Lavori da casa? Sarà meglio spegnere Alexa



Davvero vorresti che informazioni confidenziali finissero nelle mani di sconosciuti?

«Forse siamo un po' paranoici» – ammette l'avvocato Joe Hancock, dello studio legale britannico Mishcon de Reya – *«ma ci viene richiesto di riporre molta fiducia in queste organizzazioni e in questi dispositivi. Preferiremmo non assumerci questi rischi»*.

La paranoia e la fiducia di cui parla l'avvocato Hancock riguardano un'unica classe di oggetti (e le aziende che li producono): gli assistenti personali virtuali – come Alexa, ma anche Google Assistant e Siri – cui pressoché tutti possono accedere dallo smartphone e molti dallo smartspeaker.

Li abbiamo sempre vicino, sono in grado di captare ciò che diciamo (sia perché glielo ordiniamo, sia per errore) e di ciò che hanno registrato fanno un uso che nel recente passato s'è dimostrato non esattamente trasparente.

Così è capitato che spezzoni di conversazioni private (e a volte imbarazzanti) finissero nelle orecchie di sconosciuti,

senza che chi quelle a conversazioni aveva partecipato ne sapesse niente.

Il che è un problema già consistente quando si parla di argomenti normali e banali come capita spesso tra persone che vivono sotto lo stesso tetto, ma può diventare veramente grosso quando sotto quel tetto si lavora.

In epoca di telelavoro forzato, dove quanti hanno un impiego "da scrivania" hanno attrezzato una sorta di ufficio domestico, bisogna tenere conto di tutti i fattori che differenziano la stanza di casa adibita a ufficio dal luogo di lavoro reale.

Uno di questi fattori è la possibile presenza degli smart speaker – i vari Amazon Echo, Google Home o Nest e via di seguito – dotati di assistenti vocali, che a questo punto possono assorbire informazioni confidenziali e segreti inerenti l'attività lavorativa.

Ecco quindi che lo studio Mishcon de Reya ha chiesto ai suoi dipendenti che lavorano da casa di zittire o, meglio ancora, disabilitare completamente gli assistenti domestici durante le chiamate di lavoro.

Hancock ammette che, dopo le modifiche apportate al modo in cui vengono gestite le conversazioni registrate, è meno probabile essere spiati da Amazon o Google che da un prodotti di una marca sconosciuta o poco nota. D'altra parte, la prudenza non è mai troppa.

Più volte abbiamo ripetuto che usare uno smart speaker significa mettersi in casa un microfono aperto, e nutrire una fiducia sostanzialmente assoluta verso le aziende che li producono: un po' troppo, per chi tratta informazioni confidenziali.