Un dipendente infedele o uno Stato opaco?

Il problema degli accessi abusivi alla banca dati per segnalazioni di operazioni sospette sembra essere responsabilità del dipendente infedele e dei suoi ipotetici mandanti. Ma per ogni cittadino è impossibile persino sapere quali siano le banche dati a disposizione dello Stato, le finalità e le logiche di trattamento.

Carlo Blengino

Nella sentenza della Corte Suprema USA che ha imposto stringenti garanzie giurisdizionali per l'utilizzo dei dati GPS e di localizzazione da parte della polizia giudiziaria nelle attività di prevenzione e repressione dei reati (U.S. vs. Jones 2012), la giudice Sonia Maria Sotomayor nella sua *concurring opinion* scrive: "Il caso è stato agevolmente risolto con l'applicazione letterale della norma [il IV emendamento della Costituzione americana n.d.r], ma la questione giuridica sottesa all'incontenibile potere dello Stato di monitorare i cittadini rimane irrisolta".

Non so come finirà la vicenda di questi giorni sugli accessi abusivi alla banca dati SOS (segnalazioni operazioni sospette), ma visti gli argomenti trattati e la postura assunta nel dibattito da magistrati, politici e organi di informazione, temo che il caso sarà agevolmente risolto con qualche condanna più o meno esemplare e, purtroppo, per dirla con la Sotomayor, la questione giuridica sottesa all'incontenibile potere dello Stato di monitorare i cittadini rimarrà irrisolta.

E sì che la vicenda balzata agli onori della cronaca in ragione della notorietà dei soggetti interessati è un caso perfetto: una banca dati enorme, che potenzialmente contiene informazioni sulle transazioni di milioni di cittadini, alimentata da centinaia di enti, aziende private e professionisti, e basata su criteri discutibili e incerti di mero sospetto, a cui accedono diverse

agenzie statuali con diverse competenze e che si è rivelata fisiologicamente vulnerabile e fragile.

Potrebbe esser l'occasione ideale per affrontare uno dei temi centrali del nostro tempo e per porre alcune domande essenziali per le nostre democrazie.

Quanto è penetrante e granulare la sorveglianza di massa nelle nostre democrazie occidentali? Cosa sa lo Stato, o meglio cosa sanno le molteplici agenzie statuali di noi cittadini?

Quali sono e quante sono le banche dati a disposizione delle pubbliche autorità e come vengono trattate (raccolte, elaborate e utilizzate) le informazioni che la digitalizzazione delle nostre vite inevitabilmente accumula sui loro server?

E in ultimo, ma non per importanza: ci sono dei limiti all'incontenibile potere dello Stato di monitorare i cittadini oppure la presunzione del pubblico interesse, dello Stato buono e democratico (per sempre?) che agisce (sempre?) per il bene comune, elide ogni cautela? E in fine, se i dati sono informazioni e l'informazione è potere, chi è garante della protezione delle informazioni che ci riguardano e del rispetto degli eventuali limiti, se il titolare del trattamento dei nostri dati, il responsabile, è lo Stato stesso e non le voraci società commerciali della Silicon Valley e del web?

Per tentare di rispondere parto dall'ultima domanda.

A differenza che negli Stati Uniti, qui in Europa la questione giuridica che la giudice Sotomayor lamentava irrisolta quanto meno ce la siamo posta, e da più di 30anni, sin dalla Convenzione del Consiglio d'Europa n. 108 del 1981, e alla fine abbiamo addirittura creato, primi al mondo, un nuovo diritto fondamentale, inesistente prima della rivoluzione digitale, inserito nella Carta dei Diritti Fondamentali dell'Unione Europea all'art. 8: il diritto appunto alla "protezione dei dati personali".

C'è una ragione storica significativa per cui nasce proprio in Europa quel nuovo diritto fondamentale, prossimo ma assai più ampio e complesso rispetto al consolidato diritto alla riservatezza (la privacy).

Negli anni '70 del secolo scorso, quando l'informatizzazione iniziò a rendere esponenziale la capacità di trattamento di dati e informazioni, nei paesi dell'est e nella Repubblica Democratica Tedesca c'era la STASI e la

sorveglianza di massa era strumento ordinario di governo e di controllo. Il rischio per le libertà, tutte le libertà, di tutti i cittadini del vecchio continente era già evidente: il trattamento dei nostri dati, pubblici o privati che fossero, con la sorveglianza di massa alle porte di casa, assumeva grazie alle tecnologie digitali una scala di invasività inedita.

I dati personali dovevano e devono esser "protetti", e debbono esser protetti principalmente dallo Stato, dai governi e dalle mille articolazioni in cui il potere, quel potere, si manifesta, indipendentemente dalle forme più o meno democratiche che assume.

Non era necessario inventarsi un nuovo diritto fondamentale per proteggerci dallo spam, dai cookie, dalla profilazione commerciale o dalle telefonate indesiderate delle imprese commerciali: è utile, ma per quello bastava – al netto delle difficoltà di applicazione – un regolamento ordinario, una legge, il GDPR per dirne una.

Invece, per limitare e vincolare il potere statuale, porre dei limiti e scongiurare una sorveglianza di massa ambita da tutti i Governi ma devastante per la democrazia, era necessario un nuovo diritto fondamentale in Costituzione, con regole speciali e speciali forme di controllo e verifica, perché lo Stato non può esser controllore di sé stesso.

E così nella Carta dei diritti fondamentali dell'Unione Europea all'art. 8 il comma 1 enuncia il nuovo diritto alla protezione dei dati personali, il comma 2 fissa alcuni principi minimi di base per la liceità dei trattamenti dei dati personali (lealtà, stretta finalità, consenso o riserva di legge) e infine il comma 3 demanda il controllo delle regole ad una Autorità Indipendente, indipendente appunto dai governi e dallo Stato, il Garante per la protezione dei dati personali.

Una serie di direttive e di regolamenti attuano quel diritto, in relazione alle diverse legittime finalità perseguite anche dalle autorità statali.

Dunque in Europa regole e limiti ci sono, almeno in teoria, per scongiurare una sorveglianza di massa.

Nel caso che occupa i media in questi giorni in relazione agli accessi alla banca dati SOS, limiti e regole vanno ricercate nella Direttiva LED (Law Enforcement Directive - Direttiva 2016/680) che è proprio "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati

personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali".

La direttiva è stata attuata in Italia con il decreto legislativo 51/2018 ed è sulla base di questa normativa che vanno analizzate e valutate le eventuali responsabilità per la vicenda oggi agli onori della cronaca.

Ora, non è mia intenzione annoiare con la disamina della suddetta complessa normativa, ma qualche breve considerazione va fatta, perché ciò che emerge dai media e soprattutto dalle dichiarazioni ufficiali di alcuni protagonisti di questa vicenda lascia francamente assai perplessi. Mi hanno colpito in particolare le audizioni del Procuratore di Perugia Dott. Cantone, titolare dell'indagine sugli accessi abusivi del Tenente Striano, e del Dott. Melillo, Procuratore nazionale antimafia e antiterrorismo, davanti alla Commissione parlamentare di inchiesta sulla criminalità organizzata.

Nelle dichiarazioni del Procuratore di Perugia e nella lunga e dettagliata audizione del Dott. Melillo, durata quasi 4 ore con molte domande da parte di diversi parlamentari, nessuno, né gli auditi né i politici interroganti hanno mai neppure nominato il diritto alla protezione dei dati e, fatto ancora più singolare, nessun cenno è stato fatto alle articolate disposizioni di cui al d.lgs. 51/2018 che pure, come detto, è la normativa di riferimento per valutare la (il)liceità di quei trattamenti e per determinare chi debba rispondere di una così evidente violazione del diritto fondamentale dei cittadini alla protezione dei loro dati. E strano.

Si badi, il responsabile *ex lege* di ciò che accade alle informazioni personali contenute in una banca dati è il titolare del trattamento, ovvero chi crea o acquisisce la banca dati e "utilizza" le informazioni determinandone mezzi e finalità; l'impiegato infedele o la gang criminale di turno che accede abusivamente e compromette integrità e riservatezza risponderà per la sua condotta di specifici reati, ma sono piani di responsabilità diversi e distinti.

E se la responsabilità di chi sfrutta le inevitabili vulnerabilità di un sistema informativo con accessi abusivi è affidata in via ordinaria allo Stato, ovvero alla magistratura (nel caso alla Procura di Perugia in ragione del coinvolgimento di un magistrato romano), la diversa responsabilità del titolare del trattamento per la mancata protezione dei dati personali è affidata come sappiamo alla valutazione del Garante. Per le banche dati utilizzate dalle agenzie di *law enforcement*, l'art. 37 del d.lgs. 51/2008

prevede espressamente: “Il Garante è l'autorità di controllo incaricata di vigilare sull'applicazione delle norme di cui al presente decreto al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento di dati personali”.

Stupisce dunque che nell’articolata audizione di alti dirigenti dello Stato sulla vicenda e nel dibattito che ne è seguito tale Autorità sia totalmente assente e mai sia stata evocata da alcuno.

È come se la vicenda non fosse di competenza del Garante e nulla avesse a che vedere con il diritto alla protezione dei dati. La cosa è davvero inquietante.

Si noti che l’art. 26 del d.lgs. 51/2008 prevede un obbligo di immediata notifica all’Autorità Garante di ogni violazione di dati personali da parte delle agenzie statuali titolari delle banche dati, proprio come previsto dal GDPR per i *data breach* ordinari. È una garanzia per i cittadini e siamo certi che tale obbligo sia stato adempiuto anche nel caso che ci occupa e che sia in corso un’attenta istruttoria del Garante nei confronti dei titolari delle banche dati violate. Forse però, per una volta, sarebbe bene comunicare tale rassicurante circostanza ai cittadini. Perché in difetto si ha la sensazione che nulla sia accaduto e che il tema della protezione dei dati e dunque dalla gestione della sorveglianza da parte dello Stato non sia uno dei problemi nella vicenda.

Nel corso dell’audizione del Procuratore Nazionale Antimafia sono state nominate decine di banche dati con acronimi spesso incomprensibili ed ai più sconosciuti a cui accedono a seconda dei casi i diversi reparti della polizia giudiziaria, le procure, vari nuclei investigativi speciali e le agenzie di intelligence finanziaria della Banca d’Italia.

Ovviamente quello che emerge ascoltando l’audizione è solo un piccolissimo e sconfortante squarcio sul complesso sistema informativo e di sorveglianza dello Stato. La punta di un iceberg.

Va tutto bene e nessuno dubita delle finalità di pubblico interesse di tutti quei trattamenti, ma un po’ stupisce che né nel corso dell’audizione né successivamente, nessuno dei parlamentari presenti si sia posto il problema di chi siano i titolari (rectius: i responsabili!) di tutte quelle banche dati, su quali basi giuridiche tutte quelle informazioni sono acquisite, trattate e rese accessibili e per quali finalità. Come siano tutelate quelle banche dati alla luce del d.lgs. 51/2018 e come siano state redatte le valutazioni di impatto o

adempiuti gli obblighi di legge. Nulla. E questo nonostante il quadro disastroso del sistema informativo e della sicurezza descritto dagli auditi.

Il problema, sui media e nel dibattito, sembra esser solo la responsabilità del dipendente infedele e dei suoi ipotetici mandanti.

Peccato che il problema dell'integrità e della riservatezza dei dati sia una responsabilità del titolare del trattamento, ovvero dello Stato, e le persone offese siano i cittadini italiani.

Nella vicenda non c'è solo un banale (si fa per dire) problema di cyber-sicurezza che compromette il meritorio lavoro delle agenzie statuali impegnate contro la criminalità, ma un problema più ampio, che espone tutti i cittadini a costante, fragile e mal gestita sorveglianza.

È evidente che c'è un problema di cyber-sicurezza, ma quel problema è una ricaduta quasi inevitabile di un diverso problema assai più complesso e inquietante e che è totalmente assente dal dibattito, ovvero l'impressionante proliferazione di banche dati in mano allo Stato e alle sue agenzie, e la pessima gestione delle stesse.

Oggi per il cittadino è impossibile anche solo sapere quali siano le banche dati a disposizione dello Stato, quali le finalità e quali siano le logiche di trattamento; non sappiamo neppure se e quando i nostri dati finiscono in quelle banche dati.

La trasparenza è oggi, tra cittadino e Stato, totalmente asimmetrica: noi trasparenti, lo Stato totalmente opaco.

La datificazione delle nostre vite conduce inesorabilmente alla sorveglianza di massa se è lo Stato il primo a non riconoscere il valore fondante del diritto alla protezione dei dati personali e non pretende per sé una rigorosa applicazione della normativa che vi dà attuazione.

Quando non si rispettano i principi di stretta finalità, di minimizzazione e limitazione della conservazione, di proporzionalità e stretta necessità oltre che di esattezza integrità e riservatezza che la legge prescrive per la liceità dei trattamenti per pubblico interesse; quando non si adotta un principio di stretta legalità quale base giuridica e, come in Italia con il famoso Decreto Capienze (d.l. 139/21), si cancella la riserva di legge e si autorizzano i trattamenti di dati personali per pubblico interesse sulla base di semplici atti amministrativi, facilitando la proliferazione delle banche dati. E infine,

quando non si riconoscono la competenza e i poteri dell'Autorità indipendente, e come accaduto col medesimo Decreto Capienze, si limitano i poteri di intervento e controllo, ecco, quando questo è il modo di procedere, si pongono basi solide per una futura sorveglianza di massa.

La vicenda che ha interessato la banca dati SOS sarà presto archiviata. Un'occasione persa per affrontare la vera questione a essa sottesa, ovvero l'incontenibile potere dello Stato di monitorare i cittadini.