Rapporto tra IOT e categorie particolari di dati

Beatrice Nepoti

Bologna, 09.10.2019

Elementi di contesto 1/2

- **IoT:** indica la rete di dispositivi dotati di sensori, attuatori, software e connettività che gli permette di digitalizzare informazioni sull'ambiente circostante e comunicare tra loro scambiando dati attraverso Internet

- **Con IoT il focus si sposta sui dati:** si ha la consapevolezza che sfruttare i dati generati per aggregarli ed analizzarli permette di scoprire importanti correlazioni e di generare valore

- **IoT e GDPR (Regolamento UE n. 2016/679 applicabile dal 25.5.2018) come binomio indissolubile**

- Il dato **personale** (art. 4) è qualsiasi informazione che concerne una persona fisica identificata o identificabile o che riguarda una persona la cui identità può essere accertata mediante informazioni supplementari
- Il dato **particolare** (art. 9) è un dato che necessita di un trattamento speciale maggiore attenzione e protezione per garantire la privacy dei soggetti coinvolti (ad es. quelli riguardanti i minori e quelli relativi alle condizioni di salute degli individui): Divieto generale del trattamento, salvo specifiche eccezioni al divieto (interessato che ha prestato il consenso; dati resi pubblici dall'interessato...)

Elementi di contesto 2/2

- La gestione di dataset di grandi dimensioni per derivarne informazioni utili prende il nome di **Big Data → analitica descrittiva, predittiva, prescrittiva**
- Un esempio di come i sistemi complessi dipendano fortemente dalla condivisione può essere dato da una **smart city:** si pensi alla necessità di un sistema di sorveglianza cittadina intelligente di dover utilizzare i dati sull'illuminazione, o quelli sulle condizioni meteo e sul traffico; oppure si pensi ad un sistema di gestione stradale intelligente che ha bisogno a sua volta di accedere ai dati sopracitati per poter informare correttamente i guidatori
- Con l'obiettivo di fornire delle linee guida sulle quali basare i futuri sviluppi di piattaforme IoT, la Commissione Europea ha fissato un principio generale, nel 2013, dichiarando che **la protezione di privacy e dati, così come la sicurezza informatica, devono costituire un corredo gratuito dei servizi IoT.** In particolare, la sicurezza informatica dev'essere considerata come tutela delle informazioni nella loro **riservatezza, integrità e disponibilità**

Anonimizzazione e pseudonimizzazione

- I dati **anonimi** sono le informazioni non originariamente associabili ad uno specifico interessato; i dati anonimi e anche quelli anonimizzati, ovvero che sono stati privati di tutti gli elementi identificativi, non sono ritenuti dati personali e quindi non sono soggetti alle relative norme
- I dati **pseudonimi**, invece, sono quelli in cui gli elementi identificativi sono stati sostituiti da elementi diversi atti a rendere estremamente difficoltoso il riconoscimento dell'interessato; potendo consentire l'individuazione, anche se indiretta, della persona tramite l'incrocio con altre informazioni, i dati pseudonimi sono soggetti a tutela, anche se in modo minore rispetto ai dati personali veri e propri, in quanto il rischio relativo all'eventuale abuso di dati pseudonimizzati in modo sicuro è generalmente considerato improbabile. In ogni caso, **un titolare che utilizza dati pseudo-anonimi invece di evitare l'utilizzo di dati personali è tenuto a comunicare la logica e le motivazioni di tale scelta agli interessati.**

Principi

- Principio di liceità, correttezza e trasparenza
- **Principio di limitazione della finalità:** non vengono considerate finalità incompatibili ulteriori trattamenti dei dati personali **a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**
- **Principio di minimizzazione dei dati**
- **Principio di esattezza**
- **Principio di limitazione della conservazione**
- **Principio di integrità e riservatezza**
- **Principio di responsabilizzazione (accountability)**

Per **profilazione** si intende l'insieme delle attività di raccolta ed elaborazione di dati svolte sugli utenti di un servizio, per effettuarne una suddivisione in categorie; è definita come un procedimento automatizzato volto a valutare aspetti personali (e che quindi opera su dati personali) riguardanti una persona fisica. Gli scopi principali consistono nel valutare attraverso analisi o previsioni aspetti come il comportamento, le preferenze, gli interessi, gli spostamenti o l'affidabilità di una persona, o nel prendere decisioni sulla base di essi.

Consenso e Informativa

- Il titolare è sempre tenuto a comunicare l'identità e i dati di contatto di titolare e responsabile, i dati di contatto del responsabile della protezione dei dati (se presente), la base giuridica del trattamento, il suo interesse legittimo nel caso costituisca la base del trattamento, se trasferisce dati personali a paesi terzi e, nel caso, attraverso quali strumenti
- Deve essere inoltre previsto il tempo di conservazione dei dati (o i criteri seguiti per stabilire tale periodo) e il diritto dell'interessato di presentare un reclamo all'autorità di controllo
- Nel caso il trattamento comporti processi decisionali automatizzati, come ad esempio la profilazione, deve esserne specificata la presenza, insieme ad un'indicazione della logica dietro tali processi e le relative conseguenze per l'interessato
- **CONSENSO**: libero, specifico, informato, inequivocabile, verificabile, revocabile
- **Diritti dell'interessato al trattamento**: di accesso, alla cancellazione, di limitazione, alla portabilità
- Il **titolare del trattamento (data controller)** è colui che determina le finalità, le modalità e gli strumenti utilizzati nell'ambito del trattamento di dati personali: **Privacy by design** (privacy sin dalla progettazione) e **Privacy by default** (privacy come impostazione predefinita)
- Il **responsabile del trattamento (data processor)**, invece, è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati per conto del titolare

GDPR valutazione rischi e valutazione d'impatto 1/2

Nel valutare il rischio privacy, il titolare del trattamento deve individuare:

- La tipologia dei dati raccolti (dati personali comuni, categorie particolari di dati personali o addirittura dati giudiziari)
- Il numero della registrazione, ovvero la quantità dei dati in possesso del titolare del trattamento
- quali sono le misure di sicurezza tecnica ed organizzative che il titolare o il responsabile, qualora ci fosse, abbiano messo in atto per eliminare o abbassare il pericolo che possa verificarsi un data breach ovvero una violazione dei dati che si stanno trattando
- in base al risultato di questa valutazione può decidere se effettuare o meno una **DPIA ovvero una valutazione d'impatto sulla protezione dei dati**

GDPR valutazione rischi e valutazione d'impatto 2/2

L'European Data Protection Board (ex WP 29) ha elencato una lista di criteri per cui è obbligatoria una DPIA e solo nel caso si presentino almeno due delle seguenti circostanze, diventa obbligatoria.

- Quando c'è la profilazione
- Qualora ci siano decisioni automatizzate che producono effetti giuridici
- In caso di monitoraggio sistematico
- Quando vengono trattati dati sensibili o giudiziari
- Quando il trattamento dei dati è su larga scala
- Nel caso ci siano due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato
- Quando ci sono dati riferibili a soggetti vulnerabili come anziani e minori
- Quando è previsto l'utilizzo di tecnologie innovative

Quando ci sono **trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.**

Veniamo a noi: ReteIoT per la PA 1/2

- **Titolare del trattamento dei dati è Lepida S.c.p.A. che raccoglie i dati personali, li rende anonimi e li comunica alle pubbliche amministrazioni esclusivamente in forma anonima.**
- "Il trattamento dei Suoi dati personali viene effettuato da Lepida al fine di consentirLe la fruizione dei servizi di comunicazione elettronica richiesti e, in particolare, di permetterLe l'accesso alla rete Lepida ai fini della registrazione e **dell'utilizzo dei sensori di cui Lei è proprietario**."
- "Si precisa che **il conferimento dei Suoi dati è necessario ai fini della fruizione dei servizi richiesti** e sopra indicati. Pertanto, l'eventuale rifiuto al conferimento dei Suoi dati, così come la successiva richiesta di cancellazione, comporterà l'impossibilità di procedere alla fornitura di tali servizi. A seguito dell'acquisizione e ricezione dei dati, dei parametri e di qualsivoglia altra misurazione rilevati dai Suoi sensori, Lepida procederà alla loro anonimizzazione attraverso … . In particolare, il sistema mantiene queste informazioni (in chiaro) per il tempo del collegamento per poi archiviarle. **Tali dati, in forma esclusivamente anonima, potrebbero quindi essere utilizzati da Lepida per il perseguimento delle proprie finalità istituzionali."**
- "Lepida potrà inoltre comunicare – previa anonimizzazione, secondo le tecniche sopra indicate – i dati, i parametri e qualsivoglia altra misurazione rilevati dai Suoi sensori alle Pubbliche amministrazioni aderenti all'iniziativa "[Rete IoT per la PA]", le quali **utilizzeranno tali dati, in forma anonima, esclusivamente per il perseguimento di proprie finalità istituzionali e di interesse pubblico, tra cui quella di indirizzo della politica territoriale."**

Veniamo a noi: ReteIoT per la PA 2/2

- Duplice forma di protezione dell'interessato: anonimizzazione dei dati e utilizzo solo per finalità istituzionali. Attenzione alla finalità
- Il dato può ritenersi personale soltanto allorquando possa riferirsi, direttamente o indirettamente, al proprietario del sensore. Pertanto, ove il sensore sia collocato in un luogo pubblico o aperto al pubblico e raccolga parametri, indici o misurazioni che non possono in alcun modo ricollegarsi al proprietario, il dato non dovrebbe ritenersi personale (ad esempio, qualora attraverso il sensore, installato su una strada pubblica, sia possibile rilevare il livello di polveri sottili di una determinata zona).
- Al contrario, nel caso in cui il sensore sia posto all'interno di una dimora privata o in zone limitrofe alla medesima (ad esempio, giardino o cortile interno) ovvero in aree delimitate destinate ad attività produttive o di commercio, i dati raccolti potrebbero essere ritenuti personali ove consentano di inferire caratteristiche personali degli individui.

Tipologia-Finalità-Trattamento: esempi 1/3

Tipologia sensore	Finalità	Trattamento di dati
Parcheggi	Permette di rilevare la presenza degli autoveicoli parcheggiati in una determinata zona	Registra un dato anonimo sulla presenza o meno di auto in un determinato stallo (a differenza delle telecamere che, al contrario, registrano immagini)
		Ove si tratti di sensore collocato nel posto auto assegnato specificatamente ad un utente, il dato è personale in quanto idoneo a geolocalizzare indirettamente l'utente stesso
		Ove sia programmato in modo tale da riconoscere soltanto i soggetti autorizzati al parcheggio (ad es., disabili, soggetti autorizzati al carico e scarico, residenti e altre categorie specifiche), potrebbe essere suscettibile di raccogliere dati personali, finanche di natura particolare (vd. ad esempio portatori handicap), da valutare in base alle circostanze del caso concreto
		Risulterebbe posto in essere un trattamento di dati anche nell'ipotesi in cui il sensore sia dotato di un dispositivo che invii agli smartphone degli utenti il numero dello stallo su cui si è parcheggiato

Tipologia-Finalità-Trattamento: esempi 2/3

Tipologia sensore	Finalità	Trattamento di dati
Rilevazione di inquinamento / Gas	Permette di rilevare il livello di polveri sottili, emissioni elettromagnetiche, sostanze contaminanti e inquinanti derivanti da molteplici fattori (es: vernici e materiali, soprattutto se il sensore è indoor)	Outdoor: in caso di sensore collocato all'esterno di un'abitazione privata (es: strada pubblica), il dato non dovrebbe essere personale, fatte salve circostanze peculiari del caso concreto
		Indoor: i dati raccolti potrebbero essere ritenuti personali ove consentano di inferire caratteristiche personali degli individui (es: soggetto a rischio di malattie)

Tipologia sensore	Finalità	Trattamento di dati
Monitoraggio acustico	Permette di raccogliere dati in tempo reale circa il rumore in zone di ritrovo notturno, in zone centrali o vicino ad aeroporti e ferrovie	Se il sensore è configurato in modo tale da rilevare esclusivamente il livello di inquinamento acustico, i dati così raccolti non dovrebbero ritenersi personali
		Se il sensore è dotato di microfono in grado di captare non solo il rumore generico ma anche voci o conversazioni, potrebbe configurarsi un trattamento di dati personali

Tipologia-Finalità-Trattamento: esempi 3/3

Tipologia sensore	Finalità	Trattamento di dati
Raccolta e smaltimento rifiuti	Permette di rilevare la posizione dei cassonetti, di raccogliere informazioni temporali relative a quando viene eseguito lo svuotamento, nonché dati circa lo stato di riempimento dei medesimi	Ove il sensore sia collocato presso cassonetti serventi un'area densamente abitata (e.g. non è possibile individuare il soggetto che materialmente smaltisce i propri rifiuti), il dato non può ritenersi personale
		Ove il sensore sia collocato presso cassonetti ad uso esclusivo di determinati soggetti (es: condominio, villette indipendenti), sarebbe possibile desumere l'effettiva presenza dei soggetti in casa, inferendo altresì, in relazione alla quantità di rifiuti smaltita, un numero approssimativo degli individui ivi residenti. Il dato potrebbe dunque ritenersi personale

Beatrice Nepoti – beatrice.nepoti@lepida.it