COVID-19: contrasto e prevenzione tra tecnologia, privacy e criteri da seguire

avv. Maria Cupolo | Consulente, esperto Privacy & Data Privacy Officer

L'emergenza epidemiologica di queste settimane ha richiesto interventi da parte delle autorità competenti e confronti serrati anche su temi che coinvolgono l'utilizzo delle tecnologie, la tutela dei diritti e la privacy per prevenire e, soprattutto, contrastare la diffusione del virus COVID -19.

Sin dal primo momento, nonostante l'errato messaggio rispetto ad una "sospensione" della privacy - messaggio spesso veicolato dal clima poco sereno del momento - è stato invece chiaro l'invito rivolto dalla stessa Autorità Garante per la protezione dei dati italiana e anche dal gruppo EDPB (Comitato Europeo per la protezione dei dati), a non prendere iniziative "fai da te" ma, soprattutto, a non considerare la privacy come un ostacolo. E' stato pure ribadito che la finalità di prevenzione dalla diffusione del Coronavirus potesse essere invece svolta da soggetti che istituzionalmente esercitano queste funzioni in modo qualificato, secondo i requisiti richiesti ai fini del trattamento per tutelare i soggetti coinvolti ovvero in base alla normativa vigente.

Sul tema, è tornato il protocollo siglato il 14 marzo sulla sicurezza sui luoghi di lavoro, nel quale è emerso come potesse essere possibile il trattamento anche da parte dei soggetti privati - pur dovendo garantire il rispetto dei principi normativi di cui al GDPR - per perseguire finalità quali la tutela dei lavoratori, la loro salute e, dunque, la prevenzione nei luoghi di lavoro. Il tutto operando un bilanciamento degli interessi coinvolti e raccogliendo i dati necessari e pertinenti allo scopo, pertanto secondo i principi di proporzionalità, minimizzazione e adeguatezza.

Salute, prevenzione, sorveglianza sanitaria, ordine, sicurezza e pubblico interesse: sono questi gli scopi e le finalità che giustificano i trattamenti purchè vengano garantite le tutele di diritti e libertà dei soggetti interessati.

Non c'è stata e non ci sarà la necessità di interventi di deroga, così come non è possibile pensare che alla privacy si debba

o si possa rinunciare. Basti infatti osservare il considerando 46 del GDPR: *"Il trattamento di dati personali* dovrebbe essere altresì considerato lecito *quando* è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica*. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica.* Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie *e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana".*

"salute e privacy così come sicurezza e privacy non possono che essere viste come binomi inscindibili, dove non vi è contrapposizione alcuna bensì bilanciamento e contemperamento degli interessi e delle tutele da garantire"

Dunque, “salute e privacy” così come “sicurezza e privacy” non possono che essere viste come binomi inscindibili, dove non vi è contrapposizione alcuna bensì bilanciamento e contemperamento degli interessi e delle tutele da garantire. Attraverso i principi richiesti dalla normativa (GDPR, regolamenti, norme e provvedimenti o linee guida per ambiti specifici) e le garanzie ad essi sottese, operando un corretto bilanciamento sarà possibile tutelare la salute ed agire con azioni di prevenzione che tengano conto dei diritti e delle libertà dei soggetti interessati, dando valore alle iniziative, tutte, e in particolare all’impiego della tecnologia ora più che mai da considerarsi come una risorsa.

Quando parliamo di privacy e di trattamento dei dati personali, resta inteso che ci riferiamo anche e soprattutto alla raccolta di dati (i dati biometrici, la rilevazione della temperatura corporea e, ancora, i numeri di targhe e i tanto discussi dati di localizzazione e tracciamento, etc.) attraverso sistemi, soluzioni tecnologiche, sensori e dispositivi (si pensi alle soluzioni di videosorveglianza) che possano consentire le ragioni e gli scopi legati, in questo momento, all’emergenza.

Se per lungo tempo abbiamo discusso sulla necessità di raggiungere la consapevolezza di tutti i soggetti coinvolti in scenari dove le soluzioni tecnologiche avrebbero dovuto trovare la giusta collocazione e il giusto valore, e se ci siamo soffermati su concetti quali la “fiducia” (in particolare la fiducia nella tecnologia e nell’innovazione così come nella filiera dei fornitori), l’etica degli algoritmi, il consapevole sviluppo dell’intelligenza artificiale, l’ accountability e la responsabilizzazione, ebbene, ora più che mai è giunto il momento di affrontare questi temi.

In questa fase e in quella che verrà dovremo valorizzare l’impiego della tecnologia, senza dimenticare che è una risorsa e, insieme alla tutela dei dati, un’opportunità perché possano essere perseguite finalità di pubblico interesse di tutela e sorveglianza sanitaria.

Occorrerà dunque valorizzare i dati e la tecnica in tutti gli ambiti dove sarà possibile impiegare soluzioni tecnologiche (ad esempio in ambito cittadino, in ambito privato per aziende e luoghi di lavoro, in ambito sanitario e nelle relative attività necessarie, in luoghi di pubblico interesse o ancora in settori come la logistica o i trasporti) per intervenire, prevenire e contrastare la diffusione epidemiologica anche, e soprattutto, nella fase di convivenza con il rischio da contagio, senza dover rinunciare alla privacy.

L’Autorità Garante per la protezione dei dati personali, in merito alle ipotesi in corso di valutazione per utilizzare strumenti di possibile tracciamento e localizzazione ai fini di strategie anti contagio, ha così dichiarato: *“Non si dica, dunque, che la privacy è il lusso che non possiamo permetterci in questo tempo difficile, perché essa consente tutto ciò che è ragionevole, opportuno e consigliabile fare per sconfiggere questo male oscuro”.*

E ancora *“La chiave è nella proporzionalità, lungimiranza e ragionevolezza dell’intervento oltre che, naturalmente, nella sua temporaneità. Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per l’efficienza e la delega cieca all’algoritmo per la soluzione salvifica. Così, una volta cessata quest’emergenza, avremo anche forse imparato a rapportarci alla tecnologia in modo meno fideistico e più efficace, mettendola davvero al servizio dell’uomo”.*

Le restrizioni che oggi ci vedono coinvolti ci impongono ovviamente tutta una serie di limitazioni, ma non possiamo pensare che si possa rinunciare ai diritti e libertà e, dunque, alla protezione dei dati che ci riguardano. Parimenti, non possiamo delegare alla tecnologia perdendo di vista un modello dove questa deve garantire tutele e principi che tengano conto delle finalità che possiamo e dobbiamo perseguire, non senza dimenticare il valore umano e, soprattutto, sempre nella consapevolezza del rischio di ritrovarci in un modello di “sorveglianza e totalitarismo”.

Come dobbiamo muoverci?

La chiave di lettura è certamente nel rispetto della normativa vigente: l’innovazione e la tecnologia non vengono ostacolate ma, anzi, fanno parte di una visione in cui il diritto alla privacy non è contratto o limitato, ma garantito e tutelato.

Dallo sviluppo dei prodotti a quello delle strategie per rinvenire soluzioni adeguate e rispettose dei principi normativi, ogni aspetto deve essere governato da elementi

quali la trasparenza degli algoritmi, la proporzionalità del loro impiego e la garanzia di misure di sicurezza che possano fornire e accrescere, ora più che mai, i livelli di sicurezza necessari (pensiamo alle infrastrutture critiche come quelle sanitarie, a quelle produttive o all'ambito cittadino).

Le scelte tecnologiche devono ricadere su sistemi, dispositivi, sensori, soluzioni che ci consentano di perseguire le finalità e gli scopi necessari in questa fase e, si ribadisce, a maggior ragione in quella successiva di convivenza con il rischio da contagio, con un approccio "by design" sin dalla fase di progettazione e così andando a:

- analizzare il contesto in cui ci si muove e definire le basi e le finalità per agire ed intervenire
- analizzare i rischi e svolgere sempre l'opportuna valutazione di impatto
- definire quali dati si devono raccogliere e trattare adottando adeguate misure di minimizzazione ed anonimizzazione dove consentite (posso monitorare, ad esempio, un certo contesto per evitare assembramenti e intervenire senza che sia necessario memorizzare le immagini o consentire l'identificabilità dei soggetti coinvolti)
- definire il tempo massimo di utilizzo e di conservazione dei dati in funzione delle finalità da perseguire, evidentemente fino a quando sussistono le ragioni giustificatrici ovvero l'emergenza in corso
- adottare sistemi e soluzioni che garantiscono la tutela dei lavoratori pur nel rispetto delle misure da osservare
- adottare sistemi e soluzioni che garantiscano le misure necessarie per costruire un modello di gestione che possa essere monitorato anche in caso di incidenti di sicurezza
- adottare sistemi e soluzioni che garantiscano standard e misure di sicurezza adeguati considerando i rischi nei casi in cui vi sia la necessità di ricorrere a trattamento, ad esempio di dati biometrici
- costruire, nella fase di implementazione, sistemi di gestione del trattamento dati che tengano conto anche di tutti gli altri adempimenti necessari e, parimenti, adeguate misure organizzative (ad esempio informative, nomine , formazione).

Come definito anche dal gruppo EDPB nelle linee guida dello scorso gennaio dettate per il trattamento dei dati personali attraverso dispositivi video **(leggi)** è fondamentale che il ricorso all'uso di sistemi, di soluzioni di videosorveglianza, di sensori e dispositivi che consentano di raggiungere legittimamente le finalità che ci interessano, avvenga, nel rispetto di principi di legalità, necessità, proporzionalità e minimizzazione dei dati e garantendo gradualità nella scelta di detti mezzi e strumenti.

I suddetti principi infatti, come pure osservato dal Comitato, debbono in particolare essere ben valutati in tutte le ipotesi in cui si vogliano adottare sistemi come ad esempio il riconoscimento facciale che comporta certamente rischi maggiori per i diritti delle persone interessate e che dunque richiede una adeguata analisi ed una valutazione di impatto che tenga conto di quanto sin qui osservato.

L'emergenza ci ha fatto e ci farà certamente riflettere su quanto ci sia da lavorare per dare un valido supporto in ambito safety e security con una visione integrata dove diritti e tecnologia, libertà, privacy, salute e sicurezza, si bilanciano e non si contrappongono perché ci siano tutele e non rinunce.