POLITICAL POSITION PAPER

versione 1.0 - Marzo 2025

TITOLO	VERSO UN'EFFICACE CONDIVISIONE DEI DATI PERSONALI NELLA PUBBLICA AMMINISTRAZIONE
KEYWORDS	*Once-only, Digital-only, Privacy*
EXECUTIVE SUMMARY	Ad oggi non esiste una norma che definisce in modo non ambiguo il principio *once-only*, il suo ambito di applicazione e le modalità di attuazione. Nonostante il principio sia riconosciuto come guida per la trasformazione digitale e sia presente in varie norme in maniera frammentata, manca un riferimento normativo che lo concretizzi eliminando le incertezze interpretative e riducendo le difficoltà applicative. Questo vuoto normativo ostacola lo scambio efficace di dati personali tra le pubbliche amministrazioni, limitando l'efficienza dei servizi pubblici e costringendo i cittadini a conferire ripetutamente i propri dati. In particolare, la complessità degli aspetti legati al trattamento di dati personali e un'applicazione cieca delle norme sulla privacy portano spesso il settore pubblico a scegliere un approccio iper-prudenziale che frena l'innovazione tecnologica. Per superare le criticità in tema di privacy, si propone di redigere una norma nazionale a supporto del principio *once-only*.
CONTESTO	Il principio *once-only* stabilisce che "al cittadino può essere richiesto una sola volta di fornire alla pubblica amministrazione un proprio dato" [8]. Sebbene tale principio sia comparso formalmente nel Piano Triennale per l'Informatica solo nel 2020, esso è riconosciuto come principio guida della trasformazione digitale del Paese da molto prima. Difatti, una prima formulazione compare già nell'art. 43 del D.P.R. 445/2000: "Le amministrazioni pubbliche e i gestori di pubblici servizi non possono richiedere atti o certificati concernenti stati, qualità personali e fatti [...] che siano attestati in documenti già in loro possesso". A livello europeo, il Regolamento UE 1724/2018 "Single digital gateway", riconosce che "L'applicazione transfrontaliera del principio «una tantum» dovrebbe comportare che i cittadini e le imprese non siano costretti a fornire gli stessi dati alle pubbliche amministrazioni più di una volta e dovrebbe essere altresì possibile utilizzare tali dati su richiesta dell'utente". L'Italia sta cercando di realizzare il principio *once-only* istituendo la Piattaforma Digitale Nazionale Dati (PDND). Si tratta del sistema che consente lo scambio immediato e sicuro di dati tra pubbliche amministrazioni. I numeri che quantificano l'attività della PDND sembrano rassicuranti ma molte amministrazioni, pur essendo registrate in piattaforma, utilizzano un numero ridotto di servizi e operano un numero ridotto di scambi di dati.

	Per attivare uno specifico scambio di dati, un'amministrazione deve compilare una richiesta di fruizione, dimostrare di avere tutti gli attributi necessari e attendere l'approvazione del soggetto che fornisce i dati. Nella quasi totalità dei casi, lo scambio riguarda dati personali. Dunque, l'amministrazione deve dimostrare che la richiesta è effettuata per una finalità legittima ed è supportata da una idonea base giuridica che consente il trattamento, così come previsto dalla normativa europea e nazionale in materia di privacy. Questo processo si ripropone per ogni amministrazione, ogni dato e ogni nuova finalità. Inoltre, ogni volta che la finalità varia, o che è necessario chiedere un dato diverso per la stessa finalità, la richiesta di fruizione va aggiornata, se necessario ampliando e integrando la base giuridica del trattamento, e in alcuni casi va sottoposta ad un nuovo processo approvativo. Sorge spontanea la domanda seguente: "la base giuridica che consente il trattamento, ovvero la norma che autorizza l'acquisizione del dato personale, non è proprio il principio *once-only*?". La risposta è "no", in quanto non esiste, ad oggi, una norma nazionale che dia forma concreta al principio *once-only* stabilendo una definizione non ambigua, un chiaro ambito di applicazione e modalità di attuazione. Il Piano Triennale per l'Informatica 2024-2026 [7] tenta di collezionare alcune norme a supporto del principio *once-only*, ma queste non esauriscono i numerosi punti che rimangono aperti in tema di privacy e che, allo stato attuale, impediscono una piena realizzazione del principio. Questo position paper intende esplorare tali criticità e proporre una possibile soluzione, partendo dal seguente assunto: un efficace scambio di dati personali all'interno della pubblica amministrazione è motore indiscutibile di innovazione ed efficienza, nonché di trasformazione del rapporto tra cittadino e Stato, in ottica di fiducia e sicurezza. La risoluzione delle problematiche in tema di privacy e la conseguente realizzazione del principio *once-only* sono tra i fattori abilitanti del principio *digital & mobile first*, che prevede che "le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e fruibili su dispositivi mobili, considerando alternative solo in via residuale e motivata, attraverso la "riorganizzazione strutturale e gestionale" dell'ente ed anche con una "costante semplificazione e reingegnerizzazione dei processi"" [7]. Infatti, la principale obiezione all'utilizzo delle tecnologie digitali nel rapporto tra cittadino e pubblica amministrazione evidenzia come, spesso, la versione digitale di un processo amministrativo sia solo la trasposizione informatica del processo cartaceo. In altre parole, *digital-first* equivale spesso a sostituire un modulo cartaceo con un modulo PDF, lasciando

	invariato ogni altro aspetto. Uno dei modi per realizzare una effettiva "reingegnerizzazione dei processi" è abilitare lo scambio e il riutilizzo di dati che nel cartaceo non sarebbe possibile. Anche per questo motivo la risoluzione delle criticità in tema di privacy è cruciale.
POSIZIONE	Un ulteriore assunto di questo position paper è il seguente: la protezione dei dati personali è un diritto fondamentale sancito dalla Carta dei diritti fondamentali dell'Unione Europea e, in quanto tale, va tutelato con la dovuta accortezza e consapevolezza. Allo stesso tempo, la tutela della privacy non può porsi in maniera ostativa all'innovazione, alla trasformazione digitale del Paese e alla garanzia dei diritti in tema di cittadinanza digitale [6]. Una presa di consapevolezza in tal senso è necessaria, sia da parte degli organi legislativi, sia da parte dell'Autorità in materia di protezione dei dati personali, sia da parte delle amministrazioni centrali che custodiscono le basi di dati di interesse nazionale. Un'applicazione cieca delle norme in materia di privacy produce inutili controsensi e innesca atteggiamenti di immobilità e deresponsabilizzazione a tutti i livelli professionali. L'esclusiva attività di controllo e sanzione premia sistematicamente un approccio iper-prudenziale, spesso a danno dell'avanzamento tecnologico. Ferma restando tale attività di controllo, la pubblica amministrazione necessita più che mai di un supporto centrale, anche normativo, nel navigare gli aspetti legati alla privacy.
PROPOSTA	Si propone di redigere una norma nazionale a supporto del principio *once-only*, che fornisca alle pubbliche amministrazioni gli strumenti necessari per superare le criticità in tema privacy esposte sopra. La norma dovrebbe affrontare i contenuti elencati di seguito: **1. Formulazione non ambigua del principio *once-only*** **2. Obblighi di conservazione, finalità e tempi di conservazione** **3. Mezzi di attuazione** **4. Disposizioni sul principio di minimizzazione** **5. Finalità e basi giuridiche del trattamento** **6. Offerta proattiva di servizi, profilazione e intelligenza artificiale**
ARGOMENTAZIONI	**1. Formulazione non ambigua del principio *once-only*** Dalla formulazione attuale del principio risulta chiara qual è l'esperienza utente che si vuole realizzare, ma non è chiaro come siano tenute ad agire le amministrazioni per realizzare tale esperienza utente. A livello intuitivo, sembrerebbe che, quando il cittadino si interfaccia con una pubblica amministrazione qualsiasi, quest'ultima debba avere accesso al patrimonio informativo dell'intera pubblica amministrazione italiana per poter verificare se il dato personale è già disponibile. Per ovvi motivi di sicurezza e proporzionalità del trattamento, ciò non è realizzabile. Sarebbe quindi opportuno definire chiaramente cosa si intende con *once-only*, o meglio

	quali sono le azioni richieste alle amministrazioni. Una possibilità sarebbe richiedere che il dato vada ricercato almeno all'interno del patrimonio informativo dell'ente specifico con cui il cittadino si sta interfacciando, unito alle basi di dati di interesse nazionale. **2. Obblighi di conservazione, finalità e tempi di conservazione** È chiaro che, per attuare il principio, ogni volta che un'amministrazione acquisisce un dato, dovrebbe conservarlo nell'eventualità che questo sia necessario in futuro. Il GDPR prescrive però che i dati personali possano essere conservati solo per l'arco di tempo necessario al conseguimento delle finalità per le quali sono stati raccolti [1]. Dunque: il dato personale va scartato quando scadono i termini di conservazione associati alla finalità originaria per cui è stato raccolto, o può/deve essere ulteriormente conservato per consentire l'applicazione del principio *once-only*? Il GDPR permette, allo scadere dei termini per la cancellazione, l'ulteriore archiviazione nel pubblico interesse [1]. La qualificazione esplicita del principio *once-only* come fine di pubblico interesse sarebbe uno strumento giuridico importante per permettere alle amministrazioni una conservazione regolare dei dati. La norma dovrebbe anche definire, in base alla tipologia di dato (comune, particolare, di salute etc.), quanto a lungo si estende l'archiviazione finalizzata al principio *once-only*. **3. Mezzi di attuazione** La norma dovrebbe chiarire quali strumenti tecnologici costituiscono l'ecosistema *once-only* oltre alla PDND, alle basi di dati di interesse nazionale, agli open data e ai sistemi informativi delle singole amministrazioni. Un punto specifico da chiarire, soppesando sicurezza ed efficienza: è ammessa la duplicazione locale di parte delle basi di dati di interesse nazionale o il dato deve ogni volta essere reperito tramite chiamata alla PDND? **4. Disposizioni sul principio di minimizzazione** Il GDPR richiede che i dati personali siano trattati in ottica di minimizzazione, ovvero che siano acquisiti solamente i dati personali strettamente necessari per il raggiungimento della finalità. Non sempre è possibile attuare puntualmente il principio, in quanto la PDND consente l'accesso a "pacchetti" di dati. Talvolta, questi contengono dati superflui. La norma dovrebbe stabilire chiaramente se, in PDND, è obbligatoria l'implementazione di strumenti di filtro che consentano di limitare il trattamento. In alternativa, dovrebbe essere previsto esplicitamente che è lecito accedere al servizio PDND più vicino alle necessità, anche se contiene dati eccedenti. **5. Finalità e basi giuridiche del trattamento**

	Vista la complessità della gestione in piattaforma delle finalità e delle basi giuridiche del trattamento, il livello di dettaglio richiesto e la necessità di continuo aggiornamento, è necessaria una forma di semplificazione. La norma potrebbe, per ciascuna base di dati di interesse nazionale, elencare il tipo di amministrazioni che hanno diritto a richiedere l'accesso, i dati cui possono accedere e le principali finalità. La norma potrebbe prevedere che tale elenco sia integrato da AgID, sotto la supervisione dell'autorità Garante, con atto amministrativo, e che i contenuti siano resi pubblici. Resta ferma la possibilità di individuare, come base giuridica del trattamento, anche qualsiasi altra norma dell'ordinamento italiano. La norma potrebbe inoltre prevedere un meccanismo di segnalazione, ad AgID e all'autorità Garante, di cortocircuiti e difficoltà in tema privacy che impediscono alle amministrazioni di realizzare concretamente il principio *once-only*. **6. Offerta proattiva di servizi, profilazione e intelligenza artificiale** Il più recente Piano Triennale per l'Informatica auspica l'impiego dell'intelligenza artificiale al fine di "supportare la personalizzazione dei servizi incentrata sull'utente, aumentando l'efficacia dell'erogazione dei servizi pubblici anche attraverso meccanismi di proattività". Tale meccanismo di offerta proattiva è possibile solo in presenza di una discreta quantità di dati personali degli utenti e comporta la profilazione. I dati conservati dalle amministrazioni in funzione del principio *once-only* si presterebbero bene ad essere utilizzati per l'offerta personalizzata di servizi pubblici. Per questo motivo la norma dovrebbe definire i confini entro i quali ciò è consentito, anche con disposizioni specifiche sulla profilazione e sull'utilizzo dell'intelligenza artificiale.
CONTRO-ARGOMENTAZIONI	*Non abbiamo bisogno di un'altra norma, la proliferazione normativa è in contraddizione con l'obiettivo di semplificazione*: in questo caso, non si tratta di iper-regolamentare un contesto già chiaro con il rischio di ingessarlo ulteriormente, si tratta di riempire un vero e proprio buco normativo con cui si scontrano tutte le amministrazioni che provano ad attuare il principio *once-only*. Non colmare questo vuoto significa far ricadere sulle singole amministrazioni il peso della regolamentazione, causando inevitabilmente frammentazione e disomogeneità nelle soluzioni, nei tempi di implementazione e nell'efficacia. Le disposizioni normative potrebbero diventare parte del *Codice dell'amministrazione digitale* (D.Lgs. 7 marzo 2005, n. 82), senza necessità di costituire un ulteriore atto. *L'implementazione del principio once-only potrebbe compromettere la sicurezza e la proporzionalità del trattamento dei dati, sollevando preoccupazioni etiche e legali riguardo alla privacy dei cittadini*: come affermato in precedenza, la protezione dei dati personali è un diritto fondamentale e, in quanto tale, va tutelato con la dovuta accortezza e

	consapevolezza. Allo stesso tempo, la tutela della privacy non può porsi in maniera ostativa all'innovazione, alla trasformazione digitale del Paese e alla garanzia dei diritti in tema di cittadinanza digitale. La proposta normativa dovrà essere scritta a più mani, conciliando i vincoli in tema di privacy con l'urgenza di attivare la trasformazione digitale della pubblica amministrazione a servizio dei cittadini. I profili di sicurezza dovranno essere validati dall'Agenzia per la Cybersicurezza Nazionale. *Una legge, da sola, non serve a molto*: l'integrazione normativa dovrà certamente essere accompagnata da un coerente sviluppo tecnologico di PDND e una coerente presa di coscienza delle amministrazioni. Tutto questo rientra tra i compiti istituzionali di AgID, che a seguito dell'approvazione della norma dovrà integrarne le disposizioni nel Piano Triennale per l'Informatica, prevedendo una roadmap per concretizzare i risultati. Intanto, urge la modifica normativa, al fine di rendere quantomeno possibili e leciti gli obiettivi delineati sopra.
CONCLUSIONE	In conclusione, l'adozione di una norma nazionale a supporto dei principi *once-only* e *digital-first* rappresenta un passo fondamentale per semplificare l'interazione tra cittadini e pubblica amministrazione. Tale norma, affrontando le criticità in tema di privacy e definendo chiaramente i mezzi di attuazione, abiliterà lo scambio sicuro ed efficace di dati, mettendo le amministrazioni in condizione di fornire servizi pubblici migliori, più semplici e personalizzati. L'implementazione di tali principi rappresenta un investimento strategico per il futuro digitale del Paese.
MINISTERI DI RIFERIMENTO	Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri; Agenzia per l'Italia Digitale (AgID); Autorità Garante per la protezione dei dati personali, Agenzia per la Cybersicurezza Nazionale (ACN).
BUDGET	La proposta non necessita di risorse economiche ulteriori rispetto a quelle programmate ordinariamente in quanto consiste esclusivamente in un adeguamento normativo.
FONTI E RIFERIMENTI	[1] Regolamento (UE) 27 aprile 2016, n. 679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali; [2] Regolamento (UE) 2 ottobre 2018, n. 1724 del Parlamento europeo e del Consiglio, che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi; [3] Regolamento (UE) 13 giugno 2024, n. 1689 del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale; [4] D.P.R. 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", art. 43, art. 59, art. 64 e art. 72; [5] D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";

	[6] D.Lgs. 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale”, art. 15, art. 41, art. 50 e art. 60; [7] “Piano Triennale per l’Informatica nella Pubblica Amministrazione 2024-2026”; [8] Direttiva concernente “Misure per l’attuazione dell’articolo 50-ter del decreto legislativo 7 marzo 2005, n. 82”.