of the transmission and

after every commercial break, with exceptions for content that is manifestly artistic or satirical. The goal is to ensure that users are aware of the artificial nature of the content they interact with.

Article 24

This article amends the copyright law by introducing specific rules for works created with AI systems. Key provisions include:

- **Recognition of copyright ownership:** AI-generated content cannot be considered intellectual creations under copyright law unless there is human creative input.
- **Mandatory licensing for copyrighted works:** AI system providers must obtain specific licenses for the use of copyrighted works when training their models.

The European Commission's concerns

In its opinion, the Commission raised specific concerns about Article 23, emphasizing the risk of overlapping with the EU AI Regulation:

- **Article 23(1)(b):** The provision requiring AI-generated content need to be clearly identified with a visible marker or audio announcement was deemed redundant compared to the obligations under Article 50(2) and (4) of the EU AI Regulation.
- **Article 23(1)(c):** The requirement for video platform providers to protect the public from AI-generated or AI-modified informational content presented as real was criticized as unclear and overlapping with Articles 50(1), (2), and (4) of the EU AI Regulation.

The opinion also referenced case law from the Court of Justice of the EU (Cases 34/73, *Fratelli Variola*, and 50/76, *Amsterdam Bulb*), reiterating that Member States are prohibited from duplicating provisions of an EU regulation in national law, thereby obscuring their origin in EU law.

Conclusions

Although the Italian legislature sought to enhance transparency and copyright protection in the AI domain, the proposed measures could create regulatory conflicts, hindering the uniform application of the EU AI Regulation.

Specifically, duplicating or overlapping rules at the national level may lead to legal uncertainty and potentially undermine the coherent implementation of European law.



UK: Government begins consultation on copyright and AI

Author: *Noemi Canova*

On December 17, the UK government launched a public consultation on copyright and artificial intelligence, consisting of 47 questions directed at professionals of the sector, who will have the opportunity to share their opinions until February 25, 2025.

As a consequent of Brexit, UK is no longer bound by the implementation of the Copyright Directive in the Digital Single Market, which introduced important changes to copyright law, including exceptions to allow text and data mining (TDM) under certain conditions. As a result, the only exception currently in force in the UK regarding TDM is provided by the Copyright, Designs and Patents Act 1988, which, however, does not cover commercial activities.

This highlights the urgency of updating the legal framework regarding copyright and introducing a new exception that takes into account the increasingly prominent role of artificial intelligence, while balancing the interests of rights holders who should be compensated for the use of their works in AI training. A consultation on AI-generated works was already initiated in 2021, exploring the possibility of extending the text and data mining exception to commercial activities; however, this measure was not implemented.

The consultation addresses, among other issues, the following topics: transparency, technical tools, and labeling.

Regarding transparency, according to the UK government, a successful synergy between copyright and AI will depend on strengthening the relationship between developers and rights holders. It is therefore necessary to consult industry professionals on the level of transparency required for the use of works to train AI models.

As for technical tools to protect copyright, while there are already numerous such tools, there is a need for further implementation to balance the rights of copyright holders with those of AI system developers.

The government is also considering the possibility of labeling a work as "AI-generated." This process, undoubtedly beneficial for rights holders and the public, presents a significant technical challenge.

Although the most desirable option for UK policymakers is a reform that extends the copyright exception for TDM to commercial purposes, the government, through the consultation, does not rule out the possibility of maintaining the current legal framework (Option 0). The other three options, however, propose changes. The first option would aim to enhance copyright protection by requiring licenses whenever training an AI model. The second option would introduce a broad exception for data mining, allowing the extraction of data from copyright-protected works without the rights holders' permission. The third scenario would involve establishing an exception for data extraction from copyrighted works, supported by transparency measures to ensure that AI developers are clear about the works used to train their models.

We are therefore awaiting the outcome of the consultation, which could indeed pave the way for a future where copyright and artificial intelligence coexist in a fair and transparent manner, responding to the needs of a rapidly evolving sector.



Legal design tricks

LITTLE TIPS TO USE LEGAL DESIGN IN YOUR DAILY ACTIVITIES

Trick #4: How to “define” the problem?

Author: Deborah Paracchini

—✓ —× Use the 5 W(hy) rules to find more effective solutions!

To solve a problem, you need to understand it thoroughly.

- The 5 W's help you **define it clearly**
- The 5 Why's guide you to its **root cause**

Define the problem clearly and uncover its root causes.

Only then can you find effective solutions!

5 The 5 W's of Design Thinking

- Who: Who is involved or impacted?
- What: What is the specific problem?
- Where: Where does the problem occur?
- When: When does the problem occur?
- Why: Why is solving it important?

Use these questions to map the problem in its context.

? The 5 Why's of Sakichi Toyoda

- Ask “Why” about the **main problem**
- **Keep asking “Why”** for each answer
- Stop the process when you **identify the root cause**

Each “Why” brings you closer to a deeper understanding. The method suggests 5 steps, but there are no strict limits.

👁 Let's look at an example!

What's the problem?

- Your service app has a high dropout rate.
- Users abandon the app after only a few interactions!

5 W's:

- Who? the users
- What? They stop using the service
- Where? On the app
- When? After one week
- Why? There's no incentive to keep using the service

5 Why's:

1. Why do users abandon the app? They can't easily find the service they're looking for
2. Why can't they find the service easily? The user interface is complex and unintuitive
3. Why is the interface complex? Too many features are crammed into the main screen
4. Why are there too many features on the main screen? There hasn't been a prioritization of the most-used services
5. Why hasn't prioritization been done? Usage data hasn't been adequately analyzed

⚠ And the result?

Root Cause: inadequate analysis of app usage data to optimize the interface.

Solution: Redesign the interface based on the most-used features by conducting a thorough analysis of app usage data.

Did you know?

The 5 Why's technique by Sakichi Toyoda was originally created to improve efficiency in Toyota factories. Today, it's used worldwide to solve complex problems across industries, from design to healthcare.

Stay tuned for Trick #5, to discover how to generate great ideas!



Legal tech bytes

EXPERT INSIGHTS ON THE LATEST TRENDS AND INNOVATIONS

Author: *Tommaso Ricci*

Implementing AI in legal operations is both a complex challenge and an extraordinary opportunity for in-house legal teams. To harness its full potential, it's essential to approach AI strategically—identifying areas where it can genuinely enhance efficiency while maintaining the high standards of legal work.

In 2024, I had the privilege of designing and testing several AI-driven solutions, transforming our workspace into an innovative testing ground. Below, I share key use cases I personally developed and piloted in beta versions for internal testing. These solutions are already operational, demonstrating how AI can revolutionize the legal profession, streamline processes, and deliver a tangible competitive advantage.

ROI Calculator for LegalTech Investments:

Getting approval for LegalTech investments requires being able to calculate the potential benefits accurately, but traditional ROI calculations weren't capturing all the benefits unique to legal technology. So I developed a Legal Tech ROI calculation methodology and a specialized calculator that accounts for both direct cost savings and harder-to-quantify benefits like risk reduction and improved legal service delivery. The tool:

- Performs comprehensive cost analysis, including licenses, research time, proof of concept, training, and implementation
- Evaluates benefits through multiple metrics including productivity gains, risk reduction, and customer satisfaction
- Generates detailed ROI projections and reporting for different stakeholder audiences

Legaltech ROI Calculator

Costs

Licenses ⓘ
€ 1000

Research ⓘ
€ 0

Proof Of Concept ⓘ
€ 0

Training ⓘ
€ 0

Implementation ⓘ
€ 0

Benefits

Productivity ⓘ
€ 0

Risk Reduction ⓘ
€ 0

Client Satisfaction ⓘ
€ 0

Stress Reduction ⓘ
€ 0

Can be useful for:

In-house legal teams often struggle to justify technology investments to management. This tool provides a structured methodology to quantify both tangible and intangible benefits of LegalTech solutions, facilitating the approval of strategic investments and enabling monitoring of their actual return over time.

Information Visualization for regulatory trends:

Analyzing the Italian Data Protection Authority's annual reports from 2021-2023 is time-consuming due to their length and complexity. Identifying meaningful patterns in enforcement decisions and focus areas requires significant effort. So I created a data visualization tool that transforms these complex reports into clear insights by automatically extracting and analyzing key data points to reveal emerging trends in privacy enforcement and regulatory priorities. The platform:

- Automatically processes and visualizes enforcement statistics from Garante's reports
- Generates dynamic comparisons of fines, violations, and focus areas across years
- Provides interactive dashboards showing evolution of regulatory priorities
- Enables detailed analysis of specific enforcement patterns and decision rationales



Can be useful for:

Effective data visualization is crucial for communicating trends and insights to management and stakeholders. This tool can be adapted to monitor any type of relevant legal data, from litigation statistics to compliance KPIs, making complex information immediately understandable and facilitating decision-making processes.

Interactive AI audit checklist:

After the EDPB released their AI audit framework, I noticed how time-consuming it was to manually complete these assessments for each AI system in use. The process was prone to inconsistencies and it was difficult to track progress across multiple audits. So I built an automated system that:

- Guides users through a structured audit workflow
- Automatically generates risk scores based on input data
- Maintains comprehensive audit trails and documentation
- Provides configurable assessment criteria and weightings

Can be useful for:

With increasing AI use in companies, legal teams must ensure compliance for a growing number of systems. This tool automates and standardizes the audit process, significantly reducing the time needed for assessments and ensuring a consistent and documented approach to AI compliance.

In 2025, our laboratory will continue exploring new ways to apply AI in the legal sector, focusing on finding the most practical and innovative use cases. Legal professionals interested in learning more are welcome to contact me for a hands-on demonstration of our tools and to join the lab's ongoing efforts. In the next update, we'll share additional use cases and fresh insights into how AI is transforming the legal profession.









Contacts

**Giulio Coraggio**

Partner
Head of Intellectual Property
and Technology, Italy
T +39 02 80 618 1
giulio.coraggio@dlapiper.com

**Gualtiero Dragotti**

Partner
Global Co-Chair, Patent Group
T +39 02 80 618 1
gualtiero.dragotti@dlapiper.com

**Alessandro Ferrari**

Partner
Head of Technology Sector, Italy
T +39 02 80 618 1
alessandro.ferrari@dlapiper.com

**Roberto Valenti**

Partner
Head of Life Sciences Sector, Italy
T +39 335 73 66 184
roberto.valenti@dlapiper.com

**Elena Varese**

Partner
Co-Head of Consumer Good,
Food and Retail Sector, Italy
T +39 02 80 618 1
elena.varese@dlapiper.com

**Ginevra Righini**

Partner
T +39 02 80 61 863 4
ginevra.righini@dlapiper.com

**Marco de Morpurgo**

Partner
Global Co-Chair, Life Sciences
T +39 06 68 880 1
marco.demorpurgo@dlapiper.com

**Alessandro Boso Caretta**

Partner
T +39 06 68 880 1
alessandro.bosocaretta@dlapiper.com

dlapiper.com