

Smart city e compliance, la raccolta dei dati personali sarà sicura?



Si parla ormai da diversi anni di **smart city**: un concetto entrato sicuramente nell'immaginario collettivo che rimanda alla possibilità di utilizzare la tecnologia per migliorare la vita degli individui, controllare fenomeni caotici come il traffico ed elevare il livello di sostenibilità ambientale. In generale, il concetto di smart city denota la possibilità di creare un ambiente urbano "intelligente" (appunto dall'inglese "città intelligente") attraverso l'uso massiccio della tecnologia, soprattutto l'AI e il cosiddetto internet of things, cioè la possibilità di connettere gli oggetti di uso quotidiano al web.

Ciò che va sicuramente riscontrato è che la smart city viene vista, in ogni contesto e sotto ogni prospettiva, come un fenomeno necessariamente e indubitabilmente positivo: uno step ulteriore nel cammino dell'*homo sapiens* che da cacciatore si è fatto agricoltore, dalle campagne si è inurbato per, poi,

infine, passare a vivere nelle città intelligenti (o aspiranti tali). In questo senso, smart city rimanda a idee come risparmio, efficienza, ottimizzazione ma anche implementazione di politiche sociali e sostegno alla povertà poiché, attraverso un uso sapiente della tecnologia, si dovrebbe poter fornire una “casa dignitosa”, con un basso investimento, a chi ne è privo (una prospettiva, *in primis*, da adottare per i paesi in via di sviluppo).

Senza disconoscere l'*upside* delle smart city, appare, tuttavia, opportuno attirare l'attenzione sul fatto che le smart city funzioneranno attraverso la raccolta e il trattamento di dati personali su larga scala.

Si pensi, ad esempio, a un apparato intelligente che gestisca il traffico stradale in una città attraverso sensori e applicazioni basate sull'AI: i dati personali degli abitanti di tale insediamento (spostamenti, orari e tragitti personali, mezzi di trasporto utilizzati, stile di guida, etc.) saranno registrati dal sistema per l'ottimizzazione del trasporto urbano.

Smart city e compliance

In tale contesto, si pongono due pressanti problemi di **compliance**: la tutela della privacy degli individui (nel caso europeo, disciplinata dal regolamento UE 2016/679, generalmente conosciuto come GDPR) e la cybersecurity (e diversi atti normativi europei hanno posto le basi per definire un perimetro di sicurezza nazionale cibernetica).

Nel dibattito pubblico, invece, si assiste raramente (per non dire mai) alla messa in correlazione del fenomeno della smart city (di cui non si vogliono sicuramente negare gli aspetti positivi) con problematiche di *compliance* come privacy o cybersecurity (per citare solamente le principali).

Il report sulle smart city

La funzione cruciale del dato personale nella fenomenologia della smart city è stata recentemente (e indirettamente) riconosciuta da un report pubblicato di una società internazionale di *market intelligence*, dal titolo "Smart cities thematic research".

Nella presentazione del report tale società dopo aver specificato che *"by 2050, the challenges facing humanity will be lost or won in cities. By then, nearly 70% of the world's population will live in cities, against 50% now"* (entro il 2050, le sfide che l'umanità si troverà a fronteggiare saranno vinte o perse nelle città. Entro quell'anno quasi il 70% della popolazione mondiale vivrà nelle città, contro il 50% di adesso), chiaramente dichiara che *"smart cities' future infrastructure will rely on the analysis of data relayed by the sensors in buildings, infrastructure, transportation, and power grids, enabling city authorities to make critical decisions in real-time. The foundation will be smart city applications and platforms, whose governance, agility, and flexibility will be what makes a smart city smart"* (l'infrastruttura futura delle smart city si baserà sull'analisi di dati trasmessi dai sensori negli edifici, nelle infrastrutture, nel sistema dei trasporti, nelle reti elettriche, consentendo alle autorità pubbliche di adottare decisioni chiave in tempo reale).

Il fondamento saranno le applicazioni e le piattaforme delle smart city, la cui amministrazione, rapidità e flessibilità costituirà quello che rende intelligente una smart city).

In definitiva, le smart city saranno essenzialmente fondate e pensate per l'uso del dato: tutto ciò implica che i sistemi di *compliance* attualmente già in essere con riferimento alla tutela e alla protezione dei dati personali dovranno necessariamente trovare un'attenta applicazione nelle smart

city per evitare che “l’uso” si trasformi nella sua degenerazione, cioè “l’abuso”.

La spinta causata dal Covid

L’attuale pandemia del Covid-19 ha spinto l’acceleratore sullo sviluppo delle smart city. In primo luogo, infatti, i fondi (sotto una forma o un’altra, dicasi MES o Recovery Fund) che l’Unione Europea metterà sul piatto dovranno essere utilizzati in misura sostanziale per incentivare l’economia green e ciò significherà, in pratica, l’implementazione di applicazioni di smart city (efficienza energetica attraverso il controllo tecnologico degli edifici, reti di trasporto ottimizzate che limitino l’emissione di CO2, etc.). Inoltre, l’introduzione massiva dello smart working genererà un deflusso dalle grandi città alle cittadine più piccole e maggiormente a misura d’uomo (ma non si tratterà di un ritorno alla campagna, sebbene nel concetto di smart city possano rientrare anche i centri piccolissimi), le quali dovranno necessariamente dotarsi d’infrastrutture all’avanguardia per attirare nuovi residenti e, anche in questo caso, si tratterà in sostanza di applicazioni “smart”.

La crescita esponenziale delle smart city cui si assisterà nel prossimo futuro, impone che nel dibattito pubblico s’inizino a prendere in considerazione le problematiche di *compliance* delle città intelligenti.

<https://www.key4biz.it/smart-city-e-compliance-la-raccolta-dei-dati-personali-sara-sicura/329165/>