Societat

Els reptes d'una societat digitalitzada

La veu, nou forat per a la privacitat

L'ús creixent de missatges parlats i sistemes de reconeixement de la parla faciliten a les empreses perfils més complets dels seus clients i eleva el risc d'estafes per suplantació

MAYTE RIUS
Barcelona

Interactuar amb la tecnologia a través de la veu és tendència. La tramesa de missatges parlats per WhatsApp, demanar al navegador del cotxe que truqui a algú o autoritzar l'enregistrament de les nostres converses per contractar un servei formen part de la quotidianitat de moltíssimes persones. I cal afegir-hi els que recorren a Alexa, Siri o altres assistents virtuals per consultar informació, encendre els llums, canviar el canal de televisió o fer servir altres dispositius amb frases. O els que utilitzen la veu com a contrasenya. Entre unes accions i d'altres va creixent l'empremta vocal, el rastre de dades de veu que deixem. I la veu d'una persona revela moltes coses, sobretot si qui l'analitza no és un humà, sinó una màquina, una intel·ligència artificial.

"En un àudio hi ha molta informació, i una màquina pot capturar-la: es pot saber qui parla, l'emoció i la intenció de qui està parlant, el sexe, edat, procedència geogràfica i fins i tot l'estat de salut", resumeix l'investigador Javier Hernando, especialista en biometria de veu i director del Centre de Tecnologies i Aplicacions del Llenguatge i la Parla (Talp) de la UPC.

A les empreses tota aquesta informació els interessa, perquè permet crear un perfil més complet dels seus clients o usuaris. TikTok va començar a recopilar empremtes de veu l'any passat, i alguns centres d'atenció telefònica fan servir intel·ligència artificial per analitzar el comportament i les emocions de les persones durant les trucades, segons han advertit Henry Turner i Emmanuel Vicent, especialistes en tecnologies de veu de la Universitat d'Oxford (el Regne Unit) i de l'Institut Nacional d'Investigació de Ciència i Tecnologia Digital de França, respectivament, que han expressat públicament la seva preocupació per l'impacte que això té sobre la privacitat.

"Es pot saber l'emoció, la intenció, el sexe, l'estat de salut, l'edat i l'origen de qui parla", diu Javier Hernando

Al risc d'usos comercials s'hi afegeix el de la *deep voice,* la possibilitat que pirates informàtics clonin la veu d'una persona per fer-se passar per ella i cometre algun tipus de frau. "Ja s'ha vist algun cas de suplantació de veu per atacar algú del seu cercle proper i cometre una estafa monetària", explica Marc Rivero, analista de la firma de ciberseguretat i privacitat digital Kaspersky.

Un exemple d'aquestes estafes és el denominat frau del director executiu, en què l'estafador truca a un treballador amb accés als recursos econòmics fent-se passar per un alt càrrec de la companyia perquè, de manera urgent, pagui una factura o faci una transferència a un compte controlat pel delinqüent.

"És un tipus de frau que ara no té gaire impacte, però temem que augmentarà; hi pot haver ciberdelinqüents que s'especialitzin a suplantar la veu i en el futur aquest podria ser un frau tan comú com el *phishing* (la tramesa de correus electrònics fent-se passar pel banc o per una companyia de serveis per obtenir informació sobre un compte bancari o una targeta de crèdit)", comenta Ángela M. García Valdés, tècnica de ciberseguretat per a ciutadans de l'Institut Nacional de Ciberseguretat d'Espanya (Incibe).

Hernando explica que la intel·ligència artificial "ja permet generar una veu que s'assembli prou a la teva per enganyar una persona", de manera que "convé ser conscients que la veu són dades i cal ser caut quan es facilitin". Assenyala que no es tracta d'atabalar-se i deixar de parlar o distorsionar la veu per si un és gravat, perquè com a dada biomètrica, la veu està coberta per la normativa de protecció de dades i els usos que les empreses en poden fer són limitats.

Sí que aconsella que sempre se sospesi si val la pena utilitzar la veu per interactuar amb una màquina. "Per a una gestió important en línia com comprar un pis enmig de la pandèmia potser està justificat acceptar l'enregistrament de la nostra veu, però si és per comprar verdures a través d'Amazon potser no cal fer-la servir", comenta l'investigador de la UPC.

"No es tracta de tornar-nos paranoics, perquè no podem deixar de parlar per telèfon, però sí d'adoptar cauteles, utilitzar el sentit comú i tenir una mentalitat crítica sobre les trucades que ens fan per si intenten enganyar-nos", coincideix García Valdés.

Joana Marí, delegada de protecció de dades i responsable de projectes estratègics de l'Autoritat Catalana de Protecció de Dades (Apdcat), afirma que quan una companyia grava la nostra veu ha d'informar-nos sobre què farà amb aquestes dades, qui les tractarà i quins drets tenim, perquè està sotmesa a tota la normativa de protecció de

Algunes empreses fan servir intel·ligència artificial per analitzar el comportament i les emocions de les persones durant les trucades

dades. Però també recorda que "la veu té valor, i és una informació que es pot utilitzar de manera molt positiva o molt negativa, de manera que hem de ser conscients que quan deixem un rastre vocal en un dispositiu hi estem deixant alguna cosa de nosaltres, la nostra privacitat, intimitat, la nostra pròpia imatge i, per tant, abans de fer servir

"No es tracta de tornar-se paranoic, sinó de tenir sentit crític sobre les trucades que ens fan", diu García

la veu per utilitzar un dispositiu, hauríem de valorar si la comoditat compensa o no el risc".

Però més enllà que les persones siguin més o menys cautes en el moment d'interactuar a través de la veu, els experts en biometria i sistemes de reconeixement de veu creuen que aviat serà la mateixa tecnologia qui faciliti les eines per protegir la privacitat, ja sigui mitjançant sistemes d'anonimització o d'autenticació d'identitat.

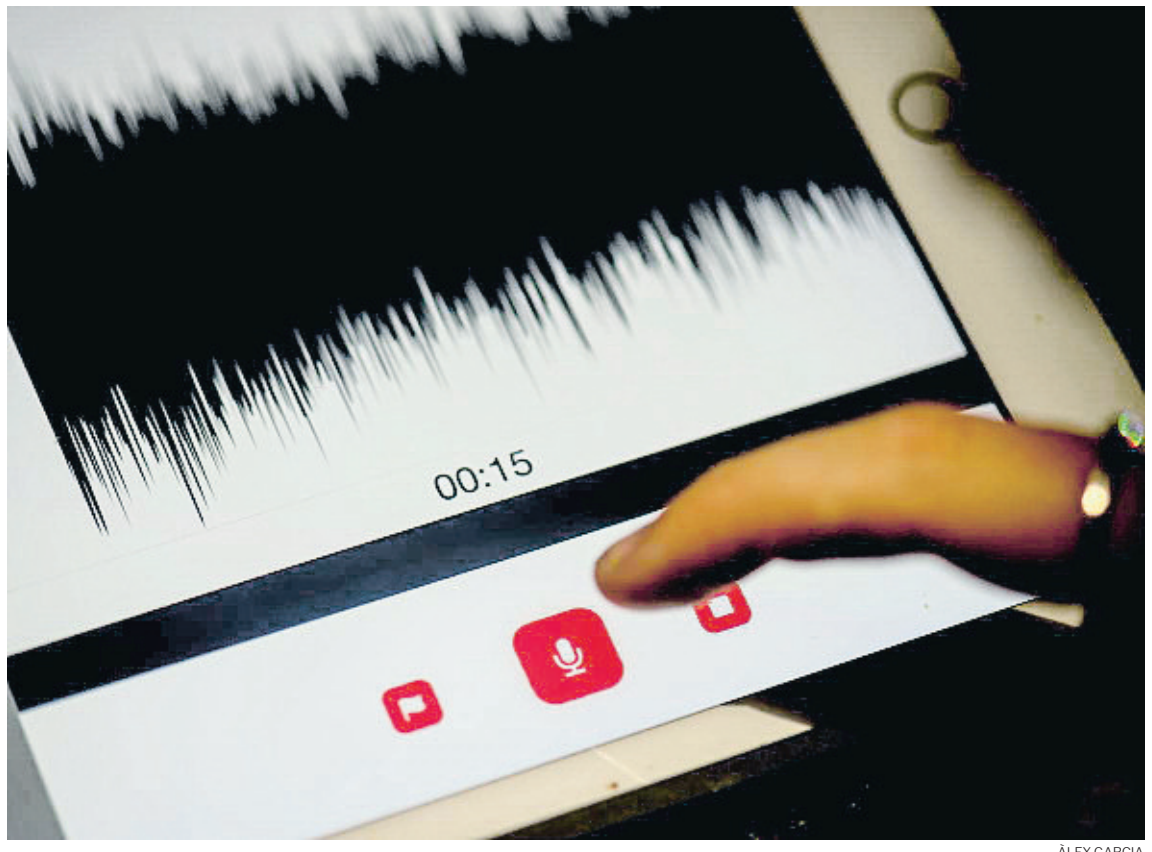
"La tecnologia està evolucionant molt ràpidament per evitar ser enganyada per enregistraments: una persona pot ser enganyada per un imitador, però una màquina amb sistemes ferms, ja no", assegura Hernando.

En la mateixa línia s'expressa Miguel Antonio García, responsable de màrqueting de Biometric Vox, empresa especialitzada en eines d'intel·ligència artificial que permeten identificar què es diu i qui ho diu mitjançant l'anàlisi dels paràmetres biomètrics del parlant. Avui aquests sistemes de verificació i autenticació els fan servir bancs, companyies d'assegurances i de venda directa o l'ONCE per fer operacions segures a través de la veu, però García està convençut que en un futur seran moltes més les empreses i els particulars que els incorporin per detectar de manera automàtica si qui truca és qui diu que és. "Igual que ara utilitzem de manera generalitzada antivirus per evitar *phishing* i altres fraus, farem servir aplicacions de biometria de veu per autentificar la identitat digital dels altres", afirma.●

ÀLEX GARCIA

Qui custodia els enregistraments

■ **"Qualsevol entitat que fa servir un sistema d'enregistrament de veu ha de complir la normativa de protecció de dades, perquè la veu és una dada de caràcter personal que permet identificar una persona", explica Joana Marí, de l'Apdcat. Això significa que s'ha d'informar la persona de qui és el responsable del tractament de les dades, quina tecnologia s'utilitza per tractar-les, tenir base jurídica (un motiu) per recollir-les i fer-les servir únicament per a aquesta finalitat i, si s'utilitzen per a una cosa diferent, anonimitzar-les. Marí afegeix que, si la veu es fa servir com a dada biomètrica per verificar la identitat d'una persona, aleshores s'exigeixen més mesures de seguretat i protecció, com disposar del consentiment explícit o una avaluació d'impacte si s'analitza mitjançant intel·ligència artificial. El que no hi ha, assenyala l'experta en protecció de dades, és un termini màxim per guardar els enregistraments de veu. "Segons per a què recullis les dades podràs mantenir-les més o menys temps i només podràs recollir les dades necessàries per a aquesta finalitat", conclou.**



ÀLEX GARCIA

To, timbre, freqüència i cavitat buconasal fan que cada parlant tingui una empremta vocal única

Tecnologies que garanteixen amb qui s'està parlant

Sistemes d'IA verifiquen la identitat per l'empremta vocal

M. RIUS Barcelona

El to, el timbre, la freqüència vocal i la cavitat buconasal són factors que determinen que cada parlant tingui una empremta vocal única, cosa que la converteix en un instrument molt útil per autentificar persones o, en la societat actual, identitats digitals.

"Avui es poden signar contractes només amb la veu, es fa servir com a biomarcador per analitzar l'estat de salut, en activitats pericials de processos judicials... Per tant, és fonamental garantir amb quina persona estem parlant", exemplifica Miguel Antonio García, director de màrqueting de Biometric Vox. I explica que la tecnologia actual facilita dos processos d'autenticació de veus molt segurs.

El primer, la verificació, consisteix a registrar una persona com a usuari d'una empresa o servei a través de l'empremta vocal que deixa quan diu una paraula clau o una contrasenya. Després, quan vulgui accedir a aquesta empresa o servei, només caldrà que repeteixi la paraula o contrasenya. "És un sistema còmode i ràpid, molt útil per a persones grans o amb discapacitat visual", comenta García.

La segona opció d'autenticació és la identificació, en què l'empremta vocal que es registra no és una paraula, sinó una conversa de 20 o 30 minuts. I quan la persona vol operar amb un banc o empresa, es comprova si la veu coincideix amb l'empremta vocal que es té registrada a la base de dades.

García subratlla que la biometria de veu té tres característiques que la fan molt segura com a sistema d'identificació: és abstracta (no és una contrasenya que puguin robar), és irreversible (a partir de la veu es pot dissenyar l'empremta vocal, però des de l'empremta no es pot replicar la veu, perquè només es guarden paràmetres encriptats i anonimitzats que identifiquen la veu) i es pot cancel·lar (a petició de l'usuari s'esborra i, si la base de dades fos atacada per hackers, podrien donar-se de baixa totes les empremtes vocals i tornar a registrar tots els usuaris).

"Les empreses que graven la veu han de complir la normativa de protecció de dades", indica Marí

Tant el directiu de Biometric Vox com l'expert en biometria i tecnologies de la parla de la UPC Javier Hernando subratllen que aquestes eines d'intel·ligència artificial són molt robustes i, a diferència de la majoria d'humans, són capaces de detectar les imitacions, els enregistraments de veu o les veus digitals, de manera que eviten suplantacions d'identitat. "La nostra tecnologia *antispoofing* (suplantació d'identitat) detecta imitacions o còpies duplicades, perquè és matemàticament impossible que, quan repeteixo una contrasenya o dic una paraula, sempre trigui els mateixos segons o ho digui exactament igual i, per tant, si una mostra de veu és molt semblant a una altra d'anterior, el sistema la rebutja; i també detecta enregistraments o còpies sintetitzades (*deepvoices*), perquè emeten unes ones que no té la veu humana", detalla García. Hernando comenta que aquestes tecnologies de reconeixement de veu són auditades per pèrits externs i cada any se sotmeten a proves i reptes d'equips d'investigació i agències de seguretat nacionals i internacionals per veure quins sistemes són els més ferms, els menys enganyats per enregistraments.●

Els sistemes antisuplantació detecten imitacions, enregistraments i còpies sintetitzades