ATTUALITÀ

Biometria e sicurezza, la sottile linea della privacy

di **Fondazione AIDR** · 11 aprile 2022, 16:22

di Biagino Costanzo, dirigente d'azienda e Responsabile dell'Osservatorio Security, Cyber, Safety, Ethic di AIDR

Ha fatto il giro del mondo, pochi giorni prima della folle invasione dell'Ucraina, la foto dove la distanza tra Putin e Macron sul tavolone bianco di rappresentanza testimoniava, plasticamente, non solo una voragine tra i due sul dossier Ucraina, appunto, ma il semplice motivo della necessità di mantenere il distanziamento sanitario, infatti, il presidente francese che aveva già fatto un tampone in partenza da Parigi, all'arrivo a Mosca è stato bloccato dalla propria intelligence nel rifare un test, voluto dai russi, dove chiaramente il rischio paventato era la sottrazione dei dati biometrici dei leader stranieri. Infatti, stesso consiglio i Servizi tedeschi hanno dato a Olaf Scholz al suo arrivo nella capitale russa, ma, comunque, per poter incontrare il presidente russo i due leader europei si sono sottoposti ad un cd Pcr eseguito però dai medici delle rispettive ambasciate e con apparecchiature portati dalle rispettive nazioni e il personale medico russo è stato invitato ad assistere alla prova.

È storia nota e antica quella per la quale tutti i servizi di intelligence del mondo siano interessati ai dati biometrici delle persone. Ma per quale motivo?

È risaputo anche che l'acquisizione del DNA umano è possibile ottenerlo anche prendendo il bicchiere usato o qualche capello lasciato su una sedia sul cuscino dell'hotel ospitante ma la leggibilità e la chiarezza dei dati è massima prelevando appunto da un test per il Covid, è tutto questo è merce preziosa, infatti, le tracce genetiche sono quelle più sensibili e personali.

Conoscere il DNA di un essere umano significa saper tutto di lui e quando le guerre non sono più quelle convenzionali ma si alimentano di quasi tutto quello che ormai ci circonda, l'informazione, la salute di un soggetto, e innanzitutto la cibernetica, avere una lista di DNA della maggior parte di individui che vanno dai leader a chi ricopre incarichi istituzionali o manager di industrie

partecipate ma fino al semplice cittadino.

Ricordiamoci che dai diversi dati biometrici è ormai possibile dedurre l'origine etnica e razziale o anche lo stato di salute di un individuo e ulteriori dati di natura particolare

Negli ultimi anni il numero di dispositivi in grado di trattare dati biometrici è aumentato in modo vertiginoso. Dai semplici diffusissimi smartphone, ai wearable device, al mondo della videosorveglianza, da quella basica a quella intelligente con funzionalità di riconoscimento, sempre più strumenti sono in grado di rilevare caratteristiche fisiche, fisiologiche o comportamentali che consentono l'identificazione univoca degli interessati.

Ed è qui che entra in gioco la normativa relativa al "famigerato "trattamento dei dati e alle implicazioni relative alla legittimità, alla compliance e ai principi del GDPR e agli interventi del Garante della privacy.

Mettendo per il momento da parte, nel nostro ragionamento, l'uso che gli apparati di sicurezza sono autorizzati a utilizzare ai fini della sicurezza nazionale, l'utilizzo dei sistemi di riconoscimento biometrico in un contesto lavorativo ha implicazioni relativamente alla legittimità del trattamento stesso.

Infatti, dinanzi alla rapida ascesa degli strumenti che trattano dati biometrici, il Garante ha sempre assunto un atteggiamento rigido al fine di garantire il rispetto della dignità della persona, dell'identità personale e dei semplici principi di finalità e proporzionalità.

La finalità di identificazione e di sorveglianza non può giustificare qualsiasi utilizzo del corpo umano che l'innovazione tecnologica può rendere possibile e giustificabile.

Prendiamo ad esempio il contesto lavorativo. Il titolare di una azienda o il Datore di Lavoro, in una ottica di un utilizzo di sistemi di riconoscimento biometrico per verificare l'effettivo svolgimento della prestazione lavorativa e permetterebbe di conoscere con assoluta certezza chi realmente stia svolgendo il proprio lavoro ma questo confligge in modo evidente con la protezione dell'identità e quindi con uno dei principi generali dettati dal GDPR.

Il titolare, quando parliamo di questa tipologia di trattamento, deve far fronte a diverse variabili; innanzitutto saper ponderare l'effettiva necessità e proporzionalità dello stesso, poi il saper individuare la giusta base giuridica di applicazione.

È infatti certo che i processi di autenticazione all'accesso basati sulle password hanno il 100% di meticolosità, ricordiamo che la password inserita da un user specifico può essere corretta, e l'accesso consentito, oppure non corretta, e l'accesso quindi negato ma se parliamo di dati

biomedici questo non vale, infatti questi possono presentare anche se residualmente dei falsi positivi

Di fatto la raccolta di tali dati, per la loro peculiare natura, richiede l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati.

È quindi necessario esser coscienti che l'uso di dati biometrici deve esser sempre esser giustificato e solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione appunto ai luoghi di lavoro, per presidiare accessi ad "aree riservate e/o sensibili", definitive tali considerando la natura delle attività in esse svolte.

Pensiamo, ad esempio, in aree dove si svolge attività e processi produttivi pericolosi o a quelle sottoposte alla custodia di infrastrutture, progetti, documentazione, apparecchiature HW e SW o beni classificati "segreti" o riservati che ai fini di legge debbono essere presidiate e controllate H24.

Bisogna ricordare che in Industria 4.0 sono presenti numerose tecnologie che riguardano il trattamento di dati biometrici e nell'ambiente industriale con progresso tecnologico avanzato questi dati sono ampiamente utilizzati.

Di cosa parliamo quando si cita "progresso tecnologico avanzato"?

Parliamo di categorie non futuristiche ma soluzioni che riguardano già oggi la robotica cd indossabile, quindi tute speciali realizzate grazie alle scansioni del corpo dei lavoratori, oppure le postazioni di lavoro auto adattive, ovvero costruite in base alle caratteristiche proprie di chi deve occuparle o gli esoscheletri per applicazioni industriali volti ad aumentare le capacità operative dei lavoratori che svolgono attività o manuali o di movimentazione.

Insomma, quando si utilizzano tecnologie sempre più avanzate ed invasive che coinvolgono sempre più la "persona" considerando inoltre che parliamo di lavoratori, è assolutamente necessario saper bilanciare gli interessi in gioco per valutare la necessita e la proporzionalità del trattamento dei dati biometrici e attribuire il giusto peso alla valutazione del rischio inerente al trattamento stesso. Questo sta a significare, prevedere soluzioni che devono portare al rendere anonimi i dati tracciati o la limitazione temporale della conservazione degli stessi.

Il rischio aumenta esponenzialmente quando si acquisiscono tutte queste informazioni se non viene mitigato dalla garanzia di un controllo severo. Infatti è bene tener a mente che le conseguenze di un data breach di dati biometrici sarebbero davvero, potenzialmente molto gravi, bisogna infatti considerare che al contrario delle password tradizionali, un dato biometrico non

può essere modificato né cancellato.

Ecco perché nel GDPR, alla sezione riguardante il trattamento dei biometrici, è previsto un divieto generale e una tutela rafforzata proprio la natura particolare del tema, per dove vi è la possibilità di derogare solo in presenza di specifiche eccezioni.

Parliamo, ad esempio e innanzitutto del consenso da parte dell'interessato, dell'assolvimento degli obblighi e l'esercizio dei diritti del titolare o dell'interessato in materia di diritto del lavoro, ed infine i motivi di interesse pubblico rilevante, quali per esempio la Sicurezza Nazionale degli Stati membri dell'Unione.

In conclusione non possiamo non constatare che con l'aumento dei rischi dovuti agli attacchi terroristici e, in generale, da una criminalità organizzata sempre più sofisticata, è contemporaneamente aumentata l'esigenza di garantire la sicurezza dei cittadini soprattutto quando si devono proteggere luoghi pubblici cd "ad alto rischio" quali stazioni ferroviarie, aeroporti, porti, etc ,etc ed è naturale, direi, che anche l'utilizzo della biometria costituisce un alleato più che valido per poter individuare soggetti potenzialmente pericolosi per la collettività, con la possibilità di poter misurare con metodologie statistiche e matematiche, tutte le possibili variabili fisiologiche e comportamentali proprie delle persone.

Ma tutto questo deve esser svolto in un contesto di massima serietà professionale, deontologica, rispettando la legge e al tempo stesso esser coscienti che una materia così delicata come questa deve essere gestita da veri professionisti in possesso, direi, anche di un alto dato valoriale ed etico. Solo così si riuscirà a coniugare, con successo, progresso, diritti, lavoro, business e sicurezza.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2022/04/11/biometria-e-sicurezza-la-sottile-linea-della-privacy/

© 2026 Istituzioni24