ISSUE N.3 | NOVEMBER 2024

Diritto Intelligente

A JOURNAL ON AI-RELATED EU LAWS, CASES, AND OPINIONS BY DLA PIPER'S ITALIAN INTELLECTUAL PROPERTY AND TECHNOLOGY GROUP.

In this issue

DLA PIPER

Contents

Editorial

The European Union stands at a pivotal juncture where the advancement of artificial intelligence (AI) intersects with stringent privacy regulations.

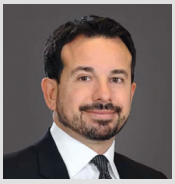
Some EU privacy authorities in the EU are increasingly advocating for explicit consent as the primary legal basis for processing personal data in AI training. While the protection of individual privacy is undeniably essential, making consent the sole avenue could inadvertently stifle innovation. AI systems thrive on diverse and extensive datasets to learn, adapt, and improve. Requiring consent from every individual whose data might be used is not only logistically daunting but could also render many AI projects unfeasible.

The crux of the matter lies in finding a balance between safeguarding personal data and fostering an environment where AI can flourish and the limits in which legitimate interest can be used as legal basis. If the EU adopts a rigid stance on consent, it risks isolating itself in the global AI arena. Competitors like the United States and China, with more flexible data policies, may surge ahead, leaving Europe trailing in technological advancements.

Moreover, the implications extend beyond economic competitiveness. AI has the potential to revolutionize healthcare, transportation, and environmental sustainability – sectors where Europe has much to gain. Overly restrictive data policies could hinder breakthroughs that benefit society at large.

It is imperative for policymakers to consider alternative legal bases provided within the GDPR, such as legitimate interest or public interest (that however requires a law maintaining it) exceptions, which could allow for responsible AI development without compromising individual rights. Establishing clear guidelines and robust oversight mechanisms can ensure that AI technologies are developed ethically and transparently.

The EU must navigate this crossroads with foresight. By fostering a regulatory environment that both respects privacy and encourages innovation, the European Union can position itself as a leader in ethical AI development. The decisions made today will shape not only the future of AI in Europe but also its role in the global digital landscape.



Giulio Coraggio
Partner
Head of Intellectual Property and Technology
Italy

Opting out of training AI with copyrighted material is not unlimited

Author: *Carolina Battistella*

The Hamburg District Court has limited the opt-out by copyright holders to the use of content for AI training.

On 27 September 2024, the District Court of Hamburg issued a significant ruling regarding copyright and the use of AI in a case involving professional photographer Robert Kneschke and the non-profit organization LAION (Large-scale Artificial Intelligence Open Network). Kneschke accused LAION of copyright infringement, asserting that the organization reproduced one of his photographs without authorization to create a dataset for training generative AI systems.

The case concerning the use of copyright-protected content for AI training

LAION developed an open-access dataset for training AI systems, which collects nearly six billion hyperlinks to publicly accessible images, accompanied by their respective textual descriptions. To create the dataset, LAION downloaded images from online archives and used software to verify that the descriptions in the source dataset corresponded to the visual content. Images that didn't match the descriptions were filtered, while those that did were included in the dataset along with relevant metadata, such as URLs and descriptions. To conduct this analysis and verify the text-image correspondence, LAION had to temporarily store the images.

The dispute arose when Kneschke claimed that LAION violated his copyright by using one of his photographs without authorization during the dataset creation process. The image in question was analysed by LAION and subsequently included in its dataset. The photograph was downloaded from the website of a photography agency with which Kneschke collaborated, and it bore the agency's watermark. Furthermore, the agency's terms of service explicitly state that users may not "use automated programs, applets, bots or the like to access the website or any content thereon for any purpose, including, by way of example only, downloading content, indexing, scraping or caching any content on the website."

Consequently, Kneschke filed a complaint against LAION, alleging copyright infringement for the unauthorized reproduction of his photograph during the dataset creation. He argued that this reproduction did not fall within the exceptions outlined in Sections 44a, 44b, and 60d of the German Copyright Act (UrhG).

In its defence, LAION contended that its actions fell within the scope of the text and data mining (TDM) exception for scientific research purposes, as provided by Article 60d of the UrhG. LAION further asserted that the use of the contested image was only temporary, as it was deleted immediately after analysis and not stored permanently. Additionally, LAION clarified that the created dataset did not contain graphic reproductions of the photographs but merely links to the images available online, so they claimed not to have violated Kneschke's copyright.

The Hamburg court's decision on the use of AI for training purposes

The District Court of Hamburg dismissed Kneschke's complaint and accepted LAION's defences, establishing that the reproduction of images for content analysis and its corresponding textual description should be distinguished from use for training AI systems. According to the German court, LAION's creation of a free dataset falls under the TDM exception for scientific research as outlined in Article 3 of the Copyright Directive and Article 60d of the UrhG.

The text and data mining exception for scientific research purposes

The court held that the reproduction of an image for the creation of a dataset intended for training AI systems qualifies under the text and data mining (TDM) exception for scientific research purposes. It noted that "scientific research generally refers to methodical and systematic pursuit of new knowledge. [...] the concept of scientific research does not presuppose any subsequent research success. [...] the creation of a data set of the type at issue, which can form the basis for the training of AI systems, can certainly be regarded as scientific research."

To affirm the absence of commercial purpose, the German court also pointed out that the dataset was made freely and publicly available. The fact that the dataset could be use by for-profit companies for training or further developing their AI systems is irrelevant to the classification of LAION's activities, as research conducted by for-profit entities is still considered research activity, contributing to the advancement of knowledge. The court further clarified that any existing relationships between LAION and commercial companies in the AI sector don't imply that such companies exert significant influence over LAION's activities. Moreover, the court noted that it was not demonstrated that LAION provided privileged access to its research findings to these companies, circumstances that could have hindered the invocation of the exception under Article 60d of the UrhG.

The "opt-out" mechanism to use data for AI training

The court based its decision primarily on Article 60b of the UrhG, considering that LAION's activities fall within the TDM exception for scientific purposes. Consequently, it limited its discussion of the opt-out issue to an *obiter dictum*. The court stated that expressing an opt-out in simple language, such as plain letters, is sufficient for rights holders to communicate their reservations. Furthermore, it established that the opt-out need not be formulated in a machine-readable format, like robots.txt files, as current technologies, including AI-based systems, should be capable of interpreting human language. So it's sufficient for the reservation to be expressed in a "machine understandable" format. But the court clarified that this is not a general rule and that each case must be evaluated based on the prevailing technological advancements at the time.

This approach introduces new challenges for businesses in the AI sector: if opt-outs articulated in natural language are considered "machine readable," data aggregators will need to deploy AI systems with natural language processing capabilities to identify and interpret such reservations. The court seems to suggest that the burden of error in searching for opt-outs in natural language should be borne by AI enterprises, given the absence of a standard TDM protocol for reservations on the web.

Temporary use of images for training purposes

Regarding LAION's defence that the images were used only "temporarily," the Hamburg Court rejected this argument, finding that the reproduction performed by the defendant could not be deemed "transient" or "incidental." The image files were downloaded and analysed intentionally and consciously, indicating that the download process was not merely an ancillary step in the analysis but rather a deliberate and controlled acquisition by LAION. Consequently, the court ruled out LAION's possibility to invoke the exception outlined in Article 44b of the UrhG in this case.

What would have been the outcome of the dispute in Italy?

If the case had been decided in Italy, the decision would probably not have been different from the one adopted by the District Court of Hamburg. Art. 70-ter of the Italian copyright law, implementing Article 3 of the Copyright Directive, allows the extraction of text and data for scientific research purposes. The provision states that research organisations include universities, institutes and other entities with research purposes. This notion doesn't require that scientific research be the only "statutory" objective of the entity, but it's sufficient that it be the main one: and is therefore compatible with the carrying out of entrepreneurial activities on *the side of* scientific research.

Article 70-ter stipulates that an entity cannot be considered a "research organisation" if it's subject to decisive influence from commercial enterprises that grants them preferential access to the results of the research. Such influence is compatible with the status of research organisation for a subsidiary, provided that the preferential access to the results of the research is excluded. So, under Italian law, even commercial companies can qualify as research organisations, if they meet the requirements of Article 70-ter.

In light of the above, an Italian court would have probably considered LAION's activity to be compliant with copyright law, since it's oriented towards scientific research and doesn't pursue commercial purposes.

Conclusion

The Hamburg Court's decision is well-reasoned and reflects the complexities of balancing intellectual property rights with the advancement of AI technology. The court thoroughly evaluated the applicability of various copyright exceptions, ultimately siding with the interests of scientific research. This ruling underscores the challenges that traditional copyright law faces in the age of AI, where mass data collection and analysis are essential for technological development.

But some aspects of the ruling leave questions unanswered, particularly regarding the adequacy of the opt-out mechanism for online content and how the exercise of reservations should be treated within the context of data mining for AI.

Big tech and the AI pact: the future of European AI regulation

Author: *Edoardo Bardelli*

On September 25, 2024, the European Commission announced that over 100 companies had signed the AI Pact, a voluntary agreement aimed at enhancing the governance of artificial intelligence. Notably absent were Meta and other major tech firms, who, just days earlier, had published an open letter expressing concerns about the potential risks to innovation posed by the EU's regulatory approach to AI. What does the future hold for artificial intelligence in the EU?

AI Act and AI Pact

On August 1, 2024, Regulation (EU) 2024/1689, which establishes harmonized rules on artificial intelligence (known as the AI Act), came into force. However, many of the Regulation's obligations—particularly those related to so-called "high-risk" AI systems—are set to be implemented at a later date. This phased approach is intended to give entities within the Regulation's scope time to better structure their AI governance policies and comply with all applicable obligations.

To support organizations during this critical transition, the European Commission launched an initiative in early 2024 aimed at preparing the ground for the full implementation of the AI Act's requirements. This initiative took shape in the form of the AI Pact, a voluntary agreement that companies can sign to commit to responsible practices in the development, management, and use of AI.

The primary goal of the AI Pact is to foster regulatory harmonization between Member States and organizations, creating an environment of trust and collaboration while paving the way for the application of the AI Act in line with its principles.

The AI Pact

The AI Pact is structured around two main pillars.

The first pillar is titled "Gathering and Exchanging with AI Pact Network." The main objective of this pillar is to create a network among the companies that have signed the pact, encouraging the exchange of information and best practices. For instance, signatories are encouraged to collaborate and share insights on strategies and steps taken to ensure compliance with the AI Act.

A key role in this regard is assigned to the European AI Office, which is tasked with creating working and training groups and providing practical training to support the implementation of the Regulation's requirements. In this spirit of full cooperation, signatories are invited to share their strategies for compliance with the Regulation with other pact members. To facilitate this exchange, the European AI Office is also responsible for creating an online platform accessible to the signatories.

While the first pillar focuses on shared consultation, the second pillar aims to provide tools for the direct implementation of the AI Act's requirements. Titled "Facilitating and Communicating Corporate Pledges," the second pillar invites companies to take on concrete commitments, representing specific actions they have taken (or plan to take) to comply with the Regulation. These actions cover a range of activities required by the Regulation, such as implementing security measures, regularizing relationships with AI supply chain partners through appropriate contractual templates, and preparing relevant documentation, including internal policies and materials concerning copyright compliance.

The first three pledges outlined by the Pact are particularly noteworthy:

1. **Adopting an AI Governance Strategy** aimed at promoting AI within the organization and ensuring future compliance with the Regulation;
2. **Identifying and mapping AI systems** that may be classified as high-risk;
3. **Promoting AI awareness and literacy** among staff to ensure the ethical and responsible development of this technology.

These are certainly challenging commitments for companies, which must prepare the necessary documentation and strive to create genuine AI awareness within their organizations. This involves using effective tools and techniques to promote a practical understanding of AI and how it should be managed.

Additionally, the call to begin mapping AI systems now underscores the need for legal and technical expertise to accurately identify all the requirements set out in the Regulation, thus enabling better planning of the activities needed before all obligations under the AI Act come into effect.

Signatories and critics

To date, over 100 companies have signed the AI Pact and committed to its proposed actions. Among them are small and medium-sized enterprises as well as tech giants such as Amazon, Google, Hewlett Packard, Microsoft, and OpenAI.

It is not surprising that Meta is not among the signatories. Recently, the company, along with other organizations – some of which are key players in the tech market like Spotify and Ericsson – issued an open letter with a title that leaves no room for doubt: "Europe needs regulatory certainty on AI: fragmented regulation means the EU risks missing out on the AI era."

The near future will reveal who - the signatories or the critics – was right about the impact of European AI regulation. However, regardless of one's stance on European legislative policies, it is clear that AI management – part of which involves compliance with the AI Act – cannot be ignored. In this context, the signatories of the AI Pact are charting a path that, in a spirit of synergy, seems capable of facilitating ethical, conscious, and compliant AI governance.

AI and GDPR: ECJ AG on balancing automated decision disclosure and trade secrets

Author: *Giulio Coraggio*

The recent European Court of Justice (ECJ) Advocate General's opinion in case C-203/22 is an important development in addressing how companies using artificial intelligence (AI) can balance automated decision transparency with the protection of trade secrets, while complying with the requirements of the GDPR.

The GDPR case on automated decision and its relevance to AI

In the case at hand, an Austrian citizen was denied a mobile phone contract following an automated credit check conducted by a company. The decision was fully automated, with no human intervention. The individual sought to understand how her personal data was processed and the logic behind the automated decision that affected her. However, the company refused to disclose critical details, citing its algorithm as a protected trade secret under Directive (EU) 2016/943.

The CJEU's involvement drew attention to two key issues:

1. **Transparency under GDPR:** How much detail about AI-driven decisions must companies disclose to data subjects?
2. **Protection of trade secrets:** Can companies refuse to disclose details of their AI algorithms by invoking trade secret protection?

The opinion of the Advocate General provides important guidance on how these issues intersect and impact the development and deployment of AI technologies.

AI and GDPR: The Right to Transparency

Under Article 22 of the GDPR, individuals have the right not to be subject to decisions based solely on automated processing, including profiling, where those decisions have legal or significant personal implications. This provision is particularly relevant for AI systems, which often make autonomous decisions without human oversight. In addition, Article 15(1)(h) of the GDPR grants individuals the right to "*meaningful information*" about the logic behind the automated decision (such as an AI decision) that affected them.

For AI developers, this means that transparency is not optional; individuals must be given enough information to understand how their personal data is processed and how AI-driven decisions are made. **The opinion clarified that this doesn't necessarily mean disclosing all the technical details of an algorithm**, but rather providing clear and understandable information about

- The **main factors** that influenced the ECJ's AG opinion
- The **weight** of those factors.
- The **outcome** of the decision.

For example, if an AI system evaluates creditworthiness, the company should explain what types of data (such as income or payment history) were used, how those factors were weighted, and how they led to the final decision. This explanation must be accessible and clear enough for the average person to understand.

The role of trade secrets in AI

Many companies using AI view their algorithms as proprietary trade secrets that give them a competitive advantage. The ECJ Advocate General's opinion recognized the importance of protecting trade secrets, but emphasized that trade secrets cannot be used as an all-encompassing shield to avoid transparency obligations under the GDPR.

Instead, the AG suggested that companies must strike a balance:

- Companies should provide **general explanations of how their AI systems work** without disclosing detailed, proprietary algorithms.
- Regulators or courts can **step in to ensure that companies provide sufficient transparency**, while protecting intellectual property.

This sets a precedent for AI developers, signaling that while trade secret protection remains important, it cannot override the rights of individuals to understand how AI-driven decisions are made about them.

Implications for AI development and deployment

The CJEU Advocate General's opinion has significant implications for businesses and industries that rely on AI for decision-making, particularly in areas such as finance, healthcare, insurance, and recruitment, where AI is often used to make decisions with significant personal impact.

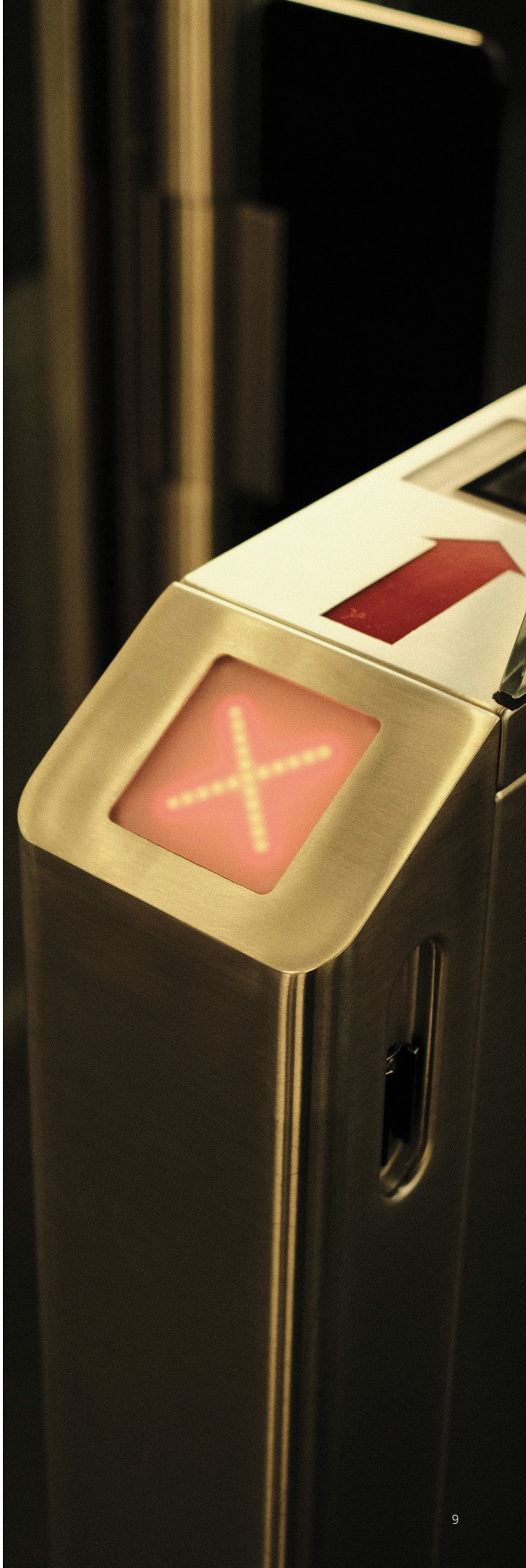
Key takeaways include:

1. **Explainable AI is non-negotiable:** Organizations must ensure that their AI systems are not only accurate, but also **explainable**. Individuals affected by AI decisions have a right to clear explanations, and companies must be prepared to provide them.
2. **Balance innovation with compliance:** AI developers need to be strategic in protecting their trade secrets, while ensuring compliance with transparency obligations under GDPR. They must focus on a **high level of transparency** – disclosing enough for individuals to understand decisions, without revealing the inner workings of their proprietary systems.
3. **Building trust in AI:** This ruling reinforces the idea that transparency is key to building trust in AI systems. Individuals are more likely to trust AI-driven decisions if they can understand how their data is being used and how decisions are being made.
4. **Regulatory oversight:** The involvement of regulators in the event of disputes is likely to become more common. As AI systems become more complex, courts may increasingly serve as arbiter in balancing transparency and the protection of trade secrets.

The future of AI and privacy

As AI continues to evolve and play a central role in decision making, ensuring compliance with the GDPR will be critical for businesses. The ECJ Advocate General's opinion in case C-203/22 provides valuable guidance on how companies can achieve this balance. Organizations must prioritize creating AI systems that are not only powerful and efficient, but also transparent, fair, and respectful of individual rights.

This obligation is further amplified by the obligations arising under the EU AI Act that are based on the same principles of transparency and human oversight.



AI and privacy: the DPAs' view on children and AI and trustworthy AI

Author: *Roxana Smeria*

From 9 to 11 October 2024, the fourth edition of the G7 Data Protection Authorities (DPA) Roundtable took place in Rome. Among the key issues discussed was AI and its impact on privacy, particularly in relation to building trustworthy AI systems and protecting children in the context of AI technologies.

The Roundtable was hosted by the Italian DPA. The event brought together privacy regulators from Canada, France, Germany, Japan, the UK, the US, and representatives from the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS). Below we outline the main points.

Trustworthy AI

One of the central themes of the event was trustworthy AI. The DPAs published a statement on trustworthy AI, in which they acknowledged that AI technologies are being deployed across all sectors of society, presenting multiple opportunities. However, these same technologies also pose significant challenges, particularly in terms of privacy, data protection, and other fundamental rights.

In their statement on trustworthy AI, the DPAs expressed concern about the potential harms posed by AI, especially in cases where personal data is processed. They noted that many AI systems, including those using generative AI models, depend on vast amounts of data, which can lead to risks such as stereotyping, bias, and discrimination, even if they're not directly using personal data. These issues can, in turn, affect larger societal trends, particularly in the form of deep fakes or disinformation.

The DPAs also underscored that it's critical to embed data protection principles into AI systems from the outset, applying the principle of privacy by design. This means that AI technologies should be built with data protection considerations in mind, ensuring that privacy is safeguarded at every stage of development and use.

AI and children

Another major focus of the Roundtable was the protection of children in the digital age, particularly in relation to AI-driven tools. The DPAs published a statement on AI and children in which they recognized that while AI offers significant opportunities for children and young people, these technologies can also expose them to heightened risks due to their developmental stage and limited understanding of digital privacy.

Several key issues related to AI and children were identified:

- **AI-based decision-making:** the complexity and lack of transparency in AI systems can make it difficult for children and their caregivers to understand how decisions are made, especially when these decisions have significant implications. Without adequate transparency, there is a risk of unintentional discrimination or bias, especially when children are involved in AI-based decision-making processes.
- **Manipulation and deception:** AI tools can be used to subtly influence users, pushing them to make decisions that may not be in their best interest. This can be particularly dangerous for children, who may struggle to recognize manipulative content. AI-powered technologies,

such as virtual companions or toys, could lead children to form emotional connections with machines, potentially causing them to share sensitive information or make decisions that expose them to risks. Specific examples include:

  - AI in toys and AI companions: children may develop emotional bonds with AI-enhanced toys or online companions, making them more vulnerable and lead them to disclose sensitive personal information or to be otherwise manipulated.
  - Deep fakes: young people are particularly at risk of being targeted by deep-fake content, which can include inappropriate or even harmful imagery of themselves.

- **Training AI models:** AI models often require large datasets to function effectively. The use of children's personal data to train these models, including when data is scraped from publicly available sources, raises concerns about privacy violations and long-term harm.

In light of these risks, the DPAs issued a series of recommendations to mitigate potential harms to children and ensure that AI systems respect their rights:

- AI technologies should be guided by the "privacy by design" principle.
- AI systems should include mechanisms to prevent online addiction, manipulation, and discrimination, especially when these systems are likely to affect children.
- Children must be protected from harmful commercial exploitation through AI.
- AI models affecting children should prioritize their best interests, both in terms of data collection and processing, and in the system's outputs.
- Data Protection Impact Assessments (DPIA) should be conducted to evaluate risks associated with AI systems involving children.
- AI models should respect the transparency principle and provide explainable results, allowing young users and their caregivers to make informed decisions about how their data is used.

Conclusions

It's no surprise that DPAs around the world are increasingly focusing on AI, given the profound implications it has for privacy. The G7 DPA Roundtable reinforced the critical link between AI and privacy, emphasizing that as AI technologies rapidly advance and become deeply woven into the fabric of everyday life, the need to prioritize privacy safeguards becomes more urgent. Companies developing AI tools should embed privacy and data protection principles into the heart of AI development to ensure the ethical, transparent, and fair use of these technologies across society.

Complementary impact assessment on the proposed AI liability directive published: the possible changes

Author: *Federico Toscani*

On 19 September 2024, the Complementary Impact Assessment (the "**Study**") on the proposed directive on adapting non-contractual civil liability rules to artificial intelligence ("**AILD**") was published. Commissioned by the Committee on Legal Affairs of the European Parliament, the Study aims to identify possible gaps and problems in the proposed legislation, as well as to respond to alleged incompleteness in the impact assessment conducted by the European Commission.

The AILD, together with the revision of the Product Liability Directive ("**PLD**"), is the main instrument to address liability arising from the use of AI. In particular, the AILD aims to harmonise the procedural aspects of AI-related claims brought before the courts of the Member States. A critical point is the simplification of the burden of proof, which is particularly complex due to the opacity of AI systems (the so-called "Black Box" problem). To address this challenge, the legislation provides, in specific cases, for the right of the injured party to obtain *disclosure* of evidence and documents relevant to the understanding of the functioning of the system, as well as a presumption of causation in the case of damage resulting from a use of AI not compliant with the provisions of the AI Act.

Interaction between AILD, PLD and the AI Act

The Study examines how the AILD interacts with other regulatory instruments on product liability and AI. In particular, it recommends to:

- Align key definitions to ensure consistency of terminology between the AILD and the AI Act to avoid ambiguity in interpretation; and
- Ensure the application of the AILD to those cases (e.g. discrimination, personal rights, damage caused by non-professional users) that fall outside the scope of the PLD.

Scope of application

The Study also suggests that the scope of the AILD should be extended beyond high-risk AI systems, to include systems that are defined as "high impact" such as *General Purpose AI* (e.g. ChatGPT) and *software* that, although not properly classified as AI systems, present similar problem of transparency and opacity as "pure" AI systems, transforming the AILD into what is defined in the Study as a "*software liability instrument*". This approach is reasonable, since in the presence of the same challenges to the traditional liability system, it would not make sense to make a distinction based on a mere technological difference, since the same rules would have to be applied to all those systems that, regardless of their qualification, pose the aforementioned problems of opacity and transparency.

Strict liability and negligence

The Study highlights the consequences of classifying liability as strict and negligent.

With regard to strict liability, which was originally envisaged by the European Parliament Resolution of 2020 for high-risk AI systems, it is confirmed as a possible solution in the case of prohibited/high-risk systems, as the protection of the public takes precedence over the stifling effect it would have on innovation. At the same time, it emphasizes the difference between "*legitimate-harm models*", which could have an adverse effect on a subject even if correctly used (e.g. scoring systems), and "*illegitimate-harm models*", which could under no circumstances cause harm if used correctly and calls for a strict liability regime only for the latter.

On the other hand, regarding negligent liability and the AIDL's systems for reducing the burden of proof, the Study emphasizes that:

- The duty of disclosure may be of little practical use given the highly technical nature of the documents covered by it. In addition, it is unclear how the requirement that the plaintiff must provide evidence to prove the plausibility of its claim will be addressed, or whether the presumption will apply in the case of a breach of the duty to provide AI training (so-called AI literacy), for example where an inadequately trained employee causes damage; and
- The presumption of causation is difficult to activate, since to obtain it, the plaintiff would still have to prove, among other things, the fault of the damaging party and the damage itself.

In any case, while acknowledging the limitations inherent in the proposal, the Study does not go as far as to propose a presumption of fault that would have disruptive effects on innovation in the Union.

From directive to regulation?

Finally, the Study considers the appropriateness of changing the AILD from a directive to a regulation. This change, which has already been initiated and consolidated in other areas, would ensure uniform application of the rules throughout the EU and avoid the discrepancies that would result from national transposition of the directive. This is particularly true given that the AILD aims for a minimum level of harmonization, leaving room for implementation to the Member States, which could then introduce more specific rules. Even in the presence of the AI Act, one would thus be exposed to possible differences in treatment in terms of civil liability.

Conclusions

The Study underlines the importance of a clear, coherent and effective liability framework for AI to provide operators with a uniform regime throughout the European Union and citizens with effective redress in the event of damage caused by AI. In this sense, the observations contained in the Study are an important starting point for the development of the directive, which is currently on hold after having been proposed almost two years ago. Indeed, if the proposal to adopt a regulation were to be followed, there would be a real risk that it would be withdrawn.

Has your organization implemented an AI governance model?

Author: *Giulio Coraggio*

It's become increasingly clear that the intersection of AI and governance is pivotal for organizations looking to use the power of AI while mitigating associated risks.

The rapid evolution of AI, coupled with stringent regulatory frameworks such as the EU AI Act, necessitates a structured and comprehensive approach to AI governance.

1. AI strategy and core principles

Effective AI governance begins with a clearly defined strategy set by senior leadership. This top-down approach ensures that AI use aligns with the company's broader vision, focusing on core principles such as ethical usage, trust, and compliance with regulatory standards. Legal and risk management teams are then tasked with developing policies, controls, and frameworks to operationalize this strategy.

2. AI internal stakeholders and committees

To execute AI governance at the tactical level, organizations have to establish dedicated AI governance committees. These committees, often comprising legal, IT, compliance, data, and cybersecurity experts, should be responsible

for overseeing AI-related risks. Reporting to the senior management, this body plays a crucial role in policy approvals, vendor management, and integrating AI into existing risk structures. At the moment, this solution is preferable to appointing a single AI Officer, who might not have all the competencies to address AI compliance.

3. Identifying use cases under EU rules

A fundamental aspect of AI governance is identifying which AI use cases fall under regulatory scrutiny. Given the broad legal definitions in the EU AI Act, even seemingly benign systems might be classified as AI. Organizations have to carefully assess their AI systems, especially those that cross borders, as they might still fall under the purview of EU regulations.

4. Risk identification and categorization

Once AI use cases are mapped, organizations have to categorize them based on risk levels – whether prohibited, high risk, or general-purpose AI. A proactive approach is essential, as risks could range from reputational damage to legal exposure, particularly in contexts like HR and credit checks, which the EU AI Act may deem high risk.

5. Implementing controls

For each identified use case, controls should be put in place to mitigate risks. These could include human oversight, bias assessments, and robust technical measures to secure systems. High-risk AI systems must comply with statutory requirements, and organizations should also focus on vendor protections through contracts to ensure compliance across the board.

Finally, given the ever-changing nature of AI and the law, governance processes must be continuously updated. Committees should stay informed of legal and technological developments, ensuring that previously approved systems remain compliant as they evolve. The organizations that invest in solid AI governance stand to gain the most from AI's capabilities, enjoying a measurable return on investment.

For organizations looking to integrate AI into their operations, a proactive approach to governance is no longer optional – it's essential. By understanding and implementing a strong governance framework, companies can mitigate risks and position themselves to fully benefit from the opportunities AI presents.

For more on this topic, read the October issue of our AI law journal and the presentation of our AI compliance tool.

Legal design tricks

LITTLE TIPS TO USE LEGAL DESIGN IN YOUR DAILY ACTIVITIES

Trick #2: How to incorporate legal design in your work?

Author: *Deborah Paracchini*

Let's adopt (Legal) Design Thinking!

Legal design merges the principles of design thinking with law to make legal information more accessible, clear, and engaging for users.

How to apply design thinking?

Design thinking follows a five-step process:

1. **Empathize** with your users
2. **Define** the problem
3. **Ideate** solutions
4. **Prototype**
5. **Test** your idea

Why design thinking?

Design thinking is a **human-centered approach** to problem-solving. It emphasizes understanding user needs, **improving user experience, fostering creativity, and encouraging collaboration** to develop innovative solutions.

Ask yourself the key questions!

In your daily work, always consider:

- Who is this for, and what do they need?
- What are you trying to achieve?
- What constraints should you keep in mind?
- How can you simplify the legal information?
- How can you we gather feedback from users?

Did you know?

Legal design is **not a one-time fix**. It's an **ongoing cycle** of testing, feedback, and improvement to meet evolving user needs.

Find new tips every month on Diritto Intelligente or check our monthly posts at dirittoaldigitale.com

Legal tech bytes

EXPERT INSIGHTS ON THE LATEST TRENDS AND INNOVATIONS

Navigating the evolution of Legal AI Agents and market maturity

Author: *Tommaso Ricci*

The legal technology landscape is witnessing a remarkable transformation, with AI agents emerging as the dominant force shaping the industry's future. This trend has become increasingly evident through recent market developments, where we're seeing a steady stream of announcements introducing new agent-based features and solutions. These observations were strongly reinforced during my participation at the 2024 Legal Geek Conference in London, which once again proved its position as the premier global gathering for legal innovation, drawing an impressive array of professionals, providers, and thought leaders from across the legal technology landscape.

The rise of AI agents has been nothing short of remarkable, marking a significant evolution from the initial generative AI wave. The conference's exhibit hall served as a compelling showcase of this trend, with numerous vendors presenting sophisticated agent-based solutions. However, much like the early debates surrounding generative AI, the industry is grappling with defining what truly constitutes an "agent" and which solutions genuinely qualify as agentic AI.

The market dynamics have notably matured since the initial AI proof-of-concept phase. Organizations are moving beyond the "AI FOMO" (Fear of Missing Out) that characterized early adoption patterns. Instead, we're observing a strategic pivot toward implementations that deliver demonstrable ROI. This shift reflects a more sophisticated understanding of AI's role in legal operations, with corporations increasingly demanding solutions that offer tangible efficiency gains and measurable business impact.

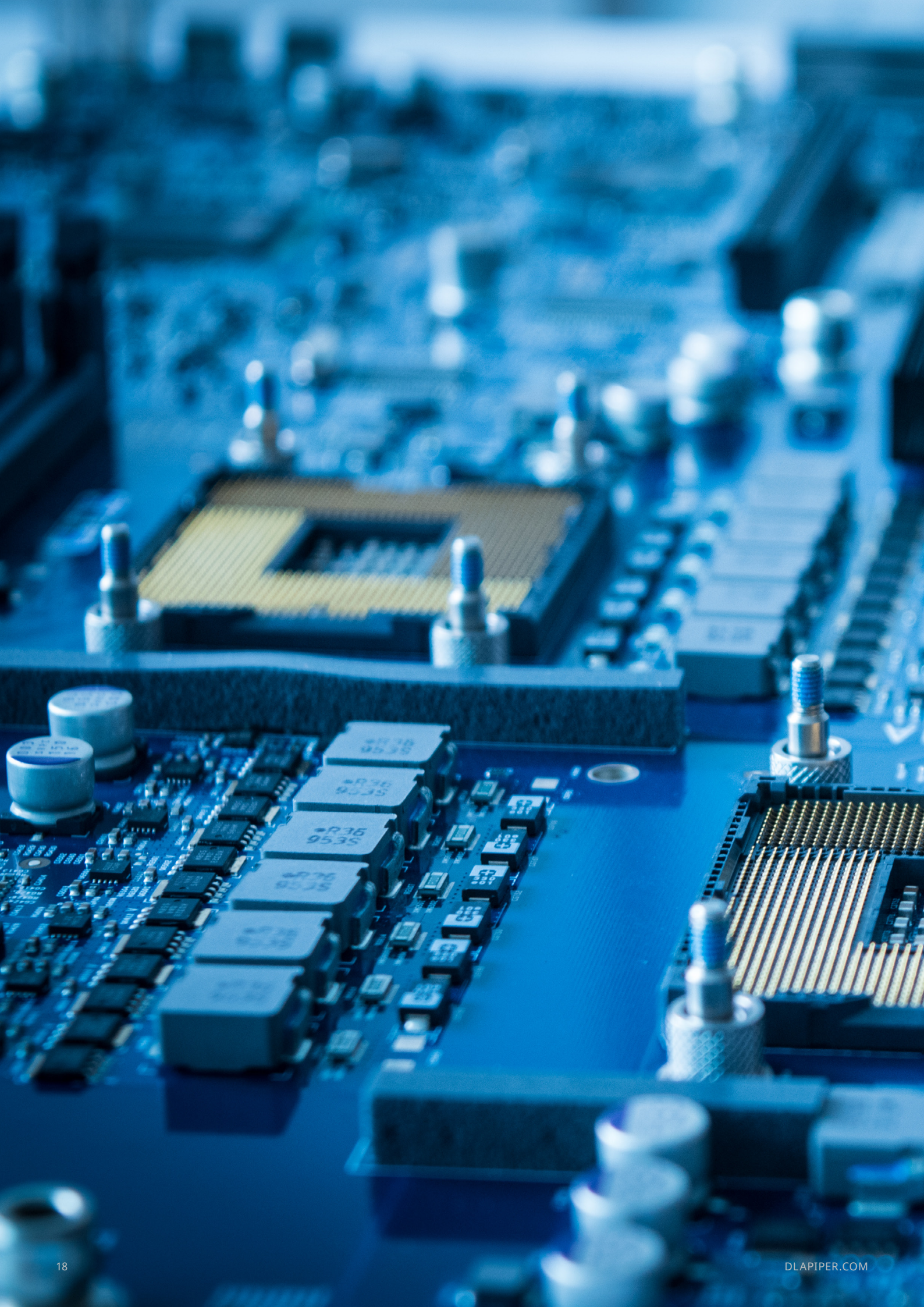
Legal tech investment patterns mirror this maturation, with funding now flowing predominantly to solutions that demonstrate clear value propositions.

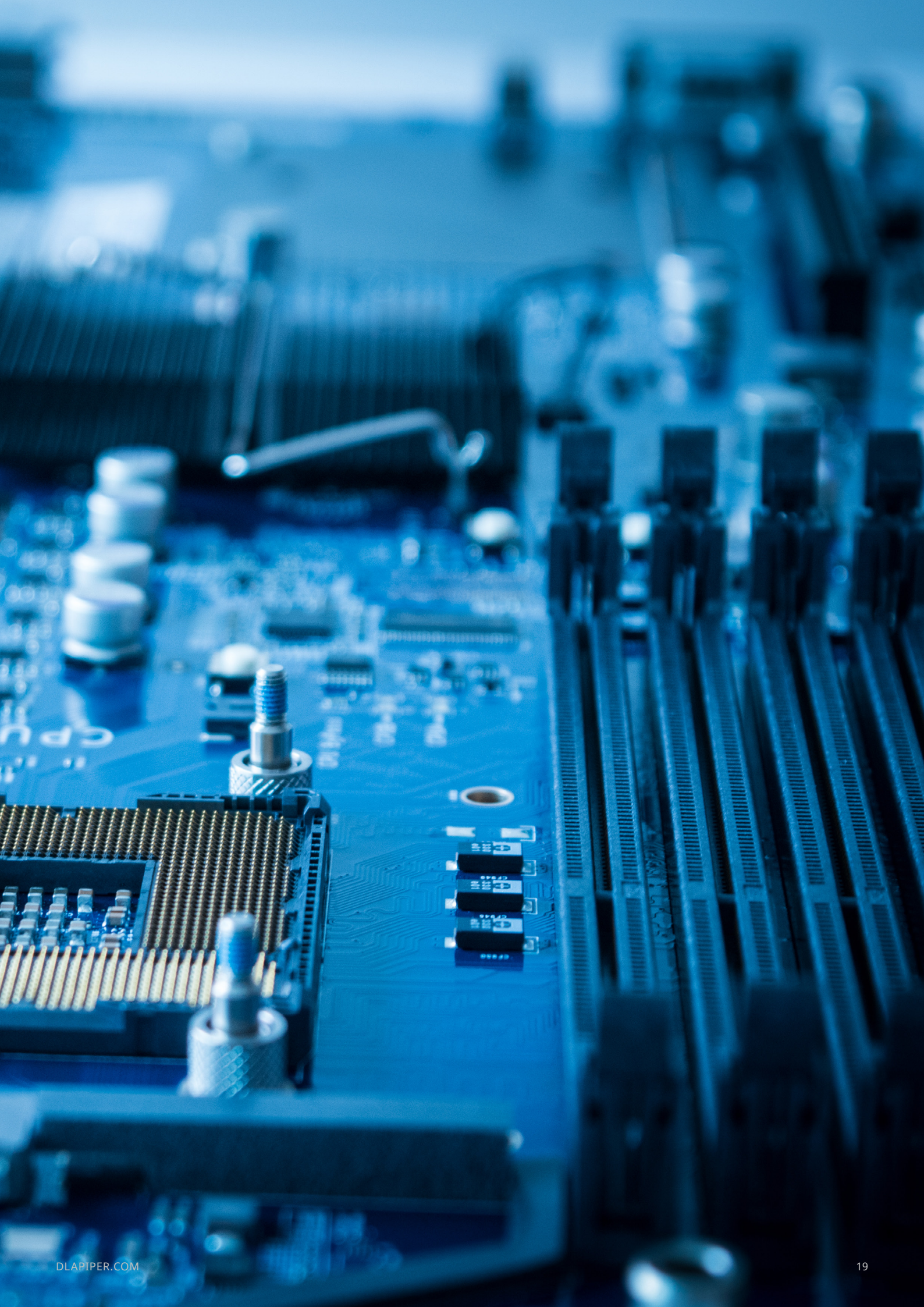
At DLA Piper in Italy, we're actively guiding corporations through this evolved landscape. Our approach focuses on:

- **Strategic assessment of AI agent implementation opportunities**, verifying whether a solution effectively addresses a specific problem and can be deployed efficiently, considering the unique workflows involved.
- **Development of robust ROI frameworks** for legal technology adoption, setting measurable KPIs specific to the legal and compliance departments'operations.
- **Compliance and risk management in AI deployment**, ensuring the solutions are aligned with the new requirements introduced by the EU AI Act, GDPR and wider EU Digital Strategy.

The future of legal tech clearly lies in purposeful innovation rather than technology for technology's sake. As the market continues to mature, the focus will increasingly shift toward solutions that deliver measurable improvements in legal service delivery while maintaining the highest standards of professional practice.

For corporations looking to explore this evolving landscape, our team of lawyers and developers at DLA Piper in Italy is able to provide strategic guidance and practical support in identifying and implementing the right solutions for your specific needs. Connect with us to learn more about how we can help plan and execute your legal innovation journey.





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