Osservazioni sulle Linee guida AgID per l'adozione di IA nella Pubblica Amministrazione presentate dal CSGIG

Contributi di
Avv. Mauro Alovisio
Avv. Chiara Bellosono
Dott. Gianluca Rotino
Avv. Giovanna Panucci
Avv. Salvatore Maugeri

Argomento:	**ACCESSIBILITA'**

Riferimenti Linee guida:

Pg. 25 ➔ punto 4.3 ➔ 4.3. Obiettivi e ambiti prioritari di applicazione:

> *Accessibilità: le PA adottano soluzioni di IA per rendere i servizi pubblici accessibili e conformi all'art. 53 del CAD, garantendo l'usabilità delle piattaforme digitali anche a persone con disabilità o con limitate competenze digitali. In particolare, l'IA deve essere utilizzata come strumento di assistenza per la creazione e la gestione di contenuti nativamente accessibili.*

Pg. 94 ➔ punto 9.2 ➔ a pg. 55-56:

> *Il rispetto di altre caratteristiche di qualità, rilevanti anche ai fini dei sistemi di IA, è garantito per via di obblighi derivanti da specifiche norme, come l'accessibilità (di cui alla legge n.4/2004 e alle relative Linee Guida AgID) o la riservatezza correlata alle indicazioni derivanti dal GDPR.*

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino apprezza molto il riferimento ai profili di accessibilità (punto 4.3 e punto 9.2), ma auspica che venga inserito, nell'ottica di inclusione e di valorizzazione delle linee guida, un paragrafo specificamente dedicato all'argomento con un riferimento più dettagliato agli standard tecnici specifici, come le Web Content Accessibility Guidelines (**WCAG**), per garantire un'applicazione più efficace dei principi di inclusione. Inoltre, si suggerisce di **prevedere espressamente l'obbligo dell'amministrazione di specificare** se il sistema è stato testato con **tecnologie assistive**,come screen reader - che consentono alle persone con disabilità visiva di accedere ai contenuti - **e di prevedere esplicitamente versioni alternative** (es. in formato audio o con linguaggio semplificato) che potrebbero favorire l'accessibilità per utenti con disabilità cognitive o linguistiche.

Riguardo alle Linee guida in consultazione, poiché il linguaggio utilizzato è **tecnico e giuridico**, nell'ottica inclusiva e al fine di valorizzare e divulgare il Vostro lavoro, **si consiglia di fornire spiegazioni semplificate** di concetti complessi in modo da incentivare la comprensione per un pubblico più ampio, anche in funzione della sensibilizzazione e formazione del personale delle amministrazioni interessate e in ottica legal design.

Argomento:	**Protezione dati personali (web scraping)**

Nulla è detto nelle Linee guida

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino, tenuto conto del fatto che il Garante per la protezione dei dati personali ha recentemente evidenziato i rischi associati alla pratica **web scraping**, soprattutto quando utilizzata per l'addestramento di modelli di intelligenza artificiale generativa, suggerisce di dedicare una sezione esplicita, sia nelle linee guida, sia nel modello di valutazione d'impatto, a tale il fenomeno integrando le Linee guida con i seguenti riferimenti specifici al web scraping:

- **Indicazioni specifiche sull'uso di tecnologie preventive**, per promuovere l'adozione di strumenti e tecnologie che impediscano o limitino il web scraping non autorizzato;
- **Obbligo di inserire Clausole anti-scraping nei termini di servizio** che vietino la raccolta massiva di dati da parte di terzi fornitori di sistemi di IA;ù
- **Divieto esplicito** di implementare sistemi di IA che sfruttino il web scraping per l'addestramento del modello.

Argomento:	**GOVERNANCE (imputabilità dell'atto amministrativo)**

PG. 28: Nulla è detto nelle Linee guida

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino suggerisce, al fine di accompagnare le amministrazioni nel percorso volto alla corretta individuazione delle responsabilità, di declinare precise indicazioni relative all'imputabilità dell'atto amministrativo prodotto attraverso l'uso di sistemi AI, ad esempio utilizzando le matrici di assegnazione responsabilità utilizzata nel project management RACI (Responsible, Accountable, Consulted, Informed) o RASCI (Responsible, Accountable, Supportive, Consulted, Informed), in modo da assicurare che ogni elemento del progetto venga affidato alla risorsa più adatta, facendo chiarezza su cosa ci si aspetta da ciascuna delle risorse coinvolte.

Argomento:	**GOVERNANCE (diritto d'autore)**

PG. 28: Nulla è detto nelle Linee guida

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino suggerisce, in ottica migliorativa, di prevedere uno specifico approfondimento sul diritto d'autore sia nelle linee guida, sia nel Modello di codice etico (Allegato D), sia nell'allegato B sulla valutazione del rischio con dettagli specifici sugli obblighi di trasparenza nella produzione di fotografie, articoli, video e mappe mentali e nei profili formativi, con un richiamo anche al codice deontologico per i giornalisti per le attività degli uffici stampa.

Argomento:	**Strategia (coinvolgimento del DPO)**

Pg. 22: nulla è previsto

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino riguardo al **modello di adozione dell'IA**, tenuto conto anche di quanto affermato a pg. 66 delle linee guida ove si legge: "*Su specifici aspetti di protezione dei dati personali trattati nel contesto dei modelli di IA, si è recentemente espresso altresì lo European Data Protection Board con il parere n. 28 del 17 dicembre 2024*, *utile strumento di indirizzo per la PA in merito alla natura dei modelli di IA in relazione alla definizione di dato personale, alle circostanze in cui i modelli di intelligenza artificiale potrebbero essere considerati anonimi e alla relativa dimostrazione, all'adeguatezza dell'interesse legittimo come base giuridica per il trattamento dei dati personali nel contesto dello sviluppo e dell'implementazione dei modelli di IA e al possibile impatto di un trattamento illecito di dati personali nello sviluppo di un modello di IA sulla liceità del successivo trattamento o funzionamento del modello di IA53.",* segnala che sarebbe opportuno puntualizzare ne**l documento la necessità di coinvolgere il DPO** nella fase di progettazione e valutazione dei rischi, prevedendo un **ruolo consultivo continuo** non solo limitato alla DPIA, prevedendo espressamente l'obbligo di adottare una specifica policy sull'argomento e di implementare un'adeguata reportistica che consenta di verificare l'adempimento di tali obblighi in un'ottica di accountability.

Argomento:	**Protezione dei Dati Personali (Registro dei trattamenti)**

Pg. 64 e ss. (Art. 10 Protezione dei dati personali)
Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino segnala l'opportunità di richiamare l'obbligo di censire nel Registro dei trattamenti previsto dall'art. 30 del Reg. Ue 2016 n.679 (GDPR) i trattamenti dei dati personali effettuati mediante sistemi di IA anche nell'ottica dell'accountability e del rispetto dei principi di protezione dei dati personali by design e by default.

Argomento:	**Protezione dei Dati Personali (Base giuridica)**

Pg. 66 parere EDPB n.28 del 17/12/2024

Contributo CSIG:

Le PA che adottano sistemi di IA che trattano dati personali hanno l'obbligo di rispettare il Reg. Ue 2016 n.679 ed in particolare quello di individuare preventivamente la base giuridica che rende lecito il trattamento. In proposito, a pg. 66 delle linee guida in consultazione, viene richiamato il parere n. 28 del 17/12/2024 che, nel trattare specifici aspetti di protezione dei dati personali nel contesto dei modelli AI, considera quale base giuridica adeguata il legittimo interesse del titolare.

Senonchè, il Centro Studi di Informatica Giuridica di Ivrea e Torino evidenzia che nel contesto dello sviluppo e dell'implementazione dei modelli di IA da parte delle amministrazioni pubbliche il legittimo interesse non sembra costituire una base giuridica idonea in forza di quanto prevede l'art. 6, paragrafo 1 ultimo periodo che esclude l'applicabilità del legittimo interesse al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Al riguardo, sarebbe opportuno che venisse precisato

- l’obbligo delle amministrazioni pubbliche che adottano tali sistemi di individuare preventivamente la base giuridica;
- se la base giuridica possa anche essere individuata anche in un atto amministrativo generale ai sensi dell’ Art. 2-ter (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) del codice privacy come modificato dal decreto capienze.
- qualora detta base giuridica venisse individuata nella necessità di eseguire un compito di interesse pubblico o connesso all’esercizio dei pubblici poteri di cui è investito il titolare (art. 6 lett. e, Reg. Ue 2016 n.679), sarebbe comunque necessario, come prevede il paragrafo 3 del citato articolo 6:
    - effettuare una preventiva valutazione in ordine all’effettiva necessità di tale trattamento per l’esecuzione di un compito svolto nel pubblico interesse o connesso all’esercizio di pubblici poteri di cui è investito il titolare;
    - verificare che il diritto dell’unione o degli Stati membri persegua un obiettivo di interesse pubblico che sia proporzionato all’obiettivo legittimo perseguito;
    - verificare che tale base giuridica contenga disposizioni specifiche per adeguare l’applicazione delle norme del Regolamento Ue 2016 n.679, tra cui, le condizioni generali relative alla liceità del trattamento da parte del titolare; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità; i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX; (sulla qualità della base giuridica si veda Corte di Giustizia sent. C-175/20, Valsts iemumu dienests, 24 febbraio 2022, par. 83 nonché Corte Europea dei Diritti dell’Uomo sentenza Glukhin v. Russia”, “application no. 11519/20”, 4 luglio 2023, par. 75).
- qualora, poi, il trattamento avesse ad oggetto categorie particolari di dati personali, sarebbe anche necessario verificare la sussistenza di una delle condizioni di liceità previste dal 2 paragrafo dell’art. 9 del Reg. Ue 1026 n.679.

Argomento:	**Obbligo DPIA per i sistemi che trattano dati personali e Parere del DPO**

Pg. 64 e ss. (Art. 10 Protezione dei dati personali)
pg. 17 modello di Valutazione d’impatto C4.2

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino segnala che nelle linee guida non viene richiamato l’obbligo di chiedere il parere del DPO sulla Valutazione d’impatto, mentre nel modello di Valutazione d’impatto (pg. 17 nella scheda C4.2 - PRIVACY E PROTEZIONE DEI DATI PERSONALI) si chiede solo di specificare se l'Amministrazione ha coinvolto o meno il Responsabile per la Protezione dei Dati (in aggiunta al RTD e a eventuali altre figure specifiche previste dall'Amministrazione) a garanzia dei dati trattati.

Al riguardo si suggerisce di precisare l’obbligo di effettuare una Data Protection Impact Assessment (DPIA) per i sistemi IA che trattano dati personali (art. 35.2 GDPR) precisando altresì che in tal caso è necessario che sulla valutazione d’impatto sulla protezione dei dati personali venga reso il parere del DPO come prevede l’art. 35, paragrafo 2 del Reg. UE 2016 n.679 (GDPR).

Argomento:	**Valutazione d'impatto**

Pg. 12: modello di Valutazione d'impatto: C3.3 - IMPLEMENTAZIONE TECNICA

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino riguardo all'Allegato C (valutazione d'impatto) suggerisce di prevedere l'obbligo delle amministrazioni di precisare nella valutazione d'impatto

- il tipo di sistema che si intende implementare, specificandone in maniera dettagliata le caratteristiche anche in relazione alle diverse tipologie di sistemi esistenti sul mercato;
- indicare in maniera specifica quali sono le misure che sono state adottate o che si prevede di adottare per ridurre il rischio in modo da renderlo accettabile.

Inoltre, poiché taluni atti e provvedimenti amministrativi devono per legge rimanere segreti e non sono ostensibili a terzi, si suggerisce di imporre l'obbligo di prevedere specifiche misure per garantire la riservatezza degli atti amministrativi il cui contenuto non debba essere reso ostensibile a terzi non aventi titolo per averne conoscenza.

Argomento:	**Responsabilità Giuridica e Governance dell'IA**

Pg. 21 modello di Valutazione d'impatto: C6 Accountability

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino suggerisce di fornire indicazioni chiare su:

- Ruoli e responsabilità giuridiche in caso di malfunzionamenti o decisioni errate dell'IA.
- Meccanismi di supervisione umana, che devono essere obbligatori per tutti i sistemi IA con impatto su diritti e servizi pubblici essenziali.
- Obblighi di notifica e trasparenza nei confronti dei cittadini, inclusa la possibilità di ricorso contro decisioni automatizzate.

Argomento:	**Cybersecurity e Rischi di Manipolazione dell'IA**

Pg. 20 modello di Valutazione d'impatto: C5.3 - ATTACCHI HACKING E CORRUZIONE DEL SISTEMA

Contributo CSIG:

Il Centro Studi di Informatica Giuridica di Ivrea e Torino suggerisce di rendere obbligatorie

- l'adozione di standard di sicurezza specifici, come quelli previsti dal Cybersecurity Act;
- l'adozione di procedure di risposta agli incidenti in caso di manipolazione dei dati o del modello.

Inoltre, sarebbe auspicabile prevedere un framework per l'audit della sicurezza nei sistemi IA con impatti critici.

Infine, il Centro Studi di Informatica Giuridica di Ivrea e Torino suggerisce di prevedere un aggiornamento annuale delle linee guida in consultazione in modo da considerare gli impatti dei successivi mutamenti tecnologici.