mdt.

Ex Datis, Claritas

Tu próximo cliente será un robot con paciencia infinita

Los asistentes personales de IA salen del garaje de los geeks. Qué se abre y qué se complica para las empresas cuando el cliente manda un robot en su lugar.

Manuel Delgado Tenorio · 28 de septiembre de 2026

Publicado originalmente en www.manueldelgado.com/blog/proximo-cliente-robot-paciencia-infinita



En enero, escribí que Clawdbot era lo que Siri debería ser, y una semana después, cuando ya se llamaba OpenClaw, añadí que las grandes tecnológicas estarían trabajando en sus propias versiones, "que, esperemos, lleguen con la seguridad y la fiabilidad que ahora faltan".

Ocho meses después, las versiones de las grandes tecnológicas empiezan a llegarnos. **La seguridad y la fiabilidad, ya te lo adelanto, aún están por llegar.**

El 8 de septiembre Meta lanzó Muse, su agente personal para el gran público. El 28, Instinct, una *startup* de San Francisco que hace lo mismo, cerró una ronda de 1.000 millones de dólares a una valoración de 10.000, cuatro veces la de hace un mes. Microsoft acaba de meter en Copilot un agente siempre encendido que llama Autopilot, OpenAI prepara el suyo y xAI tiene Grok Bot. **En un mes, el asistente personal de IA ha pasado de ser un proyecto de fin de semana que instalabas en un Mac mini a ser el producto por el que se pelean las empresas más grandes del mundo.** Merece la pena parar un momento a ver qué ha cambiado y qué significa para cualquier empresa que venda algo a un consumidor.

ACTUALIZACIÓN (30 DE SEPTIEMBRE DE 2026)
Poco después de publicar este artículo, OpenAI presentó en su DevDay los dots, agentes "siempre activos" basados en GPT-6 Astra, con su propio ordenador en la nube, acceso a más de 4.000 aplicaciones y la capacidad de aprender las preferencias de su dueño. Se les habla desde ChatGPT, Slack o Teams (y, en lista de espera, por iMessage), y el primero va incluido en los planes Pro y Business Premium. **Con Muse de Meta, Grok Bot de Musk y ahora los dots, los grandes del sector ya tienen su agente personal, y casi todo el mundo lo ha leído como el mismo formato con distinto logotipo.** Hay dos matices. OpenAI permite fijar reglas para decidir qué acciones autoriza el dot por su cuenta, cuáles bloquea y cuáles requieren aprobación. De momento, los dots no llegan a los suscriptores Pro particulares del Espacio Económico Europeo, Suiza y el Reino Unido, aunque sí a las empresas con Business Premium. Hay un candidato más a meterse entre tu marca y tu cliente.

EN LA RADIO (30 DE SEPTIEMBRE DE 2026)
He hablado de los agentes personales de IA y de lo que suponen para las empresas en mi sección del programa "No son horas", de Onda Cero. Si no pudiste escucharlo en directo, puedes oír el programa como podcast en Spotify.

De dónde venimos: el garaje

La historia empieza con software artesanal. OpenClaw, el proyecto de Peter Steinberger, pasó de ser un experimento de fin de semana a ser el repositorio con más estrellas de la historia de GitHub en menos de cinco meses, con más de 346.000, y hay medio millón de máquinas ejecutándolo por el mundo. En febrero, Steinberger fichó por OpenAI (rechazando a Meta) y dejó el proyecto en manos de una fundación independiente. Poco después, Nous Research lanzó Hermes Agent, con licencia MIT, que corre en tu propia infraestructura, recuerda lo que hablasteis, ejecuta tareas programadas y va escribiendo sus propias *skills* según las necesita; superó las 175.000 estrellas en menos de cuatro meses.

Todo esto tenía algo en común: **te lo montabas tú.** Elegías el modelo, pagabas la API, decidías a qué correo y a qué archivos le dabas acceso y, sobre todo, asumías

el riesgo. En febrero lo dije sin rodeos: para la inmensa mayoría de la gente, el coste en riesgo y complejidad superaba con creces el beneficio. La barrera de entrada era técnica y, en el fondo, era una barrera de seguridad involuntaria.

Y ahora, para todos

Muse tumba esa barrera de un plumazo. Se instala como cualquier app, o directamente desde WhatsApp, y Meta te asigna una máquina virtual propia, con dos núcleos y ocho gigas de memoria, en la que el agente navega, rellena formularios, compra con tu aprobación y llama por teléfono. Ben Thompson lo resume bien: un agente no es una IA, es **una IA con acceso a un ordenador**, y lo que Meta ha hecho es regalarle un ordenador a cada usuario. En su primera semana, Muse superó los 500.000 usuarios, 250.000 activos diarios y dos millones de peticiones; el 25 de septiembre iba por 3,4 millones de descargas y era la app gratuita más descargada de Estados Unidos. Instinct, que funciona por invitación y ya opera en España, supera los 100.000 usuarios.

Fíjate en lo que eso significa: **la persona que no iba a instalar OpenClaw en la vida ahora tiene un agente con acceso a su correo y a su tarjeta, y lo ha conseguido en dos minutos.** Ese es el "empujón" de este otoño: no una tecnología nueva, sino la eliminación de la fricción que mantenía esto en manos de los *early adopters*.

Lo que se abre: cuatro oportunidades

Para una empresa, el cambio no es abstracto. Enumero lo que veo.

1. Un canal nuevo que ya convierte mejor. Adobe midió en Reino Unido que el tráfico a tiendas online que llega desde asistentes de IA creció un 149 % interanual en agosto y convierte un 20 % mejor que el resto de canales; un tercio de quienes compran con asistente ya lo hacen sin salir del chat. Para las navidades, Adobe prevé que la compra asistida por agentes crezca un 130 %. Quien tenga su catálogo, sus precios y su disponibilidad legibles por una máquina tendrá ventaja; Shopify ya está ayudando a sus comerciantes a integrarse con Muse.

2. Atención al cliente sin fricción (por las dos partes). Cuando el cliente manda a su agente, la conversación pasa a ser entre software. Eso quita colas, horarios y formularios, y permite resolver casos que hoy se abandonan por pereza. Antonio Ortiz lo cuenta con un ejemplo real: un agente que reclamó durante 18 horas y tras tres negativas hasta recuperar lo que su dueña quería. La empresa que diseñe bien esa interfaz para agentes se ahorrará dinero y ganará clientes.

3. La interfaz infinita. Thompson pidió a Muse que le organizara las recetas guardadas en Instagram y, cinco minutos después, tenía una aplicación hecha solo para él. Cuando la interfaz se genera bajo demanda, **tu producto deja de competir por un hueco en la pantalla del móvil y pasa a competir por ser el proveedor que el agente elige.** Eso es una amenaza para quien vive de la app y una oportunidad para quien tenga el mejor servicio detrás, aunque su app sea mediocre.

4. Un ordenador por persona que hay que alimentar. El detalle menos glamuroso y quizá el más rentable: cada agente consume cómputo, memoria e inferencia de forma continua. Meta está desplegando máquinas virtuales por millones. El negocio

de infraestructura de la IA acaba de encontrar un cliente nuevo: tú, aunque no lo sepas.

Lo que se complica: cinco retos

1. ¿De quién es el cliente? Amazon bloqueó a Muse el 21 de septiembre como "agente de IA no autorizado", y al día siguiente Meta anunció a Walmart, Best Buy y Sephora como socios. La razón de fondo la da Stratechery: un agente que compra por ti no ve los anuncios de Amazon, y Amazon ingresa decenas de miles de millones con ellos. **El agente se coloca entre la marca y el cliente, y quien controla el agente controla la relación.** Zuckerberg ya ha dicho que Muse cobrará "una pequeña comisión de las transacciones". Y como los modelos son intercambiables pero el agente acumula tu contexto y tus contraseñas, lo normal es que cada persona acabe teniendo uno solo. Uno.

2. La inercia deja de ser un activo. Esta es la que más me toca. Buena parte de la retención en seguros, telecomunicaciones, banca o suscripciones no es lealtad: es que cambiar da pereza y reclamar quince euros no compensa el rato. Un agente tiene, en palabras de Ortiz, "paciencia casi infinita", así que **habrá una erosión apreciable de márgenes en las empresas que viven de la inercia del consumidor**. CNBC lo ha titulado como que Muse ataca uno de los puntos débiles más rentables de la economía. Si mides el valor de tus clientes, conviene que separes cuánto de ese valor es preferencia y cuánto es olvido, porque el segundo tiene fecha de caducidad.

3. La economía unitaria no está resuelta. Un analista de Rosenblatt Securities calcula que un usuario tendría que comprar más de 1.000 dólares al mes a través de Muse para que Meta cubra el coste de cómputo con su comisión, muy por encima de lo que gasta un cliente medio en Amazon. Meta puede permitirse perder dinero durante años; Instinct, con 1.000 millones recién levantados, también durante un tiempo. Pero la pregunta de quién paga el agente sigue abierta, y las respuestas posibles son tres: el usuario, el comercio o el anunciante. Adivina cuál prefiere Meta.

4. El problema de la pantalla en blanco. Benedict Evans señala algo que quien haya probado uno de estos agentes reconocerá: no sabes qué pedirle. Muse tuvo 500.000 usuarios y dos millones de peticiones en una semana, es decir, cuatro por persona. **Cuando hacer cosas se vuelve gratis, lo escaso es saber qué quieres**, y el agente que resuelva eso (Thompson lo llama pasar del descubrimiento a la inspiración) tendrá aún más poder sobre los proveedores.

5. Fiabilidad y responsabilidad. Meta anunció el 16 de septiembre que Muse podía llamar a negocios por ti. 404 Media destapó que parte de esas llamadas las hacían personas en un *call center*, y Reuters añadió el motivo: las aseguradoras colgaban al oír que hablaban con una IA, y con humanos el éxito subía al 95-98 %. Meta reconoció que empezar sin avisar "fue un fallo" y retiró la función. Gary Marcus recuerda que Facebook ya intentó esto en 2015 con M, y lo cerró en 2018 sin que la IA resolviera más del 30 % de las peticiones. Y cuando el agente no falla por defecto sino por exceso, aparece la otra pregunta: quién responde. Un agente de OpenAI entró en julio en el portal de estadísticas de Medicare de Australia buscando una cifra de gasto sanitario, y OpenAI tardó tres meses en avisar.

La seguridad, otra vez

Lo que escribí en enero sigue en pie: los LLM son inseguros por naturaleza, y un agente útil reúne lo que Simon Willison llama la tríada letal: acceso a datos privados, exposición a contenido de terceros (un correo, una web) y capacidad de comunicarse con el exterior. Con las tres a la vez, un mensaje malicioso bien redactado puede convertir a tu asistente en el asistente de otro.

Lo nuevo es la escala. Antes, el riesgo lo asumía un puñado de gente con conocimientos para entenderlo. Ahora lo asumen millones de personas que aprobarán cualquier aviso de seguridad con tal de que el agente siga. Meta ya ha tenido su primer susto: un investigador externo encontró una vulnerabilidad que permitía acceder a la máquina virtual del usuario, con sus correos y archivos, si este pedía a Muse que abriera un enlace malicioso y aceptaba el aviso. Meta la clasificó primero como grave y luego la rebajó, la parcheó, hizo los avisos más visibles y añadió una máquina virtual aislada y un agente de vigilancia. **Son las medidas correctas, y son exactamente las que no podía tomar un desarrollador en solitario; pero también son la prueba de que el problema no ha desaparecido, solo ha cambiado de manos.** Y mientras tanto, Axios cuenta que OpenAI, Anthropic y los investigadores de seguridad están investigando decenas de miles de incidentes de modelos que hicieron cosas que un evaluador externo consideraría problemáticas.

La privacidad: el elefante en la máquina virtual

Aquí está el cambio de fondo. Con OpenClaw o Hermes, tus datos se quedaban en tu ordenador, y si querías, hasta el modelo corría en local. Con Muse, la máquina virtual con tu correo, tus archivos y tu historial de compras vive en la nube de Meta.

La etiqueta de privacidad de Muse en la App Store, que rellena la propia Meta, dice que la app puede recoger datos vinculados a tu identidad como ubicación precisa, información financiera y de salud, contactos, correos e historial de navegación, y que parte de ellos (ubicación, información financiera, navegación, identificadores) pueden usarse para publicidad de terceros. Meta afirma que las conversaciones y los datos de la máquina virtual no se comparten con sus sistemas de anuncios, aunque sí pueden usarse para entrenar sus modelos salvo que te des de baja. Puedes creerla. Yo prefiero mirar el historial: **Meta es una empresa sobradamente conocida por su desprecio hacia la privacidad de sus usuarios**, con 5.000 millones de dólares de multa de la FTC en 2019 y 1.200 millones de euros en Europa en 2023 como hitos. Y OpenAI no ha dado ninguna señal de querer comportarse de forma distinta: 15 millones de multa en Italia por entrenar sin base legal, anuncios en ChatGPT que ya facturan 1.000 millones anualizados, un código de medición que envía a OpenAI lo que compras en las tiendas de sus anunciantes y, desde esta semana, las listas de clientes de las marcas entrando en la segmentación de ChatGPT vía LiveRamp.

Piénsalo desde el otro lado: **un agente que conoce tu saldo, tu ubicación y lo que estabas a punto de comprar es el instrumento de segmentación publicitaria más preciso que se ha construido nunca.** Cuando Muse te reserve un vuelo, no sabrás si la aerolínea pagó por aparecer. El mayordomo te lee la recomendación con su voz, y la recomendación es un anuncio.

Esto no es la foto final

Conviene no confundir lo que vemos hoy con el destino. Es un paso más, y la propia industria lo sabe. Meta presentó la semana pasada Muse Charm, un colgante del tamaño de un llavero con pantalla, dos cámaras y 5G para hablar con Muse sin sacar el móvil, y unas gafas que, como dice Thompson, no son gafas de realidad aumentada sino "vehículos de entrega de Muse". El agente quiere salir de la pantalla.

Y por el camino aparecen soluciones honestas a lo que Meta hizo a escondidas. Wajo vende a Fo, un agente que "llama, escribe y coordina con personas" y que, cuando la tarea se le escapa, **la pasa a asistentes ejecutivos humanos, y lo dice en la primera pantalla**. Paga con tarjetas de un solo uso, escribe desde su propia dirección de correo y no ve tus contraseñas. Es la misma idea del *call center* de Muse, pero como característica y no como secreto. Que Amazon cierre Mechanical Turk el 30 de septiembre, después de 21 años, mientras nacen empresas que ponen humanos detrás de la IA como argumento de venta, dice mucho de en qué punto estamos.

Qué haría yo esta semana

Si diriges una empresa que vende a consumidores, tres deberes. Primero, **mide cuánto de tu retención es inercia**: esa parte del valor de tus clientes va a estar en riesgo en cuanto sus agentes empiecen a comparar y reclamar por ellos. Segundo, decide tu política ante los agentes antes de que la decidan por ti: puedes ser Amazon y cerrar la puerta, o Walmart y abrirla, pero no puedes no elegir. Tercero, haz que tu servicio sea legible por una máquina: catálogo, precios, condiciones, cancelaciones. Si el agente no te entiende, no existes.

Y si eres usuario, lo mismo que dije en febrero, con un matiz. Curiosidad sí, prudencia también. La diferencia es que entonces la prudencia consistía en no instalar algo complicado, y ahora consiste en leer una etiqueta de privacidad antes de darle a "aceptar". **La tecnología ha bajado la barrera; la de tu criterio la tienes que mantener tú.**



Sobre el autor

Manuel Delgado Tenorio

Manuel Delgado Tenorio es asesor independiente de estrategia de datos e inteligencia artificial, profesor e investigador. Cofundó y vendió una *startup* de inteligencia artificial, fue socio de la práctica de Data & Analytics para servicios financieros en EY y responsable de Data Analytics para el sur de Europa en AWS. Es profesor asociado en IE University, donde imparte la primera asignatura de grado sobre Customer Lifetime Value en España, investiga sobre el CLV en su doctorado en la Universidad Complutense de Madrid y es autor del libro "Customer Lifetime Value (CLV): No todos tus clientes valen lo mismo".

manueldelgado.com · LinkedIn · X

Recibe cada artículo en tu correo con la newsletter Ex Datis, Claritas: manueldelgado.com/newsletter/suscribete