GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

1471/14/IT
WP 223

Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti

adottato il 16 settembre 2014

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g), del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 di detta direttiva,

visto il proprio regolamento interno,

HA ADOTTATO IL PRESENTE PARERE:

SINTESI

L'Internet degli oggetti (*Internet of Things* - IoT) sta per entrare a far parte della vita dei cittadini europei. La fattibilità di molti progetti nel campo dell'IoT non è ancora del tutto chiara, ma stanno per essere resi disponibili "oggetti intelligenti" che controllano le nostre case, le nostre auto, i nostri ambienti di lavoro e le nostre attività fisiche, comunicando con loro. Già oggi dispositivi connessi a Internet riescono a soddisfare le esigenze dei cittadini dell'UE nei grandi mercati del *quantified self* (quantificazione del sé) e della domotica. Pertanto, l'IoT apre notevoli prospettive di crescita per un gran numero di imprese innovative e creative dell'UE, grandi o piccole, che operano in questi mercati.

Il Gruppo di lavoro "articolo 29" ritiene importante che tali aspettative vengano soddisfatte, nell'interesse sia dei cittadini che dell'industria dell'UE. Tuttavia, per raggiungere i benefici previsti, si devono affrontare anche le molte sfide connesse alla vita privata e alla sicurezza che possono essere associate all'IoT. Sorgono molti interrogativi riguardo alla vulnerabilità di questi dispositivi, spesso utilizzati al di fuori di una struttura informatica tradizionale e non dotati di sufficiente sicurezza interna. Tra i molti rischi che gli attori devono affrontare nel campo dell'IoT per attrarre i potenziali utenti dei loro prodotti o servizi troviamo la perdita di dati, le infezioni da programmi maligni (*malware*), ma anche l'accesso non autorizzato a dati personali, l'uso invasivo di dispositivi indossabili o la sorveglianza illegale.

Al di là dell'ottemperanza ai requisiti legali e tecnici, il fulcro della questione sono, infatti, le conseguenze che l'IoT può avere sulla società nel suo insieme. Coloro che, nello sviluppo del prodotto, collocano al primo posto la protezione della vita privata e dei dati saranno meglio in grado di garantire che i propri beni e servizi rispettino il principio della tutela della vita privata fin dalla progettazione ("*privacy by design*") e dispongano delle impostazioni automatiche di tutela della vita privata che i cittadini dell'UE pretendono.

Finora questa analisi è stata effettuata soltanto in termini molto generali da vari regolatori e portatori di interessi all'interno dell'Unione europea e al di fuori di essa. Il Gruppo di lavoro ha deciso di approfondire la questione adottando il presente parere. In tal modo intende contribuire all'applicazione uniforme del quadro giuridico in materia di protezione dei dati nel campo dell'IoT, nonché allo sviluppo di un elevato livello di protezione per quanto riguarda la protezione dei dati personali nell'UE. La conformità con tale quadro è fondamentale per affrontare le sfide giuridiche e tecniche ma anche, dal momento che essa dipende dalla qualifica della protezione dei dati come diritto umano fondamentale, le sfide sociali illustrate sopra.

Il presente parere identifica quindi i principali rischi legati alla protezione dei dati che caratterizzano l'ecosistema dell'IoT, prima di fornire orientamenti su come il quadro normativo dell'Unione debba essere applicato in questo contesto. Il Gruppo di lavoro sostiene che i progetti dei portatori di interessi devono contenere le massime garanzie possibili per gli utenti. In particolare, gli utenti devono avere il completo controllo dei propri dati personali durante tutto il ciclo di vita del prodotto e, qualora le organizzazioni si basino sul consenso per il trattamento dei dati, tale consenso deve essere pienamente informato, libero e specifico. Per contribuire a raggiungere tale scopo, il Gruppo di lavoro ha formulato una serie esaustiva di raccomandazioni pratiche indirizzate ai diversi portatori di interessi (fabbricanti di dispositivi, sviluppatori di applicazioni, piattaforme sociali, ulteriori destinatari dei dati, piattaforme di dati e organismi di normazione) per aiutarli a mettere in pratica la protezione della vita privata e dei dati nei propri prodotti e servizi.

Infatti, responsabilizzare i singoli fornendo loro informazioni e garantendone la libertà e la sicurezza è fondamentale per creare fiducia e sostenere l'innovazione, e quindi per avere successo in questi

mercati. Il Gruppo di lavoro è pienamente convinto che i portatori di interessi che soddisfano tali aspettative avranno un vantaggio competitivo eccezionalmente forte rispetto ad altri operatori i cui modelli commerciali si basano sul mantenere i clienti all'oscuro di quanto i loro dati vengono trattati e trasmessi, e sul chiudere tali dati nei propri ecosistemi.

Considerando le grandi sfide connesse alla protezione dei dati poste dall'IoT, il Gruppo di lavoro continuerà a monitorare i suoi sviluppi e, a tal fine, resta aperto alla collaborazione con altri regolatori nazionali o internazionali e legislatori su questa tematica. È inoltre disponibile a discutere con i rappresentanti della società civile, così come con quelli del settore industriale pertinente, in particolare laddove i portatori di interessi operano come responsabili del trattamento o come incaricati del trattamento all'interno dell'Unione europea.

INTRODUZIONE

Il concetto di Internet degli oggetti (IoT) si riferisce a un'infrastruttura nella quale miliardi di sensori incorporati in dispositivi comuni di uso quotidiano ("oggetti" a sé stanti oppure oggetti connessi ad altri oggetti o persone) sono progettati per registrare, trattare, conservare e trasferire dati e, essendo associati a identificativi univoci, interagiscono con altri dispositivi o sistemi che sfruttano le capacità di collegamento in rete. Dal momento che l'IoT si basa sul principio del trattamento esteso dei dati attraverso tali sensori, che sono progettati per comunicare con discrezione e scambiarsi dati continuamente, esso è strettamente connesso alle nozioni di "pervasività" e "onnipresenza" dell'informatica.

I portatori di interessi del settore dell'IoT puntano ad offrire nuove applicazioni e nuovi servizi attraverso la raccolta e l'ulteriore combinazione di tali dati relativi alle persone, sia al fine di valutare "soltanto" i dati relativi all'ambiente specifico dell'utente, sia per osservare e analizzare espressamente le sue abitudini. In altre parole, l'IoT solitamente implica il trattamento di dati che si riferiscono a persone fisiche identificate o identificabili e che costituiscono quindi dati personali ai sensi dell'articolo 2 della direttiva dell'Unione europea sulla protezione dei dati.

Il trattamento di tali dati in questo contesto dipende dall'intervento coordinato di un gran numero di portatori di interessi (ossia fabbricanti di dispositivi, che a volte operano anche come piattaforme di dati; aggregatori o intermediari di dati, sviluppatori di applicazioni, piattaforme sociali, noleggiatori o noleggianti di dispositivi, ecc.). I rispettivi ruoli di tali soggetti verranno ulteriormente trattati nel presente parere. Questi diversi portatori di interessi possono essere coinvolti per varie ragioni, ossia per fornire funzionalità supplementari o interfacce di controllo di facile uso che consentano la gestione di impostazioni tecniche e di privacy, o perché comunemente l'utente ha accesso attraverso una distinta interfaccia web ai propri dati che sono stati raccolti. Inoltre, una volta che i dati sono stati archiviati in remoto, possono essere condivisi con altri soggetti, a volte senza che il diretto interessato ne sia al corrente[1]. Pertanto, in questi casi l'ulteriore trasmissione dei dati viene imposta all'utente, che non può impedirla senza disabilitare la maggior parte delle funzionalità del dispositivo. Il risultato di questa sequenza di azioni è che l'IoT può mettere i fabbricanti di dispositivi e i loro partner commerciali in condizione di creare o di avere accesso a profili di utenti molto dettagliati.

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

Alla luce di quanto sopra, lo sviluppo dell'IoT pone chiaramente nuove sfide importanti connesse alla protezione dei dati personali e alla vita privata[2]. Infatti alcuni sviluppi dell'IoT, se incontrollati, possono spingersi fino a sviluppare una forma di sorveglianza delle persone che può essere considerata illegale ai sensi della legislazione dell'UE. L'IoT suscita inoltre serie preoccupazioni in materia di sicurezza, in quanto le violazioni della sicurezza possono comportare gravi rischi per la vita privata delle persone i cui dati vengono trattati in tali contesti.

Il Gruppo di lavoro ha pertanto deciso di formulare il presente parere al fine di contribuire all'identificazione e al monitoraggio dei rischi derivanti da tali attività, in cui sono in gioco i diritti fondamentali dei cittadini dell'UE.

[2] Il presente parere deve inoltre essere letto in connessione con i precedenti pareri adottati dal Gruppo di lavoro nel 2014, sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto (WP 211) e sulla sorveglianza (WP 215).

1. Oggetto del parere: attenzione specifica a tre evoluzioni dell'IoT

In questa fase non è possibile prevedere con certezza la portata dell'evoluzione dell'IoT. Questo spiega in parte perché la questione di come trasformare tutti i dati eventualmente raccolti nell'ambito dell'IoT in qualcosa di utile e quindi commercialmente redditizio rimanga sostanzialmente aperta. Non sono chiare neanche le possibili convergenze e sinergie tra l'IoT e altri sviluppi tecnologici quali il *cloud computing* e l'analisi predittiva, che, in questa fase, riguardano solo gli sviluppi di mercati emergenti.

Nell'ambito del presente parere, il Gruppo di lavoro "articolo 29" ha perciò deciso di concentrarsi soprattutto su tre sviluppi specifici dell'IoT (*wearable computing* ovvero dispositivi informatici indossabili, *quantified self* e domotica) che 1) si interfacciano direttamente con l'utente e 2) riguardano dispositivi e servizi che sono effettivamente utilizzati e che in effetti si prestano quindi ad un'analisi alla luce della normativa in materia di protezione dei dati. Il presente parere perciò non tratta specificatamente delle applicazioni B2B e di questioni di più ampia portata quali le "città intelligenti", il "trasporto intelligente" e gli sviluppi M2M ("da macchina a macchina"). Tuttavia, i principi e le raccomandazioni contenuti nel presente parere possono essere applicati al di fuori del suo stretto campo di applicazione e coprire anche questi ulteriori sviluppi dell'IoT.

1.1 ***Wearable computing***

Il termine *wearable computing* si riferisce a oggetti di uso quotidiano e di abbigliamento, quali orologi e occhiali, nei quali sono stati inseriti sensori per ampliare le funzionalità. È probabile che gli oggetti indossabili vengano adottati rapidamente in quanto ampliano l'utilità di oggetti di uso quotidiano che ci sono familiari, tanto più che possono difficilmente essere distinti dai loro prodotti *look-alike* non connessi. Essi possono essere provvisti di telecamere, microfoni e sensori integrati in grado di registrare e trasferire dati al fabbricante del dispositivo. Inoltre, anche la disponibilità di un'API per dispositivi indossabili (ad esempio, Android Wear[3]) contribuisce alla creazione di applicazioni da parte di terzi, i quali possono quindi accedere ai dati raccolti da tali oggetti.

1.2 ***Quantified self***

Gli oggetti del *quantified self* sono progettati per essere portati abitualmente dalle persone che vogliono registrare informazioni riguardanti le proprie abitudini e il proprio stile di vita. Ad esempio, una persona può voler indossare uno *sleep tracker* (strumento di monitoraggio del sonno) ogni notte per ottenere informazioni esaurienti sul proprio modello di sonno. Altri dispositivi mirano a monitorare i movimenti, come i contatori delle prestazioni che misurano e rilevano continuamente indicatori quantitativi relativi alle attività fisiche della persona, ad esempio le calorie bruciate e le distanze percorse.

Alcuni oggetti misurano il peso, il battito cardiaco e altri indicatori di salute. Osservando le tendenze e i cambiamenti di comportamento nel tempo, i dati raccolti possono essere analizzati per dedurre informazioni qualitative sulla salute, ad esempio valutazioni sulla qualità e gli effetti dell'attività fisica basate su soglie predefinite e, entro certi limiti, la probabile presenza di sintomi di malattie.

I sensori del *quantified self* spesso devono essere indossati in condizioni specifiche per raccogliere i dati rilevanti. Ad esempio, un accelerometro posto alla cintura di un interessato, con gli appositi algoritmi, potrebbe misurare i movimenti dell'addome *(dati grezzi)*, raccogliere dati riguardanti il ritmo respiratorio *(dati aggregati e informazioni estratte)* e mostrare il livello di stress dell'interessato *(dati visualizzabili)*. In alcuni dispositivi, solo quest'ultima informazione viene fornita al cliente, ma il

[3] http://developer.android.com/wear/index.html

fabbricante del dispositivo o il fornitore di servizi può accedere a un numero molto maggiore di dati che possono essere analizzati in una fase successiva.

Il *quantified self* è problematico per quanto riguarda le tipologie di dati raccolti, che sono relativi alla salute e quindi potenzialmente sensibili, nonché per quanto concerne la raccolta estesa di tali dati. Infatti, dal momento che l'obiettivo del processo è quello di motivare gli utenti a mantenersi in buona salute, esso presenta molti legami con l'ecosistema *e-health*. Tuttavia, recenti indagini hanno messo in dubbio la reale precisione delle misure effettuate e dei dati dedotti[4].

1.3 **Domotica**

I dispositivi IoT possono ora essere posizionati anche in uffici o case, ad esempio lampadine, termostati, sensori di fumo, stazioni meteorologiche, lavatrici o forni "connessi" controllabili a distanza tramite Internet. Ad esempio, gli oggetti contenenti sensori di movimento possono rilevare e registrare la presenza di un utente a casa e i suoi movimenti abituali ed eventualmente innescare specifiche azioni predeterminate (ed esempio, accendere una luce o modificare la temperatura di una stanza). Molti dispositivi domotici sono costantemente connessi e possono trasmettere dati al fabbricante.

Chiaramente, la domotica pone problemi specifici in materia di protezione dei dati personali e vita privata in quanto è probabile che un'analisi dei modelli di uso in tale contesto riveli dati sullo stile di vita, le abitudini e le scelte degli abitanti o semplicemente la loro presenza a casa.

Le tre categorie di dispositivi sopra elencate sono rappresentative delle principali problematiche relative alla vita privata legate all'IoT al suo stato attuale. Occorre tuttavia rilevare che queste categorie non sono chiuse: ad esempio, un dispositivo "indossabile" come uno *smart watch* potrebbe essere utilizzato per monitorare la frequenza cardiaca e cioè per una valutazione di *quantified self*.

2. Problemi in materia di vita privata e protezione dei dati legati all'Internet degli oggetti

Il Gruppo di lavoro ha deciso di adottare questo specifico parere in considerazione del fatto che l'IoT pone varie sfide importanti relative alla protezione della vita privata e dei dati, alcune nuove, altre più tradizionali, ma talvolta amplificate a causa della crescita esponenziale del trattamento dei dati connesso con la sua evoluzione. L'importanza dell'applicazione del quadro giuridico dell'UE in materia di protezione dei dati e delle raccomandazioni pratiche in materia esposte qui di seguito deve essere valutata alla luce di tali sfide.

2.1 **Mancanza di controllo e asimmetria dell'informazione**

A causa dell'esigenza di fornire servizi pervasivi con discrezione, gli utenti potrebbero ritrovarsi, in pratica, sotto il controllo di terzi. Ciò può portare a situazioni in cui l'utente può perdere completamente il controllo della diffusione dei propri dati, a seconda che la raccolta e il trattamento di tali dati siano effettuati in modo trasparente o meno.

Più in generale, l'interazione degli oggetti tra loro, tra gli oggetti e i dispositivi delle persone, tra le persone e altri oggetti e tra oggetti e sistemi di *back-end* porterà alla creazione di flussi di dati che possono difficilmente essere gestiti dai classici strumenti utilizzati per garantire una tutela adeguata degli interessi e dei diritti degli interessati. Ad esempio, a differenza di altre tipologie di contenuto, i

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results

dati raccolti da dispositivi IoT non possono essere adeguatamente riesaminati dall'interessato prima della pubblicazione, fatto che innegabilmente comporta un rischio di mancanza di controllo e di eccessiva esposizione per l'utente. In più, la comunicazione tra gli oggetti può essere avviata automaticamente e tramite impostazioni predefinite, senza che il diretto interessato ne sia al corrente. In assenza della possibilità di controllare efficacemente l'interazione degli oggetti o di stabilire confini virtuali definendo zone attive e zone non attive per oggetti specifici, diventerà estremamente difficile controllare il flusso di dati generato. Risulterà ancora più difficile controllare il suo uso successivo per evitare un potenziale "slittamento della funzione" (*function creep*). La questione della mancanza di controllo, che interessa anche altri sviluppi tecnici quali il *cloud computing* o i *big data*, appare ancora più problematica se si pensa che queste diverse tecnologie emergenti possono essere usate in combinazione.

2.2 **Qualità del consenso dell'utente**

In molti casi, l'utente può non essere consapevole del trattamento dei dati effettuato da oggetti specifici. Tale mancanza di informazione costituisce un ostacolo rilevante quando si tratta di dimostrare la validità del consenso in base alla legislazione dell'UE, che prevede che l'interessato sia informato. In tali circostanze, il consenso non può essere utilizzato come base giuridica ai sensi del diritto dell'UE per il corrispondente trattamento dei dati.

Inoltre, i dispositivi indossabili, come gli *smart watch*, non sono riconoscibili come tali[5]: la maggior parte degli osservatori non può distinguere un orologio normale da uno connesso e quest'ultimo può essere provvisto di telecamere, microfoni e sensori di movimento che possono registrare e trasferire dati senza che le persone ne siano al corrente e quindi senza che acconsentano a tale trattamento. Ciò pone la questione dell'identificazione del trattamento dei dati attraverso il *wearable computing*, che può essere risolta prevedendo una segnaletica adeguata che sia effettivamente visibile agli interessati.

Inoltre, almeno in alcuni casi, la possibilità di rinunciare ad alcuni servizi o ad alcune caratteristiche di un dispositivo IoT è più un concetto teorico che una reale alternativa. Tali situazioni sollevano la questione se il consenso dell'utente al trattamento dei dati sottostanti possa essere considerato libero e quindi valido a norma del diritto dell'Unione o meno.

In più, i meccanismi classici usati per ottenere il consenso delle persone possono essere difficili da applicare all'IoT. Pertanto si ottiene un consenso "di bassa qualità", basato su una mancanza di informazione o sull'impossibilità di fatto di dare un consenso ben calibrato che tenga conto delle preferenze espresse dalle persone. In pratica, oggi sembra che generalmente i sensori non siano progettati per fornire informazioni da soli, né per fornire un meccanismo valido per ottenere il consenso della persona. Tuttavia, i portatori di interessi dell'IoT devono prendere in considerazione nuovi modi di ottenere il valido consenso dell'utente, anche prevedendo meccanismi atti a poter dare il consenso attraverso i dispositivi stessi. Nel corso del presente documento saranno citati esempi specifici come *privacy proxies* e *sticky policies*.

[5] Come illustrato nel parere 02/2013 sulle applicazioni per dispositivi intelligenti, il *wearable computing* comporta problemi risultanti dalla raccolta continua di dati di altri che si trovano nelle immediate vicinanze per periodi di tempo prolungati.

2.3 **Deduzioni tratte dai dati e riutilizzo del trattamento originario a fini diversi**

L'aumento della mole di dati generato dall'IoT in combinazione con le tecniche moderne di analisi e controllo incrociato dei dati possono portare a usi secondari di questi dati, relativi o meno allo scopo assegnato al trattamento originario. I terzi che richiedono l'accesso ai dati raccolti da altri soggetti potrebbero voler utilizzare questi dati per scopi completamente diversi.

Dati apparentemente insignificanti raccolti originariamente attraverso un dispositivo (ad esempio l'accelerometro e il giroscopio di uno *smartphone*) possono quindi essere utilizzati per ottenere altre informazioni con un significato completamente diverso (ad esempio le abitudini di guida della persona). Questa possibilità di ottenere dati da tali informazioni "grezze" deve essere presa in considerazione insieme ai classici rischi analizzati in relazione alla fusione dei sensori, fenomeno ben conosciuto in ambito informatico[6].

Il *quantified self* illustra anche quante informazioni possano essere tratte da sensori di movimento attraverso l'aggregazione e l'analisi avanzata. Questi dispositivi utilizzano spesso sensori elementari per acquisire dati grezzi (ad esempio i movimenti dell'interessato), si basano su algoritmi sofisticati per estrarre informazioni sensibili (ad esempio il numero dei passi) e deducono informazioni potenzialmente sensibili che saranno poi mostrate agli utenti finali (ad esempio le sue condizioni fisiche).

Tale tendenza pone problemi specifici: l'utente accettava di condividere le informazioni originarie per uno scopo specifico, ma potrebbe non voler condividere tali informazioni secondarie, che potrebbero essere utilizzate per scopi completamente differenti. È quindi importante che ad ogni livello (dei dati grezzi, di quelli estratti o ancora di quelli visualizzati) i portatori di interessi dell'IoT garantiscano che i dati siano utilizzati per scopi che sono tutti compatibili con quello originario del trattamento e che questi scopi siano noti all'utente.

2.4 **Deduzione invasiva dei modelli di comportamento e profilazione**

Sebbene oggetti diversi raccolgano separatamente singole informazioni isolate, un volume sufficiente di dati raccolti e ulteriormente analizzati può rivelare aspetti specifici delle abitudini, dei comportamenti e delle preferenze della persona. Come accennato sopra, la generazione di conoscenze da dati banali o addirittura anonimi sarà agevolata dalla proliferazione dei sensori, promuovendo importanti capacità di profilazione.

Oltre a ciò, l'analisi basata su informazioni raccolte in un ambiente IoT potrebbe permettere di rilevare i modelli di comportamento e di vita della persona in maniera ancora più dettagliata e completa.

Infatti, è probabile che questa tendenza abbia un impatto sul modo in cui la persona si comporta, così come è stato dimostrato che l'uso intensivo di telecamere a circuito chiuso ha effettivamente influenzato il comportamento dei cittadini negli spazi pubblici. Con l'IoT, tale sorveglianza potenziale potrebbe ora raggiungere la sfera più intima della vita delle persone, anche all'interno delle loro abitazioni. Questo eserciterà una pressione sulla persona affinché eviti comportamenti non comuni per prevenire la rilevazione di ciò che potrebbe essere percepito come un'anomalia. Tale tendenza sarebbe

[6] La fusione dei sensori consiste nel combinare i dati da sensori o tratti da diverse fonti al fine di ottenere informazioni migliori e più precise rispetto a quelle che sarebbe possibile ottenere se queste fonti operassero isolatamente.

molto invasiva per la vita privata e l'intimità delle persone e dovrebbe essere monitorata con molta attenzione.

2.5 **Limitazione della possibilità degli utenti dei servizi di mantenere l'anonimato**

Il pieno sviluppo delle capacità dell'IoT può mettere a dura prova le attuali possibilità di utilizzo anonimo dei servizi e in generale limitare la possibilità di passare inosservati.

Ad esempio gli oggetti indossabili, tenuti molto vicino agli interessati, rendono disponibile una serie di altri identificativi, quali indirizzi MAC di altri dispositivi, che potrebbero essere utili per generare una *fingerprint* ("impronta digitale") che permetta la localizzazione dell'interessato. La raccolta di vari indirizzi MAC di vari sensori agevolerà la creazione di *fingerprint* uniche e di identificativi più stabili che i portatori di interessi dell'IoT potranno attribuire a persone specifiche. Tali *fingerprint* e identificativi potrebbero essere utilizzati per vari scopi, compresa la *location analytics*[7] o l'analisi degli spostamenti di gruppi di persone e di singoli individui.

Tale tendenza deve essere valutata tenendo conto del fatto che questi dati possono essere successivamente integrati da altri dati emessi da altri sistemi (ad esempio telecamere a circuito chiuso o registri di accesso a Internet).

In tale contesto, alcuni dati forniti dai sensori sono particolarmente vulnerabili ai tentativi di reidentificazione.

Alla luce delle considerazioni di cui sopra, risulta evidente che la salvaguardia dell'anonimato e della vita privata nell'IoT sarà sempre più difficile. A tale riguardo, lo sviluppo dell'IoT comporta notevoli preoccupazioni relative alla protezione dei dati e alla tutela della vita privata.

2.6 **Rischi relativi alla sicurezza: sicurezza vs efficienza**

L'IoT pone vari problemi nel campo della sicurezza: i vincoli relativi alla sicurezza e l'esigenza di risparmiare risorse impongono ai fabbricanti di dispositivi di trovare un compromesso tra rendimento delle batterie e sicurezza del dispositivo. In particolare, non è ancora chiaro come i fabbricanti di dispositivi potranno trovare un compromesso tra l'applicazione delle misure di riservatezza, integrità e disponibilità a tutti i livelli del processo di trattamento e la necessità di ottimizzare l'uso delle risorse computazionali, nonché dell'energia, da parte degli oggetti e dei sensori.

Pertanto, c'è il rischio che l'IoT possa trasformare un oggetto di uso quotidiano in un potenziale obiettivo di attacchi alla sicurezza della vita privata e dei dati, al contempo diffondendo tali obiettivi in maniera molto più ampia rispetto all'attuale versione di Internet. Dispositivi connessi meno sicuri rappresentano potenzialmente nuovi modi efficienti di attaccare, che comportano l'allentamento delle pratiche di sorveglianza e la violazione di dati, con conseguente furto o compromissione di dati personali, che possono avere effetti di vasta portata sui diritti dei consumatori e sulla percezione che il singolo ha della sicurezza dell'IoT.

È inoltre previsto che i dispositivi e le piattaforme per l'IoT scambino e registrino i dati sulle infrastrutture dei fornitori di servizi. Perciò la sicurezza dell'IoT dovrebbe essere concepita prendendo

[7] Il termine *location analytics* si riferisce all'analisi volta a determinare quante persone sono in un certo luogo in un dato momento e per quanto tempo si fermano in tale luogo.

in considerazione non solamente la sicurezza dei dispositivi, ma anche i collegamenti per le comunicazioni, l'infrastruttura per la conservazione e altri input di questo ecosistema.

Analogamente, la presenza di vari livelli di trattamento, la cui progettazione e attuazione tecnica sono effettuate da diversi portatori di interessi, non garantisce un coordinamento adeguato tra di esse e può dare luogo alla presenza di punti deboli che possono essere utilizzati per sfruttare le vulnerabilità.

Ad esempio, la maggior parte dei sensori attualmente disponibili sul mercato non è in grado di stabilire comunicazioni cifrate in quanto le esigenze di calcolo avrebbero un impatto negativo su un dispositivo con una batteria di piccola potenza. Per quanto riguarda la sicurezza da punto a punto, il risultato ottenuto dall'integrazione di componenti fisiche e logiche proposta da una serie di portatori di interessi garantisce solamente il livello di sicurezza che è in grado di garantire la componente più debole.

3. Applicabilità del diritto dell'UE al trattamento dei dati personali nell'IoT

3.1 **Diritto applicabile**

Il quadro giuridico applicabile alla valutazione delle questioni relative alla protezione della vita privata e dei dati sollevate dall'IoT nell'UE è costituito dalla direttiva 95/46/CE e da disposizioni specifiche della direttiva 2002/58/CE, modificata dalla direttiva 2009/136/CE.

Tale quadro si applica qualora vengano rispettate le condizioni di applicabilità di cui all'articolo 4 della direttiva 95/46/CE. Il Gruppo di lavoro ha fornito orientamenti dettagliati per l'interpretazione delle disposizioni dell'articolo 4, segnatamente nel suo parere 8/2010[8] sul diritto applicabile.

In particolare, ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva, il diritto nazionale dello Stato membro è applicabile a tutti i trattamenti di dati personali effettuati "*nel contesto delle attività di uno stabilimento*" del responsabile del trattamento nel territorio dello Stato membro. Tale nozione di stabilimento nel contesto dell'economia basata su Internet è stata recentemente interpretata in senso molto ampio dalla Corte di giustizia europea[9].

Il diritto nazionale di uno Stato membro è applicabile anche nei casi in cui il responsabile non è stabilito nel territorio della Comunità ma ricorre a "*strumenti*" situati nel territorio di detto Stato membro (articolo 4, paragrafo 1, lettera c). Pertanto, anche quando un portatore di interessi nel settore dell'IoT qualificabile come responsabile del trattamento ai sensi della direttiva 95/46/CE non è stabilito nell'UE ai sensi dell'articolo 4, paragrafo 1, lettera a) (che sia coinvolto nello sviluppo, nella distribuzione o nel funzionamento di dispositivi per l'IoT), è probabile che sia soggetto al diritto dell'UE in quanto effettua il trattamento di dati raccolti attraverso "*strumenti*" di utenti situati nell'UE.

Infatti, tutti gli oggetti che vengono utilizzati per raccogliere e trattare ulteriormente i dati personali nel contesto della fornitura di servizi nell'ambito dell'IoT sono qualificabili come strumenti ai sensi della direttiva. Ovviamente questa qualifica è applicabile ai dispositivi in sé (contapassi, *sleep tracker*, dispositivi domestici "connessi" come termostati, sensori di fumo, occhiali e orologi *smart*, ecc.), ma anche ai dispositivi terminali degli utenti (ad esempio *smartphone* o *tablet*) nei quali sono stati precedentemente installati software o applicazioni sia per monitorare l'ambiente dell'utente attraverso

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_it.pdf
[9] Sentenza della Corte (Grande Sezione), 13 maggio 2014, causa C-131/12 (punti da 45 a 60).

sensori incorporati o interfacce di rete, sia per poi inviare i dati raccolti da questi dispositivi ai vari responsabili del trattamento coinvolti.

L'individuazione del ruolo dei vari portatori di interessi dell'IoT sarà fondamentale per qualificare il loro status giuridico come responsabili del trattamento e quindi identificare il diritto nazionale applicabile al trattamento da loro effettuato, così come le loro rispettive responsabilità. L'individuazione del ruolo delle parti coinvolte nell'IoT verrà trattata qui di seguito nella sezione 3.3.

3.2 **La nozione di dati personali**

Il diritto dell'UE si applica al trattamento di dati personali come definito all'articolo 2 della direttiva 95/46/CE. Il Gruppo di lavoro ha fornito orientamenti dettagliati per l'interpretazione di questo concetto, segnatamente nel parere 4/2007 sul concetto di dati personali[10].

Nel contesto dell'IoT, accade spesso che una persona possa essere identificata sulla base dei dati provenienti dagli "oggetti". Infatti, tali dati possono permettere di ricostruire il modello di vita di una persona o di una famiglia specifica, ad esempio i dati generati dal controllo centralizzato dell'illuminazione, del riscaldamento, della ventilazione e del condizionamento d'aria.

Inoltre è possibile che anche i dati relativi a persone il cui trattamento avviene solamente in seguito alla pseudonimizzazione o addirittura all'anonimizzazione debbano essere considerati come dati personali. Di fatto la grande quantità di dati trattati automaticamente nel contesto dell'IoT comporta rischi di reidentificazione. A tale proposito, il Gruppo di lavoro rimanda ai fenomeni illustrati nel suo recente parere sulle tecniche di anonimizzazione, che contiene indicazioni utili per identificare tali rischi nonché raccomandazioni sull'applicazione di tali tecniche [11].

3.3 **I portatori di interessi come responsabili del trattamento stabiliti nell'UE**

Il concetto di responsabile del trattamento e la sua interazione con quello di incaricato del trattamento sono cruciali nell'applicazione della direttiva 95/46/CE, in quanto condizionano le rispettive responsabilità delle varie organizzazioni coinvolte nell'applicazione di un trattamento dei dati con riferimento alla normativa dell'UE in materia di protezione dei dati. I portatori di interessi possono fare riferimento al parere del Gruppo di lavoro n. 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"[12], che fornisce orientamenti per l'applicazione di tali concetti a sistemi complessi con molteplici attori e scenari in cui agiscono responsabili e incaricati, singolarmente o congiuntamente, con diversi gradi di autonomia e di responsabilità.

Infatti, l'attuazione dell'IoT implica in maniera casuale l'intervento combinato di varie parti interessate, quali fabbricanti di dispositivi, piattaforme sociali, applicazioni di terzi, titolari o affittuari di dispositivi, intermediari di dati[13] o piattaforme di dati.

---

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_it.pdf

[11] Parere 05/2014 sulle tecniche di anonimizzazione adottato il 10 aprile 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf

[12] Parere 01/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" adottato il 16 febbraio 2010 (WP 169) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_it.pdf

[13] Gli intermediari di dati acquistano dati tramite le imprese al fine di creare liste di individui appartenenti ad una stessa categoria o gruppo. Queste categorie e questi gruppi vengono determinati dagli intermediari di dati ma possono riflettere caratteristiche demografiche, redditi o l'interesse espresso per un particolare argomento o prodotto.

La complessa rete di portatori di interessi coinvolti richiede e comporta la necessità di una ripartizione precisa delle responsabilità giuridiche tra di loro, con riferimento al trattamento dei dati personali, in base alle specificità dei loro rispettivi interventi.

3.3.1 Fabbricanti di dispositivi

I fabbricanti di dispositivi dell'IoT non si limitano a vendere oggetti fisici ai loro clienti o prodotti senza marchio ad altre organizzazioni: possono anche aver sviluppato o modificato il sistema operativo dell'"oggetto" o avervi installato software che determinano la sua funzionalità generale, compresi i dati, la frequenza di raccolta, quando e a chi vengono trasmessi i dati e per quali scopi (ad esempio, le imprese potrebbero stabilire il costo dell'assicurazione dei propri dipendenti sulla base dei dati trasmessi dai *tracker* che fanno loro indossare[14]). Per la maggior parte, essi effettivamente raccolgono e trattano dati personali che sono generati dal dispositivo per finalità e mezzi che hanno determinato nella loro totalità, e sono quindi qualificabili come responsabili del trattamento ai sensi del diritto UE.

3.3.2 Piattaforme sociali

Quando gli interessati possono condividere dati pubblicamente o con altri utenti, è ancora più probabile che facciano ricorso a oggetti connessi. In particolare, gli utenti dei dispositivi di *quantified self* tendono a condividere i dati con altri sui *social network* per stimolare una sorta di competizione positiva all'interno del gruppo.

Tale condivisione dei dati raccolti e aggregati dagli "oggetti" sui *social network* spesso ha luogo automaticamente, una volta che l'utente ha configurato l'applicazione in tal senso. Inoltre, la capacità di condivisione fa comunemente parte delle normali impostazioni di default delle applicazioni fornite dal fabbricante.

L'aggregazione di queste comunicazioni sulle piattaforme sociali attribuisce a queste ultime specifiche responsabilità in materia di protezione dei dati. Poiché questi dati sono inseriti nelle piattaforme dall'utente, quando i *social network* li trattano per scopi distinti che essi stessi hanno determinato, questi ultimi sono qualificabili come responsabili del trattamento ai sensi del diritto UE. Ad esempio, un *social network* può utilizzare le informazioni raccolte da un contapassi per dedurre che un particolare utente corre regolarmente e mostrargli pubblicità di scarpe da corsa. Le conseguenze di questa qualifica sono state affrontate nel dettaglio nel parere del Gruppo di lavoro sui *social network*[15].

3.3.3 Sviluppatori di applicazioni terzi

Molti sensori contengono API per agevolare lo sviluppo di applicazioni. Per utilizzare queste applicazioni, gli interessati devono installare applicazioni di terzi che consentano loro di accedere ai propri dati, che vengono conservati dal fabbricante del dispositivo. Installare queste applicazioni consiste spesso nel fornire allo sviluppatore dell'applicazione un accesso ai dati attraverso l'API.

Alcune applicazioni possono premiare gli utenti di oggetti specifici, ad esempio un'applicazione sviluppata da una compagnia di assicurazione sanitaria potrebbe premiare gli utenti di "oggetti" di *quantified Self* o una compagnia di assicurazione sulla casa potrebbe sviluppare un'applicazione che garantisca la corretta configurazione degli allarmi antincendio connessi dei propri clienti. A meno che

[14] With tracking devices, employers may track workers' health http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

[15] Parere 5/2009 sui social network on-line adottato il 12 giugno 2009 (WP 163) - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_it.pdf

questi dati non siano adeguatamente resi anonimi, tale accesso costituisce un trattamento ai sensi dell'articolo 2 della direttiva 95/46/CE e lo sviluppatore dell'applicazione che ha organizzato tale accesso ai dati deve essere considerato il responsabile del trattamento ai sensi del diritto UE.

Tali applicazioni vengono tradizionalmente installate sulla base dell'esplicito consenso dell'interessato ("*opt-in*"). Infatti, dal momento che tale accesso è soggetto all'ottenimento del consenso preventivo dell'utente, tale consenso deve essere espresso con chiarezza, specifico e informato. In pratica, tuttavia, le richieste di autorizzazione da parte degli sviluppatori di applicazioni di terzi spesso non contengono le informazioni necessarie perché il consenso dell'utente sia considerato specifico e sufficientemente informato e quindi valido in base al diritto dell'UE (vedi infra).

3.3.4 Altri terzi

Terzi diversi dai fabbricanti di dispositivi e dagli sviluppatori di applicazioni terzi possono utilizzare dispositivi IoT per raccogliere e trattare informazioni sulle persone. Ad esempio, le compagnie di assicurazione sanitaria possono voler fornire contapassi agli assicurati per monitorare la frequenza del loro esercizio fisico[16] e adattare di conseguenza i loro premi assicurativi.

A differenza dei fabbricanti di dispositivi, tali terzi non hanno alcun controllo sul tipo di dati raccolti dall'oggetto; tuttavia sono qualificabili come responsabili del trattamento per questi trattamenti, in quanto raccolgono e conservano i dati generati da tali dispositivi IoT per scopi specifici che essi stessi hanno determinato.

Esempio: Una compagnia di assicurazione lancia un nuovo progetto e offre un contapassi agli assicurati che vogliono fare domanda per tariffe assicurative più basse. Gli assicurati che accettano l'offerta ricevono un contapassi configurato e registrato dalla compagnia. Gli assicurati possono accedere ai dati registrati dai loro contapassi, ma i dispositivi stessi sono di proprietà di "FeelGood" che può accedere ugualmente ai dati dei propri assicurati. In tale contesto, gli assicurati dovrebbero essere considerati come interessati e dovrebbe essere concesso loro l'accesso all'account dell'applicazione contapassi, mentre la compagnia di assicurazione è qualificabile come responsabile del trattamento.

3.3.5 Piattaforme di dati IoT

A causa della mancanza di standardizzazione e di interoperabilità, l'Internet degli oggetti è visto a volte come l'"Intranet degli oggetti", in cui ogni fabbricante ha definito la propria gamma di interfacce e il formato dei dati. Pertanto l'*hosting* dei dati avviene in ambienti chiusi, che di fatto impediscono agli utenti di trasferire (o anche combinare) i propri dati da un dispositivo a un altro.

Tuttavia, *smartphone* e *tablet* sono diventati i naturali punti di accesso a Internet dei dati raccolti attraverso molti dispositivi IoT. Di conseguenza, i fabbricanti hanno progressivamente sviluppato piattaforme il cui scopo è quello dell'*hosting* dei dati raccolti attraverso i vari dispositivi al fine di centralizzarne e semplificarne la gestione.

Anche tali piattaforme possono essere qualificate come responsabili del trattamento ai sensi della normativa UE sulla protezione dei dati, quando lo sviluppo di tali servizi implica effettivamente che raccolgano i dati personali degli utenti per finalità proprie.

[16] With tracking devices, employers may track workers' health, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

3.4 **Persone in qualità di interessati: abbonati, utenti, non utenti**

Gli abbonati e più in generale gli utenti dell'IoT sono qualificabili come interessati ai sensi del diritto dell'UE. Se utilizzano i dati raccolti e conservati esclusivamente per i propri scopi personali o domestici, essi rientrano nell'ambito della cosiddetta "esenzione domestica" di cui alla direttiva 95/46/CE[17]. Tuttavia, in pratica, il modello operativo dell'IoT comporta che i dati dell'utente vengano trasferiti sistematicamente a fabbricanti di dispositivi, sviluppatori di applicazioni e altri terzi qualificabili come responsabili del trattamento. L'"esenzione domestica" avrà quindi un'applicazione limitata nel contesto dell'IoT.

Il trattamento dei dati nell'IoT può anche riguardare persone che non sono né abbonati, né effettivi utenti dell'IoT. Ad esempio, dispositivi indossabili quali *smart glasses* ("occhiali intelligenti") possono raccogliere dati riguardanti interessati che non siano proprietari dei dispositivi stessi. È importante sottolineare che questo fattore non impedisce che il diritto dell'UE sia applicabile a tali situazioni. L'applicazione della normativa dell'UE in materia di protezione dei dati non è legata alla proprietà del dispositivo o del terminale, bensì al trattamento dei dati personali in sé, chiunque sia l'interessato.

4. Obblighi a carico dei portatori di interessi

I portatori di interessi nel settore dell'IoT qualificabili come responsabili del trattamento ai sensi del diritto dell'UE (individualmente o congiuntamente ad altri) devono osservare i vari obblighi che spettano loro in applicazione della direttiva 95/46/CE ed eventualmente delle disposizioni pertinenti della direttiva 2002/58/CE. Il presente parere si occupa solamente dell'applicazione delle norme che meritano particolare attenzione in questo contesto, ma ciò non significa che le altre disposizioni non siano di applicazione.

4.1 **Applicazione dell'articolo 5, paragrafo 3, della direttiva "e-Privacy"**

L'articolo 5, paragrafo 3, della direttiva 2002/58/CE è applicabile alle situazioni in cui un portatore di interessi dell'IoT archivia le informazioni o accede alle informazioni già archiviate in un dispositivo IoT, nella misura in cui i dispositivi IoT siano qualificabili come "*apparecchiatura terminale*" ai sensi di tale disposizione[18]. La disposizione prevede inoltre che l'abbonato o l'utente in questione dia il proprio consenso a tale archiviazione o accesso perché queste azioni siano legittime, a meno che non siano "*strettamente necessarie per erogare un servizio esplicitamente richiesto dall'abbonato o dall'utente*" [19]. Tale requisito è particolarmente importante in quanto altri portatori di interessi diversi dall'utente o dall'abbonato possono accedere a dati contenenti informazioni sensibili archiviate in tali apparecchiature terminali[20].

L'obbligo del consenso di cui all'articolo 5, paragrafo 3, riguarda principalmente il fabbricante del dispositivo, ma anche tutti i portatori di interessi che vogliano accedere a questi dati grezzi aggregati archiviati in tale infrastruttura. Esso si applica anche a qualsiasi responsabile del trattamento che voglia archiviare dati supplementari nel dispositivo di un utente.

---

[17] Cfr. parere 5/2009 sui social network on-line adottato il 12 giugno 2009 (WP 163).

[18] Il concetto "*apparecchiature terminali*" di cui all'articolo 5, paragrafo 3, coincide con quello di "*strumenti*" di cui all'articolo 4, paragrafo 1, lettera c).

[19] Parere 02/2013 sulle applicazioni per dispositivi intelligenti (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_it.pdf

[20] Cfr. considerando 25 della direttiva 2002/58/CE.

In tali circostanze, i portatori di interessi dell'IoT devono garantire che la persona in questione abbia effettivamente dato il suo consenso a tale archiviazione e/o accesso, dopo essere stata informata in modo chiaro e completo dal responsabile del trattamento, tra l'altro, sugli scopi del trattamento.

Pertanto, il consenso dell'utente deve essere ottenuto prima di accedere alle informazioni del dispositivo che possono essere utilizzate per generare una *fingerprint* di qualsiasi dispositivo (compresi i dispositivi indossabili). Il Gruppo di lavoro ha già fornito orientamenti sulla nozione di consenso per i *cookie* o per tecnologie di *tracking* simili nel suo documento di lavoro 02/2013 (WP-208) e fornirà ulteriori orientamenti su tale questione nel previsto parere sul *fingerprinting*.

Esempio: Un contapassi registra il numero dei passi fatti dal proprio utente e archivia questa informazione nella sua memoria interna. L'utente ha installato sul proprio computer un'applicazione per scaricare direttamente il numero dei passi dal proprio dispositivo. Se il fabbricante del dispositivo vuole caricare i dati dai contapassi sui propri server, deve ottenere il consenso dell'utente ai sensi dell'articolo 5, paragrafo 3, della direttiva 2002/58/CE.

Una volta che il fabbricante del dispositivo ha caricato i dati sui propri server, conserva unicamente i dati aggregati sul numero di passi al minuto. Ad un'applicazione che richieda di accedere a tali dati, dal momento che sono archiviati sul server del fabbricante del dispositivo, non si applica quindi l'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche, bensì si applicano le disposizioni della direttiva 95/46/CE relative alla legittimità di questo ulteriore trattamento.

Inoltre, il proprietario di un dispositivo IoT e la persona i cui dati verranno monitorati (l'interessato) potrebbero essere persone distinte. Questa situazione può portare a un'applicazione contemporanea ma differenziata dell'articolo 5, paragrafo 3, della direttiva 2002/58/CE e della direttiva 95/46/CE.

Esempio: Un autonoleggio installa un dispositivo "intelligente" di localizzazione sulle proprie auto a noleggio. Sebbene l'autonoleggio sia considerato il proprietario/abbonato del dispositivo/servizio di localizzazione, la persona che noleggia l'auto è qualificabile come l'utente del dispositivo. L'articolo 5, paragrafo 3, prevede quindi che il fabbricante del dispositivo ottenga (perlomeno) il consenso dell'utente del dispositivo, in questo caso la persona che prende a noleggio l'auto. Inoltre, la legittimità del trattamento dei dati personali relativi alle persone che prendono a noleggio le auto è soggetta ai diversi requisiti di cui all'articolo 7 della direttiva 95/46/CE.

4.2 **Base giuridica per il trattamento (articolo 7 della direttiva 95/46/CE)**

I portatori di interessi dell'IoT qualificabili come responsabili del trattamento (cfr. la precedente sezione 4.3) devono soddisfare uno dei requisiti elencati all'articolo 7 della direttiva perché il trattamento di dati personali sia legittimo. Tali requisiti si applicano ad alcuni di questi portatori di interessi in aggiunta all'articolo 5, paragrafo 3, quando il trattamento in questione va oltre l'archiviazione di informazioni o l'accesso a informazioni archiviate nelle apparecchiature terminali dell'utente/abbonato[21].

In pratica, sono tre le basi giuridiche pertinenti in tale contesto.

[21] Sull'articolazione dell'articolo 5, paragrafo 3 e dell'articolo 7, lettera a), si veda in particolare il parere 02/2013 sulle applicazioni per dispositivi intelligenti adottato il 27 febbraio 2013 (WP202) – (pagg. 14 e seguenti) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_it.pdf e il parere 06/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP217) – (pagg. 26, 32, 46).

Il consenso [articolo 7, lettera a)] è la prima base giuridica alla quale devono fare riferimento nel contesto dell'IoT sia i fabbricanti di dispositivi, sia le piattaforme sociali o le piattaforme di dati, gli affittuari di dispositivi o gli sviluppatori terzi. In varie occasioni, il Gruppo di lavoro ha fornito orientamenti sull'applicazione simultanea dei requisiti di cui all'articolo 7, lettera a), e di quelli di cui all'articolo 5, paragrafo 3, della direttiva 2002/58/CE[22]. Anche le condizioni perché tale consenso sia valido ai sensi del diritto dell'UE sono state stabilite in un precedente parere del Gruppo[23].

L'articolo 7, lettera b), stabilisce inoltre che il trattamento è legittimo quando è necessario all'esecuzione del contratto concluso con l'interessato. L'ambito di applicazione di tale base giuridica è limitato dal criterio di "necessità", il quale richiede un nesso diretto e oggettivo tra il trattamento stesso e le finalità dell'esecuzione del contratto previste dall'interessato.

In terzo luogo, l'articolo 7, lettera f), consente il trattamento dei dati personali quando è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali dell'interessato (in particolare il diritto alla vita privata con riguardo al trattamento dei dati personali), che richiedono tutela ai sensi dell'articolo 1, paragrafo 1, della direttiva.

Nella sentenza nella causa *Google Spain*[24], la Corte di giustizia dell'Unione europea ha fornito orientamenti significativi sull'interpretazione di questa disposizione, in aggiunta a quelli già forniti nelle precedenti cause riunite ASNEF e FECEMD (C-468/10 e C-469/10). Nel contesto dell'IoT, il trattamento dei dati personali di un individuo può incidere significativamente sui suoi diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali in situazioni in cui, senza dispositivi IoT, i dati non avrebbero potuto essere interconnessi o solo con grande difficoltà. Situazioni di questo tipo possono verificarsi quando i dati raccolti sono relativi allo stato di salute dell'individuo, l'abitazione o l'intimità, la sua ubicazione e molti altri aspetti della sua vita privata. Alla luce della potenziale gravità di tale interferenza, risulta chiaro che tale trattamento sarà difficilmente giustificabile semplicemente dall'interesse economico di un portatore di interessi dell'IoT per tale trattamento. Devono concorrere altri interessi perseguiti dal responsabile del trattamento oppure dal o dai terzi cui vengono comunicati i dati[25].

Esempio: Nel quadro di un piano per promuovere l'uso dei mezzi pubblici e per ridurre l'inquinamento, il consiglio comunale vuole regolamentare il parcheggio nel centro città imponendo restrizioni all'accesso e tasse di parcheggio. L'importo della tassa dipende da vari parametri, compresi il tipo di motore (a gasolio, a benzina, elettrico) e l'età del veicolo. Quando un veicolo si avvicina a un parcheggio libero, un sensore può leggerne la targa per determinare, dopo un controllo con una banca dati, la maggiorazione o lo sconto da applicare automaticamente sulla base di criteri predefiniti. In questo caso, il trattamento dei dati della targa per determinare l'importo della tassa potrebbe soddisfare l'interesse legittimo del responsabile del trattamento. Un ulteriore trattamento, come l'ottenimento di informazioni, non rese anonime, sugli spostamenti dei veicoli all'interno dell'area soggetta a restrizioni richiederebbe il ricorso ad un'altra base giuridica.

[22] Parere WP202, pagg. 14 e seguenti.
[23] Parere 15/2011 sulla definizione di consenso adottato il 13 luglio 2011 (WP187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_it.pdf
[24] Sentenza della Corte (Grande Sezione), 13 maggio 2014, causa C-131/12 (punti 74 e successivi).
[25] Parere WP217.

4.3 **Principi relativi alla qualità dei dati**

Nel loro complesso, i principi sanciti dall'articolo 6 della direttiva 95/46/CE costituiscono una pietra miliare della normativa UE sulla protezione dei dati.

I dati personali devono essere trattati lealmente e lecitamente. Il principio di lealtà esige esplicitamente che i dati personali non debbano mai essere raccolti e trattati senza che il diretto interessato ne sia effettivamente al corrente. Questo requisito è tanto più importante in relazione all'IoT, in quanto i sensori sono effettivamente progettati per non essere evidenti, ossia per essere il meno visibili possibile. Tuttavia, i responsabili del trattamento che operano nell'IoT (in particolare i fabbricanti di dispositivi) sono tenuti ad informare tutte le persone che si trovano geograficamente o digitalmente nelle vicinanze dei dispositivi connessi quando vengono raccolti i dati relativi a loro stessi o all'ambiente che li circonda. Il rispetto di questa disposizione non è soltanto un rigoroso obbligo giuridico: la raccolta leale di dati ha fa parte delle aspettative più importanti degli utenti in relazione all'IoT, in particolare per quanto riguarda il *wearable computing*.

Esempio: Un dispositivo sanitario usa una piccola luce per monitorare il flusso di sangue che scorre nelle vene e per ricavare informazioni sul battito del cuore. Il dispositivo comprende un altro sensore che misura il livello di ossigeno nel sangue, ma non vengono fornite informazioni circa questa raccolta di dati, né sul dispositivo né sull'interfaccia per l'utente. Anche se il sensore che misura il livello di ossigeno nel sangue è pienamente funzionante, non deve essere attivato senza prima informare l'utente. Occorre il consenso esplicito per attivare questo sensore.

Il principio di limitazione delle finalità implica che i dati possano essere rilevati solo per finalità determinate, esplicite e legittime. Qualsiasi ulteriore trattamento incompatibile con tali finalità originarie sarebbe illecito in base al diritto dell'UE. Tale principio mira a permettere agli utenti di sapere come e per quali finalità i loro dati saranno utilizzati e di decidere se affidare i propri dati a un responsabile del trattamento. Tali finalità devono essere determinate *prima* che abbia luogo il trattamento dei dati e ciò esclude cambiamenti improvvisi delle condizioni fondamentali del trattamento. Questo implica che i portatori di interessi dell'IoT devono avere un quadro completo del loro progetto prima di iniziare la raccolta di qualsiasi dato personale.

Inoltre, i dati raccolti sull'interessato devono essere strettamente necessari al conseguimento della finalità precedentemente determinata dal responsabile del trattamento (principio della "riduzione al minimo dei dati"). I dati che sono necessari per tale finalità non devono essere raccolti e conservati "in caso ve ne fosse bisogno" o perché "potrebbero essere utili in seguito". Alcuni portatori di interessi ritengono che il principio della riduzione al minimo dei dati possa limitare le potenziali opportunità dell'IoT, diventando quindi un ostacolo all'innovazione, poiché i benefici potenziali del trattamento dei dati deriverebbero dall'analisi esplorativa mirante a scoprire correlazioni e tendenze non ovvie. Il Gruppo di lavoro non può condividere questa analisi e insiste sul fatto che il principio della riduzione al minimo dei dati svolge un ruolo essenziale nella tutela dei diritti delle persone in materia di protezione dei dati sanciti dal diritto dell'UE e dovrebbe essere rispettato in quanto tale[26]. Questo principio determina in particolare che, quando i dati personali non sono necessari per fornire un

[26] In ogni caso, in pratica, la ricerca esplorativa non è mai effettuata con una selezione del tutto casuale: la finalità generale di qualsiasi ricerca è tradizionalmente definita, almeno parzialmente, anche solo per motivi organizzativi e di budget. È difficile immaginare che il trattamento dei dati per una ricerca specifica sia compatibile con la finalità originaria della raccolta dei dati e pertanto ciò è in contrasto con il diritto dell'UE.

servizio specifico tramite l'IoT, all'interessato debba essere offerta almeno la possibilità di utilizzare il servizio in modo anonimo.

L'articolo 6 dispone inoltre che i dati personali raccolti e trattati nel contesto dell'IoT siano conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono stati rilevati o sono stati successivamente trattati. Questa verifica della necessità deve essere eseguita da ogni portatore di interessi nella prestazione di un servizio specifico di IoT, dal momento che le finalità dei trattamenti possono essere differenti di volta in volta. Ad esempio, i dati personali comunicati da un utente quando si abbona ad un servizio specifico di IoT devono essere cancellati non appena l'utente disdice l'abbonamento. Analogamente, le informazioni cancellate dall'utente nel proprio account non devono essere conservate. Qualora l'utente non utilizzi il servizio o l'applicazione per un periodo di tempo determinato, il profilo dell'utente deve essere impostato come inattivo. Dopo un ulteriore periodo di tempo, i dati devono essere cancellati. L'utente deve essere informato prima che siano intraprese queste misure, qualunque sia il mezzo che ha a disposizione il portatore di interessi.

4.4 **Trattamento di dati sensibili (articolo 8)**

Le applicazioni IoT trattano talvolta dati personali che possono rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute e la vita sessuale, effettivamente qualificabili come "dati sensibili" e che meritano una tutela speciale ai sensi dell'articolo 8 della direttiva 95/46/CE. In pratica, l'applicazione dell'articolo 8 ai dati sensibili nell'IoT prevede che i responsabili del trattamento ottengano il consenso esplicito dell'utente, a meno che sia l'interessato stesso a rendere pubblici i dati.

Tale situazione può verificarsi in contesti specifici come quello dei dispositivi di *quantified self*. In questi casi, i dispositivi in questione registrano principalmente dati relativi al benessere della persona. Questi dati non costituiscono necessariamente dati sulla salute in quanto tali, ma possono fornire rapidamente informazioni sulla salute della persona poiché vengono registrati nel corso del tempo, per cui si possono dedurre dati dalla loro variabilità in un determinato arco di tempo. I responsabili del trattamento devono prevedere questo possibile cambiamento di qualifica e adottare di conseguenza misure adeguate.

Esempio: L'impresa X ha sviluppato un'applicazione che è in grado di rilevare modelli d'uso di droghe, analizzando i dati grezzi dai segnali di un elettrocardiogramma generati da sensori commerciali comunemente a disposizione dei consumatori. Il motore dell'applicazione può estrarre informazioni specifiche dai dati grezzi dall'elettrocardiogramma che, in base agli esiti precedenti, sono collegati al consumo di droghe. Il prodotto, compatibile con la maggior parte dei sensori sul mercato, potrebbe essere utilizzato come un'applicazione autonoma o attraverso un'interfaccia web che richiede il caricamento dei dati. Deve essere ottenuto il consenso esplicito dell'utente per trattare i dati a tal fine. Il rispetto di questo requisito può essere raggiunto alle stesse condizioni e nello stesso momento in cui il consenso viene ottenuto dall'interessato ai sensi dell'articolo 7, lettera a).

4.5 **Requisiti di trasparenza (articoli 10 e 11)**

Oltre al requisito della raccolta leale dei dati di cui all'articolo 6, lettera a), i responsabili del trattamento devono fornire informazioni specifiche agli interessati in applicazione degli articoli 10 e 11, quali l'identità del responsabile del trattamento, le finalità del trattamento, i destinatari dei dati, l'esistenza di diritti di accesso e di opporsi (incluse informazioni su come sconnettere l'oggetto per evitare la divulgazione di ulteriori dati).

A seconda delle applicazioni, queste informazioni potrebbero essere fornite, ad esempio, dall'oggetto stesso, utilizzando la connettività senza fili per trasmettere le informazioni, oppure utilizzando l'ubicazione attraverso un controllo di prossimità a tutela della vita privata effettuato da un server centralizzato per informare gli utenti che si trovano vicini al sensore.

Inoltre, queste informazioni devono essere fornite in maniera chiara e comprensibile, conformemente al principio del trattamento leale. Ad esempio, il fabbricante del dispositivo potrebbe stampare sugli oggetti dotati di sensori un codice QR che descriva il tipo di sensori e le informazioni che acquisiscono, nonché le finalità di tali raccolte di dati.

4.6 **Sicurezza (articolo 17)**

L'articolo 17 della direttiva sulla protezione dei dati stabilisce che il responsabile del trattamento "*deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali*" e che "*il responsabile del trattamento, quando quest'ultimo sia eseguito per suo conto, deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare*".

Pertanto, ogni parte interessata qualificabile come responsabile del trattamento conserva la piena responsabilità della sicurezza del trattamento dei dati. Se le lacune in materia di sicurezza che comportano violazioni del principio della sicurezza sono dovute a una progettazione e a una manutenzione inadeguate dei dispositivi utilizzati, ciò implica la responsabilità del responsabile del trattamento. In tal senso, è necessario che i responsabili del trattamento effettuino valutazioni di sicurezza dei sistemi nel loro insieme, anche a livello dei componenti, applicando i principi della "*composable security*". Analogamente occorre applicare l'uso della certificazione per i dispositivi, così come l'allineamento con standard di sicurezza riconosciuti a livello internazionale per migliorare la sicurezza generale dell'ecosistema dell'IoT.

I subappaltatori che progettano e fabbricano componenti hardware per conto di altri portatori di interessi, senza effettivamente trattare alcun dato personale, non possono, in senso stretto, essere considerati responsabili ai sensi dell'articolo 17 della direttiva 95/46/CE in caso di violazione della protezione dei dati dovuta a lacune nella sicurezza di questi dispositivi. Tuttavia i portatori di interessi svolgono un ruolo fondamentale nel garantire la sicurezza dell'ecosistema dell'IoT. I portatori di interessi con una responsabilità diretta per ciò che riguarda la protezione dei dati nei confronti degli interessati dovrebbero garantire che questi subappaltatori si attengano effettivamente a elevati requisiti di sicurezza per quanto riguarda la tutela della vita privata quando progettano e fabbricano i loro prodotti.

Come già osservato, le misure di sicurezza devono essere attuate tenendo in considerazione gli specifici vincoli operativi dei dispositivi IoT. Ad esempio, oggi la maggior parte dei sensori non è in grado di stabilire comunicazioni cifrate a causa della priorità accordata all'autonomia fisica dei dispositivi o al controllo dei costi.

Inoltre, è difficile rendere sicuri i dispositivi operanti nell'IoT per motivi sia tecnici che economici. Dal momento che i loro componenti di solito utilizzano infrastrutture di comunicazione senza filo e sono caratterizzati da risorse limitate in termini di energia e di potenza di calcolo, i dispositivi sono vulnerabili ad attacchi fisici, intercettazioni o attacchi *proxy*. Le tecnologie più comuni attualmente utilizzate, ossia le infrastrutture a chiave pubblica (*Public Key Infrastructure*, PKI), non sono facilmente trasferibili nei dispositivi IoT in quanto la maggior parte dei dispositivi non ha la potenza di calcolo necessaria per far fronte ai compiti di elaborazione richiesti. L'IoT comporta una catena di

approvvigionamento complessa con molteplici portatori di interessi che si assumono diversi gradi di responsabilità. Una violazione della sicurezza potrebbe avere origine da una qualsiasi di esse, in particolare se si prendono in considerazione ambienti M2M basati sullo scambio di dati tra i dispositivi. Quindi, si deve tener conto del bisogno di utilizzare protocolli sicuri e leggeri che possano essere utilizzati in ambienti con poche risorse.

In questo contesto, nel quale la ridotta capacità di elaborazione può mettere a rischio una comunicazione sicura ed efficiente, il Gruppo di lavoro sottolinea che è ancora più importante rispettare il principio della riduzione al minimo dei dati e limitare al minimo necessario il trattamento dei dati personali, in particolare la loro archiviazione sul dispositivo.

Inoltre, i dispositivi che sono progettati per essere direttamente accessibili via Internet non sono sempre configurati dall'utente. Essi possono pertanto fornire una facile via d'accesso agli intrusi se continuano a funzionare con le impostazioni di default. Le pratiche di sicurezza basate su limitazioni della rete, disabilitando per default funzionalità non necessarie e impedendo l'uso di fonti non attendibili di aggiornamento del software (limitando così gli attacchi di *malware* basati sull'alterazione del codice), potrebbero contribuire a limitare l'impatto e l'entità di eventuali violazioni di dati. Tali misure per la tutela della vita privata dovrebbero essere intraprese fin dall'inizio, in applicazione del principio della *"privacy by design"* (tutela della vita privata sin dalla progettazione).

In più, l'assenza di aggiornamenti automatici causa frequenti vulnerabilità non corrette che possono essere scoperte facilmente attraverso motori di ricerca specializzati. Anche nei casi in cui gli utenti sono al corrente delle vulnerabilità dei propri dispositivi, essi possono non avere accesso agli aggiornamenti del venditore, a causa dei limiti dell'hardware o di tecnologie obsolete che impediscono al dispositivo di sostenere gli aggiornamenti del software. Se un fabbricante di dispositivo dovesse smettere di sostenerlo, dovrebbero essere fornite soluzioni alternative (ad esempio, aprendo il software alla comunità *open-source*). Gli utenti devono essere informati del fatto che i loro dispositivi possono diventare vulnerabili a errori non corretti.

Anche alcuni dei sistemi di auto-monitoraggio sul mercato (ad esempio contapassi e *sleep tracker*) sono caratterizzati da falle di sicurezza che consentono agli aggressori di alterare i valori osservati che sono comunicati alle applicazioni e ai fabbricanti di dispositivi. È fondamentale che questi dispositivi garantiscano una tutela adeguata contro l'alterazione di dati, in particolare se i valori riportati da questi sensori hanno un impatto indiretto sulle decisioni relative alla salute degli utenti.

Cosa non meno importante, anche un'adeguata politica di comunicazione delle violazioni dei dati può contribuire al contenimento degli effetti negativi delle vulnerabilità del software e della progettazione diffondendo le conoscenze e fornendo orientamenti su tali questioni.

5. Diritti dell'interessato

I portatori di interessi nel settore dell'IoT devono rispettare i diritti degli interessati conformemente alle disposizioni di cui agli articoli 12 e 14 della direttiva 95/46/CE e adottare misure organizzative di conseguenza. Tali diritti non sono limitati agli abbonati ai servizi dell'IoT o ai proprietari dei dispositivi, ma riguardano qualsiasi persona i cui dati personali vengono trattati.

5.1 **Diritto di accesso**

L'articolo 12, lettera a), stabilisce che gli interessati hanno il diritto di ottenere dai responsabili del trattamento la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati.

In pratica, gli utenti dell'IoT tendono ad essere vincolati a sistemi specifici. I dispositivi di solito inviano dapprima i dati al fabbricante del dispositivo, che poi li rende accessibili all'utente attraverso un portale web o un'applicazione. Tale progettazione permette ai fabbricanti di fornire servizi on-line che sfruttano le capacità del dispositivo, ma può anche impedire agli utenti di scegliere liberamente il servizio che interagisce con il proprio dispositivo.

Inoltre oggi gli utenti finali sono raramente in grado di accedere ai dati grezzi che sono registrati dai dispositivi IoT. Chiaramente, i dati interpretati presentano un interesse più immediato per loro rispetto ai dati grezzi, che possono non avere alcun significato per loro. Eppure, l'accesso a tali dati può rivelarsi utile per gli utenti finali per capire cosa può dedurre da essi il fabbricante del dispositivo. Inoltre, avvalersi di questi dati grezzi darebbe loro la capacità di trasferire i propri dati a un altro responsabile del trattamento e passare ad altri servizi, ad esempio nel caso in cui il responsabile del trattamento originario dovesse cambiare la sua politica di tutela della vita privata in un modo che non li soddisfa. Oggigiorno, in pratica, queste persone non hanno altra possibilità che smettere di utilizzare i propri dispositivi in quanto la maggior parte dei responsabili del trattamento non fornisce tale funzionalità, concedendo l'accesso solo ad una versione obsoleta dei dati grezzi archiviati.

Il Gruppo di lavoro ritiene che tale atteggiamento impedisca l'esercizio effettivo del diritto di accesso accordato alle persone dall'articolo 12, lettera a), della direttiva 95/46/CE. A suo parere, i portatori di interessi dell'IoT devono adottare le misure necessarie per permettere agli utenti di far valere effettivamente tale diritto e offrire loro la possibilità di scegliere un altro servizio che potrebbe non essere proposto dal fabbricante del dispositivo. Le norme di interoperabilità dei dati potrebbero essere sviluppate con profitto a tal fine.

Tali misure sarebbero tanto più importanti da intraprendere in quanto il cosiddetto "diritto alla portabilità", che sarà probabilmente previsto nella proposta di regolamento generale sulla protezione dei dati come variazione del diritto di accesso, mira a porre definitivamente fine a situazioni di "*lock-in*" dell'utente [27]. Su questo punto, l'ambizione del legislatore europeo è quella di eliminare gli ostacoli alla concorrenza e aiutare i nuovi attori ad innovare questo mercato.

5.2 **Possibilità di revocare il consenso e di opporsi**

Gli interessati devono avere la possibilità di revocare il consenso dato in precedenza ad uno specifico trattamento dei dati e di opporsi al trattamento dei dati che li riguardano. L'esercizio di tali diritti deve essere possibile senza alcun vincolo tecnico o organizzativo o impedimento e gli strumenti forniti per effettuare tale revoca devono essere accessibili, visibili ed efficienti.

I meccanismi di revoca devono essere definiti nel dettaglio e comprendere: 1) tutti di dati raccolti da un oggetto specifico (ad esempio, richiedendo che la stazione meteorologica smetta di raccogliere i dati relativi all'umidità, alla temperatura e ai suoni); 2) una tipologia specifica di dati raccolta da qualsiasi oggetto (ad esempio, un utente dovrebbe essere in grado di interrompere la raccolta di dati di qualsiasi dispositivo che registra il suono, sia esso uno *sleep tracker* o una stazione meteorologica); 3) un trattamento dei dati specifico (ad esempio, un utente potrebbe richiedere che sia il suo contapassi sia il suo orologio smettano di contare i suoi passi).

Inoltre, dal momento che è probabile che gli "oggetti connessi" indossabili sostituiscano articoli esistenti che offrono funzionalità ordinarie, i responsabili del trattamento dovrebbero offrire la

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_it.pdf

possibilità di disattivare la funzione "connessa" dell'oggetto permettendogli di funzionare come l'articolo originale non connesso (ossia disattivare la funzionalità di connessione di uno *smart watch* o di *smart glasses*). Il Gruppo di lavoro ha già precisato che gli interessati devono avere la possibilità di "*revocare il proprio consenso in qualsiasi momento, senza dover uscire dal*" servizio fornito[28].

Esempio: un utente installa un allarme antincendio connesso all'interno del suo appartamento. L'allarme utilizza un sensore di presenza, un sensore di calore, un sensore ultrasonico e un sensore di luce. Alcuni di questi sensori sono necessari per rilevare un incendio, mentre altri forniscono solo funzioni aggiuntive delle quali è stato informato preventivamente. L'utente deve poter disattivare queste funzioni per poter utilizzare solamente l'allarme antincendio e quindi sconnettere i sensori usati per fornire queste funzioni.

È interessante notare che alcuni recenti sviluppi in questo campo stanno cercando di responsabilizzare gli interessati consentendo loro il controllo di aspetti di gestione del consenso, ad esempio attraverso l'uso di *sticky-policies*[29] o *privacy proxies*[30].

6. Conclusioni e raccomandazioni

Qui di seguito sono riportate varie raccomandazioni che il Gruppo di lavoro "articolo 29" ha ritenuto utile formulare per facilitare l'applicazione dei requisiti giuridici dell'UE relativi all'IoT sopra illustrati.

Le raccomandazioni di cui sotto si limitano a fornire orientamenti che si aggiungono ai documenti adottati in precedenza dal Gruppo di lavoro.

A tale riguardo, il Gruppo intende richiamare l'attenzione in modo particolare sulle proprie precedenti raccomandazioni sulle applicazioni per dispositivi intelligenti[31]. Dato che gli *smartphone* fanno parte dell'ambiente dell'IoT e che i due ecosistemi coinvolgono una serie comparabile di portatori di interessi, queste raccomandazioni riguardano direttamente l'IoT. In particolare, gli sviluppatori di applicazioni e i fabbricanti di dispositivi devono fornire agli utenti finali un livello adeguato di informazioni e offrire meccanismi di *opt-out* e/o consenso granulare, se del caso. Inoltre, qualora il consenso non sia stato ottenuto, il responsabile del trattamento deve rendere anonimi i dati prima di utilizzarli per una finalità diversa o di condividerli con altre parti.

[28] Parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti adottato il 16 maggio 2011 (WP185) - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_it.pdf

[29] A tale riguardo, l'uso di un approccio basato sulle cosiddette *sticky policies* può favorire la conformità al quadro giuridico in materia di protezione dei dati in quanto prevede di integrare le informazioni sulle condizioni e i limiti d'uso dei dati nei dati stessi. Pertanto, tali politiche potrebbero definire il contesto di utilizzo dei dati, le finalità, le politiche riguardanti l'accesso di terzi e una lista di utenti fidati.

[30] Un modo che consenta di offrire all'interessato il controllo reale sul trattamento dei dati quando interagiscono con i sensori offrendogli anche la possibilità di esprimere preferenze, di ottenere o revocare il consenso e di limitare le finalità, potrebbe essere basato sull'uso di *privacy proxies*. Con l'aiuto di un dispositivo le richieste di dati vengono confrontate con politiche predefinite che regolano l'accesso ai dati sotto il controllo dell'interessato. Tramite la definizione di coppie formate da un sensore e una politica, le richieste di terzi di raccogliere o accedere ai dati dei sensori verrebbero autorizzate, limitate o semplicemente respinte.

[31] Parere 02/2013 sulle applicazioni per dispositivi intelligenti (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_it.pdf

6.1 **Raccomandazioni generali per tutti i portatori di interessi**

- Dovrebbero essere effettuate valutazioni dell'impatto sulla vita privata (*Privacy Impact Assessment* - PIA) prima del lancio di qualsiasi nuova applicazione riguardante l'IoT. La metodologia da seguire per tali PIA può basarsi sul quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati che il Gruppo di lavoro ha adottato il 12 gennaio 2011 per le applicazioni RFID[32]. Ove opportuno/fattibile, i portatori di interessi dovrebbero esaminare la possibilità di mettere le PIA rilevanti a disposizione del pubblico. Potrebbero essere sviluppati specifici quadri per la realizzazione di PIA per particolari ecosistemi IoT (ad esempio le città intelligenti).

- Molti portatori di interessi dell'IoT hanno bisogno solo di dati aggregati e non hanno alcun bisogno dei dati grezzi raccolti dai dispositivi IoT. I portatori di interessi devono cancellare i dati grezzi non appena hanno estratto i dati necessari per il loro trattamento. In linea di principio, la cancellazione deve avere luogo nel punto di raccolta dei dati grezzi più vicino (ad esempio sullo stesso dispositivo, dopo il trattamento).

- Ogni portatore di interessi nel settore dell'IoT dovrebbe applicare i principi della "*privacy by design*" (tutela della vita privata fin dalla progettazione) e della "*privacy by default*" (impostazioni automatiche di tutela della vita privata).

- La responsabilizzazione degli utenti è fondamentale nel contesto dell'IoT. Gli interessati e gli utenti devono essere in grado di esercitare i propri diritti e devono quindi avere il "controllo" dei dati in qualsiasi momento, secondo il principio di autodeterminazione informativa.

- Le modalità di comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. In particolare, le politiche relative all'informazione e al consenso si devono concentrare su informazioni comprensibili all'utente e non devono essere limitate a una politica generale sulla privacy pubblicata sul sito web dei responsabili del trattamento.

- I dispositivi e le applicazioni dovrebbero inoltre essere progettate in modo tale da informare gli interessati, utenti e non utenti, ad esempio attraverso l'interfaccia fisica del dispositivo o trasmettendo un segnale su un canale senza fili.

6.2 **Sistemi operativi e fabbricanti di dispositivi**

- I fabbricanti di dispositivi devono informare gli utenti circa la tipologia dei dati che sono raccolti dai sensori e successivamente trattati, la tipologia dei dati che essi ricevono e il modo in cui verranno trattati e combinati.

- I fabbricanti di dispositivi dovrebbero essere in grado di comunicare immediatamente a tutti gli altri portatori di interessi coinvolti quando un interessato revoca il proprio consenso o si oppone al trattamento dei dati.

- I fabbricanti di dispositivi devono fornire un consenso granulare nel concedere l'accesso alle applicazioni. La granularità non deve riguardare solo la categoria dei dati raccolti, ma anche il momento e la frequenza con la quale i dati vengono rilevati. Analogamente alla funzione "non

[32] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

disturbare" degli *smartphone*, i dispositivi per l'IoT dovrebbero prevedere un'opzione "non raccogliere" ("*do not collect*") per programmare o disattivare velocemente i sensori.

- Per impedire la localizzazione, i fabbricanti di dispositivi dovrebbero limitare il *fingerprinting* del dispositivo, disattivando le interfacce senza fili quando non vengono utilizzate, o dovrebbero utilizzare identificativi casuali (quali indirizzi MAC casuali per la ricerca di reti WiFi) onde evitare che un identificativo costante venga utilizzato per la localizzazione.

- Per mettere in pratica la trasparenza e il controllo dell'utente, i fabbricanti di dispositivi dovrebbero fornire strumenti per leggere, revisionare e modificare i dati sul posto, prima che vengano trasmessi all'eventuale responsabile del trattamento. Inoltre, i dati personali trattati dal dispositivo dovrebbero essere archiviati in un formato che consenta la portabilità dei dati.

- Gli utenti hanno il diritto di accesso ai propri dati personali. Essi dovrebbero disporre di strumenti che consentano loro di esportare facilmente i propri dati in un formato strutturato e di uso comune. Pertanto, i fabbricanti di dispositivi dovrebbero fornire un'interfaccia di facile impiego per gli utenti che desiderino ottenere i dati aggregati e/o i dati grezzi che essi ancora conservano.

- I fabbricanti di dispositivi dovrebbero fornire strumenti semplici per informare gli utenti e per aggiornare i dispositivi quando vengono scoperte vulnerabilità. Quando un dispositivo diventa obsoleto e non viene più aggiornato, il fabbricante del dispositivo deve informare l'utente e garantire che sia a conoscenza del fatto che il dispositivo non verrà più aggiornato. Devono essere informati anche tutti i portatori di interessi che possono subire gli effetti della vulnerabilità.

- I fabbricanti di dispositivi dovrebbero seguire una procedura di sicurezza sin dalla progettazione e dedicare alcuni componenti alle principali primitive crittografiche.

- I fabbricanti di dispositivi dovrebbero limitare quanto più possibile il volume di dati in uscita dai dispositivi, trasformando i dati grezzi in dati aggregati direttamente sul dispositivo. I dati aggregati dovrebbero essere disponibili in un formato standardizzato.

- A differenza degli *smartphone*, i dispositivi per l'IoT possono essere condivisi da vari interessati o addirittura dati in affitto (ad esempio le case intelligenti). Dovrebbe essere disponibile un'impostazione per distinguere le diverse persone che utilizzano lo stesso dispositivo, in modo tale che non possano venire a conoscenza delle rispettive attività.

- I fabbricanti di dispositivi dovrebbero collaborare con organismi di normazione e piattaforme di dati per supportare un protocollo comune per esprimere preferenze per quanto riguarda la raccolta e il trattamento dei dati da parte dei responsabili del trattamento, in particolare quando tali dati vengono raccolti da dispositivi discreti.

- I fabbricanti di dispositivi dovrebbero consentire a organismi locali di controllo e trattamento (i cosiddetti *personal privacy proxies*) di permettere agli utenti di avere un quadro chiaro dei dati raccolti dai propri dispositivi e facilitare l'archiviazione e il trattamento locale senza dover trasmettere i dati al fabbricante del dispositivo.

6.3 **Sviluppatori di applicazioni**

- È opportuno progettare notifiche o avvisi per ricordare frequentemente agli utenti che i sensori stanno raccogliendo dati. Qualora lo sviluppatore dell'applicazione non abbia accesso diretto al

dispositivo, l'applicazione dovrebbe inviare periodicamente una notifica all'utente per fargli sapere che sta ancora archiviando dati.

- Le applicazioni dovrebbero facilitare l'esercizio dei diritti di accesso, rettifica e cancellazione delle informazioni personali dell'interessato raccolte da dispositivi IoT.

- Gli sviluppatori di applicazioni dovrebbero fornire strumenti che permettano agli interessati di esportare dati grezzi e/o aggregati in un formato standardizzato e utilizzabile.

- Gli sviluppatori dovrebbero prestare particolare attenzione alle tipologie di dati in corso di trattamento e alla possibilità di dedurre da essi dati personali sensibili.

- Gli sviluppatori di applicazioni dovrebbero rispettare il principio della riduzione al minimo dei dati. Quando lo scopo può essere raggiunto utilizzando dati aggregati, gli sviluppatori non dovrebbero accedere ai dati grezzi. Più in generale, gli sviluppatori dovrebbero seguire un approccio della "*privacy by design*" e ridurre la quantità di dati raccolti a quella richiesta per fornire il servizio.

6.4 **Piattaforme sociali**

- Le impostazioni di default delle applicazioni sociali basate su dispositivi IoT dovrebbero chiedere agli utenti di esaminare e modificare le informazioni generate dal proprio dispositivo, e prendere decisioni in merito, prima della pubblicazione sulle piattaforme sociali.

- Le informazioni pubblicate sulle piattaforme sociali dai dispositivi IoT, per default, non dovrebbero diventare pubbliche o venire indicizzate dai motori di ricerca.

6.5 **Proprietari di dispositivi IoT e destinatari aggiuntivi**

- Il consenso all'utilizzo di un dispositivo connesso e al trattamento dei dati che ne consegue deve essere informato e libero. Gli utenti non devono essere penalizzati economicamente o avere un accesso limitato alle capacità dei propri dispositivi qualora decidano di non utilizzare il dispositivo o un servizio specifico.

- L'interessato i cui dati vengono trattati nel contesto di un rapporto contrattuale con l'utente di un dispositivo connesso (hotel, compagnie di assicurazione sanitaria o noleggiatori di auto) dovrebbe essere in grado di gestire il dispositivo. Indipendentemente dall'esistenza di eventuali rapporti contrattuali, qualsiasi interessato che non sia un utente deve poter esercitare i propri diritti di accesso e opposizione.

- Gli utenti di dispositivi IoT dovrebbero informare gli altri interessati (non utenti) i cui dati vengono raccolti, della presenza di dispositivi IoT e della tipologia dei dati raccolti. Dovrebbero anche rispettare l'eventuale scelta dell'interessato di non far raccogliere i propri dati dal dispositivo.

6.6 **Organismi di normazione e piattaforme di dati**

- Gli organismi di normazione e le piattaforme di dati dovrebbero promuovere formati di dati portatili e interoperabili, nonché chiari e intuitivi, al fine di agevolare i trasferimenti di dati tra parti diverse e di aiutare gli interessati a comprendere quali dei loro dati vengono effettivamente raccolti dai dispositivi IoT.

- Gli organismi di normazione e le piattaforme di dati non si dovrebbero concentrare unicamente sul formato per i dati grezzi, ma anche sulla comparsa di formati per i dati aggregati.

- Gli organismi di normazione e le piattaforme di dati dovrebbero promuovere formati di dati che contengano il minor numero possibile di elementi identificativi forti al fine di facilitare la corretta anonimizzazione dei dati dell'IoT.

- Gli organismi di normazione dovrebbero sviluppare norme certificate come punto di riferimento per le garanzie in materia di sicurezza e di tutela della vita privata degli interessati.

- Gli organismi di normazione dovrebbero sviluppare protocolli leggeri di cifratura e di comunicazione adattati alle specificità dell'IoT, che garantiscano riservatezza, integrità, autenticazione e controllo dell'accesso.