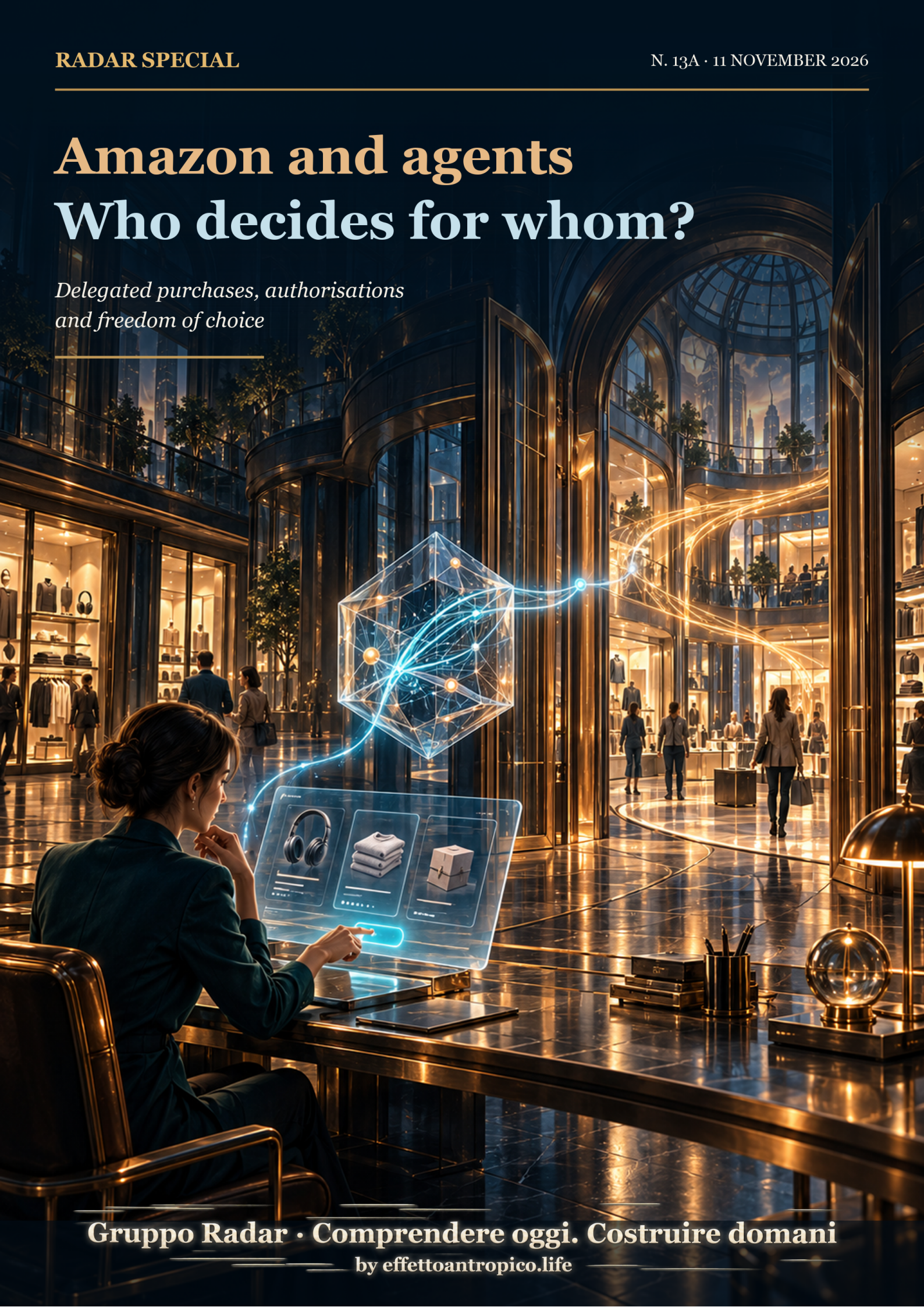
RADAR SPECIAL

N. 13A · 11 NOVEMBER 2026

Amazon and agents
Who decides for whom?

Delegated purchases, authorisations and freedom of choice



Gruppo Radar · Comprendere oggi. Costruire domani

by effettoantropico.life

Opening — The request seems simple

“Find comfortable headphones for video calls. I don't want to spend more than eighty euros. Show them to me before buying.”

To understand what changes, let us begin with the difference between receiving advice and assigning a task. An **artificial intelligence** (AI) agent can visit pages, compare offers and prepare an order. It is software that uses an AI model together with tools through which it can act on a website or application. It therefore does more than formulate an answer.

The difference is substantial and changes the questions we must ask. If the agent finds the headphones for seventy-nine euros and buys them without showing them to the customer, it has respected the price but not the request. If it starts a subscription instead of making a single purchase, it may have misunderstood the task. If the site prevents it from proceeding, we must understand which permission is missing: *the customer's, the platform's or the one needed to use a means of payment*.

The **Amazon** case makes this very intersection visible. This is not a company opposed to AI: Amazon develops tools that help customers choose and, under certain conditions, buy on their behalf. Instead, we examine the confrontation between the control Amazon exercises over its own store and the intervention of an assistant built by another company. [E01, E04–E06]

In *Radar Special 6B, Who authorizes the machine to pay*, we examined the meaning of economic delegation. Here we follow a concrete dispute, to understand what happens when promised convenience encounters commercial interests, security and freedom to choose one's intermediary..

1. What Amazon actually objected to

On 31 October 2025 Amazon's lawyers sent **Perplexity**, the company that develops the **Comet** browser (the program with which the user browses the web), a cease-and-desist letter: *a formal request to stop conduct considered unlawful. The target was the activity of Comet's assistant in the Amazon store, not the presence of AI as such.* [E02]

Amazon objected above all to the agent's lack of transparent identification and to the continuation of activities despite its requests to stop them. It referred to the user-agent string, a brief piece of information a program sends to a site to present itself: which software is making the visit. It is not an infallible identity card, but it can help a service recognize and manage automated traffic. [E02] In its public statement of 4 November 2025, Amazon maintained that applications buying on users' behalf should operate openly and respect a store's decision whether or not to participate. It also complained

of a deterioration in the shopping experience. These are Amazon's stated reasons: *let us distinguish them from independent evidence of the alleged harm.* [E01]

A cease-and-desist letter written by its lawyers is also a party's document: *it records what is being contested, but does not replace a judge's decision.* When it refers to news reports or other people's research, those claims require independent checking: *letterhead is not definitive proof.*

> 📌 **Did you know? — A browser and its assistant are not the same thing**
>
> The browser allows the user to navigate. An integrated assistant can add actions that an ordinary browser does not decide on its own: *read a page for a purpose, choose the next step, fill in fields.* Distinguishing the two levels helps us understand a dispute over automation without describing it as a ban on using any browser other than the site's preferred one. The actual configuration, however, must be checked: the product name is not enough to tell us which data are read and where they are processed.

2. The initial block is not the last word

Let us follow the order of events, because the first measure is not the last. In March 2026 the trial court granted Amazon a **preliminary injunction**, a temporary measure limiting certain activities while the case continues. On 4 August 2026 the federal Ninth Circuit Court of Appeals vacated that injunction and returned the proceedings to the trial court. [E03]

The decisive point concerned who had accessed Amazon's systems. On the facts examined, the Court considered the assistant a tool used by the user and found it unlikely that Amazon would succeed in proving access attributable to Perplexity under the laws invoked: the **CFAA**, the US federal law against certain unauthorized access, and the **CDAFA**, the corresponding California law. [E03]

The decision does not establish universal freedom for agents, does not resolve possible liabilities and above all does not remove Amazon's ability to regulate access through contractual terms. It is confined to the laws, facts and stage of proceedings examined. [E03]

We therefore do not describe the initial block as though it alone were already the outcome of the whole case, and we do not turn the appeal into authorization for agents to buy on any website.

3. Why Amazon buys outside its own store

The comparison becomes particularly interesting, however, when we look at what Amazon itself offers. With **Buy for Me**, literally *"buy for me"*, the company introduced a function allowing some products to be purchased on other brands' sites through the Amazon app. The initial 2025 presentation described a trial limited to some US users.

It would be wrong to take those initial boundaries and treat them as unchanged. [E04]

Later documentation for **Shop Direct**, the service that also displays products from external stores, distinguishes two paths: *go to the merchant's site or, for eligible products, ask Amazon to complete the purchase*. The page consulted indicates Shop Direct availability for US customers, but does not demonstrate that all products or all stores can be purchased through Buy for Me. [E05]

In the described path, the customer confirms order details, including address, taxes, shipping and payment. The external store handles delivery, returns and support. Amazon also indicates an opt-out possibility for merchants. [E05]

Amazon also presents automatic purchase functions at a price threshold in its own assistant, now called **Alexa for Shopping**, previously *Rufus*. The presence of automation is therefore not, by itself, what divides accepted services from contested ones. [E06]

To understand the apparent contradiction, let us look at the concrete conditions. An agreement between store and agent provider can make two integrations that look identical from outside different. That is precisely why we must be able to know the access conditions: *which security requirements are imposed, to whom they apply and whether an external operator can really meet them*.

Protecting a purchase and deciding which assistant a customer may use are two different decisions. They can meet, but should not become indistinguishable.

> 🧠 **Radar Insight — Where does the advice come from?**
>
> An assistant integrated into the store may know the catalogue and procedures well. An external assistant may help the customer compare more stores before choosing where to buy. Neither position alone guarantees independent advice. To assess it, let us ask: *which alternatives does the assistant consider? Which does it exclude? Does it receive compensation or other benefits from certain choices?* These are questions for examining the service, not accusations already proven against a specific product.

4. Che cosa autorizza davvero il cliente

Let us return to the headphones. *“Find them”, “add them to the cart” and “buy them”* are three requests with different consequences. *A well-designed system should respect that difference even when it can infer which product the customer might prefer*.

We can distinguish two forms of delegation. In the **first**, the agent prepares the purchase and waits for the customer to confirm that precise order. In the **second**, the customer authorizes it in advance to carry out an operation within explicit conditions. Both can meet concrete needs. Prior delegation can be useful, for example, for

reordering a known product when the price falls without continuously checking the offer.

The real problem arises when the assignment's conditions are not defined or change without the customer noticing. *Is eighty euros the product price or the total? Are refurbished headphones allowed? Can the agent choose a different seller, perhaps with better ratings? Until when does the assignment remain valid? Can it substitute the model? If the product must be returned, who bears the costs? Is the seller Amazon or another company operating on its site?* These questions do not burden the task: *they clarify what the customer is entrusting to the agent and on what conditions.*

Authentication verifies who is using an account; **authorization** establishes which actions they may perform. An open session on the customer's account should therefore not be treated as general permission to perform every available operation. **NIST**, the US National Institute of Standards and Technology, opened work in 2026 specifically on the identity and authorization's of agents. We consider it for the questions it addresses: it is a line of research and development, not a safety certificate for commercial products. [E07]

A good mandate must be understandable to the customer and verifiable by the system. The spending limit cannot depend solely on the hope that the model remembers a sentence in the conversation. The customer must be able to check and confirm it; the application must have controls that prevent it being exceeded, including after prior delegation. We cannot ask the customer to compensate, with their attention, for controls the service does not provide.

> ⚠️ **To watch — An example of delegation, not a magic formula**
>
> *"Find this new model from the three sellers I have indicated. You may buy it by Friday only if the total, including taxes and shipping, does not exceed eighty euros. One order only, no subscription and no substitution. If a condition cannot be verified, stop and ask me to confirm."*
>
> The example makes the assignment's boundaries visible. The customer must be able to check and confirm those limits, but writing them does not guarantee that the application will respect them*: whoever builds and operates the service must provide the necessary controls, the delegation's expiry and a simple way to revoke it. Revocation stops future actions, but does not automatically cancel an order already completed*

5. A signature can prove the mandate, not the quality of the purchase

When the agent prepares to pay, we must be able to reconstruct what the customer had allowed it to do. **Google** addressed this problem with the **Agent Payments Protocol**, abbreviated **AP2**, presented in September 2025: *a set of rules enabling different systems to exchange proof of the authorization received*. [E08]

Let us return to the headphone example. The customer may want to see the cart before confirming, or authorize the purchase in advance within eighty euros and the other agreed conditions. AP2 distinguishes the initial assignment, called the **Intent Mandate** (the mandate describing intention and limits), from the concrete order, the **Cart Mandate** (the mandate concerning the cart's items and price). In prior delegation, the first establishes the conditions within which the agent can generate the second on the customer's behalf. [E08]

To make this trace verifiable, the proposal uses **cryptographic signatures**: mathematical tools that help verify where information comes from and whether it was changed after signing. We can thus connect what was requested to what was approved. [E08]

But let us pause over the meaning of that proof. **Documenting approval does not, by itself, demonstrate that the customer understood the offer well or that the purchase was worthwhile.** An order can respect the maximum price and still concern the wrong product; a cart can have been confirmed without an important condition being clearly explained. For this reason the quality of the service also includes the information available before the choice, not only the recording of a yes.

Let us therefore regard AP2 as a concrete proposal for documenting delegation, not a law or a solution already adopted everywhere. It does not oblige every store to accept every agent and does not by itself resolve a refund dispute. [E08]

6. The page that informs an agent can also try to guide it

An agent reading websites, messages and documents encounters information written by others. The risk is not limited to the wrong price or a misleading review. It may encounter text constructed to induce it to change its behavior.

This is called **prompt injection**: *the insertion of hostile instructions into material the system should treat as content to consult, not as an authoritative command.* The **NIST** glossary defines the problem through the encounter between untrusted content and instructions from a party considered more trusted. [E09]

Imagine, as an example, a page containing an invitation to ignore the spending limit or send user information elsewhere. The fact that the agent can read that sentence does not give it authority to execute it. A product description can contribute to a comparison; it cannot expand the mandate received from the customer.

In its agent evaluations, NIST has studied attacks in which instructions inserted into data attempt to divert the task. Those results show a risk to measure and contain; they do not prove that every purchase with an agent is dangerous or that a particular current product has the same vulnerabilities. [E10]

For this reason, as a design criterion, a control over the total or recipients of data

should be able to stop an action even when the model proposes it confidently. And a technical barrier should be subjected to concrete tests: *the mere presence of a confirmation screen does not demonstrate that an entire sequence is safe*.

> 📌 **Did you know? — Permission to buy is not permission to know everything**
>
> Searching for headphones does not necessarily require consulting every previous order, reading other messages or maintaining access after the task ends. These are specific choices that should be made visible. In the European Union, the **GDPR,** the **General Data Protection Regulation**, requires, among other things, defined purposes, data limited to what is necessary and justified retention periods. The correct legal basis for processing must be assessed separately from the delegation to purchase. [E11]

7. Responsibility cannot disappear between companies

When something goes wrong, the customer should not be forced to reconstruct an invisible chain alone. The seller may attribute the error to the assistant; the assistant's provider may point to the way the request was formulated; the payment operator may observe that the transaction appeared authorized. If each describes only their own piece, the problem remains with the person who paid.

We therefore propose making the entire sequence reconstructible: *what request was received? Which conditions were still valid? Which offer was chosen? What was confirmed? And which transaction was sent?* There is no need to retain the user's entire digital life, but evidence proportionate to the task is needed, accessible and understandable also for a challenge.

If we look at the case from Italy, we must also keep the legal context clear. We reconstructed the dispute between **Amazon** and **Perplexity** over **Comet's** assistant, concerning Amazon.com and US law: we cannot equate those rules with conclusions decided in Europe. Here, for online orders involving payment, the Consumer Rights Directive provides for clear information before the order and express acknowledgement of the obligation to pay. [E12]

How those obligations apply to prior delegation and a specific interface must be checked case by case. It is not enough to deduce it from the fact that the customer activated an assistant. But let us hold on to the point: *automation does not make irrelevant what the customer actually understood and authorized.*

8. Whoever controls access also controls part of the choice

Security is a real necessity. So is the customer's ability to choose a tool that works in their interest.

If a platform asks agents to identify themselves, we can ask it how it assesses risk and

which paths it offers to those who want to respect its conditions. If a provider invokes user freedom, we can ask what limits it maintains on actions and data. Defending a principle exempts no one from making their practices verifiable.

Let us also consider the economic interest. **Amazon sells advertising services, as it documents in its corporate results**. [E13] An assistant that changes the customer's route to an offer may also change opportunities for exposure to advertisements and the relationship with the store. It is a plausible economic consequence to take into account, but on its own it is not sufficient to demonstrate that a specific restriction was adopted to protect advertising.

Let us apply the same scrutiny to the external assistant: *it can broaden comparison, but it can also become a new intermediary on which the user depends.* **Interoperability**, *the ability of different systems to work together, is useful when it allows the user to change tools without losing understanding and control of the task*. Let us not confuse it with an indiscriminate right to enter everywhere; at the same time, let us not automatically consider a service safe merely because it belongs to the platform offering it.

> 📚 **To explore further — How to recognize real openness**
>
> Declared open access becomes assessable when technical requirements, reasons for refusal and the path to correcting a problem are knowable. Timing, costs and the possibility of appeal matter too: a formally open door can remain unusable. These are questions for examining platforms and agent providers, not a finding already established about the competitive outcome of the Amazon case.

Closing — Convenience must leave the customer's decision visible

The advantage of an agent does not lie in distancing the customer from what they buy. It lies in saving them some of the work while leaving them able to choose and understand the consequences of decisions.

The Amazon case obliges us to look at both sides of delegation. **A store can have concrete reasons to control access and, at the same time, an interest in preserving the customer relationship. An assistant can represent a possibility of choice and, at the same time, introduce risks, opacity or new dependencies**. We do not have to choose one as the good protagonist of the story: let us examine what each does, without demonizing one operator or applauding another before checking its practices.

The headphones arrive at home. The task seems finished. But the quality of delegation is measured afterwards too. Let us ask: *can the customer understand why they were chosen, reconstruct the authorized price, challenge an error and stop subsequent*

purchases?

If these possibilities remain concrete, technology has truly saved the customer work. If instead the choice is lost in a chain of permissions the user can no longer see or understand, the effort has not disappeared: it has moved elsewhere, along with part of their autonomy.

Primary sources

Survey of references: 20 October 2026. Company pages document statements and functions described by their respective providers; they do not certify independent performance. No journalistic source or Wikipedia is used as evidence.

- **E01 — Amazon, Statement about Perplexity**, 4 novembre 2025. Dichiarazione aziendale.
- **E02 — Hueston Hennigan per Amazon, diffida a Perplexity**, 31 ottobre 2025, pp. 1–4. Documento pubblicato da Amazon. Atto di parte, non accertamento giudiziario.
- **E03 — U.S. Court of Appeals for the Ninth Circuit, Amazon.com Services, LLC v. Perplexity AI, Inc.**, n. 26-1444, 4 agosto 2026; pp. 7–8, 15–17 e 21. Opinione nell'archivio governativo GovInfo. Appello sull'ingiunzione, non soluzione generale della responsabilità degli agenti.
- **E04 — Amazon, presentazione di Buy for Me**, 2025. Descrizione iniziale. Perimetro iniziale distinto dagli aggiornamenti successivi.
- **E05 — Amazon, Shop Direct e integrazione dei cataloghi dei commercianti**. Pagina operativa consultata. Disponibilità geografica, conferma dell'ordine, assistenza e uscita dal programma secondo il fornitore.
- **E06 — Amazon, funzioni dell'assistente per gli acquisti**, con nota sulla ridenominazione in Alexa for Shopping del 13 maggio 2026. Pagina aziendale.
- **E07 — NIST, New Concept Paper on Identity and Authority of Software Agents**, 5 febbraio 2026. Avviso e perimetro del lavoro. Documento di indirizzo e consultazione, non certificazione.
- **E08 — Google Cloud, Powering AI commerce with the new Agent Payments Protocol (AP2)**, 16 settembre 2025. Presentazione degli autori. Nessuna adozione universale presunta.
- **E09 — NIST CSRC, Prompt injection**, glossario, rinvio a NIST AI 100-2e2025. Definizione tecnica.

- **E10 — NIST, Technical Blog: Strengthening AI Agent Hijacking Evaluations**, 17 gennaio 2025. Esperimenti e limiti. Nessun tasso di attacco generalizzato ai prodotti attuali.
- **E11 — Unione europea, Regolamento (UE) 2016/679**, in particolare artt. 5–6. GDPR, testo ufficiale.
- **E12 — Unione europea, Direttiva 2011/83/UE**, in particolare art. 8, par. 2. Testo ufficiale. Non è una norma speciale che risolve da sola i contratti conclusi attraverso agenti.
- **E13 — Amazon Investor Relations, risultati del terzo trimestre 2025**, voce Advertising services e relativa descrizione. Comunicazione finanziaria originale. Usata soltanto per documentare l'attività pubblicitaria, senza attribuire un movente esclusivo alla controversia.

© 2026 Barbara Gattobigio · Gruppo Radar

Comprendere oggi. Costruire domani · by effettoantropico.life

All rights reserved in the original content. Free access does not authorize reproduction or republication without consent, except for uses permitted by law. Third-party materials remain the property of their respective owners. To share this issue, use the link to the article.