

Senato della Repubblica
14[^] Commissione
AS 2481
Audizione del Presidente del Garante per la protezione dei dati personali
Prof. Pasquale Stanzone

Ringrazio, anzitutto, la Commissione per aver inteso coinvolgere il Garante in un procedimento legislativo, quale quello in esame, di significativo interesse per l'Autorità.

Il disegno di legge, in quanto tale, presenta alcune norme di particolare interesse: segnatamente gli artt. 13 e 14 recanti due deleghe legislative, rispettivamente per il recepimento della direttiva sul whistleblowing e per l'adeguamento dell'ordinamento interno al regolamento 2019/816 sul sistema ECRIS-TCN.

Per altro verso, tra gli emendamenti presentati merita attenzione il 13.01, che tra i criteri direttivi per l'esercizio della delega per l'adeguamento della normativa nazionale al regolamento (UE, Euratom) 2020/2092, prevede l'attribuzione al Garante del ruolo di istituzione nazionale indipendente per la protezione e promozione dei diritti umani, ai sensi della risoluzione dell'Assemblea generale delle Nazioni Unite n. 48/134, del 20 dicembre 1993. La rilevanza di quest'ultima previsione è tale da meritare uno spazio di riflessione più ampio, subito dopo un breve cenno alle norme del ddl d'interesse per l'Autorità.

Con riferimento all'art. 13, va anzitutto rilevato come la direttiva (UE) 2019/1937, al cui recepimento la norma delega il Governo, incida in maniera significativa sul quadro regolatorio a vigente in materia, sotto il profilo tanto soggettivo quanto oggettivo. Nelle materie coperte dalla direttiva, infatti, la tutela del segnalante non conosce differenziazione tra settore pubblico e settore privato, diversamente da quanto invece previsto dalla l. 179 del 2017. Inoltre, l'ambito di applicazione soggettivo è più esteso di quello contemplato dalla disciplina interna, che andrebbe dunque rivista sotto il profilo della categoria dei soggetti informatori tutelati.

Alquanto delicata, poi, è la "divulgazione pubblica" ammessa dalla direttiva, a certe condizioni, da parte del segnalante, non prevista dalla normativa interna. Essa, in linea più generale, reca un divieto ad ampio spettro di rivelazione dell'identità del segnalante, oltre che nel procedimento disciplinare, anche in quello penale e contabile. Nel procedimento penale, la segretezza dell'identità è tutelata nei limiti del segreto degli atti d'indagine (art. 329 cpp). Nel processo contabile, l'identità non può essere rivelata fino al termine della fase istruttoria. Nel procedimento disciplinare, l'identità del segnalante non può essere rivelata senza il suo consenso (sempre che la contestazione disciplinare si basi su elementi diversi da quelli su cui si basa la segnalazione). Se però la contestazione disciplinare si fonda (anche solo parzialmente) sulla segnalazione, l'identità può essere rivelata su consenso del segnalante, pena l'inutilizzabilità della segnalazione, ai fini del procedimento disciplinare. La riservatezza della segnalazione importa la sua sottrazione all'accesso procedimentale ex l. 241 del 1990. A questa tutela rafforzata della riservatezza del segnalante fa, tuttavia, da contrappeso la prevista inammissibilità di segnalazioni in forma anonima.

Nell'esercizio della delega per il recepimento della direttiva si dovrà tentare di realizzare un congruo bilanciamento tra l'esigenza di riservatezza della segnalazione- funzionale alla tutela del segnalante -, la necessità di accertamento degli illeciti e il diritto di difesa e al contraddittorio del segnalato. La protezione dei dati personali è, naturalmente, un fattore determinante per l'equilibrio tra queste istanze e per ciò è opportuno un coinvolgimento del Garante in fase di esercizio della delega. Va premesso, sul punto, che l'Autorità è stata costantemente e proficuamente coinvolta nei lavori per la redazione dello schema di decreto legislativo di recepimento della direttiva, nell'esercizio della delega contenuta nella precedente legge di delegazione.

La delega, come noto, non è stata tuttavia più esercitata nei termini e pertanto è stato necessario disporre una nuova, che riprende sostanzialmente quanto previsto dall'articolo 23 della legge n. 53 del 2021 (legge di delegazione europea 2019-2020).

Nell'esercizio di quest'ultima è dunque auspicabile che venga coinvolto nuovamente il Garante e che, naturalmente, siano anche in questa sede recepite le indicazioni fornite soprattutto in ordine alla complessiva coerenza delle disposizioni proposte con la normativa di protezione dati, alle garanzie di sicurezza da accordare ai flussi informativi riguardanti la segnalazione per impedirne esfiltrazioni anche solo colpose, nonché all'esigenza di determinatezza dei parametri applicativi della disciplina, a partire dalla definizione del possibile oggetto della segnalazione. E' chiaro infatti che, in assenza di una delimitazione sufficientemente netta dei comportamenti suscettibili di segnalazione, anche il relativo trattamento dei dati personali rischia di risultare, almeno in determinate ipotesi, di dubbia legittimità.

Sotto questo profilo, peraltro, un maggiore sforzo definitorio è probabilmente auspicabile già in relazione ai criteri direttivi per l'esercizio della delega. Alla lettera d), infatti, si fa riferimento al concetto di "comportamenti impropri" quale possibile oggetto della segnalazione, con una scelta probabilmente troppo ampia sotto il profilo semantico e tale, dunque, da lasciare un margine di discrezionalità eccessivo non tanto e non solo in sede di esercizio della delega, ma anche successivamente, in sede applicativa. Anche la delimitazione operata, nella norma, con riferimento a quei comportamenti impropri "che compromettono la cura imparziale dell'interesse pubblico o la regolare organizzazione e gestione dell'ente", non pare infatti del tutto sufficiente a escludere possibili dubbi interpretativi e circoscrivere sufficientemente la categoria delle violazioni da segnalare.

Particolare attenzione, nella redazione dello schema di decreto legislativo, andrà posta al tema dell'individuazione dell'Autorità competente ad acquisire le c.d. "segnalazioni esterne" aventi ad oggetto violazioni della disciplina in materia di protezione dei dati personali (ricomprese tra quelle oggetto della direttiva (UE) 2019/1937). La pur comprensibile esigenza di accentramento della gestione delle varie segnalazioni in un'unica Autorità va, infatti, coniugata con l'attribuzione al Garante (concepita dal Regolamento Ue 2016/679 e dal d.lgs. 196/03 come esclusiva) della funzione di controllo sull'applicazione della disciplina di protezione dati.

L'art. 14 delega, invece, il Governo all'adeguamento dell'ordinamento interno al regolamento 2019/816, funzionale all'istituzione di un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN). Sullo schema di regolamento, il Garante europeo per la protezione dei dati, con il parere 11/2017, aveva sottolineato- oltre all'opportunità di una generale valutazione della proporzionalità e necessità della costituzione di un sistema informativo centralizzato ad hoc- anche l'esigenza di residualità della raccolta delle impronte digitali dei cittadini di Paesi terzi, cui ricorrere solo laddove non siano ipotizzabili modalità meno invasive d'identificazione, nonché di una riflessione ulteriore sull'effettiva necessità dell'acquisizione delle immagini del volto.

Sul punto, i margini di discrezionalità del legislatore interno si riducono fortemente in ragione della natura regolamentare della fonte europea. Tuttavia, pur in questo limitato ambito sarà necessario garantire il più congruo bilanciamento tra le esigenze di giustizia e la riservatezza individuale, come pur opportunamente esige il criterio direttivo di cui alla lettera b), che andrebbe tuttavia più correttamente riformulato estendendo la clausola di salvaguardia alla normativa (anche) interna di protezione dei dati.

Naturalmente, in sede di esercizio della delega il Garante sarà ben lieto di poter offrire il proprio contributo ai fini della migliore attuazione di quel criterio direttivo.

Per quanto concerne gli emendamenti presentati, come anticipato assume particolare rilievo il **13.01**, che al comma 4 inserisce, tra i principi di delega, l'attribuzione al Garante – sulla scorta dell'AS 2109- del ruolo di istituzione nazionale indipendente per la protezione e promozione dei diritti umani, ai sensi della risoluzione dell'Assemblea generale delle Nazioni Unite n. 48/134, del 20 dicembre 1993, al fine di promuovere e tutelare i diritti fondamentali della persona riconosciuti dalla Costituzione e dalle convenzioni internazionali di cui l'Italia è parte. A tal fine, funzioni e poteri del

Garante vengono conseguentemente estesi alla materia dei diritti umani complessivamente intesa e la pianta organica subisce un contenuto incremento. Anche la disciplina dei requisiti dei componenti il Collegio viene ricalibrata sulle diverse competenze dell'Autorità.

Su tale ultimo aspetto, in relazione a criterio di delega di cui alla lettera b) del comma 4, si potrebbe forse precisare (eventualmente anche in sede di decreto) che la competenza (anche) in materia di diritti umani dev'essere presente all'interno del Collegio del Garante complessivamente inteso o, comunque, si potrebbe ipotizzare di espungere il riferimento al carattere comprovato e pluriennale di tale requisito. Potrebbe essere altrimenti difficile individuare singoli componenti che possano vantare, ad un tempo, competenze così peculiari quali quelle in materia di diritti umani e competenze specialistiche quali quelle in tema di protezione dati.

Al fine di garantire che il Collegio nella sua interezza disponga, al suo interno, di competenze adeguate alle funzioni attribuitegli, potrebbe essere infatti preferibile una valutazione complessiva e non individuale della titolarità dei requisiti o, comunque, una minore formalizzazione.

Sarebbe inoltre auspicabile chiarire che la riforma si applica a decorrere dall'elezione del nuovo Collegio del Garante, non essendo compatibile con la disciplina europea – come sancito dalla CGUE con la sentenza dell'8 aprile 2014 nella causa C-288/12- porre anticipatamente fine al mandato delle Autorità di controllo.

Ora, al di là di questi aspetti, va sottolineato come l'emendamento proponga una soluzione del tutto apprezzabile, nel metodo e nel merito. Sotto il primo profilo, infatti, si coglierebbe in tal modo l'occasione della legge di delegazione europea per ottemperare all'obbligo, di carattere internazionale, assunto dal nostro Paese sin dalla risoluzione ONU n. 48/134 del 1993 e non ancora pienamente osservato, nonostante numerose raccomandazioni abbiano sottolineato l'assenza, nel nostro Paese, di una istituzione nazionale indipendente ad hoc per i diritti umani. Come riportato nella relazione al ddl 2109, nel solo 2019, ben 41 raccomandazioni su 306 hanno interessato tale argomento.

La soluzione prefigurata dall'emendamento consentirebbe, dunque, di superare lo stallo che caratterizza, da varie legislature, il procedimento legislativo in materia, anche in questa a quanto pare arenatosi (alla Camera).

Sotto il profilo del merito, peraltro, la soluzione proposta dall'emendamento è quantomai condivisibile perché lungimirante e aderente alla realtà del diritto alla protezione dati oggi, che sempre più si caratterizza per essere non soltanto un diritto fondamentale in sé considerato, ma anche il prerequisito per l'esercizio di ogni altro diritto e libertà.

La natura ontologicamente trasversale del diritto alla protezione dati (che in quanto diritto fondamentale ai sensi dell'art. 8 Cedu non è un mero diritto di cittadinanza) e conseguentemente anche dell'attività del Garante è, infatti, il vero punto di forza di questa soluzione. Volendo, infatti, anche per evidenti ragioni di contenimento degli oneri, affidare la competenza in materia di diritti umani ad un'Autorità indipendente già istituita, è difficile immaginarne una più adeguata del Garante, per trasversalità degli ambiti d'intervento, varietà dei contesti considerati e garanzie ordinamentali di indipendenza.

Sotto il primo profilo, infatti, va infatti considerato che il Garante è l'Autorità deputata a proteggere la sfera individuale dalle indebite ingerenze di attività commerciali scorrette, di forme profilazione online invasive o del pedinamento digitale operato dalle grandi piattaforme. E' l'organo cui richiedere tutela rispetto al ricorso spregiudicato al microtargeting, volto a condizionare comportamenti e scelte, non solo di consumo (come dimostra il caso Cambridge Analytica).

Il Garante è l'Autorità investita del compito di garantire che il legittimo esercizio del diritto di (e all')informazione non degeneri in gogna mediatica o sguardo dal buco della serratura, violando così la dignità e la riservatezza individuale. E' l'Autorità dinanzi a cui ciascuno può esercitare il proprio diritto all'oblio rispetto al rischio di un uso distorsivo della rete e della sua "eterna memoria".

Oggi, al Garante i minori (se ultraquattordicenni anche autonomamente) possono rivolgersi per ottenere tutela rispetto a lesioni della loro dignità determinate dal cyberbullismo, dal revenge porn, dall'hate speech.. E' stato peraltro approvato, da questo Ramo del Parlamento, un disegno di legge

che attribuisce al Garante la competenza a decidere le istanze- presentate da minori, se ultra14enni anche in questo caso autonomamente- di rimozione di contenuti istigativi al suicidio.

Il Garante si confronta quotidianamente con il pericolo che la trasformazione digitale dell'economia degeneri in monetizzazione della libertà, con il rischio di una vera e propria rifeudalizzazione dei rapporti sociali. Ed è l'Autorità chiamata a garantire che il ricorso all'i.a. avvenga con le garanzie necessarie ad impedirne esiti discriminatori, amplificando anziché attenuando (come invece dovrebbe) le precomprensioni e i pre-giudizi da cui è più difficile liberare il pensiero umano. Il Garante si è confrontato anche con quel "caporalato digitale" cui rischia di condurre una deriva incontrollata della gig economy, anticipando la soluzione di governance proposta oggi dal draft di direttiva UE per il miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali (COM(2021) 762 def).

L'Autorità ha dovuto più volte valutare la legittimità del ricorso a tecniche investigative o anche solo a misure di tutela della pubblica sicurezza particolarmente invasive come quelle fondate sul riconoscimento facciale, fornendo indicazioni per un corretto bilanciamento tra dignità e libertà della persona ed esigenze di prevenzione dei reati. Il Garante si confronta, del resto, costantemente con le sfide che l'algocrazia pone – se priva di una guida antropocentrica – ai diritti e alle libertà fondamentali, con il rischio che proprio gli algoritmi (che ben potrebbero ridurre le iniquità e promuovere l'eguaglianza), sottendano invece nuove forme di discriminazioni.

Durante la pandemia, l'Autorità ha costantemente fornito il proprio contributo perché fosse possibile delineare il più congruo bilanciamento tra esigenze di sanità pubblica e privacy e perché anche l'uso delle nuove tecnologie in materia sanitaria (dal contact tracing digitale al green pass) promuova e non violi libertà e diritti fondamentali, scongiurando soluzioni socialmente regressive.

Da questa neppure esaustiva descrizione degli ambiti di intervento e delle funzioni del Garante emerge, dunque, come esso oggi sia un'Autorità deputata alla tutela della persona, dei suoi diritti e delle sue libertà rispetto alle vulnerabilità amplificate o indotte dalle nuove tecnologie. Nella misura in cui le libertà e i diritti si esercitano, oggi, in misura consistente (se non addirittura prevalente) online o, comunque, in forme e modi fortemente condizionati dalle nuove tecnologie, un diritto- quale quello alla protezione dati - che consente un governo antropocentrico e democraticamente sostenibile della tecnica, non può che rappresentare, infatti, il prerequisito ineludibile per la garanzia di tali diritti.

Che ne sarebbe, infatti, del diritto all'autodeterminazione in materia (non solo) sanitaria, ma anche procreativa ed esistenziale se non si potesse garantire la riservatezza su scelte essenziali quali quelle vaccinali, quelle sul fine vita o sull'aborto? E come garantire il pluralismo e le libertà in materia politico-elettorale se gli stessi contenuti offerti dalla rete sono preselezionati e modellati sul tipo di elettore attribuito al singolo dall'algoritmo? Come garantire che l'i.a. non rievochi, approfondendole anche, le precomprensioni da cui dovrebbe liberarci, in assenza di un controllo efficace sui dati con cui allenare l'algoritmo (si pensi al caso Loomis)?

Sono solo alcuni degli esempi possibili per dare conto, sia pur senza una tassonomia articolata, di come il diritto alla protezione dati rappresenti oggi la condizione necessaria per l'effettività della garanzia dei diritti fondamentali.

Ecco perché il Garante, nel tutelare il diritto alla protezione dei dati personali finisce anche, inevitabilmente, per tutelare i diritti fondamentali con un'azione che si muove ad ampio spettro, in ragione della trasversalità delle competenze affidategli. Ed ecco anche perché la soluzione proposta dall'emendamento denota una notevole lungimiranza e sensibilità nel cogliere una tendenza (quale quella della sempre più stretta interrelazione tra protezione dati e diritti fondamentali) che sarà sempre più marcata nel prossimo futuro.

Attribuire la competenza sui diritti umani al Garante vuol dire, del resto, individuare un preciso modello non soltanto di tutela ma anche di indipendenza dell'Autorità, in ragione dello specifico statuto ordinamentale che la connota. Il Garante è, infatti, assistito da garanzie di indipendenza di fonte unionale primaria (art. 8 della Carta di Nizza) e tradotte, a livello interno, nella previsione, tra le altre, dell'elezione dei componenti il Collegio da parte delle Assemblee dei due Rami del Parlamento. E' inoltre prevista la garanzia del voto limitato di cui all'articolo 153, c.1, d.lgs. 196 del

2003, volta a coinvolgere anche le minoranze nella scelta di un organo, quale il vertice di un'Autorità indipendente, che non può appunto, per sua espressa natura, rispondere neppure in fase di costituzione a logiche di tipo maggioritario.

Un'Autorità volta alla tutela di un diritto fondamentale quale quello alla protezione dei dati personali deve, infatti, essere necessariamente sottratta al 'dominio della maggioranza' e allo stesso circuito fiduciario su cui si fonda l'azione governativa. Inoltre, la stessa disciplina europea sottende un articolato sistema di garanzie perché le Autorità di controllo dispongano di poteri effettivi, da esercitarsi in piena indipendenza, oltre che in coordinamento con le altre Autorità a livello europeo (cfr., in particolare, artt. 52 Reg Ue 2016/679 e 41 direttiva 2016/680).

Anche sotto il profilo delle garanzie ordinamentali d'indipendenza, dunque, la scelta di attribuire al Garante la competenza in materia di diritti umani non può che ritenersi apprezzabile.

Vi ringrazio.