Luci ed ombre dei sistemi di digital welfare state

di Sveva Del Gatto

pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale - 4 giugno 2020

La diffusione dell'uso delle tecnologie digitali ha reso più stringente la necessità che nel trattamento dei dati personali e in qualunque altra interferenza nella vita privata delle persone siano assicurate adeguate garanzie di trasparenza e verificabilità da parte degli interessati. Quando ciò non accade, l'operato della pubblica amministrazione va censurato, come fatto dalla Corte distrettuale dell'Aia nei confronti di SyRI (system risk indication), il sistema utilizzato dal Ministero delle Politiche sociali per valutare l'attitudine a commettere frodi per l'ottenimento di sussidi pubblici di una parte più svantaggiata della popolazione.

Negli ultimi anni si è assistito ad una vasta **diffusione del *digital welfare state*** a livello globale. I sistemi di protezione e assistenza sociale sono sempre più spesso e in modo sempre più pervasivo, guidati dalla raccolta e dall'elaborazione di grosse quantità di dati e dall'uso di tecnologie digitali impiegate per prevedere, identificare, sorvegliare, rilevare ed eventualmente sanzionare. Ciò, al pari di quanto accade in altri settori che coinvolgono l'interesse pubblico, ma non solo, dà luogo ad evidenti benefici: un *welfare state* digitale può migliorare l'accesso alle prestazioni sociali, uniformare i criteri di accesso, velocizzare le pratiche e garantire efficienza ai governi.

L'uso delle nuove tecnologie genera, tuttavia, anche il rischio concreto che, attraverso le stesse, possano essere violati i diritti fondamentali della persona, rendendo di conseguenza ancor più stringente l'esigenza che siano **rispettati i principi di proporzionalità, necessarietà e trasparenza, e che siano garantite idonee garanzie procedurali, predeterminate per legge**. È su questi due pilastri che si regge il delicato equilibrio tra l'interferenza nella sfera personale degli individui e le ragioni a tutela dell'interesse pubblico, secondo quanto previsto dalla Convenzione europea dei diritti dell'uomo e dal GDPR in materia di trattamento dei dati personali.

Secondo un recente rapporto dell'Esperto Indipendente delle Nazioni Unite sulla povertà estrema e i diritti umani, Philip Alston (cfr. *Report of the Special rapporteur on extreme poverty and human rights*), tuttavia, proprio in relazione ai servizi di protezione sociale, si ravvisa una **significativa opacità nei sistemi di trattamento e utilizzo dei dati attraverso le nuove tecnologie con conseguenze in termini di violazione dei diritti degli interessati** (come il diritto alla *privacy* e al rispetto della vita privata), rischio di errori e pregiudizi nell'adozione delle politiche e delle decisioni pubbliche e scarsa responsabilità degli attori, pubblici e privati, coinvolti.

A conferma dei rischi sopra richiamati collegati ai sistemi di *digital welfare state*, è di recente intervenuta una decisione del tribunale distrettuale dell'Aia che ha dichiarato l'illegittimità di **Syri** (un **sistema di welfare digitale anti-frode**, sviluppato nel 2014 dal ministero degli Affari sociali e dell'occupazione, capace di prevedere la probabilità

di un individuo di truffare lo Stato, sulla base di dati precedentemente raccolti e analizzati per creare dei "profili di rischio") in parte accogliendo il ricorso presentato da una coalizione di associazioni locali (fra cui un Comitato di giuristi per i diritti umani dei Paesi Bassi, la fondazione *Privacy First*, un sindacato e un'associazione di consumatori. Sui fatti all'origine della causa e sul funzionamento di Syri, si rinvia a M. Mazzarella, Il *digital welfare state* e l'algoritmo *Syri*: una nuova sfida per la *privacy*).

Secondo i giudici olandesi, **l'interferenza nella sfera privata degli individui e il trattamento di dati personali da parte dell'amministrazione attarverso SyRi è giustificabile ai sensi dell'art. 8 CEDU.** Come osservato "le nuove tecnologie – comprese le opzioni digitali per collegare i file e analizzare i dati con l'aiuto di algoritmi – offrono maggiori possibilità al governo di scambiare dati tra le sue autorità nel contesto del loro dovere legale di prevenire e combattere le frodi". **Le norme che regolano SyRI, in particolare, appaiono funzionali a garantire "l'interesse al benessere economico dello Stato" e hanno pertanto uno "scopo legittimo",** rappresentato dall'adeguata verifica per quanto riguarda l'accuratezza e la completezza dei dati in base ai quali ai cittadini vengono assegnati diritti.

La Corte ha, tuttavia, **censurato SyRi in quanto opaco e privo delle garanzie necessarie a tutela dei soggetti i cui dati sono raccolti e trattati.** Il funzionamento di Syri è a tal punto "segreto" da impedire al tribunale anche un suo corretto inquadramento quale "sistema automatizzato di decisione" come chiesto dai ricorrenti e contestato, invece, dalla Stato. Sebbene scarse, le informazioni disponibili sono state ritenute dai giudici sufficienti a dimostrare l'uso, attraverso Syri, "di analisi predittive, *deep learning* e *data mining*". Ne consegue, secondo il ragionamento del tribunale, **che "la portata e la gravità dell'interferenza con la vita privata degli interessati da parte della legislazione SyRI è tale da richiedere rigore nella previsione di garanzie procedurali e di trasparenza**".

Rigore che al contrario, non è stato garantito. **Il modello di rischio, gli indicatori e i dati che sono stati elaborati concretamente non sono, infatti, pubblici né vengono resi noti agli interessati.** E ancora, la legislazione SyRI non prevede l'obbligo di informare le persone che i loro dati sono stati elaborati in SyRI, né esiste un obbligo legale di informare le persone interessate individualmente, che è stata presentata una segnalazione di rischio. Per queste ragioni, conclude la Corte, "*the application of SyRI, **does not strike the 'fair balance'** required for the conclusion that there is a justified interference within the meaning of Article 8 paragraph 2 ECHR*".

L'opacità del sistema SyRi, riscontrata dalla Corte, genera **tre effetti negativi** tra loro connessi e solo in parte rilevati dai giudici.

Il primo attiene **all'impossibilità per i soggetti interessati di verificare come viene generato l'albero decisionale** con inevitabili riflessi sui diritti di partecipazione, a

monte, (il cui esercizio può essere utile alla stessa amministrazione per evitare errori), e sulla tutela giurisdizionale a valle.

Il secondo riguarda **l'*accountability* del decisore pubblico** che utilizza i dati. L'opacità del modello si riverbera inevitabilmente in una sostanziale mancanza di responsabilità.

Il terzo, infine, è riferibile **al coinvolgimento dei privati nell'elaborazione degli algoritmi utilizzati dall'amministrazione.** La mancanza di trasparenza impedisce di cogliere eventuali conflitti tra interesse pubblico e interesse privato degli sviluppatori.

È evidente come tutto ciò mini significativamente l'obiettivo, più volte affermato a livello sopranazionale (cfr. considerando n. 7, GDPR e Libro bianco sull'intelligenza artificiale sui cui si rinvia a S. Del Gatto, Una regolazione europea dell'AI come veicolo di eccellenza e affidabilità. Gli obiettivi del Libro bianco della Commissione europea sull'intelligenza artificiale) di creare un **"clima di fiducia"** nei confronti delle nuove tecnologie, al fine di favorire lo sviluppo dell'economia digitale in tutto il mercato interno.