Il grande data breach

Cos’è la protezione dei dati personali

Proteggere i dati personali significa garantirne **riservatezza, disponibilità e integrità**. Lo ripetiamo perché questo periodo di grande paura per la COVID-19 sembra corrispondere a una vorticosa circolazione di dati personali, più o meno consapevole e più o meno controllata.

La paura e la costrizione dovuta alle misure di contenimento hanno fatto aumentare il numero di tweet, messaggi Whatsapp, post Facebook che, in molti casi, contengono **dati personali di persone contagiate** e, quindi, dati appartenenti alle particolari categorie (quelli sulla salute).

Le possibili misure di prevenzione del contagio nei luoghi di lavoro hanno disturbato i sonni di amministratori delegati e di amministratori pubblici che, senza mai essersi occupati seriamente né di *safety* né di protezione di dati personali, si sono inventati le più disparate **soluzioni investigative** (peraltro, non troppo gradite al Garante per la Protezione dei Dati Personali) che, spesso, vanno ben oltre il Protocollo Governo-Parti sociali siglato lo scorso 14 marzo 2020[1].

Inoltre vale la pena di indagare, coerentemente (ma senza alcun possibile paragone valoriale) con il saggio metodo investigativo del giudice Falcone, per capire dove vanno a finire, prevalentemente, i soldi in questo momento e, con essi, anche molti dati personali: aziende di sanificazione, supermercati e piattaforme che offrono servizi di *collaboration* online.

In questa situazione, milioni di dati personali stanno circolando confusamente in un grande *data breach* di cui, probabilmente, non avremo mai contezza e di cui ci accorgeremo solo quando tutto tornerà, gradualmente, alla normalità

(sempre che la privacy sopravviva ai recenti emendamenti al decreto Cura Italia che intendono sospendere l'applicazione del GDPR[2]).

Non eravamo pronti all'emergenza sanitaria. Ma non eravamo pronti nemmeno a reggere questa circolazione incontrollata di dati personali. Non erano pronte le **istituzioni** pubbliche, che:

- non hanno predisposto, nel tempo, sistemi strutturati e sicuri per interagire con i cittadini;
- credono che la protezione dei dati personali corrisponda soltanto alla tutela della riservatezza e che, quindi, si possa effettuare qualsiasi trattamento e che basti "mettere tutto sotto chiave" (ammesso che siano in grado di farlo).

E non erano pronte le **persone** che, ancora oggi:

- non hanno alcuna percezione dell'importanza dei loro dati personali;
- non riescono a fare a meno di riempire i loro smartphone di inutili app.

Qualche esempio di questa bulimìa potrà essere utile a comprendere le dimensioni del problema e, quindi, anche a suggerire le eventuali misure per la riduzione del danno.

Dove sono i soldi

I soggetti che in questo momento, più di altri e per motivi diversi tra loro, stanno vedendo ampliare la domanda per i loro prodotti/servizi sono:

- le aziende di sanificazione;
- i supermercati e, in generale, le attività commerciali autorizzate a operare, da ultimo, dal decreto legge n. 19 del 25 marzo 2020[3];
- le piattaforme che offrono servizi di *collaboration.*

Cerchiamo di chiarire quali effetti questa dinamica commerciale può avere sul trattamento dei dati personali.

L'attività di sanificazione su commissione delle ASL avviene, spesso, all'interno delle abitazioni private e, quindi, le aziende incaricate vengono in possesso, direttamente o indirettamente, di una mole enorme di dati personali che riguardano la salute (ma non solo) dei soggetti contagiati e dei loro familiari. È presumibile che il trattamento di questi dati, anche considerate l'**impreparazione delle aziende** a queste circostanze eccezionali e la rapidità con la quale devono intervenire, non avvenga con le tutele previste dal GDPR (misure di sicurezza, addestramento dei dipendenti, ecc.).
Oltre alla riservatezza, quindi, possono essere messe a rischio:

- l'integrità; per esempio, qualche malintenzionato può manomettere l'elenco dei soggetti per i quali si è intervenuto nella sanificazione e, successivamente, pubblicarlo su un social network per danneggiare qualche ignaro soggetto;
- la disponibilità; per esempio, può smarrirsi lo stesso elenco e, quindi, non aversi certezza che la sanificazione sia stata effettuata.

Le attività commerciali che sono rimaste operative si sono attrezzate, in molti casi, per la **consegna a domicilio** oppure con app per controllare le file. In entrambi i casi l'acquisizione e il successivo trattamento di dati personali (soprattutto per la consegna a domicilio) sta avvenendo senza le dovute garanzie per gli interessati. La consegna a domicilio, per esempio, richiede il trattamento (spesso eseguito con l'ausilio di supporti *elementari* e *poco sicuri*) dell'indirizzo, del numero di telefono e delle fasce orarie di disponibilità dell'acquirente; invece le app, spesso, tendono a essere sviluppate da soggetti terzi non ben attrezzati per proteggere i dati personali e, di solito, articolano il loro

funzionamento chiedendo l'accesso a dati presenti nel dispositivo, in palese violazione del principio di *privacy by default* previsto dal GDPR. Si tratta, quindi, di **milioni di dati personali**, anche appartenenti alle particolari categorie, che, prima della diffusione della COVID-19, non venivano trattati e per i quali è ipotizzabile un trattamento non particolarmente aderente al GDPR.

L'hashtag *#iorestoacasa* ha dato una scossa alla **modalità agile** di effettuare riunioni di lavoro, realizzare incontri a distanza e impostare lezioni e formazione da remoto. Fatta eccezione per molte istituzioni universitarie e qualche grande soggetto privato, poche organizzazioni avevano messo in piedi organicamente un servizio di comunicazione/collaborazione a distanza; sono state, quindi, imbastite **infrastrutture volanti** che hanno costretto i soggetti partecipanti (alle lezioni, alle riunioni, ecc.) a creare degli account presso la piattaforma prescelta che, di solito, è resa disponibile – in maniera apparentemente gratuita – da soggetti con forti interessi commerciali[4]. In qualche caso, nella spasmodica ricerca di una soluzione idonea, le organizzazioni hanno provato varie piattaforme prima di trovare quella che poteva fare al caso loro; in ogni prova i poveri interlocutori hanno dovuto creare account e fornire, tutte le volte, i dati personali richiesti. Com'è noto, tuttavia, la creazione di account è una procedura che, conformemente al GDPR, deve seguire regole precise e, prima di tutto, deve essere *corretta* e *trasparente* ovvero deve chiarire all'interessato le finalità del trattamento e cosa succede se non fornisce i dati che vengono richiesti. In molti casi, anche quando l'accesso al servizio è strutturato secondo canoni di correttezza e trasparenza, il furore di veder "funzionare le cose" induce gli utenti ad accettare ciecamente tutti i passaggi cruciali nei quali si accettano condizioni e si forniscono consensi.

Siamo di fronte, quindi, al trattamento di milioni di dati personali che, a causa della situazione emergenziale e della

fretta con la quale sono raccolti/conferiti (secondo il punto di vista), nasce con i seguenti (possibili) peccati originali:

- carenza di applicazione dei principi di correttezza e trasparenza;
- ambiguità delle finalità, anche perché, di solito, l'offerta gratuita dell'uso della piattaforma ha, come contropartita, proprio il successivo utilizzo dei dati personali degli utenti;
- difficoltà nell'esercizio effettivo dei diritti previsti come, ad esempio, il diritto alla revoca del consenso.

Sicurezza dei lavoratori e privacy

Oltre a questi esempi di trattamento che la situazione di emergenza ha generato, prevalentemente legati ad attività commerciali, sono germogliati altri trattamenti, anch'essi effettuati con finalità e modalità più o meno disinvolte, ideati da amministratori pubblici o manager aziendali per tutelare la salute dei propri lavoratori.

I vertici delle amministrazioni pubbliche e delle organizzazioni private, nell'ordinarietà della loro attività, sono raramente impegnati nelle vicende che riguardano la salute dei lavoratori e la protezione dei dati personali: insomma, ne sanno poco, dell'una e dell'altra materia. Tuttavia, la diffusione del COVID-19 li ha rapidamente catapultati in una realtà che doveva coniugarle. Ci sono state, quindi, *escalation* che, man mano che montava la gravità del contagio, hanno condotto a:

- chiedere ai lavoratori di autocertificare di non provenire da zone a rischio;
- chiedere ai lavoratori di segnalare situazioni di rischio riguardanti i propri familiari;
- misurare la temperatura dei lavoratori;
- chiedere ai lavoratori di elencare, giornalmente, le persone (soggetti esterni e colleghi) con i quali si è

avuto contatto diretto (anche oltre la fatidica distanza di sicurezza).

Naturalmente queste misure, spesso, non hanno rispettato il principio di **proporzionalità** e hanno generato la raccolta e il trattamento di migliaia di dati personali (spesso contenuti su supporto cartaceo) di cui non si sa quali potranno essere gli esiti futuri.

L'ultima iniziativa simile, in ordine di tempo, ha riguardato un gruppo di sindaci che, per attrezzare specificatamente gli operatori ecologici che eseguono la raccolta differenziata nel proprio territorio e tutelarne la salute, hanno chiesto alla ASL di competenza i nominativi dei soggetti affetti da COVID-19. Purtroppo, anche in questo caso, la semplice lettura sistematica del D.Lgs. 81/2008 e del GDPR avrebbe portato alle seguenti conclusioni:

- la valutazione del rischio per i lavoratori spetta al datore di lavoro;
- in caso di epidemia (cioè nella situazione attuale), conoscere i nominativi dei soggetti contagiati non incide sulla valutazione del rischio giacché la *minaccia* (come si dice in gergo) è potenzialmente diffusa anche oltre i contagiati già riconosciuti;
- le misure di riduzione del rischio, quindi, devono essere applicate a tutti gli operatori ecologici prescindendo dal fatto che il ritiro dei rifiuti riguardi o meno soggetti contagiati;

e, quindi, alla sostanziale **inutilità** di ottenere i dati personali dei contagiati.

Tracking e *tracing*

A tutti questi trattamenti di dati personali che la COVID-19 ha innescato, con la prospettiva di tante mini-violazioni che si possono tradurre in un gigantesco *data breach* **diffuso**, potrebbe aggiungersi quello governativo che sembra oscillare

tra *tracking* (corrispondente al **tracciamento continuo**) e *tracing* (corrispondente al **rintracciamento a posteriori**) ma che, si spera, sarà avviato nel rispetto dei consigli[5] del Comitato Europeo per la Protezione dei Dati Personali e solo a fronte di una solida base normativa e organizzativa (magari sottoposta preventivamente al parere del Garante per la Protezione dei Dati Personali).

Note

[1] http://www.salute.gov.it/portale/nuovocoronavirus/dettaglioNotizieNuovoCoronavirus.jsp?lingua=italiano&menu=notizie&p=dalministero&id=4237

[2] http://www.senato.it/leg/18/BGT/Schede/Ddliter/testi/52873_testi.htm

[3] http://www.regioni.it/download/news/608221/

[4] https://www.federprivacy.org/?option=com_k2&view=item&id=1373:migliaia-di-videochiamate-su-zoom-finite-su-internet-ad-insaputa-degli-utenti&Itemid=540

[5] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

Articolo a cura di **Francesco Maldera**

Francesco Maldera è Data Protection Officer e Data Scientist.

Il suo percorso professionale lo ha chiamato a responsabilità direzionali nell’ambito dei sistemi informativi, della safety&security, della privacy e dell’auditing svolgendo diversi incarichi dirigenziali nella Pubblica Amministrazione

e in aziende private.

Attualmente, accompagna l’attività consulenziale a quella di sensibilizzazione delle persone tramite il sito www.prontoprivacy.it



https://www.ictsecuritymagazine.com/articoli/il-grande-data-breach/