DATA PROTECTION

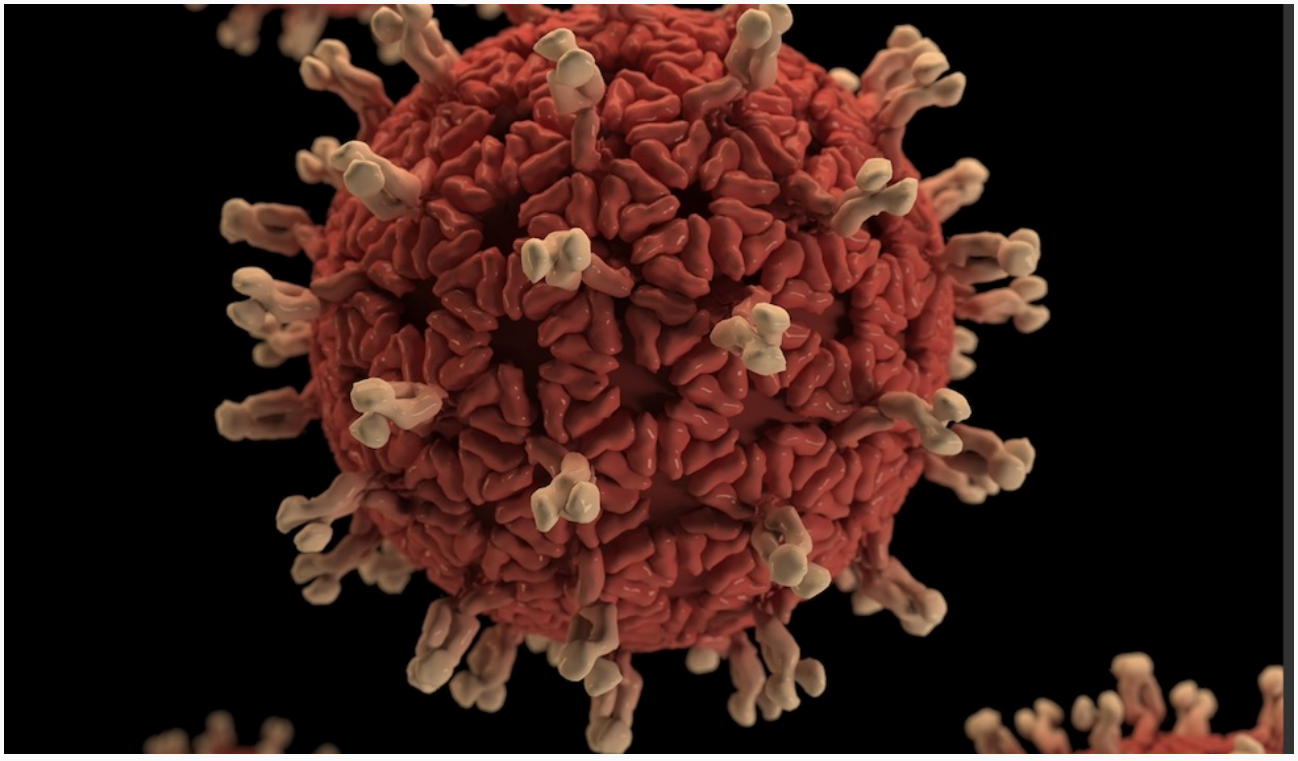
Covid19, termoscanner con riconoscimento facciale: si rischiano multe fino a 20 milioni

Condividi questo articolo

Un conto è distinguere i volti da altri elementi ripresi dalla telecamera, un altro è identificare l'individuo a partire dall'immagine. Gli strumenti di misurazione della temperatura integrati con quelli di rilevazione degli accessi implicano un trattamento di dati biometrici soggetto a stringenti requisiti. L'analisi dell'avvocato Mattia Salerno

26 Ott 2020

Mattia Salerno
avvocato Pirola Pennuto Zei & Associati



I protrarsi della pandemia da virus Covid-19 e la conseguente perdurante applicazione della normativa emergenziale (e, in particolare, del "**Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della**

diffusione del virus Covid-19 negli ambienti di lavoro" dello scorso 24 aprile) hanno reso l'adozione di **strumenti di misurazione della temperatura corporea una necessità imprescindibile per le aziende italiane**.

All'interno del mare magnum di tecnologie di rilevazione della temperatura offerti dal mercato, vengono in rilievo, in particolare, **i sistemi dotati di funzionalità di riconoscimento facciale**, che consentono di effettuare anche operazioni ulteriori rispetto alla semplice misurazione della temperatura, quali, ad esempio, la rilevazione della presenza della **mascherina sul viso e del mantenimento delle distanze di sicurezza**. Alcune soluzioni, poi, offrono persino la **possibilità di integrare le telecamere di riconoscimento facciale con i sistemi di rilevazione degli accessi**, eliminando la necessità per i dipendenti di registrare manualmente ingressi e uscite ed evitando gli assembramenti che ne derivano. La rilevazione degli accessi tramite riconoscimento facciale, tuttavia, comporta diverse criticità dal punto di vista della normativa in materia di protezione dei dati personali.

In tale contesto, è necessario soffermarsi preliminarmente sulla differenza semantica tra due nozioni di riconoscimento facciale, che può essere inteso, da un lato come **capacità di distinguere i volti dagli altri elementi ripresi dalla telecamera**, dall'altro, come c**apacità di identificare l'individuo a partire dall'immagine del volto**. **Tale dicotomia comporta notevoli differenze dal punto di vista della normativa** in materia di **data protection**, in particolare alla luce del **Considerando 51 del Gdpr**, in cui si chiarisce che "il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica".

Di conseguenza, se da una parte, **nella maggior parte dei casi, i termoscanner dotati di funzionalità di riconoscimento facciale intese secondo la prima accezione effettuano unicamente trattamenti di immagini** (dati personali soggetti alle usuali tutele previste dal Gdpr), dall'altra **gli strumenti di misurazione della temperatura integrati con i sistemi di rilevazione degli accessi configurano un riconoscimento facciale della seconda tipologia** e, pertanto, **implicano un trattamento di dati biometrici, soggetto a stringenti requisiti**.

★ WEBINAR - 3 NOVEMBRE

CISO as a Service: perché la tua azienda ha bisogno di un esperto di Cyber Security?

Sicurezza # Cybersecurity

E-mail

E-mail aziendale

Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

ISCRIVITI

Trattasi, infatti, di categorie particolari di dati personali soggette alle **garanzie di cui all'art. 9 del Gdpr,** che consente **il trattamento di tali dati solamente in presenza di precise condizioni**, quali ad esempio il consenso dell'interessato, la

necessità di assolvere obblighi o esercitare diritti del Titolare del trattamento/dell'interessato in materia di diritto del lavoro o per motivi di interesse pubblico rilevante.

Partendo dall'assunto che il consenso non può essere individuato quale base giuridica idonea per trattare tali categorie di dati personali nell'ambito del rapporto di lavoro (a maggior ragione se si tratta di dati particolari), ne consegue che l'organizzazione che intenda installare un sistema di misurazione della temperatura integrato, tramite funzionalità di riconoscimento facciale, al proprio time and attendance management system non può condizionare l'accesso alle proprie strutture al consenso dei dipendenti al trattamento dei dati biometrici. Pertanto, come osservato dallo stesso Edpb, l'organizzazione in ogni cas dovrebbe offrire una soluzione alternativa che non comporti il trattamento biometrico, mantenendo, ad esempio, il "vecchio" **sistema di vidimazione tramite badge**.

Fermo quanto precede, a parere di chi scrive, ancor prima di interrogarsi su questioni relative al consenso e all'introduzione/mantenimento di sistemi alternativi di rilevazione degli accessi, l'organizzazione che intenda implementare un tale sistema deve **preliminarmente verificare che la sua adozione non violi il principio di proporzionalità**, ossia che il trattamento di dati biometrici non sia sproporzionato rispetto alle finalità che intende raggiungere (nel caso di specie, la rilevazione egli accessi). Sul punto, giova ricordare che lo **European Data Protection Supervisor** ha ritenuto che l'adozione di sistemi biometrici di rilevazione degli accessi da parte di istituzioni Ue (non, quindi aziende private) configuri una **violazione del principio di proporzionalità**, in quanto la medesima finalità poteva essere raggiunta con mezzi meno intrusivi. Di fatto, il test di proporzionalità può essere validamente superato esclusivamente in situazioni eccezionali, ad esempio in caso di adozione da parte di aziende facenti parte del comparto della difesa.

Alla luce di queste considerazioni, è chiaro che la possibilità di **adottare termoscanner integrati ai sistemi di rilevazione degli accessi tramite funzionalità di riconoscimento facciale è riservata a pochi casi molto particolari** e, quindi, preclusa alla maggior parte delle aziende, a causa della forte invasività del trattamento di dati biometrici. In assenza di tali particolari condizioni, peraltro, l'azienda che dovesse adottare un tale sistema **si esporrebbe a sanzioni pecuniarie amministrative estremamente gravose**. Trattandosi infatti di violazioni dei principi del trattamento (art. 5 Gdpr) e dell'art. 9 del Gdpr, troverebbero applicazione s**anzioni fino a 20 milioni di euro o, se superiore, fino al 4 % del fatturato annuo (di gruppo) dell'esercizio precedente.**

@RIPRODUZIONE RISERVATA

29 Ottobre

Dati strutturati e Image Recognition: AI, la nuova frontiera dell'impresa intelligente

Argomenti del webinar

Artificial Intelligence | image recognition | machine learning

Inizia tra 1 gg 5 ore 5 min 34 sec

ISCRIVITI

White Paper

Digital transformation e sanità: come garantire incolumità, sicurezza e privacy dei pazienti

28 Feb 2020

Argomenti del whitepaper

privacy | sanità | Sicurezza

Scaricalo gratis!

DOWNLOAD

Argomenti trattati

Approfondimenti

B biometria | C covid19 | G GDPR | P privacy

Articoli correlati