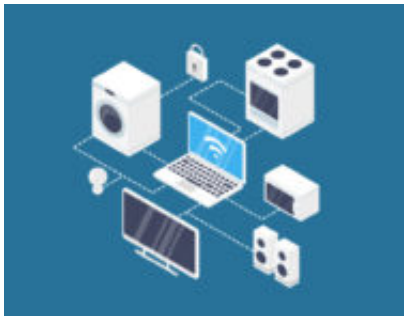
IoT e protezione dei dati: la nuova dimensione della sicurezza 3D e della data protecy

Date : 4 ottobre 2017



L'Internet delle Cose (i.e. Internet of Things) ha creato un universo di oggetti connessi alla rete e interconnessi tra loro, che offrono un ventaglio di servizi basati sull'uso di sensori e tecnologie che entrano in funzione in modo non sempre visibile a chi le utilizza. A partire dal Wearable Computing, passando per il Quantified Self, la domotica e le Smart Cities, siamo circondati da "cose" progettate per acquisire e trattare dati e informazioni, per trasferirli avviando processi di comunicazione con la rete o con *devices* diversi, per combinare le informazioni ottenute e ricavarne un profilo o un'indicazione su comportamenti, caratteristiche e abitudini degli individui.

Insomma, l'IoT propone nuove sfide alla sicurezza degli individui e dei loro dati personali e, per questo, anche al rapporto tra prodotto offerto al *data subject* e titolare del trattamento che deve fornire adeguate misure di sicurezza rispetto al trattamento stesso. Viste le sue capacità di connessione e interconnessione, l'IoT ha sollevato numerosi interrogativi legali affrontati dal Gruppo Articolo 29 [1] e tutt'ora è oggetto di attenzione da parte delle istituzioni legislative europee.

Vale la pena, però, concentrarsi su quali siano non tanto (e non solo) le criticità, ma soprattutto le soluzioni che possono essere adottate dai titolari del trattamento in virtù dell'attuale legislazione comunitaria in materia di privacy e protezione dei dati personali. A tal proposito, è utile partire proprio dal diritto alla privacy, che tutela la sfera personale dell'individuo, la sua dimora, la sua vita privata e familiare, la sua corrispondenza (art. 7 Carta dei diritti fondamentali dell'Unione Europea). Ad esso si accosta il diritto alla protezione dei dati personali, che ha a che vedere con la privacy, certo, ma non si esaurisce nella sola protezione dei dati personali intesa come riservatezza e non diffusione degli stessi. La *data protection*, infatti, assicura tutta una serie di altri diritti, quale quello di accesso ai dati, di rettifica, di cancellazione, di ricevere una idonea informativa ecc. (art. 8, Carta dei diritti fondamentali dell'Unione Europea).

Questi due diritti, però, stanno assumendo un'altra forma, nuova e più magmatica, che deriva proprio dalla natura dell'IoT. Ai sensi dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo, infatti, la privacy è intesa anche come tutela della sfera personale rispetto all'ingerenza dell'autorità pubblica. Ma cos'è, oggi, la sfera personale? Le case (e i nostri

outfit) ospitano oggetti prima inanimati che ora hanno la capacità di connettersi alla rete, raccogliere informazioni e comunicare con altri *devices*, scambiandosi i dati acquisiti e ricombinandoli tra loro. La “privacy”, dunque, non è più solo tutela della propria sfera personale “rispetto all’ingerenza dell’autorità pubblica”, ma è anche tutela “rispetto alla presenza di oggetti intelligenti” che popolano una dimensione fino ad ora considerata inviolabile, quella della vita privata.

Nel contempo, peraltro, non bisogna dimenticare che gli *smart objects* trattano non solo, ma anche e soprattutto dati personali, li aggregano, creano nuovi set di informazioni spesso senza che il soggetto sappia che tali trattamenti sono in atto o chi sia il titolare cui rivolgersi per far valere i propri diritti.

In quest’ottica, allora, come deve comportarsi il titolare del trattamento?

Innanzitutto, sembra essergli richiesto un cambio di prospettiva. Quei due diritti che la Convenzione Europea dei Diritti dell’Uomo aveva scisso agli artt. 7 e 8, infatti, si fondono in un *unicum*: privacy e *data protection* vanno a compenetrarsi, in quella che, con un neologismo sincretico, può definirsi *data protecy*. Si tratta di una nuova forma di tutela che va simultaneamente a garantire la protezione della sfera personale e quella dei dati personali [2].

In quest’ottica, sembra imprescindibile un’azione concreta da parte del titolare del trattamento, finalizzata a creare un rapporto di fiducia con gli interessati/utenti per dare attuazione concreta al principio di responsabilizzazione, sancito dall’art. 5(2) del Regolamento Generale in materia di Protezione dei Dati Personali (i.e. “GDPR”). Ad esempio, il ricorso a meccanismi di certificazione proposti dal Regolamento *ex* art. 42 faciliterebbe il soggetto che acquista il prodotto nella comprensione dell’oggetto e del trattamento che esso effettua, fornendogli garanzie circa la liceità e la correttezza del trattamento stesso.

Esemplificativo, in tal senso, è il progetto europeo Privacy Flag [3] – sostenuto dai fondi del programma Horizon 2020 – tra i cui scopi vi è quello di creare un *tool* rivolto alle piccole e medie imprese che trattano dati personali e che possono autovalutarsi in modo da comprendere il loro livello di conformità alla normativa europea, scegliendo anche di farsi assistere da alcuni esperti per un’analisi più approfondita, che condurrà alla certificazione della compliance con gli standard europei in materia di protezione dei dati.

La fiducia nell’universo dell’IoT passa dunque attraverso un ruolo attivo del titolare del trattamento che, in virtù del principio di responsabilizzazione, dovrebbe contribuire alla consapevolezza dell’interessato rispetto ai trattamenti effettuati con gli oggetti intelligenti.

Un’altra questione fondamentale deriva da due nuovi principi introdotti dal GDPR, cioè quelli della data protection by design e by default.

«*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure*

garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica». Così l'art. 25(2) del GDPR definisce il concetto di «*protezione di default*» dei dati personali, come l'impostazione a priori della massima protezione dei dati finalizzata al loro minimo trattamento.

Nel caso dell'IoT spesso i dispositivi sono progettati per accedere direttamente alla rete, senza che l'utente debba configurarli. Ciò comporta una possibile perdita di controllo del soggetto sui dati che lo riguardano, nel senso che egli potrebbe non saper (o poter) gestire il flusso di informazioni che il *device* scambia con la rete. Ecco perché le impostazioni "di fabbrica" – di default – dovrebbero essere quanto più attinenti possibile alla finalità per cui l'oggetto è stato concepito. Il titolare del trattamento non dovrebbe acquisire tutti i dati possibili nella convinzione che "potrebbero servirgli" in futuro – ad esempio per funzionalità in via di sviluppo che intende mettere a disposizione successivamente.

Questo approccio pone però, nel caso dell'IoT, non pochi problemi, nel senso che in un solo oggetto possono esservi numerose funzionalità e potrebbe essere complicato impedire un'acquisizione massiccia di dati. Si pensi al caso dello Smart Watch, che oltre a visualizzare l'ora è in grado di contare i passi, le calorie bruciate, accedere alla rubrica del cellulare (se esso viene collegato) e visualizzare chiamate e SMS in arrivo, rilevare il battito cardiaco, ricercare informazioni online ecc. Il criterio generale per far fronte a questo tipo di complessità sembra dover restare quello della combinazione dei due principi fondamentali della protezione dai dati: da un lato, la determinazione *ex ante* delle finalità (cd. limitazione delle finalità) che costituisce un obbligo per il titolare (*ex* art. 5(1)(b), GDPR) al fine di adottare tutte le misure tecniche e organizzative funzionali a tutelare i dati personali, come la *data protection by default*. Ciò garantisce all'interessato la conoscenza di predette finalità, permettendogli di esercitare i propri diritti qualora riscontri uno scostamento dalle finalità dichiarate; dall'altro lato, è fondamentale il rispetto della cd. minimizzazione [4] che riguarda la *data protection by design,* ossia la configurazione dei software utilizzati per trattare i dati personali in modo da ridurre al minimo l'uso di dati personali, raccogliendo quei soli dati che sono strettamente necessari al perseguimento delle finalità predeterminate.

Tuttavia, si è detto all'inizio che un nuovo diritto può emergere dalla rilettura di privacy e protezione dei dati, quello relativo alla cd. *data protecy.* Ciò implica, ad esempio, l'implementazione nell'oggetto "by design" di una funzione che consenta di disattivare la sua intelligenza, ripristinando la privatezza della sfera personale e impedendo la raccolta dei dati personali. Se l'utente non volesse far contare all'orologio i suoi passi o che questo rilevasse le sue pulsazioni comunicandolo ad una App che monitora la salute, ma volesse limitare le funzioni alla sola indicazione dell'orario? L'esistenza di un tasto "off" rispetto all'intelligenza "interconnessa" degli oggetti incarna la data protecy-by-design, poiché simili soluzioni costituiscono meccanismi inseriti in fase di progettazione all'interno degli oggetti stessi, consentendo il ripristino della tutela della privatezza rispetto alla pervasività dell'IoT, una privatezza che si estende anche ai dati personali che vengono acquisiti silenziosamente dalle "cose".

Vi è, poi, un ultimo interessante punto che vale la pena richiamare.

Rispetto alle sfide proposte dall'IoT, infatti, sono stati esposti alcuni accorgimenti che i titolari del trattamento potrebbero adottare affinché il trattamento sia da considerarsi legittimo.

Rimane, tuttavia, l'impossibilità di tutelare coloro che non hanno scelto di diventare soggetti del trattamento, poiché spesso i non-utenti vengono assimilati agli utenti delle funzionalità che gli oggetti intelligenti offrono, non essendo in grado di operare una scelta selettiva rispetto agli individui di cui raccogliere i dati.

In questo senso, la soluzione può essere individuata in quella che si definisce "privacy 3D". Si tratta, cioè, di utilizzare altri oggetti al fine non di raccogliere dati personali ma di schermare l'individuo rispetto a predetta raccolta.

Dal punto di vista del titolare del trattamento, la privacy tridimensionale è una vera e propria strategia di compliance e protezione che si compone di analisi dei rischi, di valutazioni d'impatto dei trattamenti *smart*, di documentazioni automatizzate, di controlli incrociati e di adozione di misure tecniche volte a tutelare anche i non-utenti. Un esempio è costituito dai celebri occhiali giapponesi che impediscono alle telecamere di mettere a fuoco la faccia di chi li indossa.

In sostanza, la partita della tutela della privacy e dei dati personali nel mondo dell'IoT non si gioca più solo nei protocolli di sicurezza – per prevenire i cd. *data breaches* – ma anche nel design degli *smart objects* e nella produzione di strumenti che costituiscano uno scudo materiale e fisico per gli individui. Il futuro è data protecy e tridimensionalità.

Bibliografia:

- [1] Gruppo Art. 29, Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf
- [2] L. Bolognini, C. Bistolfi, *Challenges of the Internet of Things: Possible Solutions from Data Protecy and 3D Privacy*, in https://link.springer.com/chapter/10.1007/978-3-319-44760-5_5
- [3] http://privacyflag.eu/
- [4] Gruppo Art. 29, Parere 01/2014 sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_it.pdf

A cura di: **Camilla Bistolfi**