100% dallo Stato polacco è stato ritenuto sufficiente per considerare che tali misure fossero da considerarsi quale utilizzo delle risorse statali, posto che ai sensi di una consolidata giurisprudenza la partecipazione di maggioranza dello Stato in una società pubblica di diritto privato non è sufficiente a dimostrare che lo Stato sia in grado, attraverso l'esercizio della sua influenza dominante, di orientare le loro scelte al fine di finanziare vantaggi nei confronti di altre società.

La CdG ha quindi concluso stabilendo che una legge nazionale, con la quale sia imposto alle imprese pubbliche e private un obbligo di acquisto di una determinata quota di energia elettrica derivante dalla cogenerazione, non costituisce un aiuto di Stato in quanto non qualificabile né come intervento dello Stato né effettuato mediante risorse statali.

Avv. Giorgio Candeloro
Freshfields Bruckhaus Deringer

LEGISLAZIONE OSSERVATORIO

INTERNET OF THINGS: ASPETTI LEGALI

L'espressione Internet of Things (letteralmente "internet delle cose") è stata utilizzata per la prima volta nel 1999 da K. Ashton, ricercatore presso il Massachussets Institute of Technology, per descrivere l'interconnessione tra gli oggetti che, attraverso appositi sensori, si connettono alla rete internet, trasferendo dati (e, quindi, informazioni) attraverso un proprio indirizzo IP che ne consente l'individuazione univoca. Ogni settore della vita quotidiana è coinvolto nel suddetto processo connettivo ed il fenomeno è destinato ad amplificarsi in maniera esponenziale: si stima, infatti, che entro il 2020, nel mondo ci saranno almeno tra i 40 e i 50 miliardi di oggetti in grado di interfacciarsi attraverso la rete. In effetti molti esempi sono sotto gli occhi di tutti: si parte dalla domotica (con termostati, serrature, lampade che si comandano con un tocco sullo smart phone, elettrodomestici di ogni tipologia e dimensione, ecc.) passando per i cosiddetti werables (orologi, occhiali, ecc.) sino ad arrivare ad ogni possibile declinazione già da tempo messa in atto in ambito aziendale. Entro breve, inoltre, intere città saranno completamente cablate ed intrise di sensori di ogni genere, anche (ma non solo) per permettere la piena implementazione dei self driving vehicles: da qualche anno sono in atto le sperimentazioni sulle automobili, ma esempi già pienamente operativi e funzionati si possono rinvenire nei servizi di trasporto pubblico (treni, metropolitane, ecc.) delle città più evolute. Come è facile intuire, l'enorme quantità di dati che vengono scambiati tra gli oggetti e, quindi, necessariamente tra i titolari del trattamento dei dati, preposti alla gestione delle relative informazioni, oltre a costituire un patrimonio enorme in termini di abitudine e profilazione degli utenti, comporta, inevitabilmente, la necessità di valutare gli aspetti legali sottesi e, spesso, non sufficientemente tenuti in debita considerazione dalle aziende che forniscono prodotti e servizi smart.
Nel settembre 2016, infatti, il Global Privacy Enforcment Network (GPEN) ha rilevato la grave carenza nella tutela della privacy degli utenti di due terzi dei dispositivi oggetto del sondaggio. Non è necessario volgere lo sguardo ai colossi oltre oceano per comprendere che le suddette criticità riguardano anche le piccole e medie aziende e ciò per ovvie ragioni: la quantità di dati scambiati è ormai tale, anche nei processi più semplici, da rappresentare una risorsa incredibile in termini di informazioni commerciali, grazie all'acquisizione dei dati personali anche sensibili (o "particolari" in base alla nuova definizione contenuta del Regolamento EU 2016/679 sulla protezione dei dati, applicabile dal prossimo maggio). Molte aziende, anche indipendentemente dal fatto che ciò rappresenti o meno il proprio core business, sono oggi impegnate, più o meno consapevolmente, nel c.d. data mining, l'operazione che consiste nell'estrazione e nell'esame di grandi quantità di dati anche attraverso software sempre meno costosi ed in grado di analizzare ed interpretare le abitudini degli utenti al fine di veicolare un'offerta commerciale sempre più personalizzata (c.d. profilazione). Già nel 2014, il "Gruppo di lavoro articolo 29" (organismo europeo preposto ad assicurare che le autorità varie garanti si uniformino nell'applicazione della normativa sulla privacy) ha evidenziato le varie problematiche relative alla diffusione dell'Internet of Things, quelle riguardanti la gestione del flusso dei dati, la perdita degli stessi, la conservazione oltre i termini necessari per le finalità per cui sono raccolti e, non da ultimo, la corretta informazione agli interessati ed la possibilità di essere anonimi. In particolare, le questioni fondamentali concernono:

- l'assenza di controllo sui dati generati dai dispositivi connessi;
- l'inadeguata informativa sul consenso richiesto all'interessato in relazione ai dispositivi connessi e l'eventualità che il consenso sia stato prestato per scopi diversi da quelli che emergono attraverso l'analisi dei dati sottesi;
- la carenza di controllo sulle informazioni relative alle abitudini e le preferenze degli interessati a seguito dell'aggregazione automatica dei dati;
- l'assenza di possibilità di rimanere anonimi e, infine,
- i rischi legati alla sicurezza fisica degli interessati.

A fronte delle suddette criticità, il Gruppo di lavoro ha elaborato delle linee guida per i soggetti convolti nel processo, valide anche alla luce della nuova normativa. Affinché il trattamento sia legittimo, primaria importanza è stata riconosciuta al consenso al trattamento dei dati: deve risultare evidente la volontà espressa dell'interessato. I titolari inoltre devono rendere semplice ed immediata la revoca del suddetto consenso. In alternativa, il trattamento deve essere necessario per l'esecuzione del contratto e tale requisito è da interpretarsi in senso restrittivo: è richiesto che ci sia un collegamento diretto tra il trattamento dei dati e lo scopo del contratto. Da ultimo, gli interessi meramente economici dei titolari non sono idonei a legittimare in trattamento dei dati in assenza delle predette eventualità (consenso o trattamento necessario per l'esecuzione del contratto). Stabilita la legittimità del trattamento, i dati devono essere trattati in ottemperanza ai principi di correttezza e conformità alla normativa e ciò implica che:

- i dati possono essere raccolti solo per finalità espressamente specificate e preventivamente individuate dai titolari;
- devono essere raccolti solo i dati necessari e per una durata minima in relazione allo scopo (ciò comporta che debbano essere cancellati non appena il contratto si estingue);
- il trattamento dei dati sensibili deve avvenire solo previo consenso dell'interessato;
- i titolari devono fornire un'idonea informativa agli interessati, mantenere un livello di sicurezza adeguato per la protezione dei dati e garantire agli interessati il diritto all'accesso, alla rettifica ed alla cancellazione dei dati;
- la valutazione di impatto preventiva (DPIA) deve essere svolta prima del lancio di qualunque applicazione;
- i dati grezzi devono essere eliminati non appena i dati necessari al trattamento sono stati estratti;
- l'adeguamento alla normativa sulla privacy deve avvenire sin dalla fase di progettazione (privacy by design) e la tutela della protezione del dato deve diventare l'impostazione predefinita affinché siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default);
- gli utenti devono avere il pieno controllo dei propri dati.

I produttori di dispositivi, i programmatori e, in generale, tutti i soggetti coinvolti nel processo IOT sono inoltre tenuti, tra le altre cose, a:

- fornire agli utenti informazioni sulle tipologie dei dati raccolti, su quali dati vengono trasmessi ai sensori, e su come tali dati saranno da processati e combinati;
- disabilitare le interfacce wireless quando non utilizzate;
- fornire all'utente strumenti per selezionare i dati che verranno trasferiti al titolare;
- garantire all'utente il diritto di accesso ai dati e l'abilità a trasferirli;
- notificare agli utenti le falle di sicurezza non appena scoperte.

Oltre a tutto quanto sopra, rimarranno valide ed applicabili tutte le norme del Regolamento, incluse le elevate sanzioni ivi previste in caso di inottemperanza.

Avv. Giacomo Gori
Cocuzza & Associati, Studio Legale

COMMISSIONE EUROPEA E MERCATO UNICO DIGITALE – LA COMMISSIONE PUBBLICA UNA PROPOSTA DI REGOLAMENTO PER LA DISCIPLINA DELLA CIRCOLAZIONE DI DATI NON PERSONALI

Nell'ambito dell'ampia strategia legata alla creazione e al rafforzamento di un "mercato unico digitale" (*Digital Single Market*), a settembre la Commissione europea (la ***Commissione***) ha adottato una proposta di Regolamento per la disciplina della circolazione di dati non personali (*Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union*).

Alla base dell'iniziativa si pone la convinzione della Commissione che attraverso politiche favorevoli e la creazione di un adeguato quadro normativo il valore dell'economia europea dei dati (stimato in oltre € 285 miliardi nel 2015, i.e. poco meno del 2% del prodotto interno lordo dell'Unione europea) potrebbe crescere notevolmente nei prossimi anni (la stima è di circa € 739 miliardi entro il 2020), con un significativo impatto per le imprese, le pubbliche amministrazioni, i lavoratori ed i consumatori europei.

Per raggiungere simili risultati, ad avviso della Commissione è necessario affrontare le criticità che attualmente ostacolano un'agevole circolazione dei dati, a sua volta considerata un "…*pre-requisite for a competitive data economy within the Digital Single Market*". In particolare, i fattori di maggiore ostacolo a tale sviluppo sono individuati:

- nelle restrizioni esistenti imposte dalle normative ed autorità nazionali circa la localizzazione dei dati all'interno dello Stato;
- nell'incertezza esistente sulla legislazione applicabile alla conservazione e al trattamento *cross-border* di questi dati;