diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Big data e Pubblica Amministrazione: la sorveglianza tramite i big data

Autore: Redazione
In: Diritto civile e commerciale

Nel corso della recente giornata europea sulla protezione dei dati personali, svoltasi a Roma il 30 gennaio 2016, l'attenzione è stata rivolta ancora una volta al tema dei "big data", che, come evidenziato dalla nostra Authority, sono "diventati un fattore strategico, non solo nella produzione o nella competizione dei mercati, ma anche nelle innovazioni di importanti settori pubblici".
Come noto, il settore pubblico gestisce ed elabora una enorme mole di dati. Secondo le statistiche dell'Osservatorio Netics, il patrimonio informativo della P.A. è contenuto in 3800 Ced e oltre 58 mila server fisici. Al di là della quantità, ciò che stupisce di più è la grande varietà di dati raccolti.
Proprio quest'ultimo aspetto sta alla base della data analysis, largamente utilizzata dai grandi player globali del mercato per finalità di profilazione commerciale, ed ora anche strumento per governare il territorio, mediante politiche in grado di rispondere ai bisogni concreti dei cittadini.

https://www.youtube.com/watch?v=LmoslNG24IE

Big Data e sicurezza delle nostre città
Ad esempio, i big data possono essere utilizzati per aumentare la sicurezza delle nostre città.
Si pensi alle denunce per fatti di rilevanza penale, che riportano giorno, orario e luogo dell'evento criminale. La loro conoscenza in tempo reale e su grande scala può rappresentare uno strumento di analisi della concentrazione criminale e, al tempo stesso, un idoneo strumento di misura del livello di sicurezza del territorio. In questa direzione è stato portato avanti un progetto internazionale[1] coordinato da un importante ateneo nazionale.
Oltre a questo, però, non va dimenticato che dietro ai big data c'è una grande varietà di informazioni su gusti, abitudini, comportamenti, esigenze, ricerche e necessità di persone in carne ed ossa. Un "mare" di informazioni fornite quando si naviga in internet, si utilizzi (o non si utilizzi) lo smartphone. Immagini, dati di traffico, di ubicazione rappresentano digitalmente la nostra persona. Cosa può accadere se un soggetto pubblico, come ad esempio un Governo, raccoglie tutte queste informazioni in enormi banche dati e le rielabora?
Analisi algoritmi Big Data
Il sociologo belga-canadese Derrick de Kerckhove, nel valutare l'utilizzo di algoritmi fondati sull'analisi dei big data per finalità di sorveglianza, ha presentato a novembre 2016[2] un'analisi sul fenomeno "Singapore".
«Singapore – afferma il sociologo – si pone come Stato precursore del controllo urbano attraverso la sorveglianza fondata su Big Data e smartphone». Un modello di vita basato sulla tecno-etica: «I cittadini di

Diritto & Diritti ISSN 1127-8579

Singapore, come la maggior parte di noi, trascorrono molta della loro vita attiva di fronte a uno schermo, lasciano tracce: sono geolocalizzati, si sa cosa scrivono e cosa dicono. Le istituzioni di Singapore hanno deciso senza alcuna remora di fare pieno uso di tali informazioni, al fine di garantire ordine sociale e comportamenti corretti. Nessuno sporca la città, nessuno trasgredisce la legge . . . l'imposizione di una trasparenza completa permette di sapere il più possibile su tutto e tutti». Il modello "Singapore" rappresenta l'inizio della fine della privacy, intesa come diritto alla riservatezza in senso stretto.
A chi pensa che i big data opportunamente anonimizzati possano rappresentare il giusto antidoto alla violazione della privacy, mi piace citare un fatto di qualche anno fa, in quanto come diceva un grande filosofo: le parole insegnano, gli esempi trascinano, ma solo i fatti danno credibilità.
Nell'Agosto del 2006, AOL mise a disposizione di alcuni ricercatori un dataset di 20 milioni di queries (ricerche), digitate da 657.000 utenti tra il 1° marzo e il 31 maggio di quell'anno, dopo che era stato anonimizzato a seguito dell'eliminazione di ogni riferimento personale, come lo username e l'indirizzo IP, che erano stati sostituiti da un codice numerico. L'idea era che i ricercatori potessero associare le queries di una stessa persona, ma senza identificarla. Dall'analisi di queries come "uomini single sessantenni", "tè per la salute" e " giardinieri Lilburn, Ga" i ricercatori identificarono nell'utente 4417749 una vedova sessantaduenne di Lilburn, in Georgia, che, quando fu raggiunta dai giornalisti del New York Times, esclamò: "Diamine, è tutta la mia vita personale . . . non immaginavo proprio che qualcuno mi sorvegliasse"[3].
La polemica, che ne seguì, portò all'allontanamento del chief technology officer di AOL e di altri due dipendenti.
Questo case history fa comprendere che i big data, non solo sono il frutto di un progresso scientifico e tecnologico che ha saputo coniugare la potenza di elaborazione dei nuovi data center con l'accresciuta velocità delle attuali connessioni ad internet, ma rappresentano un potenziale di dati inimmaginabile.
Conclusioni:
In conclusione, per evitare le derive suindicate, è opportuno che l'utilizzo dei big data da parte dei soggetti pubblici si svolga nel pieno rispetto delle garanzie fornite dalla disciplina privacy e, in particolare, dal Regolamento UE n. 679/2016 in tema di protezione dei dati personali, già entrato in vigore, ma che si applicherà a partire dal 25 maggio 2018.
[1] Il progetto internazionale e-security è un progetto di ricerca coordinato dalla Facoltà di Giurisprudenza di Trento.
[2] Analisi presentata su Avvenire il 12 novembre 2016.
[3] M. Barbaro e T. Zeller Jr., A Face Is Exposed for AOL Searcher No. 4417749, "The New York Times", 09 agosto 2006.

Digital revolution
Inder Sidhu con T.C. Doyle, 2016, Maggioli Editore
Le innovazioni digitali stanno trasformando il nostro modo di vivere, l'istruzione, il commercio, la sanità, i trasporti (si pensi al dirompente fenomeno Uber), le città che diventano sempre più "smart".

https://www.diritto.it/big-data-e-pubblica-amministrazione-la-sorveglianza-tramite-i-big-data/

Diritto & Diritti ISSN 1127-8579