

La regulación de la IA ya está aquí. La transparencia, todavía no

El uso de la IA crece mientras la información al usuario sigue siendo insuficiente

Fuente: Cinco Dïas

Mi conclusión, tras ver estos números, es sencilla y no pretendo suavizarla: la brecha entre lo que el Reglamento de IA exige ya hoy y lo que las empresas españolas están haciendo es amplia y no se explica sólo por la novedad de la norma. Cerrarla no exige un esfuerzo desproporcionado. Bastaría con identificar qué sistemas interactúan con personas físicas y qué contenidos generados con IA pueden considerarse *deepfakes*, para así ser transparentes sobre nuestro uso de la IA.

Hay, sin embargo, un dato que aporta cierta esperanza. No es una obligación legal, pero un 32% de empresas ya publica algún tipo de política o información sobre cómo usa la IA. No es una cifra brillante, pero no deja de ser positiva. El sector asegurador lidera este apartado, con más de la mitad de sus empresas informando, directa o indirectamente, sobre su uso de la IA.

Es cierto que la obligación de incluir esas advertencias corresponde a los proveedores de la solución, no a quien la implementa en sus canales de atención. Pero, desde un punto de vista de responsabilidad proactiva, es importante que el responsable de esos canales se asegure de que las soluciones que implementa cumplen este requisito, pensado para atender una necesidad real.

Alguien podría pensar que esto no es un problema real, porque ya resulta evidente que, al usar estos servicios, no hay una persona interactuando con nosotros. A eso cabría responder que no puede esperarse el mismo nivel de competencias digitales en toda la población (a nuestros mayores, y a otros colectivos ajenos a la tecnología, les resulta más difícil advertirlo). Además, cómo anécdota personal, a mí mismo me resultó complicado en algunos casos reales identificar si estaba interactuando con un sistema, hasta el punto de preguntar directamente al chat si era una IA y recibir por respuesta un mensaje de una persona diciendo que no. Si a alguien vinculado a esta materia le resulta poco intuitivo advertirlo, es normal que a otros colectivos también les cueste, y por eso es tan necesaria la advertencia expresa por parte de los responsables de estos sistemas.

Llamar asistente virtual a un *chatbot* con IA no es un error de estilo, es una decisión. Es la decisión de mantener cierta ambigüedad útil, la de no comprometerse del todo con lo que la ley exige.

Solo el 54% de los *chatbots* con IA lo dice de forma clara y directa. Del resto, un 41%, recurre a fórmulas ambiguas — asistente virtual o tu ayudante — que suenan bien pero que no cumplen con lo que pide la Comisión Europea, y otro 5% directamente no dice nada. El usuario escribe, recibe una respuesta y nunca sabe si al otro lado hay una persona, un sistema automatizado simple o un modelo de lenguaje generando texto en tiempo real.

Más preocupante es lo relativo a la segunda de las obligaciones y al uso de *chatbots*. Un 43% de las empresas atiende a sus clientes con algún asistente conversacional, y de ellas, un 84% usa técnicas de IA sujetas al Reglamento, no simples árboles de

decisión. Su adopción parece ir al alza y eso no es en sí un problema; el problema surge en cómo esos *chatbots* se lo comunican al usuario.

Puede preocupar, pero ese dato no tiene por qué ser malo. El 94% de empresas restantes puede no haber utilizado IA en sus contenidos; puede haberla utilizado sin que el resultado se califique como *deepfake* (corregir el brillo de una imagen o editar el fondo con fines estéticos no se considera *deepfake*); o puede (y este caso sí preocuparía) haber generado un *deepfake* y decidido, por acción u omisión, no marcarlo.

Sobre la primera obligación, aunque podemos suponer que la mayoría de las empresas ya usa IA para generar o editar sus contenidos, comprobamos que solo el 6% etiqueta ese contenido como generado o editado con IA.

El artículo 50 del Reglamento de IA introduce, entre otras, una obligación de marcar de forma visible los contenidos que generas o editas cuando pueden confundirse con algo real e inducir a un error (los llamados *deepfakes*, concepto que se ha interpretado de forma amplia por la Comisión Europea), y también la obligación de informar expresamente a las personas cuando están interactuando con un sistema de IA (un *chatbot*, un asistente automático en *contact centers*, etc.).

Hace unas semanas me propuse, junto a mis compañeros, comprobar cómo se están cumpliendo las obligaciones de transparencia en IA desde su entrada en aplicación el 2 de agosto. Seleccionamos un conjunto de las principales empresas (113 en total) que operan en España en distintos sectores y analizamos cómo parecen estar cumpliendo, en sus canales web, las obligaciones que les resultan de aplicación.