Memoria del Garante per la protezione dei dati personali - COM 2021(206) Proposta di regolamento (UE) sull’intelligenza artificiale

Memoria del Garante per la protezione dei dati personali - COM 2021(206) Proposta di regolamento (UE) sull’intelligenza artificiale

Camera dei Deputati - Commissioni IX e X riunite

(9 marzo 2022)

1. Linee generali

Ringrazio le Commissioni per quest’occasione di confronto che sottende, anzitutto, la consapevolezza della profonda interrelazione tra i.a. e protezione dati. Esse sono, infatti, materie entrambe trasversali, certamente, ma accomunate dal rappresentare la sfida, attuale e futura, lanciata dalla tecnica al diritto e alla sua possibilità di regolamentare anche ciò che appare, nella sua evoluzione incessante, più refrattario alla norma. Esamineremo, più dettagliatamente, i vari punti di contatto tra le due discipline, oltre che tra le due materie, ma è determinante partire da una constatazione essenziale: l’unica normativa al momento vigente in materia di i.a. è quella di protezione dati. Essa continuerà, peraltro, a disciplinare il fulcro dell’i.a. (il trattamento di dati personali funzionale a processi decisionali automatizzati) in linea generale e, in particolare, nel settore della polizia e della giustizia anche a seguito dell’approvazione del regolamento IA, che non si estende specificamente a quest’ambito. Del resto, il punto d’ineludibile incidenza delle due materie non è marginale: il trattamento di dati (in particolare personali) è funzionale, nel caso di specie, all’alimentazione dei sistemi d’i.a. in vista del loro apprendimento automatico. Evidente, quindi, come gli errori o le scorrettezze nel trattamento dei dati funzionali all’alimentazione della macchina (sia in fase di “allenamento” sia in fase esecutiva) si riflettano in altrettante distorsioni del processo algoritmico.

Non a caso, il draft di regolamento si fonda (anche) sull’articolo 16 del TFUE, quale base giuridica appropriata nella misura in cui la protezione dei dati personali rappresenta una delle componenti essenziali della regolamentazione proposta.

Di questa profonda interrelazione tra protezione dati e i.a. si dovrà tenere conto, sia in sede di esame della proposta (come del resto ha sottolineato il parere congiunto Edps-Edpb 5/2021), sia in sede di attuazione interna, al fine di evitare antinomie e rendere la disciplina della materia complessivamente più organica ed efficace; davvero “a prova di futuro”.

Sotto questo profilo, va anzitutto considerato che - con gli artt. 22 Gdpr e 11 direttiva 2016/680 che ne costituisce il corrispondente per il settore di polizia e giustizia penale - l’Europa, già nel 2016, ha introdotto un primo, essenziale statuto giuridico dell’i..a. In particolare, rispetto al processo decisionale automatizzato (che dell’i.a. costituisce un aspetto dirimente) la disciplina di protezione dati ha sancito il diritto alla spiegazione, alla revisione umana della decisione automatizzata e il divieto di discriminazione. Quest’ultimo è stato, peraltro, significativamente rafforzato sede di recepimento della direttiva 680, in relazione a giustizia penale e polizia, proprio

per meglio contrastare il rischio di overpolicing sulla base di caratteristiche soggettive suscettibili di esporre a discriminazione, quale in primo luogo l'etnia. I principi sanciti dalla disciplina privacy assumono un valore determinante nella regolazione dei processi algoritmici, al punto da aver già consentito, ad esempio alla giurisprudenza amministrativa, di rinvenirvi la disciplina di alcune determinate fattispecie.

Il draft di regolamento sottende scelte importanti, nel metodo e nel merito della regolazione. Da un lato, infatti, è determinante la stessa scelta in favore della regolazione, in un contesto in cui la frequente tendenza alla deregulation finisce per delegare alla legge del mercato la definizione del perimetro di diritti e libertà. E' una scelta, questa, che caratterizza tutta la politica europea del digitale, dal Gdpr sino ai Data Governance, Digital Services e Digital Markets Act, accomunati dall'opzione in favore della fonte regolamentare, che si consolida sempre più come la forma tipica della disciplina europea del digitale. Essa esprime, infatti, quell'aspirazione unitaria ("one continent, one law") sottesa a politiche su cui l'Unione investe, anzitutto, la propria identità, proprio come sta facendo attorno al rapporto tra diritto e tecnica, per imprimere all'innovazione un governo antropocentrico e, di più, personalista (il principio di supervisione umana e le misure volte a contrastare le distorsioni cognitive degli algoritmi sono, in tal senso, significative).

Nel merito, quest'esigenza è declinata in soluzioni particolarmente rilevanti, molte delle quali mutuate dalla disciplina di protezione dati, che ha rappresentato in un certo senso l'avanguardia nella regolazione del digitale. Da essa, in particolare, deriva la principale cornice strutturale: l'approccio fondato sul rischio (modulato secondo una piramide di gravità ascendente), con la correlativa valutazione d'impatto, sebbene il concetto di «rischio per i diritti fondamentali» vada uniformato a quello del Gdpr; i doveri di trasparenza nei confronti degli utenti (che dovrebbero tuttavia essere estesi a tutto il ciclo di vita dell'i.a.) ; il criterio della localizzazione dei destinatari dell'offerta produttiva quale parametro di applicazione territoriale della normativa; le certificazioni e i codici di condotta in funzione co-regolativa; la modulazione del trattamento sanzionatorio secondo il fatturato, così da esercitare maggiore deterrenza; la comunicazione obbligatoria degli "incidenti" potenzialmente pregiudizievoli; il coordinamento tra le autorità nazionali nell'ambito del Comitato europeo per l'i.a., cui partecipa anche il Garante europeo per la protezione dati, destinatario peraltro di competenze specifiche in materia rispetto alle attività svolte dagli organi e dalle istituzioni europee, sebbene con uno scostamento significativo rispetto al modello del Regolamento (UE) 2016/679, di cui si dirà.

La stessa tassonomia dei divieti e dei gradi di rischiosità delle applicazioni di i.a. rievoca i parametri previsti dalla disciplina di protezione dati. In particolare, si vieta il ricorso a sistemi d'i.a. correlati a tecniche subliminali idonee a condizionare il comportamento altrui o a sfruttare le vulnerabilità di gruppi sociali; a sistemi di social scoring fondati sul monitoraggio delle condotte individuali o all'identificazione biometrica, in tempo reale, per finalità di contrasto, salva la stretta necessità per esigenze pubblicistiche imperative specificamente enunciate, con l'autorizzazione preventiva (contestuale o successiva solo in casi di urgenza) rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro coinvolto 8art. 5, p.3).

Quest'ultimo divieto, in particolare, positivizza una prassi ormai consolidata delle Autorità di protezione dati e del Garante in particolare, che ha escluso più volte l'ammissibilità di sistemi di rilevazione biometrica a fini di pubblica sicurezza (oltre che, a fortiori, a meri fini facilitativi nel settore privato), in assenza di previsioni normative corredate di idonee garanzie. Quest'indirizzo si è, peraltro, cristallizzato in norma in sede di conversione del d.l. 139 del 2021, attraverso una moratoria generale del ricorso a sistemi di riconoscimento facciale salvo per fini di pubblica sicurezza o giustizia, ma in presenza di idonee previsioni normative e con avviso favorevole del Garante (salvo per i trattamenti svolti dall'a.g.) in sede di consultazione preventiva (art. 9, c.9, d.l. 139 del 2021, convertito, con modificazioni, dalla l. 205 del 2021).

2. Prospettive d'intervento

Le molte proposte condivisibili (e, anzi, meritorie) del draft di regolamento non escludono, peraltro, alcune soluzioni invece perfettibili (già oggetto di rilievi da parte dell'Edps e dell'Edpb), che si auspica possano essere migliorate in sede di esame dell'atto da parte del legislatore europeo. Limitandomi in questa sede ad indicarne solo i principali, anzitutto in relazione agli obblighi di conformità dei sistemi d'i.a., osservo come essi debbano riferirsi all'osservanza della normativa europea nel suo complesso (dunque anche quella di protezione dati, ivi inclusi i principi di minimizzazione e privacy by design), che dovrebbe rappresentare un requisito necessario per la stessa autorizzazione all'immissione sul mercato europeo.

Andrebbe, poi garantito un coordinamento più puntuale del sistema di certificazione proposto con quello proprio, in particolare, della disciplina di protezione dati, coinvolgendo le relative Autorità nella redazione di norme armonizzate e chiarendo se la protezione dei dati personali debba essere considerata uno dei «requisiti supplementari» nell'ambito dei codici di condotta. In linea più generale, una clausola di salvaguardia espressa e generale in favore della disciplina di protezione dati andrebbe inserita anche nell'articolato, oltre che nei considerando, ad evitare possibili antinomie tra i due plessi normativi e garantire un'applicazione coerente.

In ordine ai divieti, un approccio più garantista suggerisce di vietare qualsiasi sistema d'i.a. funzionale a punteggi sociali, in qualsiasi ambito utilizzati, o alla deduzione delle emozioni, nonché quelli volti a categorizzare le persone in insiemi, sulla base di dati biometrici, dell'etnia, del genere, dell'orientamento politico o sessuale ovvero in base ad altri motivi di discriminazione di cui all'articolo 21 della Carta di Nizza.

In ordine alla governance, va anzitutto osservato come, nonostante l'incidenza, sui diritti fondamentali, di molta parte dell'attività oggetto di regolazione (di natura trasversale e tangente vari settori), il novero dei soggetti indicati dal draft di regolamento come titolari di competenze di supervisione ("autorità di notifica" e "autorità di vigilanza del mercato" facenti capo ad una "autorità nazionale di controllo"[(1)]) non sia circoscritto alle autorità amministrative indipendenti (fermo restando quanto già osservato in relazione all'art. 5, p.3), pur esigendo che ne sia salvaguardata l'obiettività e l'imparzialità [nell'esercizio] dei relativi compiti ed attività.

Si tratta di un profilo non irrilevante, nella misura in cui determina un sostanziale affievolimento delle garanzie dei diritti fondamentali e, in particolare, del diritto alla protezione dei dati personali, la cui tutela effettiva si fonda appunto (ai sensi degli artt. 8 Cdfue e 16 Tfue) sulla necessaria supervisione di Autorità indipendenti.

Dovrebbe pertanto riconoscersi al Comitato europeo per l'intelligenza artificiale maggiore indipendenza -ridimensionando conseguentemente il ruolo della Commissione- nonché il potere di agire d'ufficio, su proprio stesso impulso. Analogamente, al fine di assicurare l'effettivo rispetto delle garanzie introdotte dal regolamento, andrebbero sanciti espressamente specifici requisiti di indipendenza in favore delle autorità di controllo, tenute peraltro ad obblighi di segnalazione alla Commissione poco compatibili con uno statuto di reale indipendenza.

Complessivamente, dunque, l'intera configurazione della governance, tanto a livello europeo quanto a livello interno, dell'i.a., dovrebbe caratterizzarsi per maggiore ed effettiva indipendenza, ma anche per il necessario coinvolgimento, almeno negli ambiti di propria competenza, delle Autorità di protezione dei dati.

E' infatti evidente che, nella misura in cui la regolazione dell'i.a. incida sulle condizioni e sulle garanzie del trattamento dei dati personali, il mancato coinvolgimento delle Autorità di protezione dati in tale contesto si risolverebbe in una sottrazione di (o, quantomeno, in una limitazione delle) loro competenze, in contrasto con il principio di cui all'art. 8, p.3, Cdfue[(2)]. Vista, allora, la stretta interrelazione tra i.a. e privacy, la competenza in materia già acquisita dalle Autorità di controllo in ordine al processo decisionale automatizzato e le caratteristiche d'indipendenza che ne connotano

lo statuto, sarebbe utile ragionare sulla soluzione proposta dall'Edps e dall'Edpb, volta a suggerire l'individuazione, nelle Autorità di protezione dati, delle autorità di controllo per l'i.a.

Come già rilevato dall'Edps e dall'Edpb nel citato parere congiunto, infatti, la "designazione delle autorità per la protezione dei dati come autorità nazionali di controllo assicurerebbe un approccio normativo più armonizzato e contribuirebbe all'adozione di un'interpretazione coerente delle disposizioni in materia di trattamento dei dati nonché a evitare contraddizioni nella loro applicazione nei diversi Stati membri". Tale soluzione garantirebbe, inoltre, una notevole semplificazione per gli utenti, che dovrebbero rivolgersi a un'unica autorità per i sistemi di i.a. che operino su dati personali, una maggiore coerenza della disciplina complessivamente considerata, nonché l'estensione dello statuto di garanzie (anche in termini di indipendenza) delle Autorità di protezione dati al settore dell'i.a..

Questa scelta verrebbe incontro anche alle preoccupazioni espresse dal Governo in ordine agli oneri, amministrativi e finanziari, connessi all'attuazione del regolamento, nonché ai tempi eccessivamente lunghi di attuazione, imputabili alla complessità del meccanismo di governance, che "sposterebbe sulle autorità nazionali una serie di responsabilità e competenze al momento difficilmente rilevabili negli Stati membri" (come si legge nella relazione trasmessa al Parlamento in attuazione della legge n. 234 del 2012).

L'individuazione nel Garante dell'autorità di controllo ai fini del presente regolamento consentirebbe, infatti, un adeguamento quantomai tempestivo agli obblighi ivi previsti, anche in assenza di ingenti stanziamenti, potendo esso avvalersi dell'esperienza già maturata rispetto a quell'aspetto così dirimente dell'i.a. che è rappresentato dal processo decisionale automatizzato.

Le Autorità di protezione dati (e il Garante italiano, naturalmente, non di meno[(3)]) possiedono, già oggi, i requisiti di competenza e, assieme, indipendenza necessari per garantire un'attuazione pienamente coerente del regolamento e un'applicazione lungimirante delle sue disposizioni. Il Garante – come del resto tutte le altre Autorità di protezione dati degli Stati membri – ben potrebbe, infatti, garantire entrambi questi obiettivi, in una prospettiva anche di semplificazione degli oneri amministrativi (unificando in un'unica Autorità gli adempimenti previsti dalle due discipline) e di coerenza complessiva dell'applicazione della normativa europea in materia.

Non posso, dunque, che suggerire alle Commissioni una riflessione (in particolare) su questo aspetto, nella consapevolezza di quanto la sinergia tra le due discipline – e, quindi, la loro applicazione da parte di un'unica Autorità- sia determinante per l'effettività dei diritti e delle garanzie che sanciscono, con significativa lungimiranza.

_____

(1) Non sono peraltro chiaramente distinguibili i reciproci ambiti di azione, in quanto, in base all'art. 59, par. 2, l'autorità nazionale di controllo agirebbe in qualità di autorità di notifica e di autorità di vigilanza del mercato, a meno che uno Stato membro non abbia motivi organizzativi e amministrativi, da motivare nei confronti della Commissione (art. 59, par. 3) per designare più di un'autorità.

(2) Anche in relazione ad un novero più ristretto e particolarmente delicato di sistemi IA incentrati sul trattamento di dati personali – quelli elencati nell'allegato III della Proposta al punto 1, lettera a), nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, e ai punti 6 e 7 (cfr. art. 63, par. 5) –, viene lasciata agli Stati membri un'ampia discrezionalità nel designare "come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma della direttiva (UE) 2016/680 o del regolamento (UE) 2016/679 o le autorità nazionali competenti che controllano le attività delle autorità di contrasto o delle

autorità competenti in materia di immigrazione o di asilo che mettono in servizio o usano tali sistemi". Anche rispetto a un contesto così significativo, dunque, non vi è garanzia del necessario coinvolgimento delle Autorità di protezione dati, essendo tale scelta rimessa al legislatore interno.

(3) Con riguardo alla valutazione di sistemi di riconoscimento facciale da parte delle Forze di polizia v. provvedimento del 26 febbraio 2020, n. 54, doc. web n. 9309458; provv. 25 marzo 2021, n. 127, doc. web n. 9575877. In ordine al prospettato utilizzo di sistemi di IA da parte dell'Agenzia delle entrate e della Guardia di finanza per individuare criteri di rischio utili a far emergere posizioni da sottoporre a controllo e incentivare l'adempimento spontaneo in ambito fiscale cfr. parere 22 dicembre 2021, n. 453, doc. web n. 9738520 sullo schema di decreto attuativo dell'art. 1, comma 683, della legge 27 dicembre 2019, n. 160. In sede di controllo, l'attenzione dell'Autorità si è altresì incentrata nel settore del food delivery e sulle tecniche algoritmiche di assegnazione degli ordini impartiti ai rider (cfr. provv. 10 giugno 2021, n. 234, doc. web n. 9675440) o sull'introduzione di banche dati cd. reputazionali (cfr. provv. 24 novembre 2016, n. 488, doc. web n. 5796783).