Lo scandalo delle sorveglianze illegali

# Le indagini dei pm a portata di hacker le intercettazioni nel server all'estero

**DARIO DEL PORTO**
**CONCHITA SANNINO,** NAPOLI

Destinazione Oregon, Usa. Uno sterminato "archivio" digitale con i dati sensibili di innumerevoli cittadini italiani è ancora lì, su un server di *Amazon*: con il rischio di «finire sulla rete internet pubblica», utile a scopi anche inquietanti, attività di dossieraggio o lavoro di apparati d'*intelligence*. È l'allarme del gip Rosa De Ruggiero, dopo lo scandalo sul software per investigazioni *Exodus*.

L'inchiesta della procura di Napoli ha ormai accertato come migliaia di messaggi e conversazioni intercettate – o su persone indagate per conto delle Procure di mezza Italia, o su ignari cittadini illecitamente controllati attraverso virus-spia – siano finiti all'estero, senza alcuna protezione, in uno spazio *cloud* acquistato sulla piattaforma internet americana. Nel materiale che scotta, anche indagini della Dcsa, la Direzione centrale antidroga. Tutto in violazione della legge sulla privacy, e all'insaputa delle forze di polizia e dei pm.

È quanto emerge dalle indagini coordinate in prima persona dal procuratore Gianni Melillo – pm Curatoli e Onorato, del pool cyber-crime già costituito presso la procura – dopo il sequestro di due società: la calabrese *eSurv* produttrice del software (*Exodus*), e la *Stm srl* che ne acquistava i servizi e li forniva alle procure, risultando vincitrice di appalti in varie città. Quattro gli indagati. Ma ora i magistrati dovranno rispondere alla domanda centrale: esistono burattinai, in questa storia? E che veste e quali obiettivi hanno? Uno scenario tutto da comporre: e gira intorno alla trama che dalla profonda Calabria risale lo Stivale e arriva in tutto il mondo.

**Quattro persone sotto accusa per il software usato per controllare i telefonini e fornito pure alle procure. Uno confessa: ho diffuso la trappola informatica senza autorizzazioni**

Sotto inchiesta finiscono – per ora – Giuseppe Fasano, 76enne rappresentante legale di *eSurv*, Salvatore Ansani, 43enne ingegnere informatico e direttore delle infrastrutture della stessa società, Maria Aquino e Vito Tignanelli, rispettivamente rappresentante legale e amministratore di fatto della *Stm*. Rispondono tutti di violazione della privacy e frode in pubbliche forniture; ma Ansani e Fasano anche di intromissione abusiva in sistema informatico. Uno scenario inquietante che si basa su alcune ammissioni. È stato Ansani, messo alle strette durante i primi accertamenti della procura di Benevento, a rivelare di aver inondato la rete di numerose app per cellulari che, una volta scaricate da ignari cittadini, funzionavano esattamente come virus-spia: infettavano i telefonini, trasformandoli in microcamere fuori da ogni controllo, men che meno giudiziario. Le motivazioni? Erano dei test, è la singolare risposta di Ansani. Ma il contagio allarma il gip che ha disposto il sequestro. E avverte: quei dati potrebbero essere «usati per le finalità più varie».



L'inchiesta *I pericoli dei sistemi vocali*

# Parla con me (e ti spierò) così auto e case intelligenti rubano i nostri segreti

**GIULIANO FOSCHINI**
**FABIO TONACCI,** ROMA

Mentre leggete questo articolo è possibile che qualcuno vi stia ascoltando. Se siete a casa, la spia potrebbe essere uno degli assistenti vocali come *Amazon Echo*, *Google Home Mini* e *Apple HomePod*. O magari la smart tv che avete autorizzato a funzionare attraverso comandi impartiti con la voce. Se invece siete in auto, rischiate di essere registrati dal microfono che avete sopra la testa, collegato al computer di bordo connesso a sua volta alla Rete con una sim card. Esattamente come il vostro cellulare, su cui avete installato decine di app gratuite che

**Così ci spiano**
**2**

possono aprire il microfono senza avvertirvi. Se Internet, dunque, vi ha proposto via mail o con un'inserzione pubblicitaria su Facebook proprio il prodotto di cui avevate appena parlato – e solo parlato, senza cercarlo sul web – con un amico, la colpa non è del caso. Ma di una di quelle orecchie digitali che accumulano silenziosamente informazioni e le spediscono da qualche parte nel cloud dei colossi del web.

### L'abitazione smart

In questo momento il luogo più "pericoloso" è proprio casa vostra: ci sono gli assistenti vocali, appunto, ma anche il frigorifero smart, l'aspirapolvere e il robot da cucina azionabili dal telefonino, la tv intelligente. C'è l'Internet delle cose, insomma. Tutto ciò che va online e possiede una telecamera o una videocamera, può registrare. Ed essere controllato da intrusi. Due anni fa è successo: un hacker ha scoperto una falla nel sistema di protezione degli aspirapolveri Lg, è penetrato nella rete interna e attraverso la telecamera della tv ha guardato per giorni ciò che succedeva in quella casa. Lo stesso può accadere con le vetture. Spiega l'informatico Michele Ferrazzano, consulente di alcune procure italiane e docente universitario che studia da anni i rischi delle auto connesse. «Le vetture hanno computer di bordo con microfoni integrati, che servono per gestire situazioni di emergenza come un incidente, ma allo stesso tempo tracciano l'automobilista carpendo le sue parole».

### Ascoltati a nostra insaputa

Ma è lecito? La maggior parte delle volte, sì. Siamo noi ad accettare senza leggere le clausole della privacy. Prendiamo Siri, l'assistente vocale di Apple. «Quando utilizzi Siri – riporta il consenso informato – il dispositivo invierà ad Apple anche altre informazioni, quali: il tuo nome e il tuo soprannome; i nomi e i soprannomi dei tuoi contatti e la relazione che hanno con te; i nomi dei brani delle tue raccolte, i nomi dei tuoi album fotografici e i nomi delle app installate sul tuo dispositivo». Ovviamente spiegano che tutto ciò serve per aiutare Siri a riconoscere le domande poste dall'utente, e che la registrazione si attiva solo dopo una parola chiave, in questo caso "Hey Siri". «Ma – osserva Gerardo Costabile, ex finanziere e fondatore della società di cybersecurity DeepCyber – è fin troppo ovvio dire che sono sempre accesi, altrimenti non potrebbero reagire alla parola chiave. I dispositivi che registrano l'audio imparano il vocabolario di chi parla, e questo gli consente di rendere la profilazione ancor più invasiva e personale».

### Il grande sospetto

Ufficialmente i padroni dei Big Data negano che i loro microfoni registrino quando non sono stati attivati dalla parola chiave. E sostengono che ogni 10 secondi ciò che viene captato è cancellato con un rumore di fondo. Due "incidenti", però, uno in Germania nel dicembre scorso, l'altro negli Stati Uniti, dimostrano che la faccenda dei microfoni è tutt'altro che pacifica. A un ragazzo tedesco, infatti, Amazon ha inviato una mail con 1.700 file audio registrati nella casa di uno sconosciuto. Mentre le chiacchiere private di una coppia di Portland sono state registrate a loro insaputa da Alexa (l'assistente vocale di Echo) e il file audio è stato inviato a un loro amico a Seattle. «Un errore umano», è stata la giustificazione per il primo "incidente". Per il secondo, i tecnici della società di Jeff Bezos hanno attribuito la colpa a «una concatenazione di improbabili eventi: Echo si è acceso perché ha percepito una parola simile a quella di attivazione ("Alexa") e ha spedito l'audio perché ha mal interpretato pezzi di dialogo».

In Italia il professor Stefano Fratepietro, già amministratore delegato di Tesla Consulting, sta conducendo un progetto di ricerca sugli assistenti vocali. «Non credo al Grande Fratello che ci ascolta h24, anche perché la mole di informazioni trasmessa via Internet nei database di Amazon non è compatibile, finora, con tale ipotesi».

### Il rischio spionaggio industriale

Non sono solo le grandi compagnie a volerci ascoltare. «Si rischia anche dello spionaggio industriale – ipotizza Ferrazzano – craccare i computer di bordo delle auto di lusso, dove viaggiano dirigenti di alto livello, non è impossibile: nei veicoli molte componenti informatiche sono a basso costo e con un livello ridotto di protezione. Basta anche solo penetrare nel sistema che regola la pressione degli pneumatici per attivare il microfono interno». E trasformare l'auto in una cabina d'ascolto.

**– 2. continua**



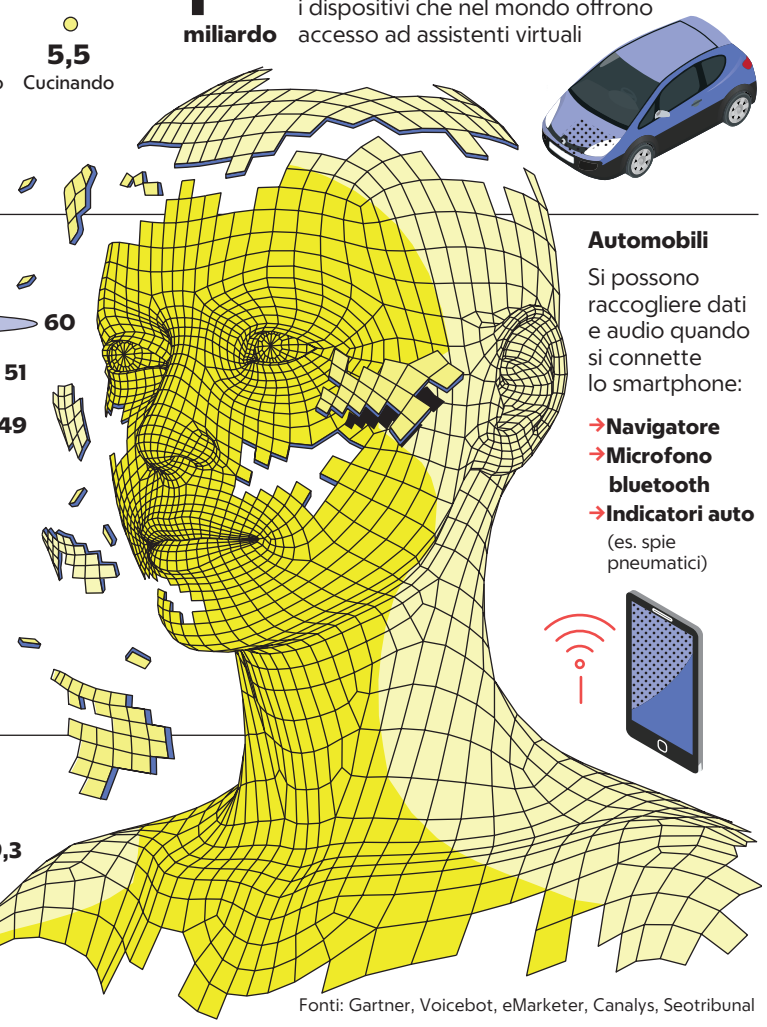
## Le ricerche vocali

**Quando si fanno ricerche vocali**

In %

52,8 Guidando
21,3 Camminando
7,5 Guardando la tv
5,5 Cucinando

**1 miliardo** i dispositivi che nel mondo offrono accesso ad assistenti virtuali



**Cosa si cerca**

In %

| | |
|---|---|
| Informazioni generiche | 60 |
| Informazioni su un prodotto | 51 |
| Domanda scherzosa | 49 |
| Indicazioni stradali | 42 |
| Chiamare qualcuno | 41 |
| Avviare un brano musicale | 41 |
| Previsioni meteo | 40 |
| Trovare un esercizio commerciale | 34 |

**Automobili**

Si possono raccogliere dati e audio quando si connette lo smartphone:

→ **Navigatore**
→ **Microfono bluetooth**
→ **Indicatori auto** (es. spie pneumatici)

**Le ricerche vocali in base all'età**

Dati 2018, in %

| | |
|---|---|
| Millennials (nati dopo il 2000) | 39,3 |
| Generazione X (1960-1980) | 17,2 |
| Baby Boomers (1946-1964) | 10,1 |

Fonti: Gartner, Voicebot, eMarketer, Canalys, Seotribunal

**Capo della redazione Cronaca** Giancarlo Mola

**Email redazione** cronaca @repubblica.it