DO **GENERATIVE AIs** THREATEN THE FUTURE OF THE INTERNET?

The development of generative Artificial Intelligence (AI) is a major innovation, full of promise and rich in potential for transforming our economies and society. In just a few years, its use has become widespread, and it has become essential to many of us. However, by becoming a new gateway to the internet, it also presents a number of risks: these technologies could challenge the founding values of the internet and its development as a "common good".

OPEN INTERNET, NET NEUTRALITY, WHAT IS IT?

Established in 2015 by a European regulation, the principle of open internet guarantees users the right to access and share content — regardless of its nature, origin, destination, or the device used — without any intermediary slowing down or blocking access. It also guarantees online innovation. To this end, the regulation imposes net neutrality obligations on internet service providers to prevent any discrimination between content and services circulating on the network. In France, Arcep is responsible for ensuring compliance with this regulation.

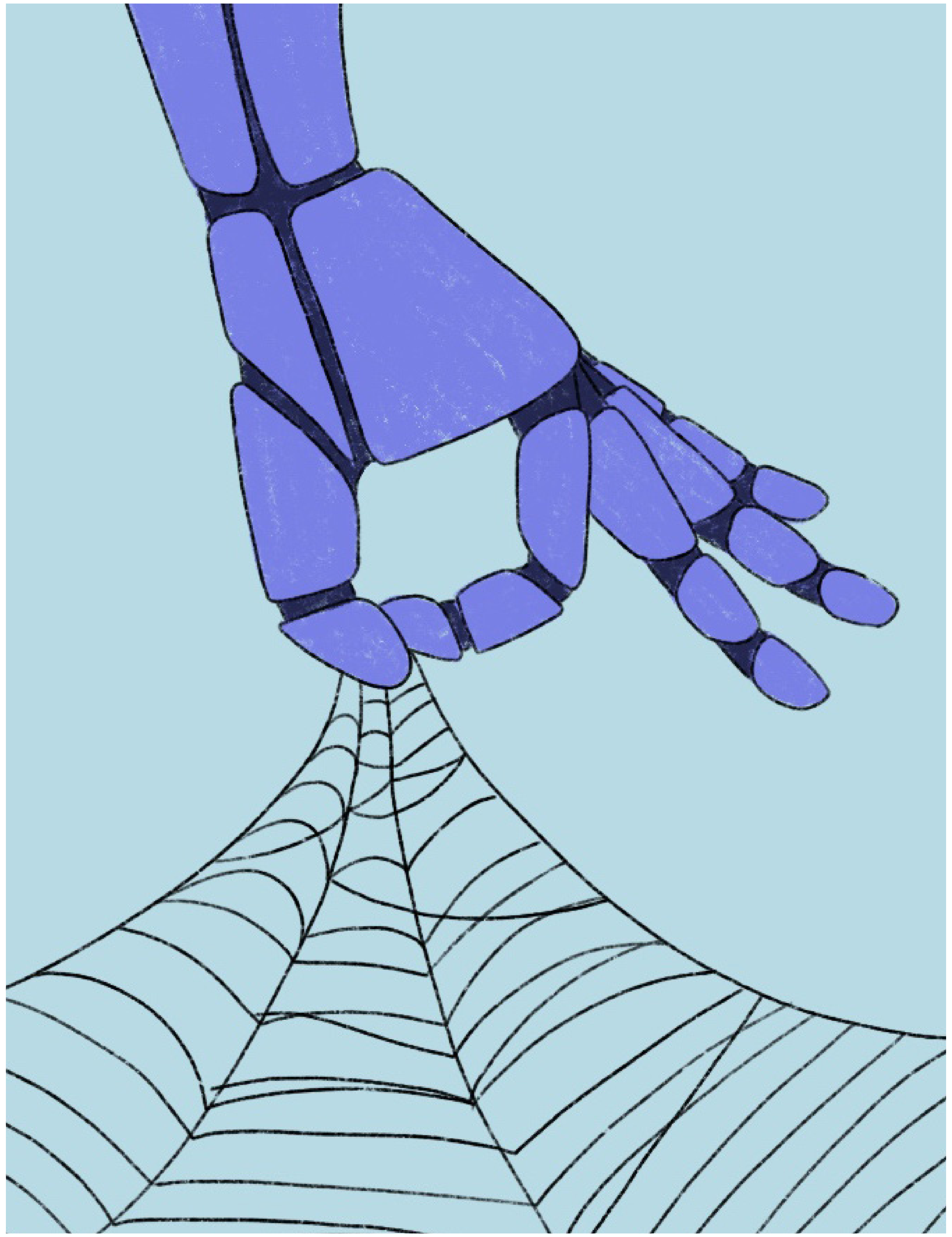
Since 2022, the Digital Markets Act (DMA) has provided additional guarantees regarding the openness of the internet, thanks to the regulation of large digital platforms or "gatekeepers."

GENERATIVE AIs, NEW "GATEWAYS" TO THE INTERNET

The emergence of generative AIs presents a new challenge to the principle of the open internet. As new interfaces between users and online content, and increasingly essential gateways to the internet, they can both limit the diversity of content and services available to internet users and reduce the ability of innovators to suggest new ones. **The internet as we know it, based on technological neutrality and the principle of openness, would be profoundly transformed, to the detriment of freedom of choice and opportunities for innovation.** To protect the principle of an open internet in the face of the challenges posed by generative AI, two main types of threats must be monitored:

01 THREATS TO USER ACCESS TO CONTENT AND SERVICES

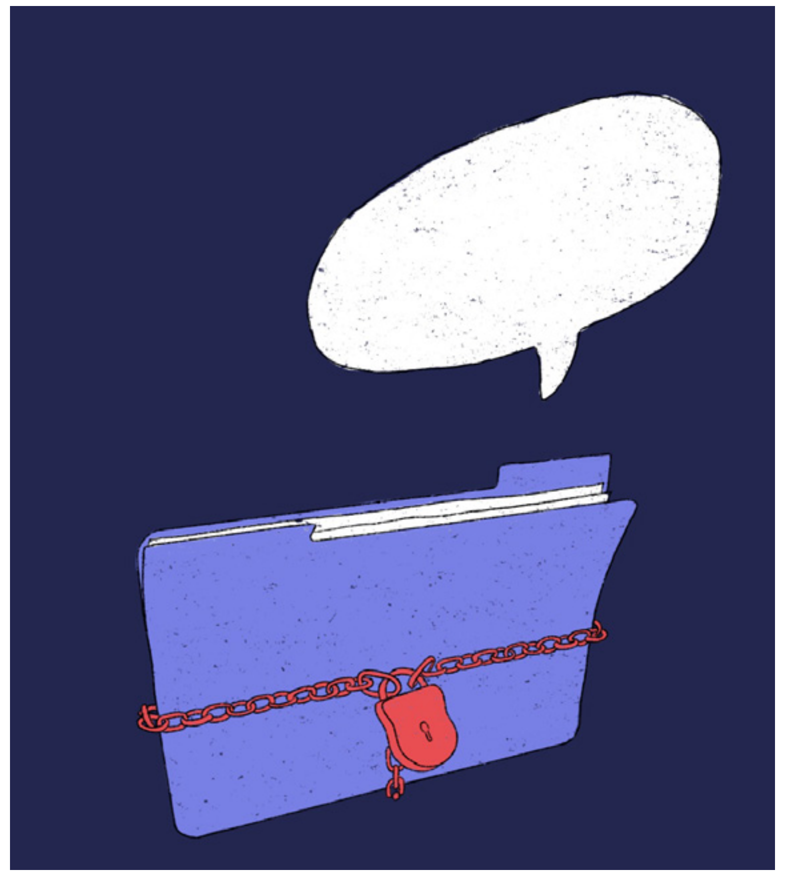
02 THREATS TO THE DIVERSITY OF CONTENT AVAILABLE ON THE INTERNET



To better understand these threats, let's fast forward to 2030, assuming widespread adoption of generative AI. Internet searches are now mainly conducted through conversational agents based on generative and agentic AI. These tools are part of everyday life for internet users such as Louise, who is planning her summer vacation, and Naël, a travel service developer.

01 THREATS TO USER ACCESS TO CONTENT AND SERVICES

June 2030. Louise asks her favorite chatbot, LittleAI, to help her plan her summer vacation. LittleAI can answer questions and perform simple tasks such as ordering products, making online reservations, sending emails, and more. Louise makes her request: "I have two weeks off at the end of July. Can you organize a low-cost vacation for me in France?"

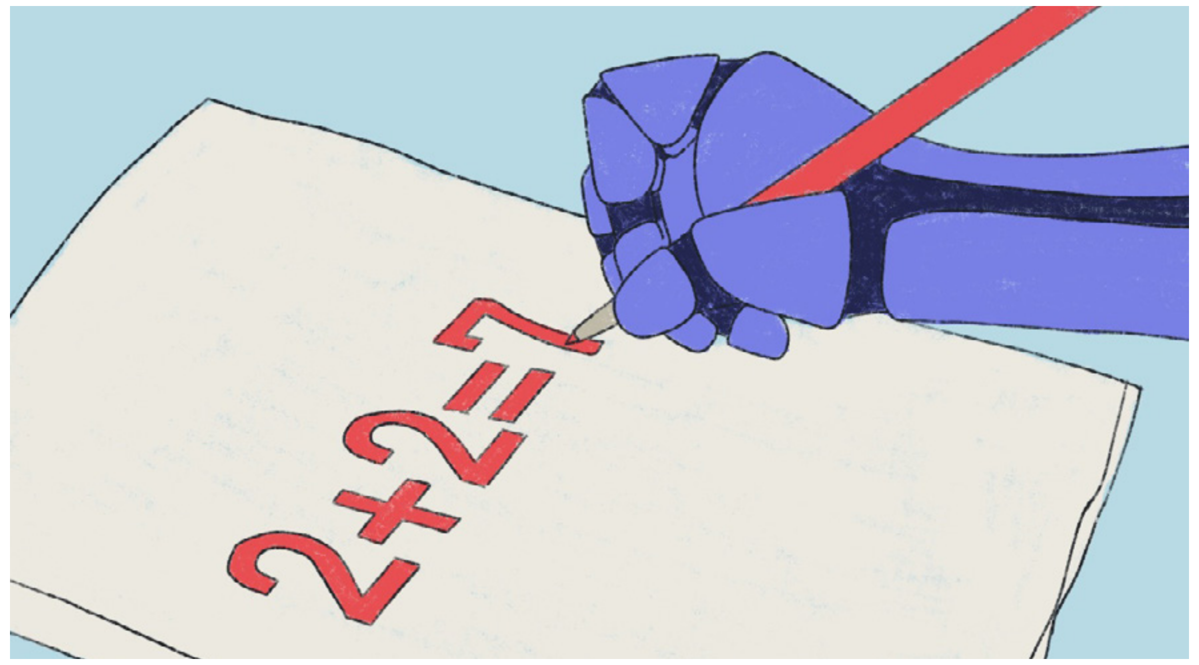


1ST RISK: A SINGLE RESPONSE AND SOURCES SOMETIMES UNCLEAR

By default, LittleAI's interface — whether voice or screen-based — provides a single answer, without systematically referencing its sources or allowing freedom of choice. Unlike a search engine or a traditional platform, Louise is unable, in most cases, to identify the author and type of sources behind the information or decision made by the AI: a hotel chain's commercial website, a tourist guide, or a hiker's blog? The virtual assistant could even make reservations, with no means of control for Louise. Generative AI makes choices on Louise's behalf, with no guarantee of transparency, plurality of sources, or explanation on the decision process.

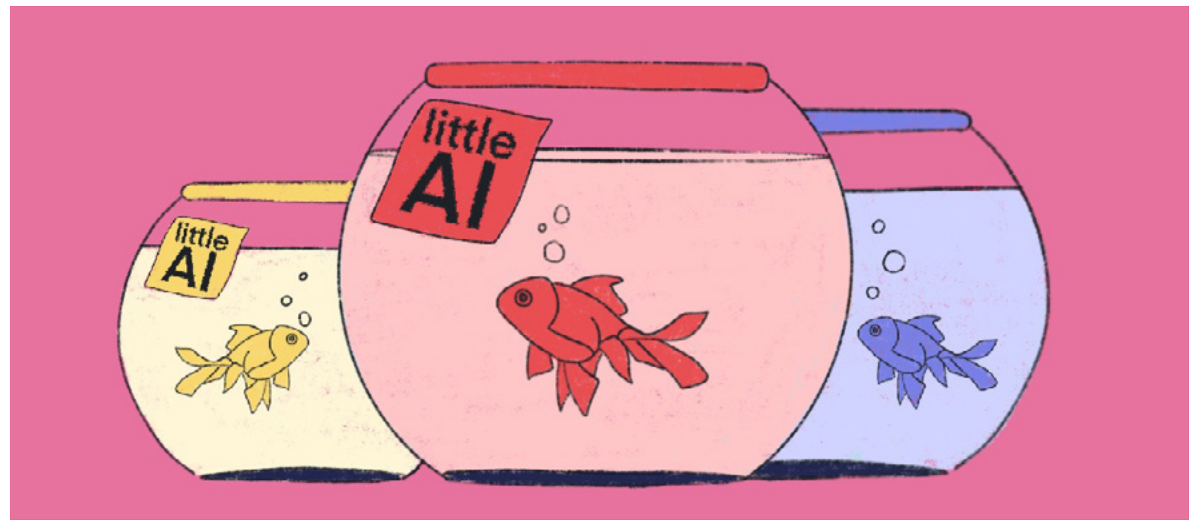
2ND RISK : A POTENTIALLY BIASED RESPONSE

With this request, Louise relies on LittleAI to select, process, and summarise information to respond. LittleAI's response depends on the data AI has been trained on and the parameters chosen by the developer to program the model. Especially, it may repeat and amplify the dominant content in terms of tourism or biases — for example, gender bias — present on the internet, and base its responses on a standardized and stereotypical view of society. For example, Louise might be offered culinary activities during a beach vacation, even though she prefers trekking in the outdoors.



3RD RISK : "HALLUCINATIONS"

Generative AI can suffer from a major problem: "hallucinations." Based on a system of statistical links between content on the internet, results that appear to be true may include errors: based on the data and training method used, LittleAI may simply "predict" the most likely information, but not necessarily the most accurate! Louise could thus be given a hiking route in a forest that has become a residential area, or book diving lessons with a fictitious company...



4TH RISK : THE "FILTER BUBBLE" EFFECT

By conducting multiple researches, Louise provides LittleAI with information about her tastes, background, and interests. In order to capture her attention and maximise usage time, LittleAI's settings could "over-personalise" its responses and adapt to her identified expectations and tastes. For example, if Louise has previously searched for a car to help a colleague, LittleAI could suggest vacation itineraries that require a car, even though she doesn't have a driver's license yet or prefers cycling and walking.

5TH RISK : THE IMPACT OF THE AI ECONOMIC MODEL

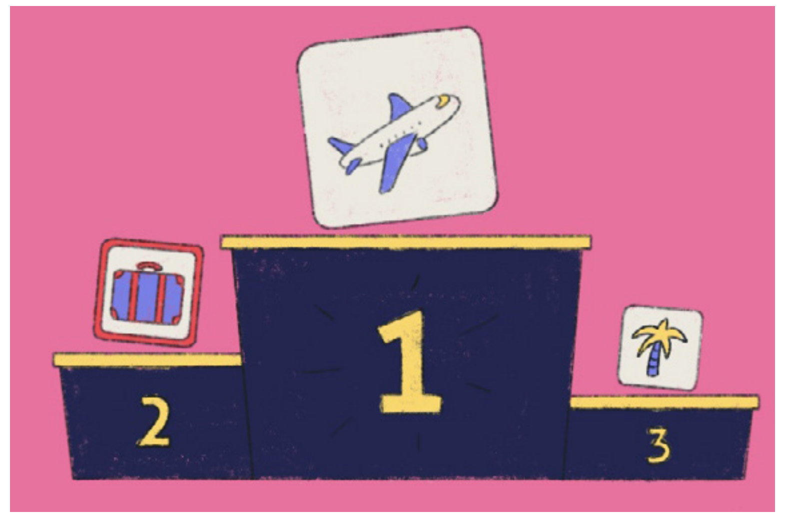
Considering that in 2030, advertising will partially finance most chatbots, companies are signing contracts with generative AI service providers in order to be more often recommended in AI responses. In Louise's case, LittleAI could have entered into a commercial agreement with a travel agency. It could then direct her to or even directly book her on vacations organised by the agency, or by other sponsors of the generative AI tool, instead of less expensive options, without Louise being informed of this commercial agreement.

02 THREATS TO THE DIVERSITY OF CONTENT AVAILABLE ON THE INTERNET

July 2030. The development of generative AI has also profoundly changed the way content and services are created and distributed. Naël is a developer offering a new service for sharing original hiking trails between internet users. This is ideal for Louise, who is herself a mountain trekking enthusiast. However, despite the relevance of his service to Louise's search, she may never be able to access it *via* Little AI...

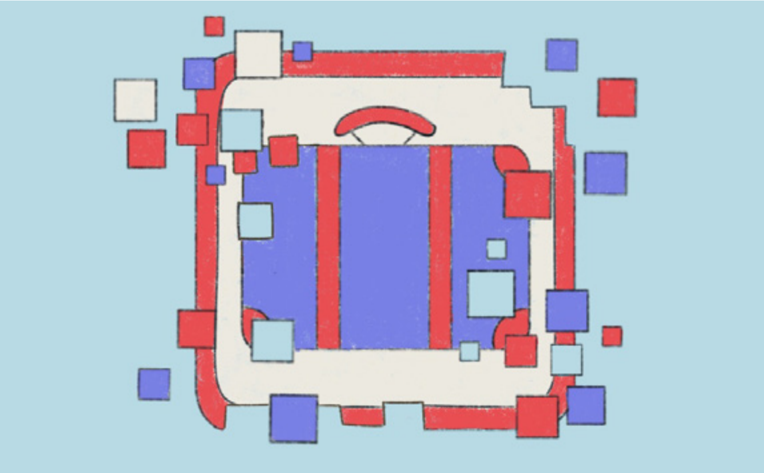
1ST RISK : ATTENTION LOCKING BY THE INTERFACE

The LittleAI interface does not allow free navigation like a web browser. It channels the user's attention towards unique responses or a limited number of choices selected by the AI. This means that even if Naël's app is referenced somewhere in the depths of the web, Little AI may never suggest it to Louise, even though she could have discovered it by exploring search engine results or a travel forum.



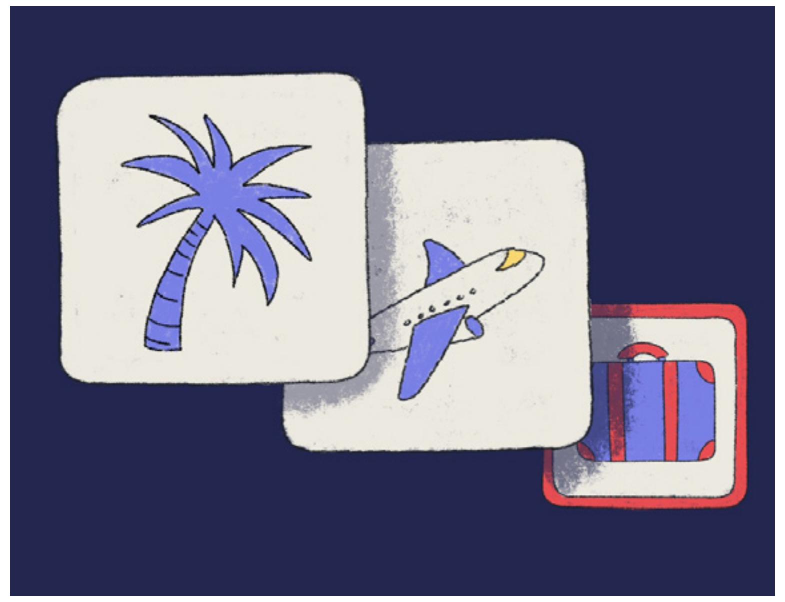
2ND RISK : GENERATIVE AIs FAVOUR THE MOST POPULAR CONTENT

LittleAI is based on an AI model that uses deep learning to provide the most likely response, not the most accurate or truthful one. Assistants based on generative AI are trained on massive data sets, which are often biased toward the most visible and popular content. By providing a single response, the use of generative AI can hinder the ability to discover emerging, independent, or alternative services such as Naël's, whose content is unlikely to be referenced by LittleAI. Local innovation is drowned out by the noise of mainstream content.



3RD RISK : THE DISINCENTIVE TO CREATE AND THE VICIOUS CIRCLE OF GENERATED CONTENT

Naël's app relies on the motivation of passionate internet users to share their own itineraries and travel recommendations, in order to stimulate the travel community. However, some users may be discouraged by the risk that their content will be “scraped” by generative AI and used without being referenced. Naël himself may be tempted to use LittleAI to generate content, rather than relying on original recommendations from internet users. On a larger scale, this logic could impoverish the content available on the internet, discourage the production of valuable information, and fuel a vicious circle: if AIs train on content they have generated themselves, their errors and biases are likely to multiply... to the point of threatening their own reliability, or even leading to the model’s collapse.



4TH RISK : THE DOMINANCE OF A HANDFUL OF PLAYERS OVER CONTENT PRODUCED ON THE INTERNET

Finally, Naël wonders whether he will be able to continue working as an independent developer for much longer: in 2030, the dominance of big players in the digital sector has been further reinforced by the emergence of generative AI as a new gateway to the internet. These companies can take advantage of their often closed ecosystems (services, data, cloud infrastructure, computing power, and technical expertise) to dominate the generative AI market. If Naël cannot — or does not want to — pay to have his service listed by one of the major generative AI providers, his application will remain invisible to millions of users, even if it proves to be more relevant than the content and services sponsored by these AIs.

HOW CAN WE PREVENT THESE THREATS AND WORK TOWARDS A DESIRABLE FUTURE FOR THE INTERNET?

Louise and Naël's experiences illustrate how, without appropriate action or framework, the development of generative AI could reduce users' freedom of choice, impoverish the diversity of accessible content, and undermine online innovation.

The internet would thus evolve from a network of networks providing access to a plurality of third-party content, to a browsing experience guided by a few AI agents, which select and act on behalf of internet users, in a web that is partly “artificialized” by a majority of generated online content...

While the example presented in this comic strip concerns the travel industry, these issues are even more acute when it comes to sensitive topics such as health, education, and politics.

In the face of these risks, action can be taken. The development of generative AI is not incompatible with the founding principles of the internet, provided that its growth is accompanied with appropriate technical, economic, and regulatory choices.

With this in mind, Arcep, the French regulatory authority responsible also for ensuring net neutrality, launched an analysis project in 2025 involving experts, researchers, businesses, and stakeholders. The goal was to consider how to preserve an open internet in the era of generative AI.

IN ITS REPORT PUBLISHED IN JANUARY 2026 TO MARK THE 10TH ANNIVERSARY OF THE EUROPEAN REGULATION ON THE OPEN INTERNET, ARCEP HIGHLIGHTS SIX LEVERS FOR ACTION:

1. Reaffirm the principles of the open internet in public policy and international discussions on AI;
2. Encourage the development of open technologies and protocols to enable generative AI to interact transparently and fairly with online content and services;
3. Ensure fair conditions for access to and promotion of content, so that creators, developers, and publishers can continue to innovate and be visible;
4. Mobilise existing regulations to limit excessive concentration and preserve users' freedom of choice;
5. Enhance the transparency and auditability of generative AI, in order to better understand its responses, sources, and limitations;
6. Empower internet users to control their uses through better information, configuration options, and training efforts.

To read the full report