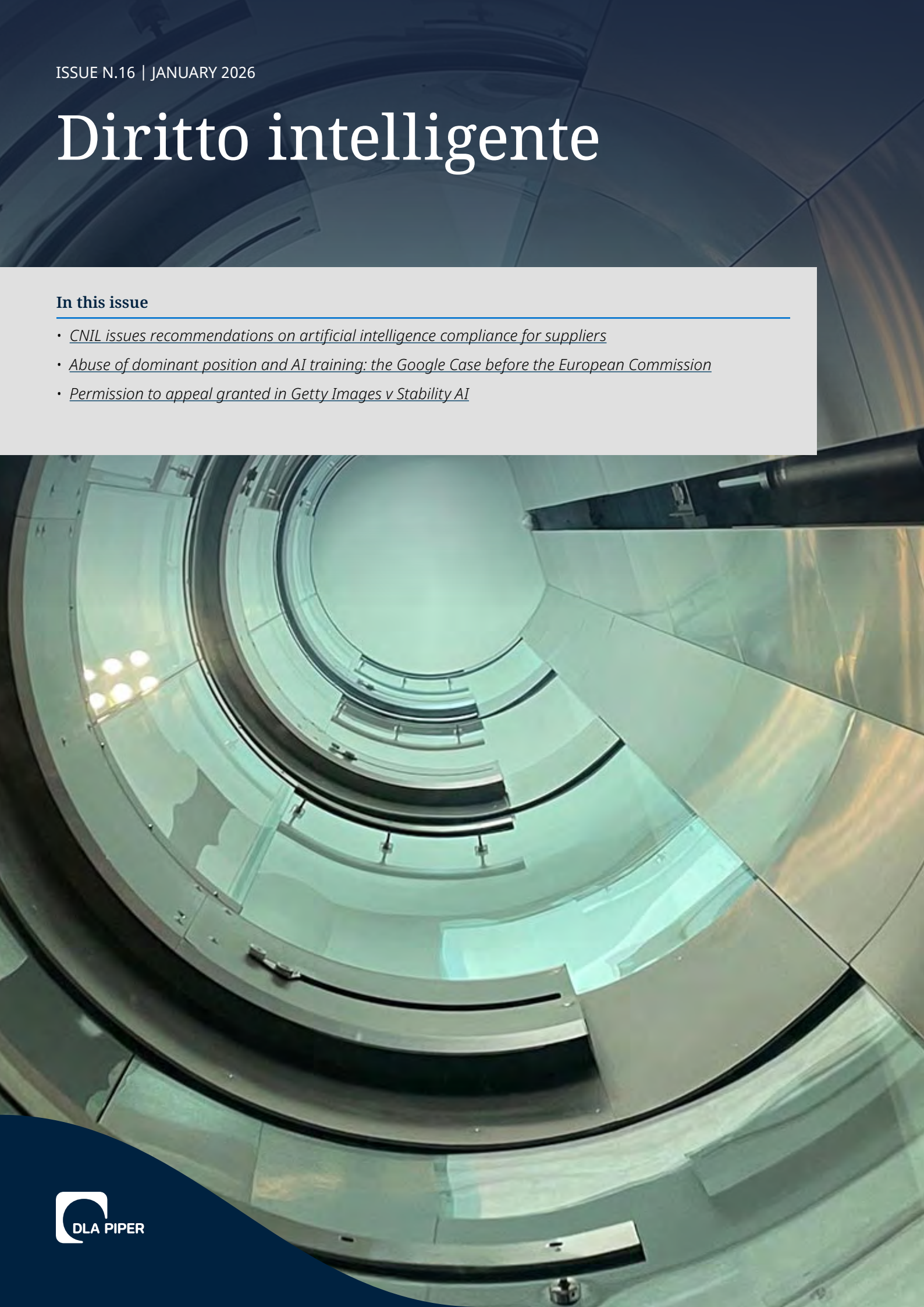
ISSUE N.16 | JANUARY 2026

Diritto intelligente

In this issue

- *CNIL issues recommendations on artificial intelligence compliance for suppliers*
- *Abuse of dominant position and AI training: the Google Case before the European Commission*
- *Permission to appeal granted in Getty Images v Stability AI*



DLA PIPER

Contents

CNIL issues recommendations on artificial intelligence compliance for suppliers 4

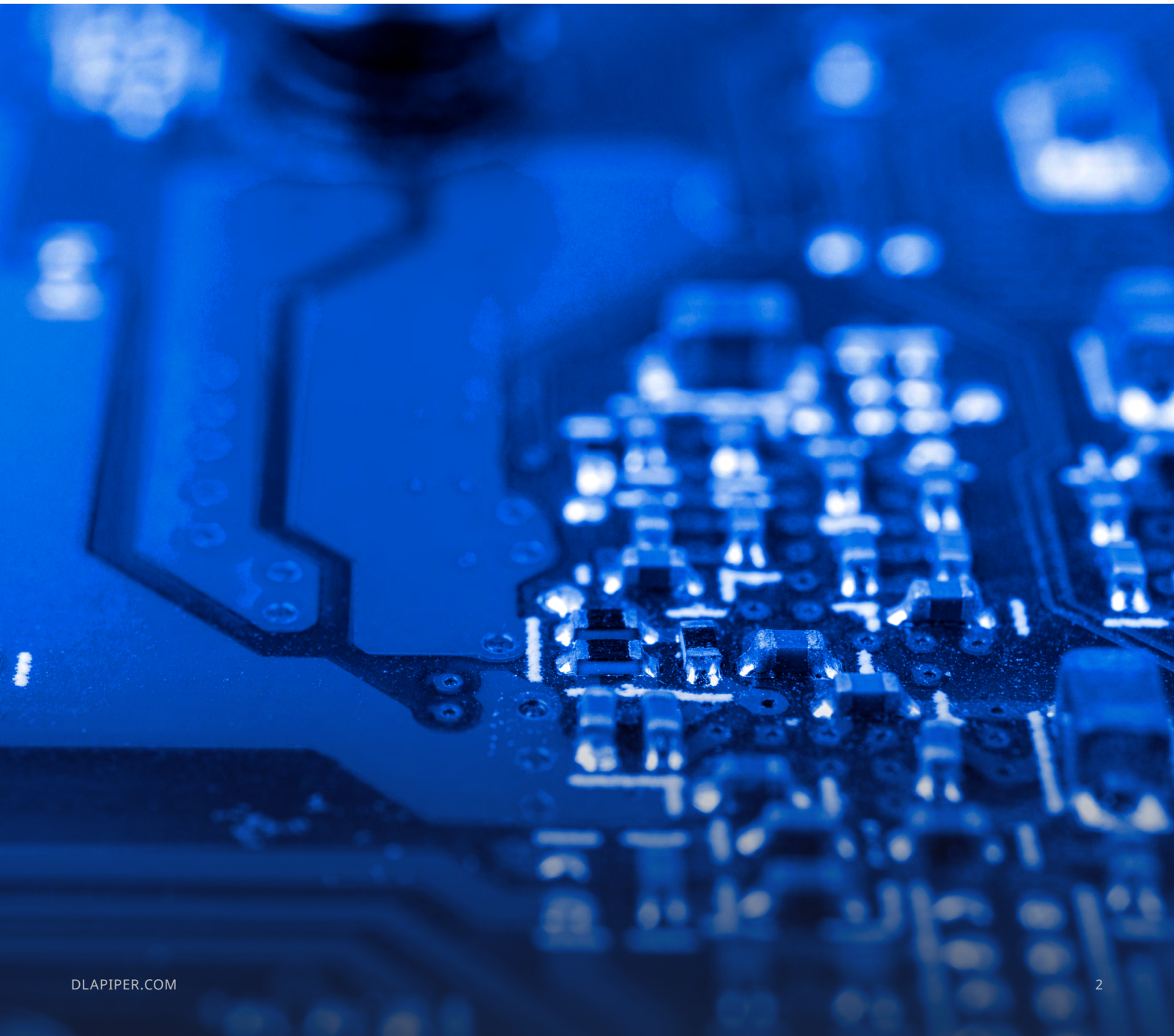
Abuse of dominant position and AI training: the Google Case before the European Commission 8

Permission to appeal granted in Getty Images v Stability AI 10

Artificial Intelligence and the future of drug discovery: Recursion case 11

Legal design tricks
Little tips to use legal design in your daily activities 12

Legal tech bytes 14



Editorial

Artificial intelligence is no longer living in a legal grey zone. The contributions in this January issue of Diritto Intelligente show a clear shift: AI has moved from experimentation to accountability.

The CNIL's January 2026 Recommendations on AI and GDPR compliance set the tone. Rather than creating new legal categories, the French authority applies existing data protection principles with renewed rigour. The focus on AI models – not just systems – makes one point clear: anonymity cannot be assumed, and risk cannot be outsourced downstream. Compliance becomes a continuous exercise, not a one-off assessment.

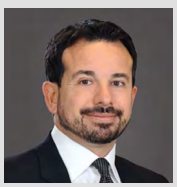
A similar logic runs through the European Commission's investigation into Google's use of publishers' and creators' content to power generative AI services. AI is no longer treated as a neutral layer of innovation, but as a tool that can reshape visibility, traffic, and revenue in digital markets. Control over data and distribution matters, and competition law is beginning to reflect that reality.

The uncertainty surrounding AI training and intellectual property emerges sharply in Getty Images v Stability AI. The decision to allow an appeal on whether an AI model itself can be an "infringing copy" shows how unresolved the legal boundaries remain – and how high the stakes are for the generative AI ecosystem.

The issue then looks beyond disputes and enforcement, showing how AI is transforming drug discovery through the Recursion case. Here, efficiency gains are real, but they do not eliminate the need for governance, explainability, and regulatory discipline.

Finally, the focus on legal engineering brings the discussion back to organizations. AI tools are everywhere, but value is not automatic. Without the skills to translate legal needs into workable systems, technology risks falling short.

Together, these contributions tell the same story: AI has grown up. And with maturity comes responsibility.



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

CNIL issues recommendations on artificial intelligence compliance for suppliers

Author: *Giulio Napolitano*

With the Recommendations published on 5 January 2026 (hereinafter, the "**Recommendations**"), the French data protection authority, *Commission Nationale de l'Informatique et des Libertés* (hereinafter, "**CNIL**") made available an operational methodology aimed at enabling suppliers of artificial intelligence (hereinafter, "**AI**") models to assess and document whether a model, or a system incorporating it, falls within the scope of Regulation (EU) 2016/679 (hereinafter, "**GDPR**"). However, the French Authority's contribution does not seek to redefine the categories of personal data protection law conceptually, but deliberately moves within already known coordinates, applying them to a technological vector that is currently testing their systemic resilience.

The starting point for the analysis is, in fact, deliberately sober. CNIL takes as its reference point the classic criterion, now well established in European case law and practice, according to which processing falls within the scope of the GDPR when it concerns data relating to identified or identifiable natural persons, taking into account the means reasonably likely to be used for identification.

The Recommendations clarify that an AI model can only be considered excluded from the scope of the GDPR if the probability of re-identification of the persons whose data were used in the training phase can be qualified as insignificant. In this sense, CNIL's position is explicitly in line with the guidance expressed *by the European Data Protection Board* (hereinafter, "**EDPB**"), which clarified Opinion 28/2024 that the classification of an AI model as anonymous can never be presumed in the abstract, but must be the result of a case-by-case assessment. This assessment must take into account not only the intrinsic characteristics of the model, but also the concrete methods of access, use and interaction, as well as the state of the art of data extraction techniques.

1. AI Model and System: methodological premises

One of the most significant and least obvious steps in the methodology proposed by CNIL concerns the conceptual and functional distinction between AI model and AI system. This distinction is not merely terminological but has a direct impact on the logical order of the analysis required for the purposes of GDPR applicability.

In CNIL Recommendations:

(i) the AI model is understood as a statistical representation of the characteristics of the *dataset* used for training. As such, it may incorporate information that is sufficiently granular to allow the direct or indirect reconstruction of personal data relating to individuals in the training set. The legally relevant risk therefore lies at this level: it is in the model that a storage or inference capacity may be hidden that makes re-identification possible.

(ii) The AI system, on the other hand, represents the application and organizational level that governs the use of the model. Interfaces, access controls, query methods, *output* filters, functional limits, security measures and organizational safeguards all contribute to defining how, and to what extent, the model is actually accessible and exploitable. It is the system that determines the operating context, but it does not, in itself, eliminate the intrinsic risk that may be embedded in the model.

The legal consequence of this distinction is central to CNIL's approach: the analysis of the applicability of the GDPR must necessarily start from the model. Only after ascertaining that the model cannot be considered anonymous does it become relevant to question whether integration into a system equipped with robust measures reduces the probability of re-identification to the point of rendering it insignificant. In other words, the Authority implicitly excludes a 'reverse' approach, according to which the absence of perceptible risk at the system level would render the nature of the underlying model irrelevant. Risk must be assessed at the point closest to its possible origin, i.e. where information relating to natural persons is stored, even if only potentially. The system can mitigate or neutralize this risk, but it cannot retroactively erase it or render the analysis of the model superfluous.

CNIL also clarifies that the status assessment applies to any model trained on personal data, regardless of its stated purpose or the functions for which it was designed. It is not decisive that the model is intended to produce information about specific individuals; what matters is the technical possibility, even accidental, of extracting or inferring personal data by reasonably usable means. In other words, the purpose of the model does not operate as a legal

exemption criterion. This approach is fully in line with the EDPB's guidance, according to which a model designed to produce or infer information about natural persons necessarily contains personal data, while a model trained on personal data but not designed for such purposes can only be considered anonymous if the risk of direct or indirect identification is highly unlikely, both through parameter analysis and through queries.

This has a significant systemic effect on the entire AI supply chain. If the model is considered anonymous, a system that uses it exclusively will, in principle, be excluded from the scope of the GDPR. If, on the other hand, the model is not anonymous, any exclusion of the system will require an independent and additional analysis, based on appropriate measures and tests to demonstrate that the risk of re-identification has been effectively neutralized. In the absence of such demonstration, the processing inevitably extends to downstream actors as well.

2. From the dataset to the model, risk analysis as an accountability obligation

One of the most significant elements of the methodology outlined by CNIL is the unambiguous statement that the analysis of *the status* of an AI model is not an option left to the technical discretion of *the provider*, but a genuine legal obligation, directly attributable to the principle of *accountability* enshrined in the GDPR. Whenever a model is trained on personal data, the re-identification risk analysis must be conducted systematically, regardless of the outcome it may produce.

The underlying logic is fully consistent with the framework of European data protection law. It is not necessary for the processing to have immediate effects on the data subjects for an assessment obligation to arise. It is sufficient that the processing incorporates a legally relevant risk, i.e. the non-negligible possibility that natural persons may be identified, directly or indirectly, from the model. The analysis required by CNIL does not serve to confirm a given assumption of anonymity, but to verify whether that assumption can be supported in the light of objective and verifiable criteria.

In this context, the role of the model *provider* takes on clear centrality. It is the *provider* who, in most cases, determines the purposes and means of development processing: they select the training *dataset*, define the model architecture, establish the training methods and envisage the contexts of use. Therefore, the provider has the primary responsibility for conducting the analysis and drawing a reasoned conclusion about the applicability or otherwise of the GDPR.

- When the *provider* concludes that the model should be excluded from the scope of application of the GDPR, this conclusion cannot be confined to an internal or purely declarative assessment. It must be supported by documentation suitable for submission to the supervisory authority for review, allowing the logical and technical path followed to be reconstructed. It is not only the outcome of the analysis that is relevant, but also its traceability: the measures taken to reduce the risk of data storage, the assessments made on the state of the art, and any tests conducted to verify the model's resistance to re-identification attacks. In this sense, the documentation takes on an eminently probative function. It becomes the tool through which the provider demonstrates that it has fulfilled its *accountability* obligation, making its position defensible in the event of verification or dispute.
- CNIL extends this logic to the system level as well. If a model cannot be considered anonymous, it is not impossible that its use within a larger system could reduce the risk to the point of making it insignificant. However, even in this case, the analytical burden does not disappear but is shifted. The system provider is required to conduct its own independent analysis, taking into account not only the characteristics of the model, but also the measures implemented in terms of access, interaction, output filtering and usage monitoring. This analysis cannot be limited to referring to assessments made upstream on the model but must be based on specific checks relating to the system as a whole.

Another important aspect concerns the relational and informational dimension of *accountability* throughout the AI supply chain. When a system *provider* claims that the use of the system does not fall within the scope of the GDPR despite the use of a non-anonymous model, CNIL recommends sharing sufficient documentation to allow users to verify this claim. This is good practice which, although not a formal obligation, has a concrete impact in terms of the allocation of responsibilities.

3. 'Reasonably usable means': the true legal standard of anonymity

The criterion of 'reasonably usable means' is the cornerstone of the entire assessment of the anonymity of AI models. The approach adopted by CNIL is particularly rigorous on this point and fully consistent with European data protection law: anonymity is not assessed in the abstract, nor in the light of purely theoretical scenarios, but in relation to the concrete and realistic possibilities of re-identification.

The Recommendations clarify that what is technically possible in extreme or academic conditions is not relevant, just as it is not sufficient to limit the analysis to the 'ordinary' or declared usage scenario of the provider. The assessment must be made in an intermediate area, based on objective criteria, taking into account the capabilities of a realistic attacker and the overall context in which the model is developed and used. It is precisely this balance that makes the notion of reasonably usable means an eminently legal category, rather than a mere technical variable.

- From this perspective, the risk of re-identification does not arise from the model considered as an isolated object, but from the information ecosystem in which it operates. The possibility of combining the information obtainable from the model with additional data, whether publicly available or otherwise accessible, directly affects the assessment. Identifiability is therefore the result of a correlation, not a single source. This approach is consistent with the established interpretation of the GDPR, which requires consideration of all available means, not just the intrinsic characteristics of the processing.
- Another key element is the cost and time required to extract personal data. CNIL recognizes that attacks requiring disproportionate resources, highly specialized skills or timeframes incompatible with realistic use and may, in certain circumstances, not be considered reasonably usable means. However, this assessment is by definition dynamic. What appears complex or burdensome today may quickly become accessible in a context of accelerating attack techniques and the spread of pattern analysis tools. As a result, it is impossible to crystallize anonymity in a snapshot of the state of the art frozen in time.
- Particularly significant is the attention paid to access to the model by unauthorized parties. The analysis cannot be limited to legitimate users or use cases envisaged by the provider, but must include the possibility – far from remote – of unauthorized or non-compliant access. In this sense, CNIL reiterates a principle of great practical importance: merely restricting access does not guarantee the anonymity of the model. Contractual, organizational or access control measures may reduce the likelihood of re-identification, but they do not automatically render it insignificant.
- The assessment of reasonably usable means must also take into account the *deployment* context. A model made accessible to the public, or integrated into a service usable by an indefinite number of users, has a structurally different risk profile than a model used in an internal and controlled environment.

The conclusion of the argument is particularly clear from a legal point of view. A model can only be considered excluded from the scope of the GDPR if, in light of the reasonably usable means, the probability of extraction or inference of personal data is insignificant. It is not sufficient for this probability to be low, limited or difficult to achieve: the required standard is deliberately high and reflects the centrality of the principle of *accountability* in European law.

4. Anonymity as an intrinsically unstable condition

One of the most relevant aspects of the approach outlined by CNIL concerns the inherently non-definitive nature of the analysis of the anonymity of AI models and systems. The conclusion that the probability of re-identification is insignificant cannot be taken for granted once and for all, but must be constantly reviewed in light of technological, scientific and operational developments. In this sense, anonymity is not a static property of the model, but rather a contextual and temporal assessment, subject to review.

CNIL expressly clarifies that a model or system initially considered outside the scope of the GDPR may subsequently fall within its scope. This may occur, for example, in the presence of new attack techniques, previously unknown vulnerabilities or a significant change in the state of the art that makes previously unrealistic methods of extracting personal data feasible. The decisive factor is not the correctness of the original analysis, but the provider's ability to recognize and manage the evolution of risk over time. This approach gives rise to a specific obligation of continuous review. Model and system providers are required to periodically verify the validity of the assessments carried out, considering both developments in scientific research and the operational experience gained in the practical use of the model. From this perspective, compliance does not end at the design or production stage but accompanies the entire life cycle of the technological artefact.

Incident management is a crucial test in this context. If personal data is extracted – or even if there is a reasonable likelihood that this has occurred – the provider must assess whether the conditions for a personal data breach under the GDPR are met. The fact that the model was legitimately classified as anonymous on the basis of a diligent analysis does not, in itself, exclude the existence of a *data breach*. What matters, from a legal point of view, is the ability of the to react correctly to the event, documenting it and, where appropriate, activating the notification and communication obligations provided for in Articles 33 and 34 of the GDPR.

CNIL takes a balanced approach on this point. The emergence of vulnerability does not automatically imply liability on the part of *the provider*, provided that the initial analysis was based on the state of the art and adequately documented. However, the legitimacy of *the provider's* position will depend crucially on the timeliness and adequacy of the measures taken following the incident.

Once anonymity has been called into question, a structured response is required, not a merely formal defence. This approach is closely aligned with the broader European regulatory framework, and in particular with Regulation (EU) 2024/1689 (hereinafter, the "**AI Act**"). Although operating on different levels, the GDPR and the AI Act share a convergent vision of compliance as a dynamic process. The *post-market* surveillance, risk management and incident reporting obligations for high-risk AI systems are consistently reflected in CNIL's methodology, including in terms of personal data protection. Continuous monitoring of the model's ability to 'remember' individuals thus becomes a structural element of AI *governance*.

Ultimately, the methodology proposed by CNIL redesigns the very way in which AI model *compliance* is conceived. Anonymity is not a statement of principle, nor a technical attribute to be applied once and for all, but an unstable legal condition that needs to be kept under constant review. In a constantly evolving technological ecosystem, trust is not based on assumptions, but on the ability to demonstrate, over time, that the risk to individuals' fundamental rights remains effectively below the threshold of legal relevance.

Abuse of dominant position and AI training: the Google Case before the European Commission

Author: *Giovanni Chieco*

The widespread adoption of generative artificial intelligence has raised complex questions concerning compliance with competition rules and the use of digital content. In this context, on 9 December 2025 the European Commission opened an antitrust investigation into Alphabet/Google to assess whether the company may have infringed Article 102 of the Treaty on the Functioning of the European Union (TFEU) by using content from web publishers and videos uploaded to YouTube to train and operate AI services such as AI Overviews and AI Mode.

The investigation also stems from complaints lodged by independent European publishers, supported by associations committed to safeguarding an open and competitive web. In June 2025, these stakeholders reported to EU institutions that the introduction of AI Overviews had led to a significant diversion of traffic away from original news websites, with reductions of up to 50% in visits to articles and, consequently, in advertising revenues. The complaints highlighted the possible existence of abuses of dominant position and discriminatory practices in access to information, stressing that Google's position in the online search market – with a market share close to 90% in Europe – effectively makes it impracticable for many publishers to refuse the use of their content without suffering a substantial loss of visibility and economic relevance.

Based on these complaints and further investigative activities, the European Commission has identified two distinct ways in which Google may be exploiting third-party content to power its AI services while abusing its dominant position. With regard to web publishers' content, Google uses such material to generate AI Overviews and AI Mode, integrating summaries and conversational responses directly into search results pages. AI Overviews produces automated summaries displayed above organic search results, while AI Mode operates as an interactive, chatbot-style interface capable of responding to users' queries in a conversational manner. The Commission seeks to determine whether these services rely on editorial content without adequate remuneration and without offering publishers a genuine possibility to refuse such use without losing visibility on Google Search – an issue of particular importance given that many publishers depend on search-driven traffic to sustain their business models.

Separately, Google uses videos and other content uploaded to YouTube to train its generative AI models. In this case, creators automatically grant Google the right to use their content for various purposes, including model training, without receiving any specific remuneration and without being able to opt out without restrictions on access to the platform. At the same time, competing developers are unable to access the same content, potentially creating an unjustified competitive advantage.

This distinction between textual and audiovisual data flows is crucial. Publishers' content directly affects traffic and advertising revenues linked to search, whereas YouTube content influences competitive dynamics within the generative AI ecosystem, with significant implications for the development opportunities available to competing AI providers.

The investigation is grounded in Article 102 TFEU, which prohibits the abuse of a dominant position, and is also governed by Regulation (EC) No 1/2003, which sets out the rules for the exercise of the European Commission's competition enforcement powers. The opening of proceedings pursuant to Article 11(6) of Regulation 1/2003 relieves national competition authorities of parallel application of EU antitrust rules, while Article 16(1) requires national courts to avoid decisions that would conflict with the Commission's ongoing investigation.

In this context, Google has responded by emphasizing the benefits of AI for citizens and businesses and has expressed its willingness to cooperate with European authorities, while cautioning that overly restrictive regulation could slow the development and adoption of artificial intelligence. The Commission, however, has reiterated that technological innovation must comply with the principles of fair competition and equitable access to data, and that AI cannot be used as a means to unjustifiably consolidate dominant market positions.

The investigation has no predetermined deadline and entails an in-depth assessment of contractual, technical and market data. Should infringements of Article 102 TFEU or Article 54 of the Agreement on the European Economic Area be established, Google could face fines of up to 10% of its worldwide annual turnover, as well as corrective measures that may include changes to content usage terms or the opening of fairer access channels for competing AI developers.

The practical implications are extensive: the outcome of the proceeding could redefine the ways in which digital content is monetized and exploited within the artificial intelligence ecosystem, affecting publishers, content creators, and developers of models based on third-party data. This investigation represents a legal frontier in the regulation of AI and digital markets, constituting one of the first cases in which European rules are applied directly to commercial practices involving artificial intelligence. Its outcome will have a profound impact on regulatory standards concerning competition protection in the context of AI.

Permission to appeal granted in Getty Images v Stability AI

Author: *Maria Vittoria Pessina*

The dispute between Getty Images and Stability AI represents one of the most significant precedents to date concerning the relationship between artificial intelligence and copyright law, as well as one of the earliest attempts to apply traditional intellectual property concepts to generative AI models. The proceedings, commenced in 2023 before the High Court of England and Wales, placed at the centre of legal debate the use of protected works for the training of AI systems such as Stable Diffusion.

Getty Images, a group founded in 1995 and operating globally in the creation and licensing of visual content through the Getty and iStock brands, brought proceedings against Stability AI alleging that the Stable Diffusion model had been trained using millions of copyright-protected images without authorization. The original claims were wide-ranging and included allegations of copyright infringement, database right infringement, trademark infringement, and passing off, relating to both the model itself and its training process, as well as the images generated by it.

Stability AI, a company specializing in the development of generative artificial intelligence tools, contested these allegations, arguing that Stable Diffusion neither stores nor reproduces protected images, and that the model's development and training occurred outside the United Kingdom. On this basis, Stability submitted that the copyright and database rights relied upon by Getty, as rights governed by UK law, were not applicable to the activities complained of, as those activities had occurred outside the UK.

Over the course of the proceedings, the scope of the case was progressively narrowed. Getty significantly curtailed its claims relating to the model's outputs, saw its attempt to proceed by way of a representative action on behalf of tens of thousands of third-party photographers rejected, and ultimately abandoned its claims of primary copyright and database right infringement in full. This withdrawal occurred at a late stage of the proceedings, largely due to difficulties in establishing the geographic location of the training activities.

By the conclusion of the trial in June 2025, only two issues remained. The first concerned alleged secondary copyright infringement, namely, whether the making available in the UK of files containing the so-called "model weights" of Stable Diffusion could amount to indirect infringement. The second concerned alleged trademark infringement arising from the appearance, in certain generated images, of elements resembling Getty's watermarks.

In its November 2025 judgment, the High Court delivered a detailed decision that, overall, favored Stability AI. As regards secondary copyright infringement, the Court dismissed Getty's claim, accepting that the files containing the model parameters could fall within the broad statutory notion of an "article" under UK copyright law, which is not limited to tangible objects and may include intangible digital entities. However, the Court held that those files could not be characterized as "infringing copies", since – on the interpretation adopted by the judge – an article can only qualify as such if it has in fact incorporated, contained or stored a copy of a copyright-protected work, a condition that was not met in the case of the Stable Diffusion models.

The Court's findings on trademarks were more nuanced. While the judge rejected the broader claims and dismissed the allegation based on enhanced trademark protection, she nevertheless identified extremely limited instances of infringement in relation to early versions of the model, in which certain generated images displayed watermark-like features sufficiently similar to the Getty or iStock marks.

In December 2025, the Court considered the parties' applications for permission to appeal. Getty was granted permission to appeal the dismissal of its secondary copyright infringement claim – specifically, the contention that Stable Diffusion itself constitutes an "infringing copy" of the works on which it was trained. This raises a question of law of considerable importance, namely the interpretation of the concept of "infringing copy" in the context of artificial intelligence models, an issue never previously addressed by the courts and one with potentially significant implications for the generative AI sector.

By contrast, Stability AI was refused permission to appeal the Court's limited findings on trademark infringement.

Taken as a whole, Getty Images v Stability AI highlights the difficulty of applying traditional intellectual property concepts to fundamentally new technologies. The outcome of the appeal on secondary copyright infringement will be particularly significant, as it may directly affect the ability to distribute and commercialize in the UK AI models trained on protected works without authorization, thereby contributing to the definition of the legal boundaries for the development of artificial intelligence in the years to come.

Artificial Intelligence and the future of drug discovery: Recursion case

Author: *Noemi Canova*

The development of a new drug is one of the most complex and time-consuming industrial processes. On average, it takes over ten years and investments of more than two billion dollars to bring a new molecule to market, with failure rates that remain very high, especially in the advanced clinical phases. Against this backdrop, artificial intelligence is transforming the way drugs are discovered, designed, and evaluated.

In recent years, a growing number of pharmaceutical companies have started integrating machine-learning models and advanced data-analysis tools into their entire research and development pipelines. The goal is to reduce time and costs, increase the probability of success and enhance decision – making quality in the early stages, before projects require particularly expensive clinical trials. One of the main advantages of artificial intelligence in this field is its ability to analyze vast volumes of heterogeneous data, such as cellular images, genomic and transcriptomic information, and chemical structures. This approach is particularly useful in the study of complex diseases, including cancer and neurodegenerative disorders.

The case of Recursion Pharmaceuticals is emblematic of this evolution. The Salt Lake City–based company has built its industrial model on the integration of artificial intelligence, high-throughput phenotypic screening, and laboratory process automation. Recursion's platform can generate and analyze millions of cellular images, accelerating the identification of new therapeutic hypotheses by taking an integrated approach to the entire drug-discovery process. Rather than applying artificial intelligence to a single phase, the company aims to coordinate data and models across all stages of research. This produces more robust biological hypotheses and significantly reduces experimental timelines compared with traditional standards.

Early results show a substantial compression of timelines in the initial phases, which are characterized by a high degree of automation. If these programmes demonstrate clinical efficacy in more advanced stages, this model could establish itself as a benchmark for the entire sector.

While Recursion is among the pioneers of this approach, it is not an isolated case. An increasing number of pharmaceutical companies are investing in proprietary artificial-intelligence platforms or entering into collaborations with technology startups and high-performance computing specialists. Today, AI is used to design new molecules, predict interactions between drugs and biological targets, analyze data, and improve the design of clinical trials.

Despite these promising prospects, the adoption of artificial intelligence in drug development still presents significant challenges. The quality and availability of data remain central issues, as do the transparency and interpretability of models – particularly important in a highly regulated sector – and the actual ability of algorithms to translate statistical correlations into tangible clinical benefits.

However, the path forward is now clearly defined. Artificial intelligence is no longer a marginal experiment, but a strategic tool set to have a profound impact on the organization, costs, and underlying logic of pharmaceutical research.

Legal design tricks

Little tips to use legal design in your daily activities

Authors: *Deborah Paracchini and Enila Elezi*

Trick #14: Accessibility: why, without Legal Design, rights stay on paper

After having explored the role of the Legal Designer in the AI human on the loop, let's now investigate how the Legal Designer can help accessibility.

For years, accessibility was treated as a marginal, technical issue, relevant only in a few specific contexts. Not anymore.

European and national regulations on the accessibility of digital products and services make one thing clear: accessibility is not just a best practice, it is a legal obligation. And when we talk about digital services, the law inevitably passes through documents as well.

Contracts, privacy notices, and terms and conditions are not just texts: they are tools through which people understand, choose, and access their rights.

If they are not accessible, those rights risk remaining purely formal.

This is where the Legal Designer comes in.

What is the role of the Legal Designer in accessibility?

The Legal Designer:

- structures legal content
- organizes information in a clear and navigable way
- reduces cognitive and informational barriers
- translates legal obligations into usable experiences

The goal is not to oversimplify the law, but to make it usable.

An accessible document is one that people can read, understand, and use to make informed decisions.

What does accessibility mean in legal documents?

A legal document is accessible when information is:

- perceivable (also through assistive technologies)
- usable (easy to explore and consult)
- understandable (not only legally correct)

Accessibility does not mean writing less.

It means designing better.

1. Structuring content to break down the "wall of text"

Many legal documents still rely on very long paragraphs, a single generic heading, and multiple concepts packed into the same block of text.

From an accessibility perspective, this is a real barrier.

The Legal Designer works on structure by:

- separating topics
- creating informative headings
- organizing content into clear sections

The legal content remains the same, but the reading experience changes completely.

2. Making content navigable and easy to orient

An accessible text is not only readable, but also easy to explore.

The Legal Designer:

- turns "hidden" lists into real lists
- uses white space to separate concepts
- takes care of the visual and logical order of information

This makes consultation easier, reduces misinterpretation, and ensures the document is usable even by people using screen readers or other assistive tools.

3. Working on understandability

A document can be formally correct and still be incomprehensible to those who read it. This is often where true accessibility is lost.

The Legal Designer intervenes in the language when needed by:

- shortening excessively long sentences
- removing unnecessary redundancy and jargon
- making practical consequences explicit

Stating that a right or an obligation exists is not enough. People must be able to understand what it actually means for them.

4. From information duties to user experience

Accessibility regulations require information to be clear, simple, and accessible. The risk is treating this as a purely formal obligation, resulting in long and defensive documents.

The Legal Designer does the opposite: it turns information duties into orientation tools. In this way, the document is no longer a barrier, but a guide.

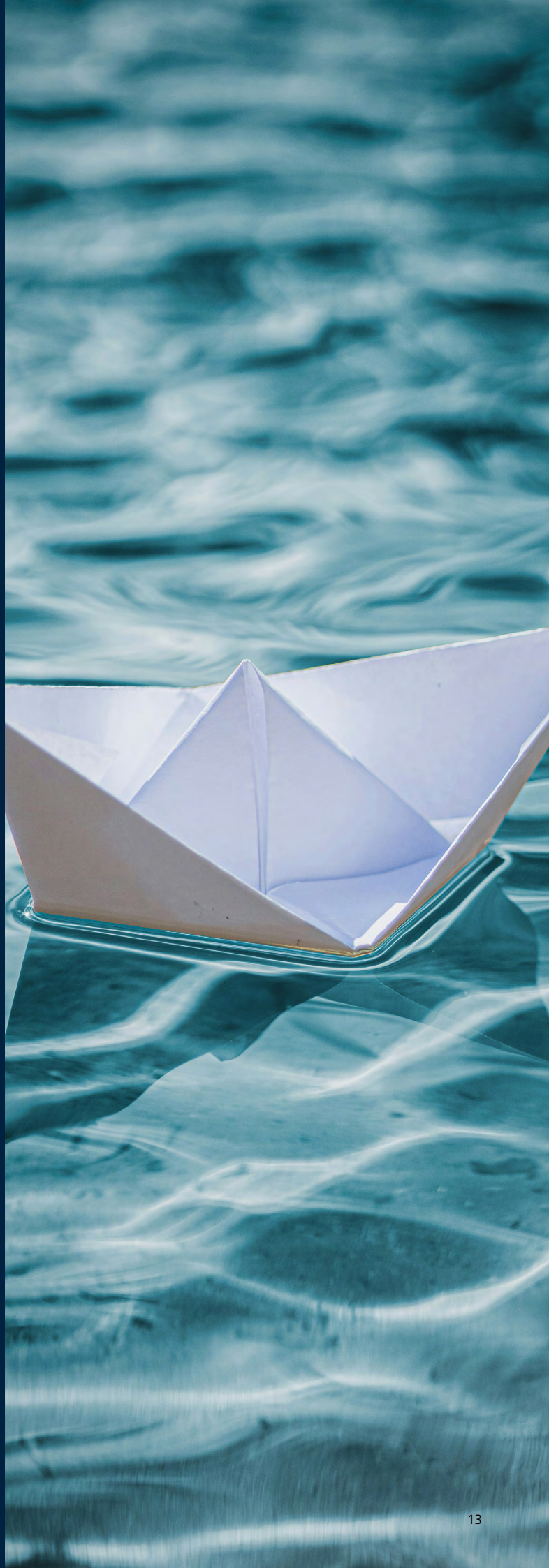
In summary

Accessibility is not only about design or technology. It concerns how the law is communicated and made effective.

In this context, the Legal Designer is:

- a legal information architect
- a facilitator of access to rights
- a bridge between rules, documents, and people

Without accessibility, the law remains theoretical. With Legal Design, it becomes truly usable.



Legal tech bytes

Expert insights on the latest trends and innovations

Author: *Tommaso Ricci*

Legal Engineering: new capabilities for in-house teams

In alignment with the ongoing evolution within legal operations, a new legal role has emerged to meet the changing needs of the profession. Rather than reducing the need for legal professionals, advancements in technology have highlighted the necessity for a different set of skills – specifically, those that can effectively bridge the gap between technological innovation and practical application. This emerging capability is now frequently referred to as **legal engineering**, and it is becoming increasingly essential for legal departments seeking to realize the full potential of modern legal technologies.

The implementation gap is real

The data tells a clear story. According to Clio's Legal Trends Report, AI adoption among lawyers jumped from 19% to 79% between 2023 and 2024. Yet the Thomson Reuters Generative AI in Professional Services Report 2025 indicates that only 20% of organizations currently measure ROI from their AI investments, while 59% conduct no measurement at all.

For in-house legal teams, this gap represents a significant risk. Budget holders expect demonstrable returns. Technology vendors promise transformation. But without the right capabilities to connect these two realities, legal departments find themselves with expensive tools that never quite deliver.

The missing element is not more powerful AI. It is the human capability to translate between legal practice and technological possibility.

What legal engineering means for in-house teams

Legal engineers analyze workflows to identify genuine bottlenecks, translate pain points into technical requirements, design automation solutions that respect legal complexity, and ensure that technology investments generate measurable returns rather than becoming expensive experiments.

For in-house counsel, this translates into concrete advantages. Contract lifecycle management implementations that actually reduce turnaround times. Matter management systems that lawyers use rather than work around. Self-service tools that genuinely deflect routine requests from the legal queue.

Why this capability has become essential

In-house legal teams face a unique set of pressures that make legal engineering capabilities particularly valuable.

Teams operate under constant scrutiny from business stakeholders who measure value in operational terms. When a technology initiative fails to deliver promised efficiency gains, the consequences are visible in budget discussions and headcount decisions.

You cannot simply scale headcount when workload increases. The pressure to do more with less makes effective technology integration essential rather than optional.

Your technology decisions have long-term consequences. In-house teams typically commit to platforms that shape workflows for years. Getting these decisions right the first time matters enormously.

As legal teams sit at the intersection of legal requirements and business operations this position creates unique opportunities to design technology solutions that serve both constituencies, but only if you have the capability to articulate requirements that neither pure technologists nor traditional lawyers would identify on their own.

How to assess your current capabilities

Before investing in new tools, in-house leaders should evaluate whether their teams possess the capabilities needed to implement them effectively.

Ask yourself these questions.

- When your last technology initiative underperformed, was the problem the tool itself or how it was integrated into existing workflows?

- Do your lawyers understand technology well enough to articulate what they actually need rather than what vendors tell them they need?
- Can your team distinguish between pain points that technology can solve and those that require process redesign?
- Do you have someone who can translate between IT requirements and legal workflows?

If these questions reveal gaps, you have identified a capability problem that no tool purchase will solve.

Three approaches to building legal engineering capability

Depending on your department's size and resources, consider these options.

- For **larger legal departments**, hiring dedicated legal engineers makes strategic sense. Look for candidates with genuine legal practice experience who have demonstrated interest in technology and process improvement. The best candidates are often mid-career lawyers who want to solve systemic problems rather than work around them.
- For **mid-sized teams**, developing existing talent may be more practical. Identify lawyers who show natural curiosity about technology and process. Invest in their development through training programs, conference attendance, and exposure to implementation projects. Create space in their workload for innovation work rather than treating it as an add-on to existing responsibilities.
- For **smaller departments**, accessing these capabilities through external relationships becomes essential. This might mean working with law firms that have developed legal engineering expertise, or negotiating vendor relationships that include genuine implementation support rather than just training sessions.

What to look for in external partners

If you choose to access legal engineering capabilities externally, evaluate potential partners carefully.

Do they have genuine legal practice experience? Can they demonstrate successful implementations in environments similar to yours? Do they approach engagements by understanding your workflows first, or do they lead with their preferred solutions? Will they help you build internal capabilities over time?

The best partners act as capability builders rather than permanent dependencies. They should leave your team stronger and more self-sufficient after each engagement.

Practical next steps

Start by mapping your current technology stack against actual usage patterns. Identify tools that have been purchased but underutilized. Understand why adoption failed. These failures often reveal capability gaps more clearly than success stories.

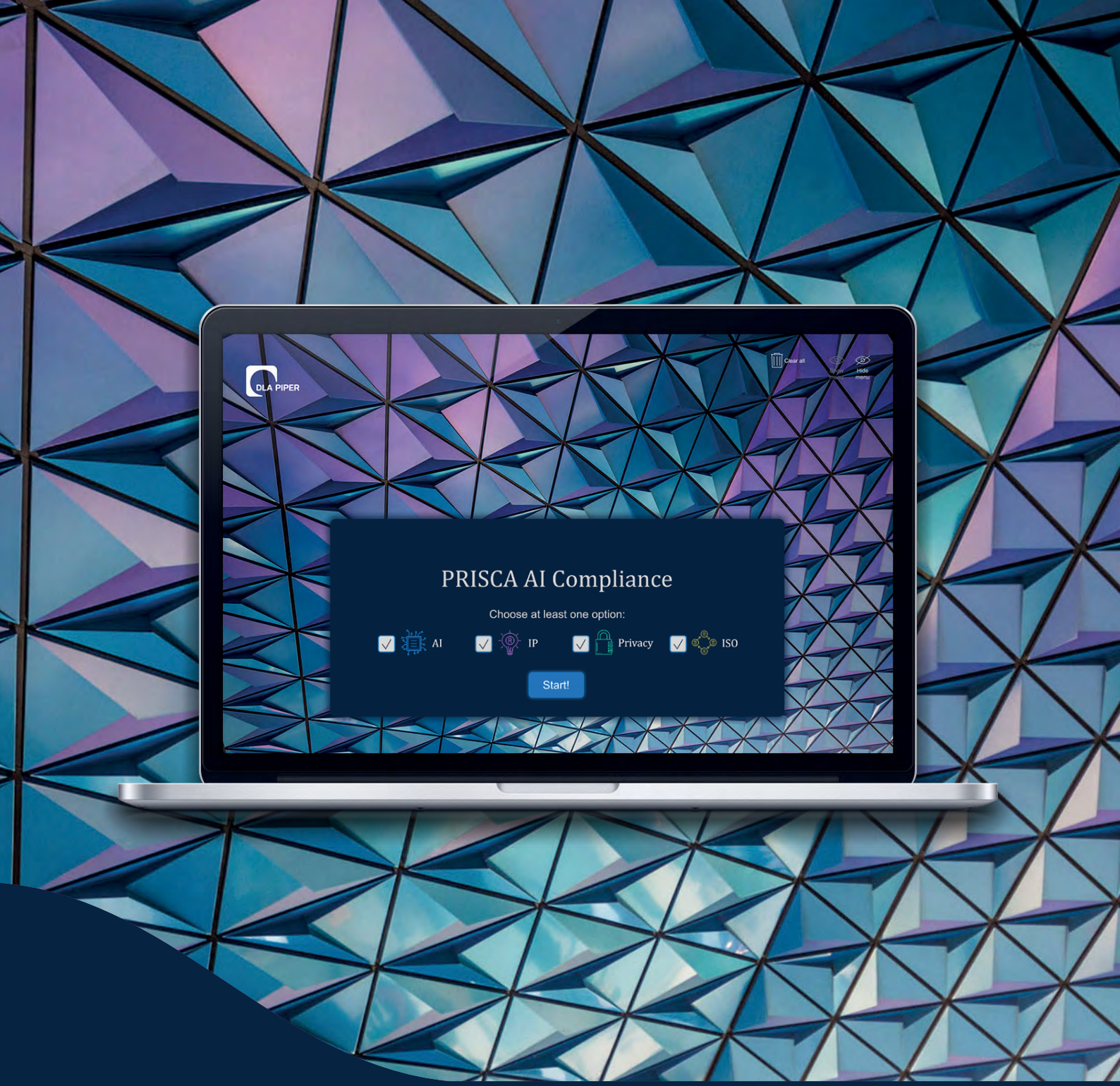
Next, assess your team's current capabilities honestly. Where do you have strength? Where are the gaps? Who shows potential for development?

Then determine which approach to building capability makes sense for your organization. Hiring, developing existing talent, or accessing external expertise each have different cost structures, timelines, and risk profiles.

Finally, start small. Choose one technology initiative where you can apply legal engineering thinking from the beginning. Use it as a proof of concept to demonstrate value before scaling.

For in-house counsel navigating budget pressures and rising expectations, developing these capabilities is the foundation for sustainable innovation.

Our team has developed methodologies specifically designed to help in-house legal departments assess their current capabilities and build effective technology implementation strategies. Contact us to discuss how we can support your team's development.

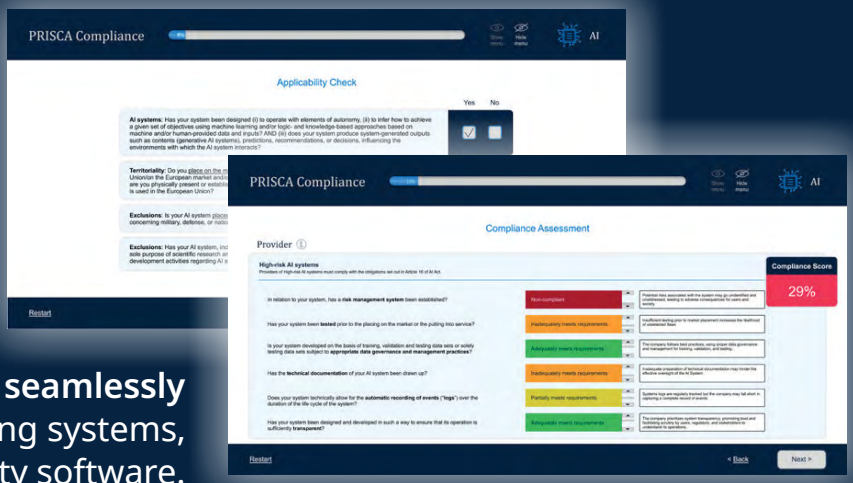


Prisca AI Compliance

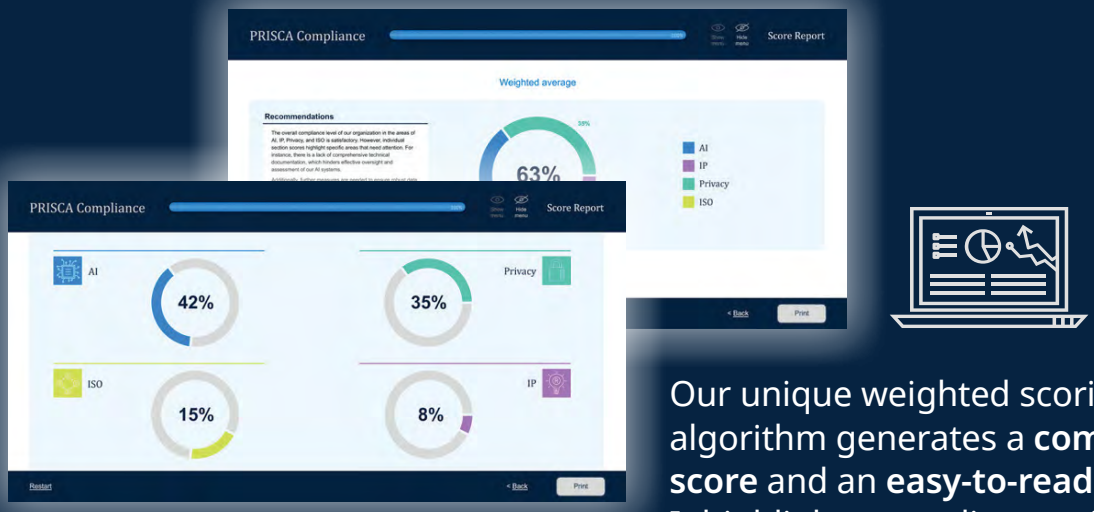
Empowering Legal Compliance in the Age of Artificial Intelligence

Is your business ready to embrace the opportunities of AI, but worried about legal risks?

Introducing PRISCA AI Compliance by DLA Piper lawyers, a cutting-edge tool to assess your AI solutions' compliance with laws and ISO standards.



PRISCA AI Compliance **seamlessly integrates** into your existing systems, with no need for third-party software. It's available in **English** for global use.



Our unique weighted scoring algorithm generates a **compliance score** and an **easy-to-read report**. It highlights compliance with laws (privacy, IP, AI) and ISO standards.

Whether you're a user, provider, importer, or distributor of AI solutions, PRISCA AI Compliance supports your operations in **complying with regulations**.

Scan the QR Code to watch the video

Contact us for a demo:

giulio.coraggio@dlapiper.com
alessandro.ferrari@dlapiper.com
gualtiero.dragotti@dlapiper.com
elena.varese@dlapiper.com

Scan this qr code to access all issues of Diritto Intelligente

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