SORVEGLIANZA DI MASSA, ALGORITMI E INTELLIGENZA ARTIFICIALE: LO STATO DELL'ARTE AL LIVELLO NAZIONALE ED EUROPEO

Relazione al Seminario "Stati Generali del Diritto di Internet" – Università LUISS Guido Carli, Roma, 17 dicembre 2021[1]

di *Luca D'Agostino*

SOMMARIO: 1. Introduzione – 2. Intercettazione di massa e sistemi di monitoraggio. Il caso Big Brother Watch c. UK – 3. L'esperienza nazionale – 4. Dalla intercettazione di massa ai sistemi di identificazione biometrica. La Proposta di Regolamento 2021/0106 (COD) – 5. Classi di rischio, obblighi e sanzioni. Alcuni punti critici della Proposta di Regolamento.

1. Introduzione

Vorrei anzitutto ringraziare gli organizzatori degli Stati Generali e la Rivista Diritto di Internet per questa interessante iniziativa interdisciplinare. Una rivista davvero all'avanguardia, che apprezzo per l'attualità e l'immediatezza dei temi trattati; basta sfogliare la casistica e i commenti alla giurisprudenza che affrontano questioni di grande interesse e significativo impatto pratico.

Quanto all'oggetto di questa relazione, trovo estremamente coerente la collocazione del mio intervento in chiusura del panel dedicato al diritto penale, prima dell'inizio della sessione dedicata al diritto processuale penale. Tratterò infatti di un tema "cerniera", che si colloca nel crocevia tra diritto e procedura penale: quello dell'utilizzo di algoritmi e di sistemi di Intelligenza Artificiale nella sorveglianza di massa, per la prevenzione dei reati e la sicurezza pubblica.

Un tema che solleva alcuni interrogativi di fondo: la sorveglianza di massa è una realtà o una prospettiva futuribile? Esistono davvero programmi governativi di questo genere, oppure è un discorso soltanto ipotetico (cioè un esercizio scolastico o una discettazione sul rapporto tra "tecnicamente possibile" e il "giuridicamente lecito")? È legittimo il ricorso a strumenti massivi di monitoraggio degli individui da parte dello Stato? Quali sono i beni giuridici a rischio di compromissione/lesione per effetto dell'utilizzo di tali sistemi? Esiste un nucleo duro di garanzie che, *de iure condito*, non può essere sacrificato in nome della sicurezza nazionale o dell'esigenza di prevenire reati?

Tenuto conto che l'utilizzo di tali strumenti sfugge, in Italia come negli altri Paesi europei, a una disciplina organica, sarà interessante analizzare quale strada il Legislatore europeo deciderà di percorrere nella prospettiva di una prima disciplina della materia. A tal fine merita particolare attenzione la Proposta di regolamento sull'IA presentata dalla Commissione lo scorso 21 aprile.

[1] Il presente saggio è una semplice rielaborazione discorsiva della relazione tenuta dall'autore agli Stati Generali del Diritto di Internet. Essa non ha pretese di esaustività.

Ovviamente in questa sede non potrò in questa sede esaminare *funditus* ciascuno di questi aspetti, sicché mi limiterò a fornire alcune indicazioni di massima sullo stato dell'arte a livello nazionale ed europeo

2. Intercettazione di massa e sistemi di monitoraggio. Il caso Big Brother Watch c. UK

Anzitutto, per cercare di dare una risposta al primo quesito, sembra proprio che il tema della sorveglianza di massa sia una realtà dei giorni nostri, una pratica più pervasiva di quanto si possa credere. Una attività, quella di sorveglianza degli individui, riconducibile non soltanto a soggetti pubblici, ma anche privati (piattaforme, gatekeeper, provider di Internet, agenzie non governative), talvolta d'intesa con Stati o Organizzazioni internazionali.

Ne parla già da qualche anno, sia pur in chiave sociologica e filosofica, la Prof.ssa Shoshana Zuboff, autrice di un noto libello denominato "Il Capitalismo della Sorveglianza", tradotto in italiano da Luiss University Press.

Un tema così attuale che qualche mese fa (precisamente il 25 maggio 2021) è stato oggetto di una importante senza della Grande Camera della Corte di Strasburgo, che si è pronunciata nel caso noto come "Big Brother Watch c. Regno Unito", relativo ai programmi di sorveglianza massiva del governo britannico. Una sentenza a mio avviso di estrema rilevanza e di spiccato interesse; una sentenza complessa, ma ricca di spunti e di argomentazioni, che trae origine da una vicenda per certi versi preoccupante.

Le inchieste sul tema della sorveglianza di massa sono iniziate circa un decennio fa, in seguito alle dichiarazioni di Edward Snowden e alla pubblicazione in rete di numerosi documenti top secret provenienti dalla Nation Security Agency statunitense, che svelavano l'esistenza di programmi intergovernativi di controllo sui flussi di comunicazione. Nati con la giustificazione della lotta al terrorismo e la preservazione della sicurezza nazionale, i vari programmi di sorveglianza sono poi stati impiegati – almeno così sembrerebbe – per valutare la politica estera e la stabilità economica degli altri Paesi, e per raccogliere informazioni riservate di natura commerciale industriale, anche riguardanti soggetti privati.

Nella sentenza sopra richiamata la Corte EDU ha stabilito che i programmi di raccolta massiva di dati nel Regno Unito violano i diritti umani, non essendo stabilite adeguate salvaguardie per la vita privata degli individui. L'Associazione Big Brother Watch denunciava tre strumenti di sorveglianza gestiti dall'Agenzia Britannica di Intelligence e precisamente: 1) l'intercettazione di massa delle comunicazioni nell'ambito del programma TEMPORA; 2) la condivisione di informazioni in collaborazione con i programmi PRISM e Upstream gestiti dalla National Security Agency statunitense attraverso la dorsale Internet, che è composta da chilometri di cavi sottomarini in fibra ottica e reti di scambio e commutazione dei pacchetti; 3) l'ottenimento di dati sulle comunicazioni dai fornitori di servizi.

Va precisato che la normativa britannica prevede nel Regolamento sui poteri investigativi (RIPA) la possibilità per il Segretario di Stato di autorizzare "l'intercettazione di massa" di "comunicazioni esterne nel corso della loro trasmissione per mezzo di un sistema di telecomunicazione" se è ritenuta necessaria nell'interesse della sicurezza nazionale, allo scopo di prevenire o accertare gravi delitti, o per salvaguardare il benessere economico del Regno Unito.

La Corte ha disatteso l'argomentazione dei ricorrenti secondo cui il ricorso alla sorveglianza di massa si renderebbe legittima soltanto in caso di "ragionevole sospetto" in relazione alle persone per le quali i dati vengono richiesti. Nel disattendere la censura la Corte osserva che *«l'intercettazione di massa è per definizione non mirata, e richiedere un 'ragionevole sospetto' renderebbe impossibile il funzionamento di un tale regime»*.

La sentenza argomenta a fondo sul diritto al rispetto della vita privata e familiare (sancito dall'art. 8 della Convenzione EDU) e sul diritto alla libertà d'espressione ai sensi dell'art. 10 della Convenzione, ritenendo che il Governo Britannico abbia violato tali diritti attuando i programmi di sorveglianza di massa. In una società democratica la sorveglianza deve essere "accessibile alla persona interessata" e "prevedibile nei suoi effetti". Nello stabilire la prevedibilità e la necessità per ogni fase, la Corte ha indicato alcuni requisiti minimi: i) la natura dei reati che possono dar luogo a un ordine di intercettazione; ii) una previa definizione delle categorie di persone suscettibili di avere le loro comunicazioni intercettate; iii) un limite alla durata dell'intercettazione; la procedura da seguire per esaminare, utilizzare e conservare i dati ottenuti; iv) le precauzioni da prendere nella comunicazione dei dati ad altre parti; v) i casi in cui i dati intercettati possono o devono essere cancellati o distrutti.

La violazione dell'art. 8 della Convenzione è dovuta, in sostanza, alla mancanza di garanzie procedurali nel processo di selezione delle reti di interscambio da intercettare e di criteri per la selezione dei dati.

In alcuni passaggi argomentativi la Corte EDU cita la nota sentenza della Corte di Giustizia *Digital Rights Ireland* che ha affrontato il tema della conservazione dei dati di traffico telefonico e telematico (interessante esempio di c.d. dialogo tra le Corti), ricordando come l'accesso ai dati conservati dai provider dovrebbe essere limitato *«a ciò che è strettamente necessario per l'obiettivo perseguito, e, se tale obiettivo è la lotta alla criminalità, dovrebbe essere limitato alla lotta alla criminalità grave»*.

3. L'esperienza nazionale

Conviene anticipare che il tema della sorveglianza di massa non è regolato a livello nazionale. Vi sono infatti regole soltanto per alcuni aspetti che incidono *lato sensu* sulla sorveglianza di massa, quali ad es. la conservazione e l'acquisizione dei dati di traffico da parte dei provider di servizi, e i termini di *data retention* (cfr. art. 132 del Codice della Privacy, con le deroghe previste dall'art. 24 della Legge 167/2017).

Come noto, il termine ordinario è di 24 mesi per dati di traffico telefonico; 12 mesi per quelli di traffico telematico; elevati a 72 mesi (cioè sei anni) per delitti gravi e delitti di terrorismo. In sostanza, quella che si presentava come una disciplina emergenziale e dunque derogatoria, assume i caratteri dell'ordinarietà, facendo perdere, sotto questo aspetto, qualsiasi operatività all'art. 132 co. 1 e 1-*bis*.

L'assenza di una disciplina specifica sulla sorveglianza nei luoghi pubblici ha condotto il Garante Privacy ad esprimere un parere negativo sull'utilizzo del sistema Sari Real Time da parte del Ministero dell'interno (parere dello scorso 25 marzo 2021). Il sistema sottoposto all'esame dell'Autorità e non ancora attivo consente, attraverso una serie di telecamere installate in una determinata area geografica, di analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (denominata "watch-list"), che può contenere fino a 10.000 volti.; si immagina dunque un impiego del sistema non ad ampio spettro a livello nazionale, ma in realtà più circoscritte (es. individuare un sospettato in una folla o durante una partita di calcio).

Ebbene, secondo il Garante il sistema (i) è privo di una base giuridica che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza, e (ii) realizzerebbe per come è progettato una forma di sorveglianza indiscriminata e di massa.

4. Dalla intercettazione di massa ai sistemi di identificazione biometrica. La normativa sovranazionale e la Proposta di Regolamento 2021/0106 (COD)

Venendo ora al quadro normativo dell'Unione, va detto che l'attuazione di programmi di sorveglianza massiva sul modello di quello britannico non è disciplinata dal diritto derivato UE. In tempi recenti è stata presentata al Parlamento e al Consiglio la Proposta di Regolamento 2021/0106 sull'IA; nell'ultimo numero della Rivista Diritto di Internet la proposta è stata oggetto di un interessante saggio del Prof. Franco Pizzetti che consiglio di leggere.

La Proposta ha affrontato il tema dell'utilizzo di sistemi di identificazione biometrica in tempo reale inclusi tra i sistemi ritenuti "ad alto rischio", sottoposti a un regime di cautele e adempimenti più rigoroso. L'iniziativa della Commissione guarda più in generale agli algoritmi impiegati in attività di contrasto (es. per le valutazioni individuali dei rischi delle persone fisiche al fine di determinare il rischio di reato o recidiva; per rilevare lo stato emotivo di una persona fisica; per valutazione dell'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati), ma per quel che qui interessa, essa pone il divieto di utilizzare sistemi di identificazione biometrica remota "in tempo reale" (c.d. sistemi di sorveglianza) in spazi accessibili al pubblico, a meno che l'impiego sia strettamente necessario per la repressione di reati in determinate circostanze (cfr. art. 5, par. 1, lett. d).

Inoltre sul versante processuale si prevede che l'uso di tali strumenti debba avvenire in conformità alle regole del diritto nazionale e nel rispetto delle garanzie necessarie e

proporzionate tenuto conto dell'incidenza sui diritti e sulle libertà delle persone (art. 5, par. 2 e seguenti).

Si profila tuttavia la questione relativa alla discrezionalità di ciascuno Stato membro nello stabilire le condizioni di ammissibilità e le garanzie procedurali per l'impiego dei sistemi di sorveglianza, che probabilmente richiederà nel prossimo futuro un'ulteriore opera di armonizzazione anche in relazione alla disciplina sul trattamento dei dati personali nelle attività di contrasto di cui alla Direttiva 680/2016/UE.

È questo un ambito da armonizzare a livello UE, o meglio lasciarlo alla discrezionalità degli Stati membri, tenuto conto delle marcate differenze anche a livello di garanzie costituzionali?

5. Classi di rischio, obblighi e sanzioni. Alcuni punti critici della Proposta di Regolamento.

Tra gli aspetti meritevoli di attenzione, vi è poi quello relativo alle sanzioni applicabili per l'inosservanza degli obblighi posti da regolamento. La proposta, come noto, individua quattro classi di rischio (rischio minimo; rischio limitato; rischio alto e rischio inaccettabile).

Ebbene, nelle ipotesi di sistemi c.d. ad alto rischio, i fornitori sono sottoposti agli obblighi previsti dall'art. 16, tra cui quello di assicurare la conformità ai requisiti posti dal regolamento, di predisporre adeguati sistemi di valutazione e mitigazione del rischio, di registrare le attività e garantire la tracciabilità dei risultati, di fornire tutte le informazioni necessarie sul sistema e sul suo scopo affinché le autorità possano valutarne la conformità etc.

Le sanzioni amministrative sono contenute nell'art. 71 della proposta che, ricalcando il modello del GDPR, individua diversi scaglioni sanzionatori a seconda della tipologia di violazione. La sanzione più elevata riguarda le violazioni dei divieti di cui all'articolo 5 e le ipotesi di mancata conformità dei sistemi ai requisiti prescritti[2]. Limiti edittali meno elevati sono invece previsti per tutti i restanti obblighi imposti dal regolamento[3], e in particolare per l'inosservanza degli obblighi informativi nei confronti delle Autorità o degli organismi notificati[4].

La Commissione europea insiste sullo strumento della sanzione amministrativa, prevedendo una ampia forbice sanzionatoria, delimitata nel massimo ma non nel minimo, che accomuna svariate violazioni, a seconda della gravità.

---

[2] La disposizione prevede che *«Le seguenti violazioni sono soggette a sanzioni amministrative pecuniarie fino a 30 000 000 di EUR o, se l'autore del reato è una società, fino al 6 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) inosservanza del divieto delle pratiche di intelligenza artificiale di cui all'articolo 5; b) non conformità del sistema di IA ai requisiti di cui all'articolo 10».*

[3] Ai sensi del successivo par. 4, la non conformità del sistema di IA ai requisiti o agli obblighi previsti dal regolamento, diversi da quelli di cui agli articoli 5 e 10, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 di EUR o, se l'autore dell'illecito è una società, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

[4] Ai sensi del par. 5, la comunicazione di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 di EUR o, se l'autore dell'illecito è una società, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

La tecnica utilizzata desta comunque perplessità sotto diversi profili. Pur non considerando il grado di severità delle sanzioni (discutibile, e probabilmente eccessivo), la ricostruzione del precetto è resa farraginosa dal rinvio alla disciplina contenuta nei capi 2 e seguenti, effettuato in modo tutt'altro che puntuale: anziché richiamare un preciso dovere o divieto sancito dal regolamento, si effettua un rinvio puro e semplice a interi articoli, o addirittura, come del caso del par. 4 *«ai requisiti o agli obblighi previsti dal regolamento»*. Inoltre, non è chiaro se le predette sanzioni saranno direttamente applicabili oppure se gli Stati godranno di un certo margine di manovra nel modulare la portata delle sanzioni amministrative.

Andrebbe inoltre considerata attentamente la facoltà lasciata agli Stati di decidere se e in che misura applicare le sanzioni alle autorità pubbliche in caso di violazione delle disposizioni del regolamento. Invero, ai sensi dell'articolo 71, par. 7, della Proposta, *«ciascuno Stato membro può prevedere regole che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro»*.

Risulta così estremamente concreto il rischio di creare un privilegio per gli organismi pubblici e di incorrere in ingiustificate disparità di trattamento; peraltro una simile facoltà non trova riscontro in altri testi legislativi. Ad esempio l'art. 83 GDPR non opera alcuna distinzione tra violazioni commesse da privati e violazioni commesse dalla pubblica amministrazione.

Del resto, appare poco opportuno lasciare carta bianca sull'adozione di sistemi di intelligenza artificiale da parte della pubblica amministrazione, soprattutto laddove si consideri che un elevato numero di sistemi IA qualificati "ad alto rischio" prevedono il loro maggiore utilizzo in ambito pubblicistico. La mancanza di sanzioni potrebbe condurre a facili strumentalizzazioni a scapito dei diritti dei cittadini.

In tal senso si auspica che l'apparato sanzionatorio del regolamento – se mai entrerà in vigore – possa essere rivisto in omaggio al principio di certezza e conoscibilità del diritto, di proporzionalità delle sanzioni e, nei termini anzidetti, anche del principio di eguaglianza.