GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 3898704]

[v. anche Comunicato stampa]

[v. anche Avviso]

Avvio della consultazione pubblica su Internet delle cose (Internet of Things) - Deliberazione del 26 marzo 2015

Registro dei provvedimenti
n. 179 del 26 marzo 2015

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTA la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

VISTA la direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);

VISTE le indicazioni fornite dal Gruppo di lavoro per la tutela dei dati personali ex art. 29 nella *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, adottata il 16 settembre 2014, disponibile al *link http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf* ;

VISTE le indicazioni contenute nella *Mauritius Declaration on the Internet of Things*, adottata il 14 ottobre 2014 nel corso della 36ma Conferenza internazionale delle Autorità di protezione dei dati personali tenutasi a Mauritius, disponibile al *link http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf* ;

VISTA la delibera n. 708/13/CONS dell'Autorità per le garanzie nelle comunicazioni, recante "*Indagine conoscitiva concernente i servizi di comunicazione machine to machine (M2M)*" del 12 dicembre 2013;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento n. 1/2000;

RELATORE il dott. Antonello Soro

PREMESSO

L'*Internet of Things* (IoT) fa riferimento ad infrastrutture nelle quali innumerevoli sensori sono progettati per registrare, processare, immagazzinare dati localmente o interagendo tra loro sia nel medio raggio, mediante l'utilizzo di tecnologie a radio frequenza (ad es. RFID, *bluetooth* etc.), sia tramite una rete di comunicazione elettronica.

I dispositivi interessati non sono soltanto i tradizionali computer o *smartphone*, ma anche quelli integrati in oggetti di uso quotidiano ("*things*"), come dispositivi indossabili (cd. *wearable*), di automazione domestica (cd. domotica) e di georeferenziazione e navigazione assistita; ciò comporta la raccolta e la gestione di dati relativi a comportamenti, abitudini, preferenze e stato di salute degli utenti spesso inconsapevoli, con l'effetto di consentirne l'identificazione, diretta o indiretta, mediante la creazione di profili anche dettagliati.

Se ne induce, quindi, l'importanza di fornire agli utenti un'informazione trasparente, con particolare riguardo ai dati raccolti, agli scopi per i quali ciò avviene e alla durata della conservazione dei dati stessi, anche ai fini dell'eventuale prestazione di un valido consenso al trattamento dei dati.

In tale quadro, una attenzione particolare deve essere allora riservata ai rischi relativi alla qualità dei dati che potrebbero derivare dal loro grado di affidabilità, specie considerati gli usi in campo medico-sanitario, nonché ai rischi che vengano realizzati, quali un invasivo monitoraggio dei comportamenti degli utenti, anche a loro insaputa, ovvero un condizionamento degli individui tale da limitarne anche significativamente la libertà e la capacità di autodeterminazione.

Al pari occorre considerare gli ulteriori rischi relativi alla sicurezza indotti, in particolare, da operazioni di comunicazione a terzi, dall'utilizzo improprio e dalla perdita delle informazioni oggetto di trattamento, soprattutto in ragione del novero dei soggetti coinvolti, dei volumi e dei tipi di dati trattati, nonché dell'estensivo utilizzo di interfacce radio, strutturalmente di particolare vulnerabilità.

Le misure di sicurezza da adottare devono allora essere in grado di proteggere i dati trattati dai rischi di interferenze ingiustificate e/o manomissioni e, prima ancora, di minimizzare i rischi, laddove possibile.

In tale prospettiva ed allo scopo, altresì, di valutare i possibili rischi del trattamento nel corso dell'intero ciclo vitale del prodotto o della fornitura del servizio, l'Autorità ritiene auspicabile che fin dalla fase della progettazione dei servizi e degli oggetti destinati ad interagire nell'*Internet of things* gli operatori coinvolti ricerchino soluzioni improntate ad una concreta applicazione dei paradigmi e delle strategie basate sul cd. approccio di *privacy and data protection by design*, come descritto ad esempio nel *report* pubblicato al riguardo da Enisa – European Agency for Network and Information Security (di seguito Enisa), del 12 gennaio 2015, disponibile al link https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.

È al pari opportuno acquisire elementi relativi alle possibili tecniche di cifratura delle informazioni impiegate in relazione alle operazioni di trasmissione dei dati tra diversi dispositivi o piattaforme, anche alla luce delle risultanze dello studio realizzato al riguardo da Enisa, del 21 novembre 2014, disponibile al link https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols/.

Si ravvisa inoltre la necessità di indagare le modalità di trattamento dei dati personali con specifico riguardo all'eventuale ricorso a tecniche di anonimizzazione anche alla stregua dei criteri fissati nell'Opinion del Gruppo di lavoro per la tutela dei dati personali ex art. 29 n. 05/2014 adottata il 10 aprile 2014 e disponibile al link http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf.

Per una compiuta valutazione del fenomeno, per la corretta allocazione delle responsabilità tra i soggetti a diverso titolo coinvolti nelle operazioni di trattamento dei dati, nonché per l'individuazione della normativa applicabile, appare necessario approfondire anche aspetti legati ai modelli di *business* utilizzati, come pure esaminare i temi connessi all'interoperabilità dei servizi e alla portabilità delle informazioni, con particolare riferimento agli aspetti di standardizzazione, anche al fine di valutare la possibilità per gli utenti di esercitare un reale controllo sui propri dati e sulle modalità di fruizione dei servizi *IoT*.

Allo scopo di favorire un generale incremento del livello di fiducia (*trust*) tra interessati e titolari potrebbe rivelarsi opportuna l'adozione di strumenti di certificazione anche eventualmente a livello sovranazionale nonché di protocolli di autenticazione ovvero di meccanismi di mutuo riconoscimento diretto ovvero intermediato.

Sullo specifico tema, l'Autorità intende favorire la più ampia partecipazione possibile dei soggetti interessati, sia in adempimento di una logica partecipativa, sia con l'obiettivo di acquisire osservazioni e commenti sul fenomeno oggetto di interesse e sulle relative modalità attuative, nonché eventuali proposte operative.

Si ravvisa, pertanto, l'opportunità di avviare una consultazione pubblica volta ad acquisire elementi conoscitivi in merito alle tematiche sopra delineate, con specifico riguardo agli aspetti implementativi dei principi enunciati nonché alle criticità riscontrabili o anche già sperimentate nel settore di riferimento.

Tutto ciò premesso, il Garante

DELIBERA

di avviare una consultazione pubblica volta ad acquisire osservazioni e proposte riguardo agli aspetti di protezione dei dati personali sopra delineati connessi alle nuove tecnologie classificabili come *Internet of Things*, con specifico riguardo ai risvolti implementativi dei principi enunciati nonché alle criticità riscontrabili o anche già sperimentate nel settore di riferimento e, in particolare:

- alle possibili attività di profilazione di utenti anche inconsapevoli;
- alla necessità di fornire un'informazione trasparente anche al fine dell'eventuale acquisizione del consenso al trattamento dei dati;
- ai rischi relativi innanzitutto alla qualità dei dati nonché a possibili monitoraggi o condizionamenti dei comportamenti degli interessati, così come a quelli connessi ad aspetti di sicurezza ed alle relative misure;
- all'applicabilità di paradigmi di *privacy and data protection by design*;
- al possibile ricorso a tecniche di cifratura e di anonimizzazione dei dati;
- ai modelli di *business* utilizzati;
- agli aspetti di standardizzazione;
- alla possibile adozione di strumenti di certificazione ovvero di autenticazione tesa al mutuo riconoscimento diretto ovvero

intermediato.

A tal fine, invita tutti i soggetti interessati – anche eventualmente attraverso le associazioni di categoria rappresentative dei settori di appartenenza quali ad esempio quelle imprenditoriali e dei consumatori ove presenti, nonché del mondo universitario e della ricerca scientifica,– a far pervenire le osservazioni, i commenti, le informazioni, le proposte e tutti gli elementi ritenuti utili. I contributi, così individuati, dovranno pervenire, entro 180 giorni dalla pubblicazione dell'avviso pubblico di avvio della consultazione sulla Gazzetta Ufficiale, all'indirizzo dell'Autorità di Piazza Monte Citorio n. 121, 00186 – Roma, ovvero all'indirizzo di posta elettronica

iot@gpdp.it

indicando nell'oggetto il tema di riferimento.

I contributi inviati dai partecipanti alla consultazione non precostituiscono alcun titolo, condizione o vincolo rispetto ad eventuali successive determinazioni del Garante.

Roma, 26 marzo 2015

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia