# ARTICOLO DI PUNTOSICURO

## Anno 22 - numero 4684 di Giovedì 23 aprile 2020


# Sicurezza e privacy dell'APP per il controllo dei contagi da Covid-19

***In questi giorni si parla di applicativi che utili a tenere sotto controllo il contagio da Coronavirus. Le pubbliche autorità parlano di garanzie, non meglio precisate, di sicurezza e privacy delle app. Vi è un errore di fondo, che è bene chiarire.***

Le cronache quotidiane, stampate e televisive, sono piene di notizie in merito ad una app, che potrà permettere di tenere sotto controllo il movimento di soggetti positivi alla COVID 19, permettendo quindi di mettere in guardia soggetti che, per vari motivi, potrebbero essersi avvicinati a questi soggetti contagiati.

In continuazione, anche le autorità che dovrebbero selezionare e gestire questi applicativi di tracciamento, parlano di "sicurezza e privacy". Vorrei chiarire ai lettori che vi è un errore semantico fondamentale nell'usare due parole, quando sarebbe più che sufficiente utilizzare solo la seconda parola, per assorbire in essa anche i concetti di sicurezza. Basta leggere il regolamento generale sulla protezione dei dati per vedere che il rispetto di questo regolamento comporta la adozione di una serie di misure di sicurezza documentate, che sono forse ancora più incisive di quelle che potrebbero essere richieste per applicativi aventi altre finalità.

Credo di poter affermare, senza timore di smentita, che una app che rispetti pienamente i dettati del regolamento generale sulla protezione dei dati certamente rispetterà anche i dettati in tema di sicurezza informatica, custodia dei dati, protezione da accesso abusivo e via dicendo. Il fatto che il comitato europeo per la protezione dei dati, autorità suprema in Europa su questi argomenti, abbia sviluppato uno specifico documento ed abbia dato incarico a specialisti di tracciare specifiche linee guida nello sviluppo di queste app dimostra come, lavorando solo sulla protezione dei dati, di riflesso si attua tutta una serie di misure di sicurezza, assai più incisive di quanto non si potrebbe sospettare.

Ad oggi, le pubbliche amministrazioni coinvolte non hanno dato alcuna informazione concreta in merito alle misure di "sicurezza e privacy". È l'ormai famoso approccio, che mi insospettisce sempre, del tipo: "Dottò, si fidi di me!".

Invece di fidarsi di chi fa queste affermazioni, vorrei invece sottoporre una serie di quesiti, ai quali queste autorità, o la azienda che svilupperà l'applicazione prescelta, dovrebbero dare tempestiva risposta. Questi quesiti non fanno altro che riprendere i punti chiave del regolamento generale e, come i lettori ben vedranno, fanno riferimento ad una incisiva protezione dei dati, che di riflesso porta ad una altrettanto incisiva sicurezza nel trattamento dei dati.

**1-Il titolare dell'azienda, cui verrà affidato lo sviluppo di questo applicativo, ha già portato a termine il documento afferente alla protezione fin dalla progettazione e di minimizzazione dei dati acquisiti?**

L'articolo 25 del regolamento generale europeo obbliga tutti coloro che effettuano trattamenti a sviluppare questo documento, mettendo in evidenza i rischi presenti e le modalità con cui tali rischi vengano messi sotto controllo. Se, nello sviluppo di questo documento, si fa riferimento alla norma internazionale ISO EN UNI 31000, lo sviluppo sarà stato portato a termine in conformità alla regola d'arte.

**2-Il titolare dell'azienda, cui verrà affidato lo sviluppo di questo applicativo, ha già portato a termine la valutazione di impatto sulla protezione dei dati, prevista dall'articolo 35 del regolamento generale europeo, quando il trattamento è suscettibile di presentare rischi particolarmente elevati per i soggetti coinvolti?**

L'elaborazione di questo documento non è obbligatoria, se non nel caso di applicazioni critiche, come certamente è la presente. Faccio presente che un documento di valutazione di impatto non è costituito da un paio di fogliettini scritti a doppia interlinea, ma è un massiccio documento, che richiede, per un appropriato sviluppo, competenze specifiche.

**3-Il titolare dell'azienda, cui verrà affidato lo sviluppo di questo applicativo, ha già designato un responsabile per la protezione dei dati, dotato di appropriate qualifiche e certificazioni?**

Non v'è dubbio che se un titolare del trattamento decide che si debba un documento di valutazione di impatto, ex articolo 35, ha bisogno del supporto di un responsabile della protezione dei dati. È compito del titolare selezionare un responsabile della protezione dei dati dotato di soddisfacenti qualifiche e certificazioni; a questo proposito, ricordo l'esistenza della norma UNI 11697, che permette appunto ad istituti di certificazione accreditati di certificare il profilo professionale in questione.

**4-Il titolare dell'azienda, cui verrà affidato lo sviluppo di questo applicativo, si avvale di codici di condotta, certificazioni e sigilli e marchi, applicabili allo sviluppo di questa specifica attività?**

La domanda la pongo, ma purtroppo so già che la risposta è negativa, perché oggi, almeno in Italia non esistono strumenti di convalida afferente a questo settore. Tuttavia, pongo egualmente la domanda, perché, ove in futuro nascessero questi strumenti di convalida della sicurezza, il titolare che sviluppa la app si impegni ad applicarli subito.

5-Il titolare dell'azienda, cui verrà affidato lo sviluppo di questo applicativo, è in grado fin da adesso di garantire che questo applicativo risponderà alle indicazioni del comitato europeo per la protezione dei dati e, in particolare, della squadra di esperti, di livello multinazionale, che sta sviluppando linee guida specifiche?

Il documento cui faccio riferimento è intitolato "Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020". Si legga anche la perentoria affermazione del presidente del comitato per le libertà civili del parlamento europeo, Juan Fernando López Aguilar (S&D, ES), che ha affermato l'assoluta necessità che vengano rispettate, nello sviluppo di questi applicativi, sia le indicazioni del regolamento generale europeo sia quelle della direttiva sulla e-Privacy.

**6-Il titolare dell'azienda, cui verrà affidato lo sviluppo di questo applicativo, ha esaminato le modalità con cui in altri paesi è stato affrontato lo stesso tema, in modo da avere a disposizione un panorama allargato delle strategie di sviluppo e messa sotto controllo di queste critiche applicazioni?**

Ricordo che ad oggi numerosi paesi europei ed extra europei hanno affrontato lo stesso tema e hanno dato indicazioni preziosissime, che vengono attentamente lette dal comitato europeo per la protezione dei dati; tra le nazioni che hanno già

affrontato il tema mi permetto di citare l'Argentina, l'Australia, il Canada, il Cile, Hong Kong, Israele, il Giappone, il Messico, la Nuova Zelanda, le Filippine, la Russia, Singapore, la Svizzera, la Turchia, gli Emirati Arabi Uniti, gli Stati Uniti e l'Uruguay. Anche se forse nessuno di questi documenti è perfetto, non dubito che ognuno di essi possa dare un contributo ad elaborare delle linee guida migliori.

Quando le autorità pubbliche ci illustreranno le risposte a questi quesiti, indipendentemente dall'azienda selezionata, forse cominceremo a essere un poco meno preoccupati.

**Adalberto Biasiotti**