Ca' Foscari
University
of Venice

Corso di Laurea magistrale
in Lingue, economie e istituzioni dell'Asia e dell'Africa mediterranea

Tesi di Laurea

La tutela dei dati personali nei sistemi di intelligenza artificiale: il modello giapponese

Dall'APPI alle Identità Digitali

Relatore
Ch. Prof. Giorgio Fabio Colombo

Correlatore
Ch. Prof. Marco Zappa

Laureando
Riccardo Giulianelli
Matricola 903754

Anno Accademico
2024 / 2025

要旨

近年、人工知能の利用は急速に広がり、場面が増えている。医療、採用、金融、行政サービスなど、意思決定を支える仕組みとしてAIが使われる場面が増えた。とくに2022年以降は生成AIが普及し、文章作成や検索機能などを通じて、一般の利用者がAIの出力に触れる機会も多くなっている。こうした変化の中で、個人情報をどのように扱うべきかが、制度運用において重要な論点になっている。本論文の目的は、日本における人工知能のガバナンスを整理し、その中心となる個人情報保護法（APPI）がAIに伴うリスクにどこまで対応できるのか、またどの部分に限界が生じるのかを明らかにすることである。

生成AIの登場により、法律が向き合う問題の内容も変わってきた。以前は学習用データを集める段階が主な焦点だったが、現在ではAIが推論によって作り出す情報や、出力される内容そのものが問題になっている。データは一度使われて終わりではなく、保存され、再利用され、別の処理に回されることがある。このように循環する性質は、データを集め、使用し保存するという直線的な流れを想定していた法制度の枠組みと比べ、誤差が生じやすい。日本のガバナンスには特徴がある。早い段階で包括的な法律を整えるというよりも、ガイドラインや指針といったソフトローを中心に、段階的に対応を進めてきた。このような進め方は、一般にライトタッチ型のガバナンスとして理解される。制度を運用する機関も一つではなく、政策の調整、産業面での方針、デジタル社会の推進、個人情報保護の運用が、それぞれ進められている。柔軟なやり方は利点がある一方で、責任範囲が不明確になりやすいという課題もある。

こうした仕組みの中で、APPIは人工知能だけを対象にした特別な法律ではない。それでも、個人情報とは何か、利用目的をどう決めるか、第三者への提供、業務委託、国境を越えた移転といった基本的なルールを通じて、AI分野でのデータ処理を実質的にコントロールしている。しかし、難しい点も残る。AIが推論で作ったデータ、モデルの内部に保存される情報、生成AIが出力する文章が、どこまで「個人情報」として扱われるべきかの判断は、その人を特定できるかどうかや、処理される状況に大きく左右される。これらの判断基準がはっきりしない領域が、いわゆる「グレーゾーン」となっている。また、運用面でも課題がある。個人情報保護委員会（PPC）は、ガイドラインや注意喚起を通じて事業者に改善を促す段階的な対応を基本としてきた。しかし、2023年にOpenAI社に対して行政指導が出された事例が示すように、技術の仕組み自体がリスクの中心となる場合、個別の対応だけでは標準的な義務として定着しにくい。また、利用者が削除を求めても、学習済みモデルに取り込まれた情報を実質的に取り除くことは技術的に難しい場合がある。法律上の権利と、実際にできることの間にずれが生じやすい。

こうした問題は、実際の制度運用でも見られる。リクナビ事件では、内定辞退率の予測といった推論データの扱いをめぐって大きな議論が起きた。また、マイナンバー制度では、情報連携が進む一方で、登録ミスや情報漏えいへの不安が社会的な信頼に影響した。さらに、ブロックチェーン技術を用いた分散型IDの議論では、技術の選び方そのものがガバナンスのあり方を左右するのである。本論文では、これらの具体例を参照しながら、APPIがAIのリスクにどう対応しているのか、そしてどこに構造的な限界があるのかを検証する。その上で、制

度上のずれを小さくするために必要な条件と、今後の政策が目指すべき方向を示す。これは、デジタル時代における個人情報保護のあり方を問い直す試みである。

Sommario

INTRODUZIONE 1
Capitolo 1: Intelligenza artificiale e dati personali: quadro teorico e giuridico 5
1.1 Definizione di intelligenza artificiale in ambito giuridico 6
1.2 Il concetto di dato personale, dato anonimo e dato derivato 8
1.3 Il ciclo del dato nei sistemi di intelligenza artificiale 9
1.3.1 Raccolta, selezione e trasformazione iniziale dei dati 10
1.3.2 Addestramento dei modelli e produzione di dati derivati 11
1.3.3 Continuità del ciclo e impatto cumulativo sui diritti 12
1.4 Trattamento automatizzato, profilazione e addestramento dei modelli 13
1.4.1 Trattamento automatizzato: definizione e implicazioni giuridiche 14
1.4.2 Profilazione: rischi, criteri e applicazioni 14
1.4.3 Addestramento dei modelli: dati derivati, bias e responsabilità 15
1.5 Hard law e soft law nella regolazione delle tecnologie emergenti 16
1.5.1 Hard law: vincoli, tutela e limiti nel contesto dell'IA 16
1.5.2 Soft law: flessibilità, orientamento e rischi 16
1.5.3 Integrazione di hard e soft law: esempi e applicazioni pratiche 17
Capitolo 2 – Il modello giapponese di regolazione dell'intelligenza artificiale 19
2.1 L'approccio giapponese all'innovazione tecnologica 20
2.2 Governance "light-touch" e configurazione istituzionale della regolazione 21
2.3 Ruolo delle autorità competenti: PPC, METI e MIC 23
2.4 Linee guida e strumenti di soft law per l'intelligenza artificiale 24
2.5 Limiti strutturali del modello giapponese 26
Capitolo 3 - L'APPI e il trattamento dei dati personali nell'era dell'intelligenza artificiale 29
3.1 Struttura e principi fondamentali dell'APPI 30
3.1.1 Struttura operativa dell'APPI 30
3.1.2 Scopo e logica dell'APPI 31
3.1.3 Principi fondamentali come criteri di verifica nei contesti algoritmici 32
3.2 Definizione e classificazione dei dati personali nell'APPI 33
3.3 Trattamento dei dati personali e sistemi di intelligenza artificiale 36
3.3.1 Acquisizione e costruzione dei dataset 37
3.3.2 Dal dato grezzo al dato trattabile 38
3.3.3 Addestramento e modello 39
3.3.4 Servizi di IA, fornitori esterni e trasferimenti 40
3.3.5 Output e inferenze 41

3.4 Intelligenza artificiale generativa e problematiche emergenti 42
3.4.1 Prompt e dati immessi dagli utenti 42
3.4.2 Dataset di addestramento e filtraggio 43
3.4.3 Riemersione in output e rischio di estrazione 44
3.4.4 Integrazione nei processi, prompt injection e RAG 45
3.5 Adeguatezza dell'APPI rispetto allo sviluppo tecnologico 47
3.5.1 Profili di tenuta 47
3.5.2 Profili di attrito 48
3.5.3 Nodi critici di effettività 49
CAPITOLO 4 – ZONE GRIGIE E CRITICITÀ DELLA REGOLAMENTAZIONE GIAPPONESE 51
4.1 Zone grigie concettuali e applicative 51
4.1.1 Identificabilità mobile 51
4.1.2 Nuovi oggetti dell'IA 52
4.1.3 Personal related information e filiere di data brokerage 54
4.1.4 Filiera distribuita, modelli foundation e responsabilità 55
4.2 Problemi di enforcement e limiti applicativi 56
4.2.1 Poteri della PPC e struttura graduale dell'enforcement 56
4.2.2 Tre limiti applicativi ricorrenti 57
4.2.3 Il caso Rikunabi 58
4.2.4 Il caso OpenAI 61
4.2.5 Effettività dei rimedi ed evoluzione dell'enforcement 65
4.3 Il paradosso del paradiso per l'addestramento 67
4.3.1 L'eccezione per il machine learning 68
4.3.2 Dai record statici ai rischi comportamentali 69
4.3.3 Frammentazione istituzionale e standardizzazione internazionale 70
4.4 Tensione tra tutela dei dati personali e competitività economica 71
4.4.1 Society 5.0 e Data Free Flow with Trust 71
4.4.2 Competitività industriale e scelte normative 72
4.4.3 Il paradosso della fiducia 73
CAPITOLO 5 – DUE CASI APPLICATIVI: MY NUMBER E BLOCKCHAIN .. 75
5.1 Struttura del sistema My Number 76
5.1.1 Presidi giuridici ed evoluzione del sistema 78
5.2 Criticità e Limiti del My Number 80
5.2.1 Incidenti, "trust shock" e risposta istituzionale 80
5.2.2 Responsabilità e rimedi 83

5.2.3 Dinamiche strutturali 84
5.3 Blockchain e identità digitali 85
5.3.1 Struttura della blockchain 85
5.3.2 I registri di fiducia 87
5.3.3 Trusted Web 88
5.3.4 Compatibilità con APPI e My Number 89
5.4 Confronto tra My Number e Blockchain 91
5.4.1 Collocamento della fiducia 91
5.4.2 Rischi speculari 93
5.5 SPID come terza via 95
CONCLUSIONI 101
BIBLIOGRAFIA 106

INTRODUZIONE

L'intelligenza artificiale è ormai entrata stabilmente in molti ambiti della vita economica e sociale. Sistemi algoritmici supportano decisioni in contesti sensibili come la sanità, la selezione del personale, la valutazione del credito e l'erogazione di servizi pubblici. Con la diffusione dei modelli di intelligenza artificiale generativa a partire dal 2022, l'interazione con sistemi capaci di produrre testi, immagini e altri contenuti è divenuta un'esperienza quotidiana per un pubblico molto ampio di utenti. In questo scenario, la gestione dei dati personali non è più soltanto una questione tecnica, ma si colloca al centro di tensioni giuridiche e sociali che riguardano la prevedibilità delle regole, l'effettività della tutela e la fiducia nei sistemi digitali.

Questa tesi analizza il modello giapponese di governance dell'intelligenza artificiale, concentrandosi sul ruolo svolto dall'Act on the Protection of Personal Information (APPI). L'obiettivo è valutare in che misura la disciplina giapponese riesca a intercettare i rischi legati ai trattamenti algoritmici e quali limiti emergano quando tecnologie basate su apprendimento automatico, inferenza e generazione di contenuti entrano in contatto con categorie normative costruite in un contesto diverso. La diffusione dell'IA generativa ha infatti modificato la natura stessa dei problemi giuridici. Se nella fase iniziale il nodo principale era la raccolta dei dati per l'addestramento, oggi l'intero ciclo di vita dell'informazione solleva interrogativi. I sistemi oltre a elaborare dati inseriti dagli interessati, producono anche nuove informazioni attraverso processi di inferenza, generano output che possono includere riferimenti a persone reali e riutilizzano dati e contenuti in modo iterativo. Questo comporta una dinamica circolare che entra in contrasto con modelli normativi pensati su sequenze lineari di raccolta, utilizzo e conservazione.

Il Giappone ha adottato un approccio peculiare alla regolazione dell'innovazione tecnologica. Più che introdurre fin da subito una disciplina dettagliata e vincolante, ha privilegiato strumenti di soft law, facendo affidamento su linee guida, raccomandazioni e orientamenti interpretativi prodotti dalle autorità competenti. Questo assetto, spesso descritto come light-touch governance, mira a preservare la flessibilità necessaria per

adattarsi a un contesto tecnologico in rapida evoluzione. La governance risulta inoltre distribuita con il coordinamento delle politiche pubbliche e la tutela dei dati personali che procedono su canali distinti e affidati a istituzioni diverse. Tale architettura può favorire reattività e sperimentazione, ma porta con sé rischi di frammentazione delle responsabilità e di incertezza applicativa, soprattutto quando i soggetti coinvolti in una filiera algoritmica non coincidono.

In questo quadro, l'APPI non è una legge speciale dedicata all'intelligenza artificiale, ma una normativa generale sulla protezione dei dati personali che, attraverso definizioni, principi e obblighi trasversali, finisce per disciplinare anche trattamenti effettuati mediante sistemi algoritmici. Le principali categorie e gli strumenti di tutela dell'APPI delineano il perimetro entro cui operatori pubblici e privati possono trattare informazioni riferibili alle persone, ma l'applicazione di tali categorie ai contesti di IA presenta difficoltà interpretative rilevanti. Particolarmente difficile è capire quale statuto giuridico attribuire alle informazioni che il sistema genera da solo. Punteggi di rischio, profili comportamentali e raccomandazioni personalizzate non vengono forniti dall'utente, ma sono prodotti dall'algoritmo attraverso calcoli statistici. Stabilire quando queste informazioni debbano essere considerate dati personali è una questione che dipende dal contesto concreto e che spesso resta aperta. In queste situazioni il confine tra informazioni protette e non protette tende a sfumare, generando vere e proprie zone grigie che rendono meno prevedibile l'applicazione delle regole.

Le criticità non riguardano soltanto la qualificazione dei dati, ma anche l'effettività della tutela. La Personal Information Protection Commission opera prevalentemente attraverso interventi cooperativi, privilegiando il dialogo con gli operatori rispetto all'imposizione di obblighi vincolanti. Questo approccio mostra i suoi limiti quando il rischio è incorporato nella struttura stessa del sistema tecnologico, come emerso nel 2023 con la diffusione di servizi generativi su larga scala. Inoltre, l'esercizio concreto dei diritti degli interessati si scontra spesso con barriere tecniche. Quando informazioni personali sono state incorporate nei parametri di un modello addestrato, la loro rimozione effettiva può risultare difficilmente praticabile. Si produce così una distanza tra diritti formalmente riconosciuti e tutela sostanziale.

Queste tensioni non restano confinate al piano teorico e si manifestano anche in casi

concreti di particolare rilievo. Il caso Rikunabi ha riguardato l'uso di strumenti predittivi per stimare la probabilità di rinuncia all'assunzione da parte dei candidati e la circolazione di tali informazioni inferenziali verso le imprese, evidenziando le difficoltà nel ricondurre dati derivati a categorie giuridiche pensate per dati raccolti. L'intervento della PPC ha messo in luce problemi di trasparenza e anche l'incertezza sulla qualificazione giuridica di output algoritmici utilizzati in contesti decisionali ad alto impatto. Analoghe frizioni emergono nel sistema My Number, infrastruttura nazionale di identificazione digitale. Da un lato, l'interoperabilità tra banche dati promette efficienza e semplificazione, dall'altro nel 2023 sono emersi casi di errata associazione delle informazioni della tessera sanitaria a soggetti diversi, insieme ad altre forme di mis-registrazione e disallineamenti nei servizi collegati alla My Number Card, con un impatto diretto sulla fiducia sociale e sulla legittimazione dell'intera architettura. Quando l'identificazione digitale diventa condizione ordinaria di accesso a prestazioni fondamentali, errori anche percentualmente contenuti possono generare un effetto di sfiducia sistemica difficilmente recuperabile. Infine, il dibattito su identità digitale e blockchain introduce una prospettiva ulteriore, mostrando come le scelte tecnologiche influiscano direttamente sul modo in cui la governance può essere progettata. Ad esempio, l'immutabilità del registro e la logica dei sistemi distribuiti pongono interrogativi sulla compatibilità con principi di rettifica e cancellazione tipici della protezione dei dati, aprendo un confronto tra verificabilità tecnica e requisiti giuridici consolidati.

Sul piano metodologico, la ricerca combina l'analisi normativa del quadro giapponese in materia di protezione dei dati personali con lo studio dei documenti interpretativi e applicativi della PPC, essenziali per comprendere l'operatività concreta dell'APPI. L'esame giuridico è affiancato da un confronto con la letteratura giuridica giapponese e internazionale sui principali punti di frizione tra IA e protezione dei dati, e dall'analisi di casi concreti e materiali ufficiali, integrati da fonti giornalistiche. Nel corso della tesi si è scelto, dove opportuno, di mantenere alcuni termini tecnici in lingua inglese per coerenza con le fonti primarie e per ridurre ambiguità interpretative, dato il frequente uso di terminologia straniera nei documenti giapponesi e nel dibattito internazionale.

La tesi si articola in cinque capitoli. Il primo ricostruisce le nozioni concettuali necessarie per inquadrare il rapporto tra IA e dati personali, con attenzione al ciclo di vita del dato e

ai processi di inferenza. Il secondo esamina il modello giapponese di regolazione dell'IA e la logica della governance light-touch. Il terzo analizza struttura e principi dell'APPI e le modalità con cui la disciplina incide sui trattamenti algoritmici. Il quarto mette a fuoco le zone grigie e le criticità applicative, evidenziando i limiti strutturali e i problemi di enforcement. Il quinto approfondisce i casi del sistema My Number e delle sperimentazioni legate a identità digitale e blockchain. L'analisi si chiude con una riflessione sulle condizioni necessarie per ridurre la distanza tra disciplina formale e tutela effettiva, individuando possibili direzioni di policy capaci di mantenere un equilibrio tra promozione dell'innovazione e protezione dei diritti fondamentali.

Capitolo 1: Intelligenza artificiale e dati personali: quadro teorico e giuridico

L'evoluzione delle tecnologie digitali e in particolare il rapido sviluppo dei sistemi di intelligenza artificiale hanno inciso in modo profondo sulle modalità di raccolta, trattamento e utilizzo dei dati personali. A differenza delle tecnologie informatiche tradizionali, l'intelligenza artificiale non si limita a elaborare informazioni fornite in modo diretto dagli individui, ma è in grado di generare nuove informazioni, dedurre caratteristiche personali e costruire profili complessi a partire da grandi volumi di dati eterogenei e spesso non strutturati (OECD, 2019). Tale capacità rende il rapporto tra intelligenza artificiale e protezione dei dati personali particolarmente delicato dal punto di vista giuridico.

Nel contesto attuale, i dati costituiscono la risorsa essenziale per il funzionamento dei sistemi di intelligenza artificiale. Gli algoritmi di apprendimento automatico, in particolare quelli basati su tecniche di *machine learning* e *deep learning*, richiedono infatti ingenti quantità di dati per le fasi di addestramento, validazione e miglioramento continuo dei modelli (OECD, 2024). Questo processo solleva interrogativi centrali per il diritto della protezione dei dati: quali dati possono essere legittimamente utilizzati e secondo quali condizioni? In che misura è possibile fare ricorso a dati apparentemente anonimi senza incidere sulla sfera privata degli individui? Le categorie giuridiche tradizionali di "dato personale" risultano ancora adeguate a descrivere fenomeni quali i dati derivati o ricavati dai sistemi di intelligenza artificiale?

Il presente capitolo ha lo scopo di fornire il quadro teorico e concettuale necessario per affrontare, nei capitoli successivi, l'analisi della regolamentazione giapponese dell'intelligenza artificiale, con particolare riferimento al trattamento dei dati personali ai sensi dell'*Act on the Protection of Personal Information* (APPI). Prima di esaminare il modello normativo giapponese e le sue principali caratteristiche, appare infatti indispensabile chiarire cosa si intenda per "intelligenza artificiale" in ambito giuridico, quali tipologie di dati assumano rilevanza ai fini della tutela della privacy e come si articoli il ciclo di vita del dato all'interno dei sistemi automatizzati.

In questa prospettiva, il capitolo intende delineare un quadro concettuale unitario volto a chiarire le principali nozioni giuridiche rilevanti per l'analisi del rapporto tra intelligenza artificiale e protezione dei dati personali. L'attenzione si concentra sulla definizione giuridica dei sistemi di intelligenza artificiale, sulle categorie di dati che assumono rilievo nell'ambito dei trattamenti automatizzati e sulle modalità attraverso le quali tali dati vengono raccolti, elaborati e riutilizzati. Particolare rilievo è attribuito alle forme di trattamento automatizzato e di profilazione, che costituiscono il presupposto operativo per l'addestramento e il funzionamento dei modelli. Il capitolo si conclude con una riflessione sul ruolo degli strumenti normativi vincolanti e non vincolanti nella regolazione delle tecnologie emergenti, fornendo le basi teoriche necessarie per comprendere l'approccio giapponese alla governance dell'intelligenza artificiale.

1.1 Definizione di intelligenza artificiale in ambito giuridico

La nozione di intelligenza artificiale non nasce in ambito giuridico, ma affonda le proprie radici nelle scienze informatiche e cognitive. Tuttavia, recentemente il diritto è stato chiamato a confrontarsi con l'esigenza di definire l'intelligenza artificiale in termini sufficientemente chiari da consentire l'applicazione di regole giuridiche, senza al contempo irrigidire eccessivamente una tecnologia caratterizzata da un'elevata dinamicità.

In ambito giuridico, una delle definizioni più autorevoli è quella elaborata dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), secondo cui un sistema di intelligenza artificiale è "un sistema basato su macchine che, per obiettivi espliciti o impliciti, inferisce, dai dati ricevuti, come generare output quali previsioni, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali" (OECD, 2019, p. 7). Tale definizione mette in evidenza tre elementi centrali: il ruolo dei dati come input essenziale, la capacità di inferenza del sistema e la produzione di output idonei a incidere sulla realtà esterna. Un successivo *Explanatory Memorandum* ha precisato che i sistemi di intelligenza artificiale si distinguono dalle forme tradizionali di automazione per la loro capacità di apprendere e adattarsi anche dopo la fase di implementazione iniziale (OECD, 2024, p. 4).

Nel contesto europeo, il Regolamento sull'Intelligenza Artificiale (*AI Act*) ha introdotto

una definizione giuridica vincolante, qualificando come sistema di IA "un sistema software progettato per funzionare con diversi gradi di autonomia e che, per obiettivi espliciti o impliciti, inferisce dai dati in ingresso come generare output quali previsioni, contenuti, raccomandazioni o decisioni che influenzano ambienti fisici o virtuali" (European Union 2024/1689, art. 3, par. 1). La scelta del legislatore europeo riflette un'impostazione funzionale, volta a ricomprendere un ampio spettro di applicazioni tecnologiche sulla base delle loro caratteristiche operative e degli effetti prodotti sugli individui, piuttosto che sulla base di criteri tecnici o antropomorfici.

Il Giappone ha adottato un approccio differente. Piuttosto di una definizione giuridica rigida contenuta in una fonte normativa vincolante, le autorità giapponesi hanno privilegiato l'elaborazione di definizioni flessibili nell'ambito di strumenti di *soft law*, quali le "*AI Guidelines for Business*" predisposte dal Ministero dell'Economia, del Commercio e dell'Industria (METI). In tali documenti, l'intelligenza artificiale è descritta come "l'insieme di tecnologie che consentono ai sistemi informatici di svolgere compiti che normalmente richiederebbero l'intelligenza umana, attraverso processi di apprendimento dai dati e di riconoscimento di pattern" (METI, 2024, p. 10). Pur non avendo natura giuridicamente vincolante, queste linee guida svolgono una funzione rilevante di orientamento per le imprese e per le amministrazioni.

Questa scelta si inserisce in un più ampio approccio alla regolazione delle tecnologie emergenti, spesso definito come light-touch governance, volto a favorire l'innovazione e la competitività economica evitando un eccessivo irrigidimento normativo (Cabinet Office, 2025). Al contempo, l'assenza di una definizione giuridica vincolante di intelligenza artificiale può rendere meno immediata l'individuazione dell'ambito di applicazione degli obblighi previsti dalla normativa sulla protezione dei dati personali, in particolare dall'APPI.

Ai fini della presente analisi, e in coerenza con gli standard internazionali in materia precedentemente citati, l'intelligenza artificiale viene qui intesa come l'insieme dei sistemi basati su tecnologie digitali che, a partire da dati in ingresso, generano con un certo grado di autonomia output idonei a incidere su situazioni giuridiche o di fatto riferibili a persone fisiche. Questa definizione costituirà il riferimento per l'analisi delle categorie di dati e del ciclo del dato nei sistemi di intelligenza artificiale sviluppata nelle

sezioni successive.

1.2 Il concetto di dato personale, dato anonimo e dato derivato

Per comprendere appieno l'impatto dei sistemi di intelligenza artificiale sul trattamento dei dati, è fondamentale chiarire quali tipologie di informazioni rientrino nella sfera di protezione offerta dal diritto. Le categorie di dato personale, dato anonimo e dato derivato rappresentano il lessico minimo necessario per analizzare il funzionamento dell'IA e per valutare quanto le pratiche operative siano compatibili con i principi di tutela della privacy e dei dati personali.

L'APPI definisce il dato personale come qualsiasi informazione relativa a una persona fisica vivente che consenta di identificarla, direttamente o indirettamente, attraverso elementi quali nome, data di nascita o altri descrittori, inclusi codici identificativi e dati biometrici (Act on the Protection of Personal Information, 2021, art. 2). La definizione europea contenuta nel GDPR è molto simile: considera dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile", comprendendo sia identificatori diretti sia indiretti (European Union 2016/679, art. 4, n.1). Pur usando termini diversi, entrambe le normative condividono l'obiettivo di garantire protezione quando le informazioni consentono di risalire all'individuo.

Oltre al dato personale, l'APPI distingue tra personal data, ossia dati contenuti in database strutturati che ne permettono la facile gestione, e retained personal data, cioè dati che un titolare conserva e controlla, per i quali valgono obblighi specifici come accesso, rettifica e cancellazione da parte dell'interessato (Amended APPI, 2022, art. 2, par. 4-7). Queste distinzioni sono essenziali per comprendere le responsabilità legali dei soggetti che gestiscono dati automatizzati.

Il concetto di dato anonimo assume un ruolo cruciale. Nel GDPR, i dati anonimi sono informazioni che non si riferiscono più a una persona identificabile, mentre l'APPI distingue tra Anonymously Processed Information e Pseudonymously Processed Information. La prima categoria include dati trattati in modo tale da rendere impossibile l'identificazione dell'individuo, secondo gli standard tecnici e organizzativi stabiliti dalla Personal Information Protection Commission (PPC). La seconda comprende dati

pseudonimizzati: l'identificazione diretta è impedita, ma è possibile risalire all'individuo combinando informazioni aggiuntive separate (Amended APPI, 2022, art. 2). Questo approccio consente alle organizzazioni di utilizzare i dati per analisi interne senza compromettere completamente la privacy degli interessati.

Un'ulteriore categoria rilevante è quella del dato derivato o inferito, ossia informazioni generate dai sistemi di IA a partire da dati originari. Tra gli esempi si possono citare punteggi di rischio, profili di consumo, stime comportamentali o rappresentazioni numeriche interne ai modelli IA (OECD, 2024). Questi dati, pur non raccolti direttamente dall'interessato, possono avere un impatto reale sulla sua sfera di diritti. La loro qualificazione giuridica rimane complessa: secondo il GDPR, possono essere considerati dati personali se riferibili a individui identificabili, mentre l'APPI non li regolamenta ancora in modo esplicito, anche se spesso rientrano nelle categorie di personal information, pseudonymously processed information o anonymously processed information a seconda del grado di collegamento con l'identità del soggetto.

Ai fini di questa tesi, il concetto di dato derivato sarà considerato come una categoria analitica trasversale. Per "dato derivato" si intende qualsiasi informazione generata a partire da dati personali preesistenti mediante analisi, trasformazione o inferenza, inclusi profili individuali, cluster comportamentali e output personalizzati prodotti dai sistemi IA. La questione centrale resta stabilire se tali dati debbano essere considerati dati personali ai sensi dell'APPI, con tutti i diritti e obblighi correlati, oppure se possano essere trattati come dati "non personali" pur continuando a influenzare concretamente la vita degli individui.

1.3 Il ciclo del dato nei sistemi di intelligenza artificiale

L'analisi giuridica dei sistemi di intelligenza artificiale richiede di superare una concezione statica del dato personale, tradizionalmente legata al momento della raccolta o della conservazione dell'informazione. A differenza dei trattamenti informatici convenzionali, i sistemi di IA operano attraverso flussi informativi complessi, caratterizzati da una continua trasformazione dei dati e da un loro riutilizzo iterativo nel tempo. In questo contesto, il concetto di *ciclo del dato* assume un ruolo centrale come strumento interpretativo per comprendere come i dati personali vengano trattati,

valorizzati e riutilizzati, nonché per valutare l'impatto complessivo di tali processi sui diritti e sulle libertà degli individui.

La letteratura internazionale ha evidenziato come il valore economico e funzionale dell'intelligenza artificiale non risieda nel singolo dato considerato isolatamente, bensì nella capacità dei sistemi di combinare, correlare e rielaborare grandi quantità di informazioni in modo ripetuto e adattivo nel tempo (OECD, 2019). Questa caratteristica distingue radicalmente i trattamenti algoritmici dai modelli tradizionali di gestione dei dati, mettendo in crisi le categorie giuridiche fondate su una sequenza lineare di fasi (raccolta, utilizzo, conservazione, cancellazione) su cui si basa gran parte della normativa in materia di protezione dei dati personali.

1.3.1 Raccolta, selezione e trasformazione iniziale dei dati

Il ciclo del dato prende avvio dalla fase di raccolta delle informazioni, che nei sistemi di intelligenza artificiale può avvenire attraverso modalità eterogenee: conferimento diretto da parte dell'interessato, osservazione del comportamento, acquisizione da fonti terze, integrazione di dataset preesistenti o generazione automatica a partire da altre informazioni. A differenza dei trattamenti tradizionali, la raccolta nei sistemi di IA è spesso orientata a utilizzi plurimi e non completamente determinabili al momento iniziale del trattamento.

Dal punto di vista giuridico, tale caratteristica entra in tensione con il principio di limitazione della finalità, che costituisce uno dei cardini sia del GDPR europeo sia dell'APPI giapponese. Come osservato dalla dottrina, nei contesti di apprendimento automatico risulta difficile, se non impossibile, definire ex ante in modo puntuale tutte le finalità per le quali i dati verranno utilizzati. Poiché i modelli si evolvono nel tempo e possono essere riadattati a scopi diversi rispetto a quelli originariamente previsti, il principio di limitazione della finalità diventa particolarmente complesso: non si applica soltanto ai dati di addestramento, ma anche ai modelli stessi, che diventano essi stessi una forma di dato e possono essere riutilizzati per applicazioni ulteriori (Mühlhoff, Ruschemeier, 2024).

Una volta raccolti, i dati vengono sottoposti a una serie di operazioni preliminari

(selezione, pulizia, normalizzazione, etichettatura e aggregazione) finalizzate a renderli idonei all'elaborazione algoritmica. Sebbene tali operazioni siano spesso presentate come meramente tecniche, esse rivestono un rilievo giuridico significativo. Le scelte effettuate in questa fase incidono infatti sul modo in cui gli individui vengono rappresentati all'interno del sistema, determinando quali caratteristiche vengano considerate rilevanti e quali, invece, vengano escluse.

Numerosi studi hanno dimostrato come decisioni assunte nella fase di preparazione dei dati possano generare distorsioni sistematiche nei risultati prodotti dai modelli, dando origine a fenomeni di discriminazione indiretta o di trattamento iniquo di determinati gruppi sociali (Barocas, Selbst, 2016). Da un punto di vista giuridico, ciò pone interrogativi rilevanti in relazione ai principi di correttezza, trasparenza e non discriminazione, che trovano riconoscimento tanto nel diritto europeo quanto, seppur in forma meno articolata, nell'ordinamento giapponese.

Anche nella dottrina internazionale è stato evidenziato come l'utilizzo dei dati e dei modelli nell'ambito dei sistemi di apprendimento automatico contemporaneo segua una logica sempre più circolare e iterativa, in cui le informazioni e i modelli vengono costantemente riutilizzati e rielaborati per finalità nuove e mutevoli nel corso del ciclo di vita del sistema. Questo modello si discosta in modo significativo dallo schema lineare su cui si fondano molte disposizioni dell'APPI e del GDPR, contribuendo a creare zone di incertezza interpretativa già nella fase iniziale del trattamento (Ashmore et al., 2021).

1.3.2 Addestramento dei modelli e produzione di dati derivati

La fase di addestramento del modello costituisce il nucleo centrale del ciclo del dato nei sistemi di intelligenza artificiale. In questa fase, i dati raccolti e trasformati vengono utilizzati per consentire al sistema di individuare correlazioni statistiche, schemi ricorrenti e relazioni probabilistiche, che permettono al modello di generare output quando riceve nuovi input. Il risultato di questo processo non consiste in una semplice rielaborazione dei dati originari, bensì nella creazione di nuove informazioni sotto forma di parametri interni, pesi numerici e rappresentazioni matematiche.

Da un punto di vista giuridico, questa fase segna l'emersione dei cosiddetti *dati derivati*

o *dati inferiti*, ossia informazioni che non sono state fornite direttamente dall'interessato, ma che vengono generate dal sistema attraverso operazioni di analisi e inferenza. Profili individuali, punteggi di rischio, categorie comportamentali o preferenze dedotte rappresentano esempi emblematici di tale fenomeno (Article 29 Data Protection Working Party, 2018).

La qualificazione giuridica dei dati derivati costituisce uno dei nodi più problematici della regolazione dei sistemi di IA. Nell'ordinamento europeo, l'interpretazione prevalente ritiene che tali dati possano essere considerati dati personali qualora siano riferibili a una persona identificata o identificabile e siano idonei a incidere sulla sua sfera giuridica o fattuale (Article 29 Data Protection Working Party, 2018). Nel contesto giapponese, invece, l'APPI non disciplina espressamente la categoria dei dati derivati, lasciando ampi margini di incertezza interpretativa.

Parte della dottrina giapponese e i commentatori delle disposizioni APPI hanno sostenuto che i dati derivati possono essere ricondotti alle categorie esistenti di personal information, pseudonymously processed information o anonymously processed information, a seconda del grado di collegamento residuo con l'identità dell'individuo. Tuttavia, tale soluzione appare solo parzialmente soddisfacente, poiché non affronta in modo sistematico la questione del potere informativo esercitato dai modelli attraverso inferenze che possono produrre effetti rilevanti sugli individui, pur non basandosi su dati direttamente identificativi (PPC, 2024c; Article 29 Data Protection Working Party, 2018).

Un ulteriore elemento critico è rappresentato dall'opacità dei processi di addestramento, in particolare nei modelli di apprendimento profondo. La complessità strutturale di tali sistemi rende spesso difficile ricostruire il nesso causale tra i dati utilizzati e le decisioni prodotte, limitando la possibilità di controllo da parte degli interessati e delle autorità competenti. Questa opacità solleva interrogativi rilevanti in relazione ai principi di trasparenza e responsabilità, che costituiscono pilastri fondamentali della protezione dei dati personali (Burrell, 2016).

1.3.3 Continuità del ciclo e impatto cumulativo sui diritti

Il ciclo del dato nei sistemi di intelligenza artificiale non si esaurisce con la

produzione di un output. Al contrario, gli output stessi vengono frequentemente archiviati, riutilizzati e reinseriti nei processi di affinamento del modello, dando origine a meccanismi di apprendimento continuo. Questa caratteristica ciclica pone problemi specifici per l'applicazione del principio di limitazione della conservazione, poiché risulta difficile individuare un momento in cui il trattamento possa dirsi effettivamente concluso.

Dal punto di vista giuridico, il rischio principale non deriva da una singola fase isolata del trattamento, bensì dall'effetto cumulativo delle diverse operazioni che compongono il ciclo del dato. È possibile che ciascuna fase, considerata separatamente, appaia conforme ai requisiti normativi, mentre l'insieme delle operazioni produca forme di sorveglianza sistematica o di influenza pervasiva sulle scelte degli individui. Questo fenomeno è stato ampiamente analizzato nella letteratura critica sugli ecosistemi digitali, che ha messo in luce come l'analisi massiva dei dati possa essere utilizzata per prevedere, orientare o condizionare il comportamento umano (Pasquale, *2015).*

Alla luce di queste considerazioni, il ciclo del dato si configura non solo come una descrizione tecnica del funzionamento dei sistemi di IA, ma come un parametro essenziale per valutare l'adeguatezza dei modelli di regolazione esistenti. Nel caso giapponese, l'approccio flessibile e orientato alla promozione dell'innovazione ha favorito lo sviluppo tecnologico, ma ha anche lasciato ampi spazi di incertezza nella qualificazione giuridica dei trattamenti algoritmici. Tali incertezze emergeranno con particolare evidenza nei capitoli successivi, dedicati all'analisi dell'APPI e all'individuazione delle zone grigie della regolamentazione giapponese.

1.4 Trattamento automatizzato, profilazione e addestramento dei modelli

Nei sistemi di intelligenza artificiale, il trattamento dei dati personali non si limita alla semplice raccolta o archiviazione. Il trattamento automatizzato comprende tutte le operazioni eseguite mediante strumenti digitali, dalla classificazione e analisi dei dati fino alla generazione di decisioni che incidono concretamente sulla vita degli individui. La profilazione, ossia la costruzione di profili dettagliati sugli interessati, è uno strumento centrale per applicazioni economiche come marketing mirato, concessione di credito o gestione del rischio assicurativo (Zuboff, 2019). L'addestramento dei modelli trasforma

dati grezzi in capacità predittive complesse, ma genera anche questioni critiche sul piano della responsabilità e della protezione dei diritti degli individui.

Analizzare come trattamento automatizzato, profilazione e addestramento dei modelli interagiscono permette di evidenziare opportunità economiche e rischi giuridici, in particolare alla luce dell'APPI giapponese e del confronto internazionale.

1.4.1 Trattamento automatizzato: definizione e implicazioni giuridiche

Il trattamento automatizzato include operazioni come raccolta, registrazione, organizzazione, conservazione, estrazione, consultazione, utilizzo, comunicazione e cancellazione dei dati. La definizione europea di "trattamento" nel GDPR (European Union 2016/679, art. 4, n. 2) abbraccia questa ampia gamma di operazioni. Nel contesto giapponese, sebbene l'APPI non distingua formalmente tra trattamento manuale e automatizzato, la letteratura critica ha evidenziato che l'uso di sistemi digitali introduce rischi specifici di trasparenza, accountability e possibilità di errore sistematico, soprattutto nel contesto dell'intelligenza artificiale ((PPC, 2024c; Article 29 Data Protection Working Party, 2018).

Dal punto di vista economico, la capacità di elaborare grandi volumi di dati consente vantaggi competitivi significativi e ottimizzazione dei processi decisionali. Tuttavia, errori o bias nei dati possono amplificare impatti negativi sui diritti degli individui e comportare responsabilità civili e regolamentari, come evidenziato dalla letteratura critica sugli algoritmi (Barocas, Selbst, 2016). L'accountability, come previsto dall'APPI e dal GDPR, richiede misure tecniche e organizzative adeguate: documentazione del funzionamento degli algoritmi, monitoraggio delle decisioni e procedure di revisione in caso di anomalie (Article 29 Data Protection Working Party, 2017).

1.4.2 Profilazione: rischi, criteri e applicazioni

La profilazione consiste nell'analisi dei dati degli interessati mediante trattamenti automatizzati per valutare caratteristiche personali, abitudini o comportamenti, influenzando decisioni future, in linea con quanto definito dal GDPR (art. 4, n. 4). È utilizzata sia in ambito commerciale che pubblico, ad esempio per valutazioni di rischio creditizio o personalizzazione di servizi sanitari e amministrativi, e si inserisce in quello

che Pasquale descrive come un ecosistema di “black box” che classificano e valutano costantemente gli individui (Pasquale, 2015).

Dal punto di vista giuridico, la profilazione pone problemi di trasparenza, minimizzazione dei dati e non discriminazione. L'APPI stabilisce che le finalità del trattamento siano determinate al momento della raccolta e comunicate agli interessati (Amended APPI, 2022, art. 15). Nei sistemi di IA, le finalità possono evolvere con l'addestramento, creando zone grigie rispetto alla limitazione della finalità.

Economicamente, la profilazione ottimizza marketing e riduce rischi, ma può produrre discriminazioni indirette se gli algoritmi replicano bias storici (Barocas, Selbst, 2016). Per mitigare questi rischi, la dottrina giuridica europea e giapponese sottolinea l'importanza di implementare linee guida interne rigorose e condurre audit periodici per garantire la conformità normativa e minimizzare l'esposizione a responsabilità legali (Article 29 Data Protection Working Party, 2018).

1.4.3 Addestramento dei modelli: dati derivati, bias e responsabilità

L'addestramento dei modelli utilizza dati personali e derivati per generare capacità predittive. I sistemi elaborano parametri, pesi e rappresentazioni matematiche complesse che consentono al modello di generalizzare a nuovi dati. Il bias algoritmico, cioè la tendenza di un modello a produrre risultati discriminatori a causa di dati di addestramento sbilanciati o scelte metodologiche distorte, rappresenta un rischio significativo (Burrell, 2016, p. 3). L'APPI richiede misure preventive, ma non definisce procedure dettagliate; audit indipendenti e documentazione dei processi di addestramento sono strumenti chiave per mitigare i rischi (PPC, 2024c; Article 29 Data Protection Working Party, 2018). Dal punto di vista economico, modelli ben addestrati aumentano efficienza e competitività, mentre errori o mancata mitigazione dei bias possono comportare sanzioni, danni reputazionali e perdita di fiducia (Pasquale, 2015). Emerge chiaramente, già da questa fase iniziale, che il ciclo di trattamento dei dati non è una questione meramente tecnica, bensì implica questioni cruciali di tutela dei diritti fondamentali degli individui e, contemporaneamente, di sostenibilità economica delle imprese.

1.5 Hard law e soft law nella regolazione delle tecnologie emergenti

L'evoluzione rapida dei sistemi di intelligenza artificiale ha evidenziato la necessità di strumenti regolatori capaci di governare le tecnologie emergenti senza soffocare l'innovazione. In questo contesto, la distinzione tra hard law e soft law diventa fondamentale per comprendere approcci diversi adottati nei vari ordinamenti. L'hard law comprende norme vincolanti, come leggi, regolamenti o decreti, che impongono obblighi precisi e prevedono sanzioni in caso di violazione. La soft law, invece, include linee guida, codici di condotta, raccomandazioni e best practice che orientano i comportamenti senza creare vincoli giuridici diretti, favorendo flessibilità e adattabilità in contesti tecnologici in rapido cambiamento (Hasan et al., 2023).

1.5.1 Hard law: vincoli, tutela e limiti nel contesto dell'IA

Dal punto di vista giuridico, l'hard law garantisce certezze e tutela dei diritti fondamentali, in particolare nel settore della protezione dei dati personali. In Giappone, l'APPI costituisce il principale esempio di hard law applicabile all'intelligenza artificiale, imponendo obblighi vincolanti sul trattamento dei dati personali, la trasparenza e la responsabilità dei titolari dei dati. La normativa definisce limiti precisi su raccolta, conservazione e utilizzo dei dati, prevedendo sanzioni in caso di violazioni e offre un quadro stabile e prevedibile per cittadini e imprese.

Tuttavia, l'hard law può diventare un vincolo nei contesti tecnologici in rapida evoluzione. Nuove tecniche di IA o modalità di trattamento dei dati possono emergere più velocemente della normativa, creando zone grigie dove non è chiaro quale comportamento sia conforme alla legge. Nel caso giapponese, l'assenza di una normativa generale sull'IA ha significato che l'APPI, pur efficace sulla protezione dei dati personali, non affronta tutti i rischi specifici dell'intelligenza artificiale moderna, lasciando spazi di interpretazione e incertezza (PPC, 2024c; Article 29 Data Protection Working Party, 2018).

1.5.2 Soft law: flessibilità, orientamento e rischi

La soft law svolge un ruolo complementare e, in certi casi, essenziale nelle fasi di sviluppo e sperimentazione di tecnologie innovative. Linee guida elaborate da organismi

internazionali e autorità nazionali forniscono indicazioni pratiche su come implementare principi di protezione dei dati e prevenire bias algoritmici, senza creare obblighi vincolanti (Wallach et al., 2023). Questa flessibilità consente alle imprese di adattare rapidamente le proprie soluzioni tecnologiche, bilanciando innovazione ed etica dei dati.

Tuttavia, l'assenza di vincoli legali concreti può generare incertezze applicative e frammentazione. Se le aziende seguono linee guida diverse o le interpretano in modo differente, la protezione dei cittadini può variare significativamente. Inoltre, la soft law manca della forza sanzionatoria che induce conformità generalizzata, affidando il rispetto principalmente all'autoregolamentazione e alla pressione reputazionale (Article 29 Data Protection Working Party, 2017, pp. 3-4). Questo aspetto è particolarmente rilevante nel contesto giapponese, dove la soft law è prevalente.

1.5.3 Integrazione di hard e soft law: esempi e applicazioni pratiche

Un esempio dell'interazione tra hard e soft law riguarda la gestione dei dati derivati nei modelli di IA. L'APPI, come hard law, impone obblighi su sicurezza, accesso e rettifica dei dati personali, ma non disciplina in modo esaustivo il trattamento dei dati inferiti. Le linee guida soft della PPC e di organismi internazionali offrono indicazioni operative per anonimizzare o pseudonimizzare i dati derivati, prevenendo violazioni dei diritti senza limitare l'innovazione (Mühlhoff, Ruschemeier, 2024). Dal punto di vista economico, questo approccio integrato permette alle aziende di sviluppare prodotti basati su IA con maggiore sicurezza legale e operativa, riducendo rischi legali e danni reputazionali.

Un altro caso riguarda la profilazione predittiva nel marketing digitale e nella gestione dei rischi. L'hard law richiede consenso dell'interessato e rispetto dei principi di minimizzazione e non discriminazione. La soft law suggerisce metodologie per il controllo dei bias, la validazione periodica degli algoritmi e la documentazione dei processi decisionali (Barocas, Selbst, 2016). Così, le imprese possono ottimizzare i risultati economici pur rispettando diritti fondamentali, ottenendo un equilibrio tra efficacia operativa e tutela giuridica.

L'integrazione di hard e soft law si rivela quindi essenziale nella regolazione delle tecnologie emergenti. L'hard law offre certezze e tutela giuridica, mentre la soft law

garantisce adattabilità e promuove l'adozione di best practice in tempo reale. Nel contesto dell'IA, dove dati personali e derivati sono continuamente elaborati, la sola hard law rischierebbe di diventare rigida e disallineata alla realtà tecnologica, mentre la sola soft law potrebbe generare vuoti di tutela. L'esperienza giapponese dimostra come l'uso combinato di APPI e linee guida soft favorisca innovazione economica e protezione dei diritti, pur lasciando margini di incertezza che saranno analizzati nei capitoli successivi, anche nel confronto con il modello europeo e l'AI Act (Villasenor, 2024).

Capitolo 2 – Il modello giapponese di regolazione dell'intelligenza artificiale

Il presente capitolo analizza il modello giapponese di regolazione dell'intelligenza artificiale, con attenzione alle scelte istituzionali e agli strumenti giuridici adottati. L'obiettivo non è valutare il sistema in chiave comparativa né anticipare un confronto con l'ordinamento europeo, ma comprendere la logica interna che ha portato il Giappone a privilegiare un approccio regolatorio flessibile.

Come evidenziato nel Capitolo 1, la regolazione dell'intelligenza artificiale comporta questioni giuridiche complesse, soprattutto in relazione al trattamento dei dati, all'automazione dei processi decisionali e alla tutela dei diritti individuali. In particolare, il ciclo del dato e i dati derivati dai sistemi di IA pongono problemi di trasparenza e responsabilità che richiedono risposte normative differenziate. In questo contesto, il Giappone si distingue per aver evitato, almeno in una fase iniziale, un quadro normativo vincolante, facendo largo uso di strumenti di soft law e di autoregolamentazione.

Questo approccio, noto come governance "light-touch", parte dall'idea che una regolazione troppo rigida possa rallentare l'innovazione. La scelta è coerente con una strategia più ampia di politica economica e industriale, che attribuisce all'intelligenza artificiale un ruolo centrale nel rafforzamento della competitività e nella gestione di sfide strutturali come l'invecchiamento della popolazione e la riduzione della forza lavoro (OECD, 2024).

Il capitolo si articola come segue. Il paragrafo 2.1 ricostruisce l'approccio giapponese all'innovazione tecnologica, evidenziando i presupposti politici e istituzionali delle scelte in materia di IA. I paragrafi successivi approfondiranno il modello di governance, il ruolo delle autorità competenti e l'uso delle linee guida come principale strumento regolatorio. Infine, si metteranno in luce criticità strutturali senza confronti diretti con altri ordinamenti.

2.1 L'approccio giapponese all'innovazione tecnologica

L'approccio giapponese alla regolazione dell'intelligenza artificiale è strettamente legato alla concezione dell'innovazione tecnologica nelle strategie di sviluppo nazionale. Da circa il 2015, il Governo ha progressivamente inquadrato l'IA come tecnologia trasversale, capace di incidere su vari settori, dalla manifattura avanzata ai servizi, fino all'amministrazione pubblica (Cabinet Office, 2016).

Un elemento centrale è rappresentato dal concetto di *Society 5.0*, modello di società che punta a integrare spazio fisico e cyberspazio. L'intelligenza artificiale viene qui vista non solo come fenomeno da regolare, ma come strumento per raggiungere obiettivi pubblici, come migliorare l'efficienza dei servizi, aumentare la produttività e affrontare problemi sociali complessi (Cabinet Office, 2017). Questo spiega perché, nel dibattito giapponese, la regolazione dell'IA sia considerata da calibrare con attenzione, senza diventare un fine a sé stante.

Coerentemente, le autorità giapponesi hanno mostrato prudenza nell'introdurre obblighi vincolanti in fasi iniziali. Una regolazione troppo dettagliata rischierebbe di limitare la capacità delle imprese di sperimentare nuove soluzioni e adattarsi ai cambiamenti tecnologici. Tale preoccupazione emerge chiaramente nei documenti strategici del Ministero dell'Economia, del Commercio e dell'Industria (METI), che segnalano come un intervento normativo rigido possa tradursi in un freno all'innovazione (AI Strategy, 2019).

Accanto a queste considerazioni, il contesto economico-strutturale gioca un ruolo importante. Il Giappone affronta un importante declino demografico e una progressiva riduzione della popolazione attiva, fenomeni che incidono sulla sostenibilità economica. L'IA è stata individuata come una possibile risposta, permettendo di automatizzare processi produttivi e compensare almeno in parte alla carenza di forza lavoro. Una regolazione percepita come eccessivamente restrittiva potrebbe dunque ridurre la diffusione dell'IA e i suoi benefici economici.

Queste scelte si inseriscono in una tradizione di governance tecnologica tipica del Giappone, dove l'intervento pubblico tende a orientare e coordinare piuttosto che imporre

obblighi coercitivi. Nel settore dell'IA ciò si traduce in linee guida, raccomandazioni e standard volontari elaborati insieme agli attori privati (CSIS, 2025). La soft law diventa così lo strumento centrale della regolazione.

In questo quadro, il diritto funge da accompagnamento più che da controllo preventivo. Le autorità monitorano l'evoluzione delle pratiche, intervenendo solo se emergono rischi significativi per i diritti fondamentali o l'interesse pubblico. La gradualità è esplicitamente richiamata in documenti governativi che sottolineano l'equilibrio tra innovazione e tutela degli individui.

Nonostante i vantaggi, questa scelta comporta implicazioni problematiche. La flessibilità normativa favorisce l'adozione dell'IA e sostiene la competitività, ma solleva dubbi sulla sufficienza delle tutele, soprattutto in settori sensibili come i dati personali e i sistemi decisionali automatizzati. La fiducia nell'autoregolamentazione richiede responsabilità elevata da parte degli operatori e capacità di intervento reale delle autorità (METI, 2021).

Dunque, possiamo dire che l'approccio giapponese privilegia sviluppo e sperimentazione, accettando un certo grado di rischio regolatorio. È coerente con gli obiettivi di politica economica, ma pone le basi per criticità che emergeranno nei paragrafi successivi, in particolare riguardo alla frammentazione degli strumenti di governance e alla gestione delle zone grigie normative.

2.2 Governance "light-touch" e configurazione istituzionale della regolazione

Come illustrato nel paragrafo 2.1, la scelta strategica del Giappone di privilegiare lo sviluppo tecnologico trova riscontro anche nella configurazione istituzionale della governance dell'intelligenza artificiale. L'espressione governance "light-touch" non descrive semplicemente un atteggiamento permissivo, bensì riflette un sistema specifico di distribuzione dei poteri regolatori e di utilizzo di strumenti non vincolanti per orientare l'innovazione.

La regolazione dell'intelligenza artificiale non si articola mediante norme legislative di carattere generale. Piuttosto, emerge da processi coordinati all'interno dell'esecutivo,

frequentemente attraverso comitati di esperti e organismi interministeriali. Il Cabinet Office non esercita poteri normativi diretti, ma svolge una funzione di regia nel coordinamento delle politiche e nella promozione di un approccio coerente tra i diversi attori istituzionali, contribuendo a definire l'indirizzo complessivo della governance dell'IA (Cabinet Office, 2019).

In assenza di una legge quadro specifica, i ministeri competenti assumono un ruolo cruciale nel definire le modalità operative della governance. Il METI e il MIC producono documenti che, pur non avendo valore giuridicamente vincolante, esercitano una significativa influenza sulle pratiche degli operatori economici. Questi strumenti non prescrivono comportamenti specifici, ma individuano ambiti di attenzione e principi di riferimento, lasciando alle imprese la responsabilità di tradurli in soluzioni concrete adeguate ai rispettivi contesti applicativi.

Le *AI Governance Guidelines* del METI rappresentano il dispositivo centrale di questo modello. Pubblicate nella versione 1.0 nel luglio 2021, non introducono obblighi formali né prevedono meccanismi sanzionatori. Il loro obiettivo è delineare una cornice concettuale per la gestione dei rischi associati all'uso dell'IA, riconoscendo agli operatori economici un elevato grado di autonomia nell'implementazione. La scelta di non adottare standard tecnici dettagliati consente agli attori di adattare le indicazioni generali alle specificità dei diversi ambiti applicativi (METI, 2021).

Una caratteristica distintiva della governance giapponese è la separazione tra la definizione degli obiettivi pubblici e i mezzi di controllo. Le autorità fissano finalità generali (come l'affidabilità dei sistemi o l'equità dei processi decisionali) senza determinare direttamente le modalità tecniche attraverso cui tali obiettivi devono essere perseguiti. Questo assetto riflette una fiducia nei meccanismi di autoregolamentazione e nelle capacità organizzative degli operatori privati di rispondere agli indirizzi pubblici in modo responsabile.

Dal punto di vista strutturale, il sistema di governance dell'IA giapponese è di natura policentrica. Non esiste un'autorità unica responsabile; le competenze sono distribuite tra soggetti distinti con ambiti di intervento specifici. Il Cabinet Office coordina le strategie generali, il METI si concentra sulla governance industriale e sulle politiche di regolazione

dell'innovazione, mentre il MIC interviene sui profili legati alle infrastrutture digitali e alle comunicazioni. Il *Report of the AI Network Society Promotion Conference* del MIC sottolinea come tale distribuzione contribuisca al mantenimento di una governance flessibile e adattabile (MIC, 2020).

La centralità della soft law consente inoltre un aggiornamento relativamente rapido degli strumenti di governance. Le linee guida possono essere riviste o ampliate senza ricorrere a procedure legislative complesse, permettendo alle autorità di reagire all'evoluzione tecnologica con maggiore tempestività. Nei documenti governativi, questa capacità di adattamento è indicata come un elemento essenziale per garantire l'efficacia della regolazione dell'intelligenza artificiale.

Nel complesso, la governance "light-touch" giapponese si configura come un sistema basato sull'indirizzo politico, sulla cooperazione tra settore pubblico e privato e sull'uso prevalente di strumenti non vincolanti. La regolazione assume una funzione di orientamento e monitoraggio, piuttosto che di controllo preventivo e diretto, attribuendo una parte significativa della responsabilità agli attori coinvolti nello sviluppo e nell'utilizzo dei sistemi di intelligenza artificiale.

2.3 Ruolo delle autorità competenti: PPC, METI e MIC

La governance dell'intelligenza artificiale in Giappone si fonda su una distribuzione funzionale delle competenze tra più autorità pubbliche, senza un ente unico centrale. Questo assetto policentrico riflette la filosofia *light-touch*: la regolazione emerge da processi di coordinamento interministeriale e consultivo, più che da imposizioni normative dirette.

La *Personal Information Protection Commission* (PPC) presidia il corretto trattamento dei dati personali nei sistemi di IA, fornendo orientamenti tramite linee guida interpretative e raccomandazioni. L'autorità interviene principalmente sulla compatibilità dei processi automatizzati con i principi di protezione della persona, lasciando agli operatori ampio margine di responsabilità nell'implementazione, pur conservando poteri ispettivi e di enforcement in caso di violazioni (PPC, 2023a).

Il *Ministry of Economy, Trade and Industry* (METI) si concentra sulla governance industriale e organizzativa dei sistemi di IA. Le linee guida del METI delineano un quadro concettuale flessibile per valutare i rischi e gestire i sistemi intelligenti, senza creare vincoli giuridici obbligatori, favorendo così l'autonomia delle imprese e un'applicazione adattativa dei principi generali (METI, 2021).

Il *Ministry of Internal Affairs and Communications* (MIC) interviene sugli aspetti infrastrutturali, delle reti di comunicazione e dell'ecosistema digitale. Attraverso organismi consultivi come l'*AI Network Society Promotion Conference*, il MIC individua aree prioritarie, raccomandazioni operative e principi generali per sicurezza, affidabilità e trasparenza dei sistemi intelligenti, stimolando il dialogo tra istituzioni, settore privato e società civile (MIC, 2020).

Insieme, PPC, METI e MIC costituiscono un sistema di governance complementare: la PPC tutela i dati personali, il METI orienta le pratiche organizzative e industriali e il MIC definisce il contesto infrastrutturale e digitale. La responsabilità è distribuita e la governance dipende dalla capacità di coordinamento e cooperazione tra le autorità, riflettendo la filosofia della soft law: orientare, monitorare e lasciare spazio di autonomia agli operatori, con possibilità di intervento mirato in caso di rischi significativi.

2.4 Linee guida e strumenti di soft law per l'intelligenza artificiale

In Giappone, la regolazione dell'intelligenza artificiale si realizza prevalentemente attraverso strumenti di *soft law*, ossia linee guida e raccomandazioni che non impongono obblighi giuridici vincolanti, ma forniscono orientamenti pratici agli operatori per una gestione responsabile dei sistemi IA. Questo approccio consente di garantire una governance coerente senza frenare la sperimentazione tecnologica e rappresenta una declinazione concreta del modello "light-touch" descritto nei paragrafi precedenti.

Il documento principale è l'**"***AI Guidelines for Business Ver.1.0***"** pubblicato da METI nel 2024, che unifica le linee guida precedenti in un quadro operativo coerente. Le linee guida forniscono non solo principi generali (trasparenza, equità, sicurezza, protezione dei dati), ma anche metodologie e strumenti operativi concreti come check-list per audit interni e schemi di valutazione dei rischi (METI, 2024).

Le linee guida distinguono tre categorie di attori: sviluppatori di sistemi IA, fornitori di servizi basati su IA e utilizzatori. Questa distinzione aiuta a chiarire responsabilità e ruoli durante l'intero ciclo di vita dei sistemi. Ad esempio, uno sviluppatore che realizza un algoritmo predittivo per la selezione del personale deve documentare i criteri adottati, indicare i possibili bias residui e fornire indicazioni ai fornitori o utenti del sistema su come gestire tali rischi.

Il processo operativo delineato dalle linee guida si articola in diverse fasi. La prima fase consiste nella mappatura del contesto e dei rischi, comprendendo non solo aspetti tecnici o legali, ma anche impatti sociali e percezioni degli stakeholder. La fase successiva prevede la definizione di obiettivi chiari e misurabili per la gestione dell'IA, comunicati all'interno dell'organizzazione e agli interlocutori esterni. Facendo un esempio concreto, un'azienda di servizi finanziari può stabilire come obiettivo la riduzione dei bias nei modelli di scoring creditizio, monitorando costantemente i risultati rispetto agli indicatori definiti.

Durante la fase operativa, le organizzazioni implementano sistemi di governance interni che combinano procedure di controllo dei processi, valutazioni periodiche dei modelli IA e formazione del personale. Il monitoraggio continuo dei risultati consente di correggere errori, aggiornare algoritmi o modificare procedure, garantendo che le decisioni automatizzate rimangano coerenti con i principi etici e normativi indicati dalle linee guida.

Infine, le linee guida prevedono una valutazione periodica dell'efficacia complessiva del sistema, che include consultazioni con stakeholder esterni. Questa fase permette di aggiornare obiettivi, procedure e priorità in funzione delle evoluzioni tecnologiche e delle richieste della società civile, senza ricorrere a interventi legislativi formali. In tal modo, la soft law diventa uno strumento dinamico, capace di accompagnare l'evoluzione dell'ecosistema IA e di orientare le decisioni organizzative in contesti complessi e diversificati (METI, 2024).

Alcuni osservatori internazionali sottolineano che, nonostante la chiarezza metodologica delle linee guida METI, la loro natura non vincolante può generare ambiguità nell'interpretazione pratica da parte delle imprese, soprattutto in contesti ad alta complessità tecnologica o regolatoria (Citadel AI, 2024).

Possiamo quindi osservare che le linee guida METI illustrano come la soft law giapponese traduca i principi generali in strumenti concreti di gestione dei rischi e di governance, preservando flessibilità e sperimentazione. L'approccio differenziato per tipologia di attore consente di equilibrare la responsabilità dei singoli operatori con la necessità di una direzione coerente a livello di sistema, senza ricorrere a standard tecnici uniformi o a regolazioni vincolanti premature.

2.5 Limiti strutturali del modello giapponese

La governance giapponese dell'intelligenza artificiale, pur caratterizzandosi per flessibilità e capacità di adattamento, presenta limiti strutturali derivanti dalla natura non vincolante degli strumenti regolatori e dalla distribuzione policentrica delle competenze. Il modello si fonda sulla convinzione che linee guida volontarie e coordinamento informale possano indirizzare le pratiche aziendali verso risultati socialmente responsabili, ma questa assunzione può risultare fragile in contesti tecnologicamente complessi e con forti incentivi economici (BIICL, 2025).

L'architettura policentrica comporta che le responsabilità siano distribuite tra più autorità senza un coordinamento centralizzato formale. Se un sistema IA coinvolge simultaneamente trattamento dei dati personali, gestione industriale dei rischi e infrastrutture digitali, non è chiaro quale autorità abbia competenza primaria o come dovrebbero cooperare. Di conseguenza, le imprese possono ricevere indicazioni divergenti, mentre le autorità rischiano sovrapposizioni o lacune operative (CSIS, 2025).

La dipendenza dalla soft law amplifica la vulnerabilità del modello. Linee guida METI, raccomandazioni PPC e orientamenti MIC non sono giuridicamente vincolanti e non prevedono enforcement diretto. Il livello di conformità dipende quindi dalla volontà delle imprese di rispettarle, situazione che in settori ad alta competitività può condurre a una minore aderenza. La ricerca internazionale sottolinea che la soft law funziona come strumento di orientamento, ma solo la hard law può imporre il rispetto (BIICL, 2025).

Questa flessibilità comporta inoltre differenze significative tra operatori. Senza standard tecnici uniformi, le interpretazioni dei principi generali (come equità, trasparenza e sicurezza) variano da azienda ad azienda. Startup e piccole imprese, spesso prive di

competenze dedicate, possono applicare protocolli meno rigorosi rispetto a grandi multinazionali, generando asimmetrie nelle pratiche di gestione dei rischi (CSIS, 2025).

Il modello non prevede rimedi diretti per i soggetti danneggiati da sistemi IA. A differenza di normative più stringenti come il GDPR o l'AI Act europeo, le linee guida giapponesi non creano cause legali dirette né sanzioni amministrative per la mancata conformità. Un cittadino discriminato da un algoritmo di selezione del personale, ad esempio, dovrebbe far valere i propri diritti attraverso leggi preesistenti sulla protezione dei dati, riducendo la funzione preventiva della regolazione (DDG, 2025).

Le sfide emergenti dei sistemi IA complessi, in particolare dei modelli generativi, mettono in evidenza ulteriori limiti. Questi sistemi operano con elevata opacità e potenziale impatto sociale, difficile da prevedere tramite linee guida non vincolanti. I rischi includono bias, allucinazioni semantiche e responsabilità non chiaramente imputabile, fenomeni che possono manifestarsi solo dopo la distribuzione dei sistemi (DDG, 2025).

Il modello si basa anche su processi volontari di reporting e auto-monitoraggio. Le imprese sono invitate a raccogliere dati, identificare bias e segnalare incidenti, ma l'assenza di obblighi formali e sanzioni lascia discrezionalità su cosa comunicare, generando informazioni asimmetriche e limitando l'intervento preventivo delle autorità (AI CERTS, 2025).

Per affrontare alcune criticità, l'AI Promotion Act del 2025 ha istituito un AI Strategy Headquarters e introdotto l'obbligo di cooperazione delle imprese con le politiche governative. Tuttavia, l'obbligo rimane non cogente e senza sanzioni legali; l'efficacia pratica dipende da fattori reputazionali e dal coordinamento volontario tra enti (Baker McKenzie, 2025). La governance giapponese resta quindi un sistema che bilancia innovazione e tutela dei diritti, ma la natura volontaria degli strumenti, il policentrismo e l'assenza di rimedi diretti creano spazi di vulnerabilità normativa, particolarmente evidenti in scenari tecnologici complessi e ad alto rischio economico (OECD, 2024).

Possiamo concludere che il modello giapponese di regolazione dell'IA si fonda su una filosofia di fiducia nei meccanismi di mercato, nell'autoregolamentazione delle imprese e nella flessibilità necessaria per adattarsi a tecnologie in rapido sviluppo. A differenza di

approcci più vincolanti, la governance è distribuita tra diverse autorità, ciascuna responsabile di specifici aspetti (protezione dei dati personali, gestione dei rischi industriali, infrastrutture digitali) attraverso strumenti di soft law che forniscono principi e metodologie senza obblighi legali coercitivi. La flessibilità consente alle imprese di adattare i processi di governance ai contesti specifici, favorendo innovazione e riducendo oneri normativi. Il coordinamento informale tra autorità ha permesso risposte rapide a esigenze emergenti, come mostrano gli aggiornamenti costanti delle linee guida METI tra il 2021 e il 2024. La soft law incoraggia inoltre una responsabilità condivisa tra pubblico e privato, traducendo principi etici generali in pratiche organizzative concrete.

Tuttavia, la natura non vincolante degli strumenti e la distribuzione policentrica delle competenze comportano vulnerabilità. Il rispetto delle linee guida dipende dalla disponibilità volontaria delle imprese e le competenze disperse possono generare ambiguità e ritardi di coordinamento. Mancano meccanismi diretti di rimedio per individui danneggiati da decisioni automatizzate e standard tecnici uniformi, riducendo l'efficacia preventiva della regolazione.

Queste limitazioni emergono con particolare evidenza con sistemi IA complessi e generativi, dove opacità e impatto sociale non possono essere completamente affrontati tramite linee guida non vincolanti. Processi volontari di reporting e auto-monitoraggio lasciano discrezionalità significativa alle imprese, creando informazioni asimmetriche e riducendo la capacità di intervento preventivo.

Il governo ha tentato di mitigare alcuni limiti con l'AI Promotion Act del 2025, istituendo l'AI Strategy Headquarters e introducendo un obbligo di cooperazione formale, ma l'efficacia resta subordinata a incentivi reputazionali e coordinamento volontario. Il modello giapponese rappresenta quindi un equilibrio delicato tra innovazione e tutela dei diritti, dove la flessibilità è un vantaggio strategico ma comporta vulnerabilità normative in contesti tecnologici complessi.

Nel Capitolo 3 verrà analizzato come l'APPI risponde alle sfide poste dal trattamento dei dati personali nell'era dell'IA, valutandone l'efficacia nel proteggere individui e dati in contesti tecnologici sempre più sofisticati e meno trasparenti.

Capitolo 3 - L'APPI e il trattamento dei dati personali nell'era dell'intelligenza artificiale

Questo capitolo si colloca nel punto di raccordo tra due esigenze già emerse nei capitoli precedenti. Da un lato, la ricostruzione del trattamento algoritmico ha mostrato che l'impatto sui diritti non si esaurisce nella raccolta, ma dipende anche dalle fasi successive, in cui l'informazione viene trasformata, combinata e impiegata per produrre inferenze. Dall'altro lato, l'analisi del modello giapponese di regolazione dell'IA ha evidenziato un'impostazione complessivamente flessibile, in cui la governance si costruisce spesso attraverso indirizzi e strumenti non vincolanti. In una situazione di questo tipo, la questione diventa verificare quale sia la base giuridica che nella pratica delimita e condiziona i trattamenti che coinvolgono informazioni riferibili a persone fisiche.

In questa prospettiva, l'Act on the Protection of Personal Information (APPI) costituisce il principale riferimento normativo. La sua rilevanza non deriva dall'essere una normativa speciale sull'intelligenza artificiale, ma dal fatto che essa definisce concetti, soglie e obblighi attraverso i quali può essere valutata la tenuta dei trattamenti basati sui dati sotto il profilo della tutela dell'interessato. In questo capitolo si sostiene che l'APPI, pur mostrando una notevole capacità di adattamento ai trattamenti algoritmici, presenti limiti strutturali proprio dove l'impatto sui diritti deriva da inferenze, riusi modellistici e filiere complesse piuttosto che dalla semplice gestione di dati identificativi.

Bisogna sottolineare che i rischi dell'IA non dipendono esclusivamente dalla fase di acquisizione. Una parte rilevante delle criticità emerge quando l'informazione entra nei dataset, alimenta l'addestramento e produce inferenze utilizzate in processi decisionali che risultano difficili da verificare dall'esterno. In questa direzione, la riflessione internazionale ha messo in evidenza l'esistenza di un *accountability gap*, in cui il punto non è il dato originario, ma l'insieme delle inferenze ad alto impatto generate e impiegate operativamente (Wachter, Mittelstadt, 2019).

Allo stesso tempo, nel sistema giapponese le definizioni e le soglie non possono essere trattate come elementi neutri. La costruzione del perimetro applicativo, ovvero ciò che rientra nella tutela e le condizioni in cui vi rientra, è il luogo in cui tendono ad aprirsi

zone grigie. Infatti, una parte della dottrina giapponese ha evidenziato come l'accento posto sull'identificabilità possa non intercettare pienamente danni connessi a profiling e attribuzioni, anche in assenza di un'identificazione nominativa in senso stretto (Takagi, 2020).

Il presente capitolo chiarisce i presupposti giuridici offerti dall'APPI per valutare la disciplina dei trattamenti di dati personali in contesti di intelligenza artificiale. La ricostruzione delle definizioni e dei criteri applicativi consente di individuare le aree di maggiore frizione, che costituiranno la base per l'analisi delle criticità sistemiche sviluppata nel capitolo successivo.

3.1 Struttura e principi fondamentali dell'APPI

3.1.1 Struttura operativa dell'APPI

L'APPI è una legge generale, tuttavia per comprendere come gli obblighi vengano concretamente applicati non è sufficiente considerare il solo testo legislativo. La disciplina opera in modo stratificato: alla legge si affiancano atti di attuazione, un apparato di linee guida e Q&A che contribuisce a stabilizzare l'interpretazione rendendola utilizzabile dagli operatori.

Sul piano formale, oltre al testo dell'APPI, si affianca il Cabinet Order (Shikōrei, 施行令), che integra profili applicativi e procedurali. Sul piano sostanziale, un ruolo centrale è svolto dalla Personal Information Protection Commission (PPC), che non agisce soltanto come organo di controllo a posteriori, ma produce anche standard interpretativi. I materiali sono organizzati e pubblicati in modo sistematico nella sezione "Legal / Guidelines", dove il testo normativo è collocato accanto a documenti di implementazione e orientamento.

In tale cornice, il documento più rilevante per ampiezza e funzione sono le Guidelines (Tsūsoku-hen, 通則編), che traduce concetti generali in criteri applicativi e offre esempi utili a delimitare categorie e soglie, riducendo l'incertezza della compliance (PPC, 2024a). Questo livello interpretativo, pur non coincidendo con la legge in senso formale, costituisce parte della struttura operativa dell'APPI, perché numerose questioni non vengono risolte solo tramite disposizioni generali, ma attraverso esempi, precisazioni e

aggiornamenti.

Questa configurazione presenta un effetto duplice. Da un lato, consente un adattamento relativamente rapido di fronte a mutamenti tecnologici e pratiche emergenti. Dall'altro lato, una parte della certezza applicativa tende a dipendere dalla stabilità e dalla continuità della produzione interpretativa. Tale dinamica emerge anche nella ricostruzione storico-istituzionale della disciplina giapponese, in cui l'evoluzione non appare come un processo lineare di codificazione, ma come un aggiustamento tra norme, istituzioni e interpretazioni nel tempo (Horibe, 2025).

Nel contesto dell'IA, il funzionamento per strati è particolarmente visibile nei casi in cui l'autorità è chiamata a tradurre concetti giuridici in oggetti tecnici. Un esempio è il Q&A della PPC relativo ai parametri addestrati (Omomi keisū, 重み係数) generati dall'addestramento su dataset contenenti dati personali. La PPC afferma che tali parametri non rientrano nella nozione di "*personal information*" nella misura in cui sia escluso un rapporto di corrispondenza con individui specifici (PPC, 2022a).

La soluzione è comprensibile sul piano applicativo, poiché evita di qualificare come dato personale, per definizione, qualunque modello addestrato. Tuttavia, la condizione posta (l'esclusione del legame con individui specifici) presuppone un quadro tecnico non immutabile. Infatti, l'anonimizzazione e le tecniche di de-identification possono fallire in presenza di informazioni esterne e che la distinzione tra dato personale e non personale non costituisce una barriera stabile in maniera definitiva (Ohm, 2010).

In questo punto si inserisce l'osservazione della dottrina giapponese secondo cui, se l'accesso alla tutela dipende in modo eccessivo da soglie costruite attorno all'identificabilità, possono risultare sottovalutati danni derivanti da *profiling, scoring e classificazioni*, anche quando non è possibile (o non è necessario) risalire immediatamente al nome del soggetto (Takagi, 2020). Questo chiarisce perché la costruzione delle soglie interpretative costituisca parte del problema, come affronteremo in un paragrafo successivo.

3.1.2 Scopo e logica dell'APPI

Lo scopo dichiarato dell'APPI orienta l'intera disciplina. L'articolo 1 colloca la

protezione dei diritti e interessi individuali entro una cornice che prende atto dell'espansione dell'uso dell'informazione personale nella società digitale e considera l'utilità dei dati come elemento del contesto (Amended APPI, 2022, art. 1).

Questa impostazione contribuisce a spiegare perché la disciplina tende a privilegiare obblighi di gestione e responsabilità organizzativa piuttosto che divieti rigidi e generalizzati. Nel contesto dell'IA, tuttavia, la sostenibilità dell'equilibrio dipende dalla capacità di rendere effettivi gli strumenti di controllo, soprattutto quando pratiche di riuso e inferenza riducono la prevedibilità del trattamento dal punto di vista dell'interessato.

Alcuni studi hanno evidenziato che la protezione non può essere affidata esclusivamente a un modello che presuppone un controllo individuale pienamente informato, poiché le asimmetrie informative e la complessità delle catene di trattamento rendono tale premessa strutturalmente fragile (Yamamoto, 2020). La rilevanza dell'osservazione, ai fini di questo capitolo, risiede nella necessità di distinguere tra adempimento formale e tutela sostanziale.

Accanto alla finalità generale, l'articolo 3 introduce un principio di base, rispetto della persona e cautela nel trattamento, che svolge una funzione valoriale ma resta necessariamente generale (APPI, art. 3). La portata concreta di tale principio dipende dalla capacità degli obblighi più specifici e delle interpretazioni della PPC di renderlo operativo.

3.1.3 Principi fondamentali come criteri di verifica nei contesti algoritmici

L'obiettivo di questo paragrafo non è riprodurre l'APPI in forma descrittiva, ma isolare alcuni snodi che, nei trattamenti algoritmici, tendono a concentrarsi e a generare attriti applicativi.

Su tutto, riguarda la finalità. La legge richiede di specificare la finalità di utilizzo e di limitare l'uso a un perimetro coerente (APPI, artt. 17–18). In trattamenti tradizionali ciò contribuisce a rendere il trattamento prevedibile e valutabile. Nell'IA, soprattutto quando si tratta di addestramento e miglioramento del modello, la finalità tende però a essere formulata in modo più elastico, poiché il valore del dato è spesso collegato a riusi e generalizzazioni.

Inoltre, assume rilievo la correttezza dell'acquisizione e la governabilità della filiera. Nella pratica dell'IA generativa, il punto non riguarda soltanto la raccolta puntuale, ma la costruzione, gestione, utilizzo e soprattutto l'eventuale pubblicazione o condivisione dei dataset, che può inserirli in una catena di riusi difficilmente controllabile (Kakinuma, 2023).

Un ulteriore punto è la sicurezza. L'APPI tratta la sicurezza come obbligo e le Guidelines forniscono indicazioni operative volte a evitare una conformità puramente formale (PPC, 2024a). Nei sistemi di IA, tuttavia, oltre al rischio di *data breach* (violazione dei dati personali), è importante anche la possibilità che l'informazione personale emerga in output o venga estratta in modo non previsto. In questa direzione, l'intervento della PPC sui servizi di AI generativa segnala un tentativo di collegare i rischi a pratiche operative concrete, senza trasformare l'intervento in una regolazione tecnologica generale (PPC, 2023a).

Infine, ci sono la trasparenza e i rimedi. L'APPI prevede diritti e strumenti di intervento, ma la loro effettività dipende dalla tracciabilità delle informazioni e dalla possibilità di individuare il dato controllabile. Nei trattamenti modellistici, ciò che conta non è sempre un record accessibile, ma una catena di trasformazioni. Quando l'impatto deriva da inferenze, il controllo successivo richiede strumenti che vadano oltre l'accesso al dato originario (Wachter, Mittelstadt, 2019).

Su queste premesse si innesta il prossimo paragrafo, che chiarisce definizioni e classificazioni centrali per delimitare l'ambito applicativo dell'APPI.

3.2 Definizione e classificazione dei dati personali nell'APPI

L'APPI costruisce la tutela attraverso un sistema di definizioni che non ha una funzione unicamente descrittiva. Concretamente, queste categorie stabiliscono quando un'informazione entra nel perimetro degli obblighi e quando invece resta fuori o si colloca in un'area intermedia disciplinata in modo diverso (Amended APPI, 2022, art. 2).

La categoria di base è la *personal information* (個人情報, kojin jōhō), cioè informazione relativa a una persona fisica vivente che consente di identificare uno specifico individuo. La definizione non si esaurisce nell'identificazione diretta, ma include anche

l'identificazione indiretta, quando il collegamento con altri elementi rende possibile risalire alla persona. In questo senso, la qualificazione non dipende soltanto dal contenuto del frammento informativo isolato, ma anche dal contesto in cui esso è inserito e dalla possibilità concreta di ricomporre l'identità attraverso collegamenti (PPC, 2024a).

La soglia più discussa è quella della facile confrontabilità con altre informazioni (容易に照合, yōi ni shōgō). Un'informazione può rientrare nella *personal information* anche se da sola non identifica, purché possa essere collegata con ragionevole facilità ad altri dati e portare così all'identificazione. La "facilità" non è un criterio statico e tende a muoversi con l'evoluzione delle infrastrutture e delle prassi di *matching*, cioè di collegamento tra basi dati. Su questo punto la dottrina giapponese ha sottolineato che se la soglia viene letta in modo troppo elastico, la qualificazione rischia di dipendere da valutazioni contingenti, pur in presenza di effetti individualizzanti (Takagi, 2025).

Accanto a questa via relazionale dell'identificazione, l'APPI prevede una seconda strada più netta: il *personal identification code* (個人識別符号, kojin shikibetsu fugō), ossia un identificatore che consente di individuare la persona in modo diretto o funzionalmente equivalente. In questa categoria rientrano, tra l'altro, codici e numeri attribuiti in contesti amministrativi o documentali e anche elementi biometrici quando trattati in modo idoneo a identificare (Amended APPI, 2022, art. 2). L'elenco e la tipizzazione operativa degli identificatori rinviano anche alla disciplina di attuazione (Shikōrei, 2003).

Una volta chiarito che cosa possa costituire *personal information*, l'APPI introduce categorie che dipendono dal modo in cui l'informazione è organizzata e gestita. La *personal data* (個人データ, kojin dēta) indica la *personal information* contenuta in un insieme sistematicamente organizzato e ricercabile, cioè un *personal information database* (個人情報データベース等, kojin jōhō dētabēsu tō) in senso giuridico. La distinzione segnala il passaggio dal trattamento occasionale al trattamento strutturale e rende applicabili obblighi che presuppongono gestione sistematica (Amended APPI, 2022, art. 2).

All'interno di questa area si colloca la categoria decisiva per i diritti dell'interessato: la *retained personal data* (保有個人データ, hoyū kojin dēta), cioè i dati personali rispetto

ai quali l'operatore ha un potere effettivo di intervento (ad esempio accesso, rettifica, sospensione dell'uso). L'impostazione è coerente con l'idea che i rimedi siano praticabili solo quando il soggetto destinatario della richiesta sia in grado di agire sul dato e rispondere del trattamento. Tuttavia, già in analisi critiche precedenti alle riforme più recenti si è osservato che questa scelta tende a restringere l'area dei diritti esercitabili e che la distanza tra chi utilizza informazioni e chi controlla tecnicamente la base dati può indebolire la tutela nei trattamenti complessi (Pardieck, 2024).

L'APPI prevede poi una categoria che richiede cautele rafforzate: la *special care-required personal information* (要配慮個人情報, yōhairyo kojin jōhō), spesso assimilabile, per funzione, alla nozione di dato sensibile. Si tratta di informazioni idonee a generare discriminazioni o svantaggi ingiustificati (ad esempio profili sanitari o precedenti), per le quali la disciplina irrigidisce soprattutto alcune condizioni di acquisizione e trattamento (Amended APPI, 2022, art. 2). In questa parte emerge che la legge non si limita a un criterio neutro di identificabilità, ma introduce anche un criterio di contenuto che modula gli obblighi.

Nel sistema definitorio hanno un ruolo crescente le categorie ottenute tramite trasformazione del dato. L'APPI distingue l'*anonymously processed information* (匿名加工情報, tokumei kakō jōhō), progettata per rendere non identificabile l'individuo e impedire il ripristino del dato originario, e la *pseudonymously processed information* (仮名加工情報, kamei kakō jōhō), che mira a ridurre l'identificabilità senza necessariamente eliminarla in modo assoluto, vincolando l'operatore a regole e divieti specifici. In questo punto l'apparato interpretativo dell'autorità di controllo, la *Personal Information Protection Commission* (PPC), è determinante, perché detta requisiti e standard operativi nelle linee guida dedicate (PPC, 2024a).

La scelta di riconoscere categorie processate è comprensibile sotto il profilo del bilanciamento tra tutela e circolazione dei dati, ma non elimina un problema noto in letteratura. Infatti, la stabilità dell'anonimizzazione come garanzia dipende dal contesto e dalla disponibilità di dati esterni con cui effettuare correlazioni. In questo senso, l'argomento di Ohm sul fallimento dell'anonimizzazione come promessa strutturale resta utile per comprendere perché la soglia tra dato personale e non personale sia esposta a

pressioni tecnologiche (Ohm, 2010).

Infine, l'APPI introduce una categoria residuale che intercetta una fascia intermedia particolarmente rilevante nell'economia digitale: la *personal related information* (個人関連情報, kojin kanren jōhō), definita come informazione relativa a una persona vivente che non rientra né nella personal information né nelle categorie processate (Amended APPI, 2022 art. 2). La PPC chiarisce, con esempi, che possono rientrare in questa categoria informazioni come attributi, cronologie di navigazione o dati di localizzazione, se non consentono (nel contesto considerato) l'identificazione dell'individuo (PPC, 2024b).

Il punto più delicato riguarda la circolazione verso terzi. Quando il fornitore mette a disposizione personal related information sapendo o potendo ragionevolmente prevedere che il destinatario la acquisirà come personal data (cioè in forma organizzata e riferibile stabilmente), l'ordinamento introduce obblighi di verifica legati al consenso. In dottrina questa scelta è stata letta come un tentativo di ridurre l'area grigia senza estendere automaticamente l'intero apparato più oneroso dell'APPI a ogni informazione potenzialmente identificativa (Pardieck, 2024).

Possiamo riassumere dicendo che il sistema definitorio dell'APPI funziona come un meccanismo a soglie. L'attivazione della tutela dipende dall'identificabilità, dalla forma organizzativa del trattamento e dal grado di controllo che l'operatore ha sul dato. Nei contesti di intelligenza artificiale questa architettura tende a essere messa sotto pressione perché l'identificabilità e la riferibilità, intesa come possibilità di ricondurre l'informazione a un individuo, non sono proprietà statiche ma risultati di correlazioni e trasformazioni che possono cambiare la qualificazione giuridica dell'informazione nel tempo (Ohm, 2010).

3.3 Trattamento dei dati personali e sistemi di intelligenza artificiale

L’APPI disciplina il trattamento dei dati personali attraverso obblighi che, in astratto, sono pensati per qualunque trattamento organizzato e continuativo. Quando il trattamento avviene mediante sistemi di intelligenza artificiale, la difficoltà non è tanto stabilire *se* la legge si applichi, quanto capire *come* funzioni in concreto, lungo una catena

che tende a includere raccolta massiva, costruzione di dataset (insiemi organizzati di dati), addestramento del modello, riutilizzi successivi e produzione di output informativi. In questo passaggio, due elementi diventano decisivi e allo stesso tempo meno stabili rispetto a trattamenti tradizionali: la possibilità effettiva di ricondurre l'informazione a un individuo e la distribuzione dei ruoli lungo la filiera tecnica, cioè chi decide finalità e mezzi del trattamento e chi invece opera come fornitore o incaricato.

3.3.1 Acquisizione e costruzione dei dataset

Nella logica dell'APPI, i primi vincoli operano già nella fase di acquisizione. La legge impone che la finalità di utilizzo sia specificata e soprattutto che l'uso dei dati resti dentro il perimetro di tale finalità: è un vincolo che, sul piano giuridico, serve a rendere il trattamento riconoscibile e controllabile (Amended APPI, 2022 artt. 17–18). Nei progetti di IA questo punto non si traduce automaticamente in un divieto, ma introduce una frizione strutturale. Questo significa che la raccolta e la preparazione dei dati è spesso orientata al riuso e l'utilità del dataset può essere legata proprio alla possibilità di impiegarlo in fasi o applicazioni ulteriori rispetto a quelle inizialmente previste.

La tensione emerge con particolare chiarezza quando la raccolta avviene su larga scala da fonti online mediante *crawling* o *scraping*, cioè tramite software che visitano pagine web e copiano contenuti in modo sistematico, trasformando informazioni disperse in un archivio ricercabile e riutilizzabile. Il punto non è la consultazione occasionale di informazioni pubblicate in sè, ma l'industrializzazione della raccolta, perché cambia sia la scala sia la funzione dei contenuti raccolti. In una nota di attenzione dedicata ai servizi di IA generativa, la PPC richiama proprio questo rischio: la costruzione del dataset può includere, anche senza accorgersene, categorie che richiedono cautele rafforzate e chiede misure organizzative e tecniche volte a evitare l'inclusione o a rimuovere tali dati prima che entrino stabilmente nel dataset (PPC, 2023a).

Qui diventa centrale la nozione di *yōhairyo kojin jōhō* (要配慮個人情報, "special care-required personal information"), cioè informazioni che, per natura, possono generare discriminazioni o svantaggi ingiustificati e che quindi richiedono cautele più rigide soprattutto sul versante dell'acquisizione (Amended APPI, 2022 art. 20, co. 2). In termini pratici, il problema dell'IA non è solo "se" questi dati compaiano, ma quanto sia realistico

pretendere un controllo assoluto su corpora enormi. È significativo che la ricerca tecnica giapponese abbia iniziato a trattare la questione come un problema operativo: Minamoto, Oda e Kawahara discutono la possibilità che corpora raccolti tramite web crawling per l'addestramento di large language models (LLM, "modelli linguistici di grandi dimensioni") contengano *yōhairyo kojin jōhō* e propongono metodi per rilevarli e filtrarli, proprio perché l'esclusione manuale diventa impraticabile su larga scala (Minamoto et al., 2025).

Questa dinamica è coerente anche con l'impostazione istituzionale. Nelle discussioni governative recenti sul rapporto fra tecnologia, privacy e gestione dei dati, la questione è spesso posta in termini di misure ragionevoli e di governance del rischio, più che come pretesa di controllo totale su ogni singolo elemento informativo (Cabinet Secretariat, 2025). Per l'analisi giuridica, la conseguenza è evidente: la fase di acquisizione non si esaurisce nella raccolta, ma include il modo in cui si seleziona, si pulisce, si documenta e si governa ciò che finisce nel dataset, perché è lì che si costruisce la base materiale dell'addestramento.

3.3.2 Dal dato grezzo al dato trattabile

Nella fase intermedia, tipica dei progetti di IA, l'operatore lavora spesso su dati trasformati per ridurre l'identificabilità. Nell'APPI, *tokumei kakō jōhō*, (anonymously processed information) e *kamei kakō jōhō* (pseudonymously processed information) non sono trattati come stati naturali del dato: sono l'esito di un processo, con requisiti, divieti e vincoli che mirano a evitare un uso meramente dichiarativo dell'etichetta. La PPC, nelle linee guida dedicate, insiste proprio sul fatto che la qualificazione dipende dal rispetto di condizioni tecniche e organizzative e non da una semplice auto attribuzione dell'operatore (PPC, 2024a).

Sul piano operativo, la pseudonimizzazione può ridurre l'esposizione immediata e rendere più gestibile la sperimentazione, ma non elimina il problema del collegamento. Se esiste una chiave o un set di informazioni di contesto che rende possibile la riconduzione all'individuo, la questione torna immediatamente ad essere una questione di governance, cioè chi può ricostruire il legame, con quali controlli e con quali divieti interni di riutilizzo o divulgazione.

Come già richiamato nel Capitolo 1, la letteratura ha mostrato che la promessa di un'anonimizzazione stabile è strutturalmente fragile: la possibilità di re-identificazione dipende dal contesto informativo complessivo e dalla disponibilità di dati esterni. Nei sistemi di IA, in cui dataset e output circolano e si combinano, questa fragilità pesa ancora di più, perché la soglia tra dato personale e non personale può spostarsi nel tempo.

3.3.3 Addestramento e modello

Nell'addestramento, una parte della criticità giuridica riguarda l'oggetto che risulta dal processo. In molti casi, i parametri del modello (重み係数, *omomi keisū*, "pesi") sono valori numerici ottimizzati per produrre determinate uscite e non sono, di per sé, un insieme di record riferiti a una persona. La PPC, in una FAQ specifica, afferma che i parametri generati usando dataset contenenti dati personali non rientrano nella nozione di personal information finché è escluso un rapporto di corrispondenza con individui specifici (PPC, 2022a).

La clausola è importante perché evita una soluzione automatica ("il modello è sempre dato personale" oppure "il modello non lo è mai"), ma sposta il problema sulla verifica concreta dell'esclusione del legame. In termini tecnici, il punto non riguarda solo l'intenzione dell'operatore, ma anche fenomeni come la memorizzazione involontaria. Infatti, un modello può "ricordare" porzioni di dati di addestramento e riprodurle in output quando stimolato in un certo modo. La letteratura di sicurezza ha mostrato, con esempi empirici, che da grandi modelli linguistici può essere possibile estrarre dati di training tramite interrogazioni mirate (Carlini et al., 2021). Questo non implica che ogni modello contenga necessariamente dati personali in forma estraibile, ma rende meno banale il presupposto secondo cui il legame con individui specifici sia "realmente escluso" in qualunque scenario.

Sul piano dell'APPI, resta comunque fermo che l'addestramento è un uso dei dati quando gli input rientrano nelle categorie protette. Di conseguenza, tornano centrali i vincoli di finalità e le regole di acquisizione corretta, perché la liceità del training dipende anche dal modo in cui il dataset è stato costruito, documentato e mantenuto nel tempo (Amended APPI, 2022, art. 17). In altre parole, anche se i pesi non sono qualificati come dato personale, l'intero processo che porta a quei pesi può essere un trattamento rilevante ai

sensi della legge.

3.3.4 Servizi di IA, fornitori esterni e trasferimenti

Nella pratica, molti trattamenti non restano dentro un singolo soggetto. Dataset e modelli sono spesso gestiti tramite piattaforme cloud o servizi di IA offerti come API (Application Programming Interface, cioè interfacce che permettono a un sistema di "chiamare" un servizio esterno per ottenere un risultato). In termini APPI, il nodo è stabilire se il trasferimento di personal data verso un fornitore sia una fornitura a terzi (第三者提供, *daisansha teikyō*) oppure un affidamento/outsourcing (委託, *itaku*).

In generale, l'affidamento è costruito come estensione organizzativa dell'operatore. Il fornitore tratta i dati per conto e non per finalità proprie e proprio per questo la disciplina non lo tratta come terza parte nel senso pieno della regola sulla fornitura (PPC, 2024a). La distinzione, però, diventa fragile nei servizi digitali complessi. Questo dipende da elementi contrattuali e tecnici che l'utente del servizio potrebbe non percepire immediatamente. Il problema non è astratto, se il provider riutilizza gli input dell'utente per finalità autonome (ad esempio miglioramento del servizio o training), l'operazione tende ad assomigliare più a una circolazione verso terzi che a un mero affidamento.

Su questo, una parte della discussione giuridica pratica, in Giappone, ha insistito sul fatto che quando un prompt (cioè il testo o contenuto inserito come input in un sistema di IA generativa) contiene personal data e viene riutilizzato oltre la mera risposta, l'operatore deve interrogarsi sulla disciplina della fornitura a terzi e sulla necessità di assicurare condizioni di liceità e tracciabilità. In parallelo, la PPC ha richiamato l'esigenza di verificare attentamente le condizioni di utilizzo del servizio e le impostazioni rilevanti, proprio perché, in alcuni casi, l'input può entrare in processi ulteriori rispetto alla generazione della risposta (PPC, 2023a).

Quando si rientra nella disciplina della fornitura a terzi, l'APPI richiede regole più strutturate. In via generale: il consenso, eccezioni tipizzate e obblighi di conservazione delle evidenze del trasferimento e della ricezione. Il *record keeping*, in concreto, è l'obbligo di tenere registrazioni del passaggio dei dati (quando, a chi, con quale base), ed è una condizione pratica per rendere verificabile la circolazione (Amended APPI, 2022,

art. 29). La PPC dedica a questi obblighi linee guida specifiche, che chiariscono anche le verifiche richieste in certe catene di trasferimenti (PPC, 2024a).

Un ulteriore livello è quello dei trasferimenti verso l'estero, cioè la fornitura verso "terzi situati in Paesi stranieri" (外国にある第三者への提供, *gaikoku ni aru daisansha e no teikyō*). Nell'uso di servizi cloud e API, la dimensione transfrontaliera non è marginale, perché l'infrastruttura e i soggetti coinvolti possono essere collocati fuori dal Giappone anche quando l'utente finale opera in Giappone. La disciplina richiede cautele informative e condizioni di legittimità specifiche e la PPC ha adottato linee guida dedicate che precisano criteri e verifiche richieste (PPC, 2025). In questo quadro, ridurre la valutazione a "dove si trova il server" è spesso insufficiente. Infatti, ciò che conta è se il soggetto estero sia un destinatario che tratta i dati e con quali garanzie e come tali garanzie siano rese conoscibili e verificabili.

3.3.5 Output e inferenze

Il trattamento mediante IA non si esaurisce nell'uso dei dati in input, produce anche informazione nuova, spesso sotto forma di inferenze, classificazioni o contenuti generati. Questo è un passaggio che mette sotto pressione un impianto normativo centrato sull'identificabilità e sulla gestione del dato, perché l'impatto sui diritti può derivare da ciò che viene dedotto e usato operativamente, anche quando l'informazione iniziale è frammentaria. Come già evidenziato da Wachter e Mittelstadt, questo genera un vero e proprio divario di responsabilità: la disciplina si concentra sul controllo del dato originario, mentre le inferenze ad alto impatto, che producono gli effetti più incisivi sulla persona, restano spesso meno presidiate. (Wachter, Mittelstadt, 2019).

Nel quadro APPI, una risposta settoriale all'IA non esiste, quindi la gestione del rischio passa attraverso strumenti già presenti come limitazione della finalità, misure di sicurezza, controllo della filiera e disciplina dei trasferimenti. Tuttavia, in contesti di IA generativa, l'idea di sicurezza non coincide soltanto con la prevenzione dell'accesso non autorizzato a un database. Include anche il rischio che l'informazione personale emerga in output, oppure venga resa ricostruibile tramite interrogazioni e combinazioni non previste. Il richiamo della PPC ai servizi di AI generativa è indicativo proprio perché collega la gestione del rischio a pratiche concrete (ad esempio l'inserimento di dati personali nei

prompt e la verifica delle condizioni di trattamento lato provider), senza trasformare l'intervento in una regolazione totale della tecnologia (PPC, 2023a).

Possiamo quindi notare che ciò che emerge è che l'APPI riesce a "entrare" nei sistemi di IA, ma lo fa lungo punti che non coincidono perfettamente con la catena tecnica. La tutela non si gioca solo nella fase di raccolta, né solo nella sicurezza classica, ma nella capacità di mantenere controllo su finalità, circolazione e possibilità di ricostruire legami con individui anche quando il sistema produce informazione nuova e potenzialmente sensibile.

3.4 Intelligenza artificiale generativa e problematiche emergenti

L'intelligenza artificiale generativa (生成AI, *seisei AI*) ha reso più visibili alcuni attriti tra categorie dell'APPI e pratiche tecniche, soprattutto perché sposta il punto di contatto con l'informazione personale su più livelli contemporaneamente. Nei servizi basati su grandi modelli linguistici (大規模言語モデル, *daikibo gengo moderu*, spesso indicati come LLM), l'informazione può entrare come dato di addestramento, ma anche come input dell'utente in linguaggio naturale e può riemergere come output testuale. Questa compresenza rende meno pulita la distinzione tra fase di raccolta e fase di utilizzo, che nei trattamenti più tradizionali resta invece più separabile.

3.4.1 Prompt e dati immessi dagli utenti

Una specificità dei servizi generativi è che l'utente tende a immettere contenuti in linguaggio naturale senza sempre percepire che quel testo può contenere dati personali propri o di terzi. Il prompt (プロンプト, puromputo) è l'istruzione o la richiesta che guida la generazione della risposta, ma spesso include frammenti di documenti, descrizioni di casi, informazioni identificative, o dettagli che diventano immediatamente trattamento nel senso dell'APPI.

In questa fase conta molto meno la definizione astratta di dato e molto di più la gestione concreta del flusso. Due termini ricorrono spesso nella documentazione tecnica e contrattuale dei provider e vanno chiariti perché, sul piano giuridico, incidono direttamente sulla qualificazione del rapporto. Il primo è *data retention,* cioè la conservazione dei dati: indica se e per quanto tempo input e output vengono memorizzati dal fornitore del servizio. Il secondo è il *riuso per finalità ulteriori,* ad esempio per

miglioramento del servizio o addestramento di versioni successive. In questi casi non si tratta più soltanto di ottenere una risposta, ma di stabilizzare una traccia di contenuti e metadati che può assumere, in concreto, la forma di un archivio organizzato.

La PPC, nell'avviso del 2023 dedicata ai servizi di AI generativa, ha insistito proprio su questo passaggio pratico. L'indicazione, infatti, non è formulata come divieto generalizzato, ma come richiesta di valutazione: verificare condizioni del servizio, modalità di trattamento del contenuto immesso e rischi specifici legati all'inserimento di informazioni personali, soprattutto quando l'uso avviene in contesti organizzativi (PPC, 2023b; Ushijima & Partners, 2023). Parlando di coerenza con l'impianto dell'APPI, la fragilità non nasce dal fatto che l'input è "testo" anziché "campo" in un form, ma dal fatto che il canale conversazionale facilita l'immissione di informazioni non necessarie e rende più difficile controllare a monte cosa stia realmente entrando nel trattamento.

3.4.2 Dataset di addestramento e filtraggio

Il secondo blocco di criticità riguarda i dataset di addestramento. Nel contesto dei LLM, il web crawling (クローリング, *kuroringu*) indica la raccolta automatizzata su larga scala di contenuti online tramite software che esplora pagine web; lo scraping (スクレイピング, sukureipingu) riguarda invece l'estrazione di informazioni in forma più strutturata. Anche quando le fonti sono pubbliche, la trasformazione in un dataset riutilizzabile cambia la natura del rischio. contenuti dispersi e poco accessibili diventano aggregati, interrogabili e replicabili.

Nel contesto giapponese, questa dinamica è stata trattata in modo esplicito anche in materiali istituzionali. Nei documenti di hearing della PPC del 2024 emerge un punto molto concreto. Su dataset di dimensioni elevate garantire l'esclusione completa di categorie delicate può essere tecnicamente difficile e la difficoltà cresce in presenza di riusi e circolazione dei dati nella catena di sviluppo dei modelli (PPC, 2024b). Il riferimento è particolarmente rilevante perché mostra che l'area grigia non dipende soltanto da interpretazioni elastiche della legge, ma dal rapporto tra categorie giuridiche e capacità tecniche di controllo.

Questa difficoltà diventa più sensibile quando si tratta di *yōhairyo kojin jōhō* (special

care-required personal information). Il punto operativo non è soltanto evitare di raccogliere, ma rendere realistiche procedure di identificazione e filtraggio all'interno di corpora molto grandi. In questo senso, è significativo che una parte della ricerca giapponese si stia muovendo su soluzioni tecniche orientate alla rilevazione automatica di elementi potenzialmente riconducibili a *yōhairyo kojin jōhō* nei corpora destinati al pre-training (事前学習, jizen gakushū), proprio perché controlli manuali risultano impraticabili su scala (Minamoto et al., 2025). Dal punto di vista giuridico, questo rafforza l'idea che la conformità non possa dipendere soltanto dalla provenienza del dato, ma anche dalla capacità organizzativa di controllare cosa viene effettivamente utilizzato per apprendere.

3.4.3 Riemersione in output e rischio di estrazione

Le problematiche emergenti non si fermano all'input né al dataset di addestramento. Un tema distintivo dei modelli generativi è che l'output stesso può diventare vettore di informazione personale. Qui conviene tenere separati due fenomeni che, nella discussione pubblica, vengono spesso confusi.

Il primo riguarda la possibile riproduzione di contenuti presenti nei dati di addestramento o comunque memorizzati dal modello. La letteratura tecnica ha documentato scenari in cui, in condizioni specifiche, è possibile estrarre porzioni dei dati di addestramento interrogando ripetutamente un modello linguistico, soprattutto quando nel training set erano presenti stringhe rare o altamente distintive (Carlini et al., 2021). Per quanto riguarda questa tesi, l'importante non è trasformare questo risultato in una presunzione generale di illecito, ma chiarire perché la clausola esclusione del legame con individui specifici possa diventare un punto fragile se, in concreto, l'informazione personale può riemergere o essere estratta.

Il secondo fenomeno è diverso, l’output può includere informazioni inesatte su persone. Nel contesto dei LLM si parla di "hallucination" (ハルシネーション, *harushineshon*) per indicare la produzione di contenuti plausibili ma non corretti, dovuta al fatto che la generazione avviene in modo probabilistico e non come recupero garantito di un fatto. Quando queste inesattezze riguardano individui, il rischio non è solo tecnico e può diventare reputazionale o decisionale se l'output viene riutilizzato in contesti organizzativi,

come ad esempio per valutazioni, screening o reportistica. Anche qui la PPC, nell'avviso del 2023, richiama la necessità di considerare i rischi legati all'uso dei servizi generativi, includendo la possibilità che output e gestione del servizio generino trattamenti problematici (PPC, 2023b). La differenza rispetto a una classica violazione dei dati personali (accesso o divulgazione non autorizzata) è che anche senza fuga da un archivio si può produrre e diffondere informazione personale non appropriata o non verificata. Tuttavia, è necessario fare un chiarimento sul perimetro APPI rispetto alle hallucinations. L'hallucination, di per sé, non coincide automaticamente con una violazione dell'APPI. La disciplina dei diritti dell'interessato (accesso, correzione, cancellazione/cessazione) è costruita attorno al concetto di *personal data the business holds* (in termini PPC, "retained personal data"), cioè dati personali che il titolare effettivamente detiene e sui quali ha potere di disclosure e rettifica. Ne consegue che, se l'output resta effimero (non viene conservato né riutilizzato) la tutela APPI è meno lineare, perché manca un oggetto stabile su cui esercitare i rimedi tipici. Diversamente, quando l'output viene loggato/storato (come cronologie, audit log, dataset di miglioramento, ticket, note interne) o viene riutilizzato in processi organizzativi, esso entra nel perimetro del dato detenuto. In tal caso l'interessato può chiedere la correzione di contenuti non fattuali e (ricorrendone i presupposti) la cessazione d'uso/cancellazione. Inoltre, se l'output riemerso riflette una perdita di controllo su dati personali (es. leakage di dati contenuti in log o basi documentali), il problema non è solo reputazionale. In questo caso entra in gioco l'obbligo di sicurezza e, nei casi rilevanti, anche report di incidenti di leakage secondo la disciplina dell'APPI.

In Giappone, questa lettura è coerente con la discussione più ampia sulla sicurezza dei sistemi generativi. Una ricognizione in ambito IPSJ (Digital Practice) ricostruisce i principali rischi di sicurezza legati all'IA generativa includendo anche profili di riservatezza e gestione dei contenuti immessi e generati, sottolineando che input e output diventano entrambi superfici rilevanti (PPC, 2023a). In ottica APPI, questo aiuta a spostare la nozione di sicurezza dal solo database al comportamento del sistema e alla governance del flusso.

3.4.4 Integrazione nei processi, prompt injection e RAG

Nei casi d'uso più recenti, l'IA generativa non viene impiegata solo come

interfaccia conversazionale, ma viene integrata in processi aziendali. In questi scenari è comune l'uso di *RAG* (retrieval-augmented generation), una configurazione in cui il modello genera risposte dopo aver recuperato documenti da una base interna (manuali, ticket, knowledge base). In termini più semplici, il modello non sa solo ciò che ha appreso in addestramento, ma viene alimentato al momento della risposta da contenuti recuperati da un archivio.

Questa architettura ha un vantaggio evidente, perché riduce la necessità di addestrare il modello su dati interni. Tuttavia, crea una superficie di rischio specifica. L'input può contenere istruzioni malevole e anche i documenti recuperati possono contenere testo corrotto che induce il sistema a comportamenti non desiderati. La prompt injection (プロンプトインジェクション, puromputo injekushon) indica proprio tecniche in cui l'input viene costruito per aggirare vincoli e istruzioni del sistema, inducendolo a rivelare informazioni o a seguire direttive non autorizzate. Materiali di settore giapponesi hanno iniziato a trattare questo rischio in modo operativo, collegandolo alla necessità di policy interne, limitazioni sugli input e controlli sugli output, soprattutto quando il sistema è collegato a basi documentali o strumenti esterni (JNSA, 2025).

Il punto, in chiave APPI, è che questi scenari non vanno letti solo come risposte sbagliate, ma come un problema di sicurezza e controllo degli accessi lungo la catena di trattamento. In un'architettura RAG il modello diventa di fatto un'interfaccia verso un archivio interno (manuali, ticket, knowledge base). Se un input malevolo (oppure un testo inquinato contenuto nei documenti recuperati) riesce a piegare le istruzioni del sistema, l'effetto pratico può essere l'estrazione e la divulgazione di dati che l'utente non dovrebbe vedere. In questa prospettiva, il rischio si collega direttamente agli obblighi di predisporre misure appropriate per prevenire accessi non autorizzati e dispersioni informative, perché la superficie di attacco non è più solo il database ma l'intero flusso input–retrieval–output e le integrazioni con strumenti esterni. Inoltre, quando l'output finisce per comunicare dati personali a soggetti che non sono legittimati a riceverli il problema smette di essere soltanto tecnico diventando una questione di circolazione non corretta dell'informazione e di tracciabilità delle responsabilità nella filiera (chi decide le regole di accesso, chi gestisce l'archivio, chi gestisce il servizio), cioè esattamente il tipo di criticità organizzativa che l'APPI tende a far emergere nei trattamenti complessi.

Il fulcro per questa tesi è che questi rischi non sono risolvibili solo con una lettura testuale dell'APPI. La disciplina offre strumenti di base, ma l'effettività dipende dalla governance: chi può usare il sistema, con quali permessi, quali dati possono essere immessi, quali log vengono conservati, quali controlli sono applicati prima che l'output venga riutilizzato. In questo senso, le linee guida METI sugli operatori dell'IA sono utili come quadro di responsabilità distribuita lungo la catena di sviluppo, fornitura e utilizzo, includendo attenzione a dati e sicurezza (METI, 2025). L'IA generativa rende più evidente che i presìdi non possono essere collocati solo a monte né solo a valle. Devono seguire il ciclo concreto, perché l'informazione personale può entrare e uscire in più punti, spesso con tempi e modalità difficili da ricostruire a posteriori.

3.5 Adeguatezza dell'APPI rispetto allo sviluppo tecnologico

La questione centrale è se l'APPI riesca a garantire una protezione effettiva quando il trattamento non riguarda più soltanto la raccolta e la gestione di informazioni registrate, ma è inserito in architetture data-driven in cui il valore informativo nasce da correlazioni e inferenze. Una valutazione netta, che sia positiva o negativa, rischia di essere fuorviante. Da un lato, l'APPI mostra una capacità di adattamento concreta, perché combina una legge generale con un apparato interpretativo aggiornabile e con interventi istituzionali che nel tempo hanno introdotto categorie e regole pensate per contesti tecnologici più complessi. Rimangono tuttavia attriti strutturali. Due aspetti rendono la disciplina fragile: primo, il perimetro applicativo si costruisce attorno all'identificabilità; secondo, nei sistemi contemporanei l'impatto spesso deriva da inferenze e output, non da dati identificativi classici.

3.5.1 Profili di tenuta

Un primo profilo di tenuta è la natura stratificata della disciplina. L'APPI non opera soltanto attraverso la formulazione legislativa, ma anche tramite linee guida che trasformano enunciati generali in criteri applicativi, collegando la legge a pratiche che evolvono più rapidamente del ciclo legislativo (PPC, 2024a). In questo senso, il ruolo della PPC non è solo quello di intervenire a posteriori, ma anche di stabilizzare interpretazioni operative, con effetti diretti sulla conformità delle organizzazioni.

Questa architettura consente anche interventi mirati quando emergono usi nuovi.

L’attenzione della PPC del 2023 sui servizi di AI generativa è significativa perché traduce in indicazioni concrete alcuni rischi che nella pratica dipendono dalla gestione degli input utente, dalla conservazione dei contenuti e dalle modalità di riuso dei dati in funzione di miglioramento del servizio (PPC, 2023a). In questo caso, l’importante è sottolineare che l’adattamento nel modello giapponese passa spesso da chiarimenti amministrativi e da standard interpretativi.

Un secondo profilo di tenuta riguarda la convergenza, almeno parziale, tra l’APPI e la più ampia logica di governance del rischio che caratterizza l’approccio giapponese all’IA. Le linee guida METI sugli AI business operators insistono sulla gestione dei rischi lungo la catena di sviluppo, fornitura e utilizzo, includendo profili legati a dati e sicurezza tra gli snodi che richiedono presìdi organizzativi (METI, 2025). Ciò aiuta a leggere l’APPI come parte di un’architettura di responsabilità distribuita, soprattutto quando sviluppatore, fornitore e utilizzatore non coincidono.

3.5.2 Profili di attrito

Il punto più delicato resta la costruzione delle soglie. L’APPI aggancia l’attivazione di molte regole alla possibilità di identificare una persona, anche attraverso il facile confronto con altre informazioni. In contesti ad alta densità informativa questa soglia tende a muoversi. Quello che appare non identificativo in un dataset isolato può diventarlo quando è combinato con archivi terzi, identificatori persistenti o capacità di correlazione più avanzate.

Takagi ha mostrato come questa instabilità non sia solo un dettaglio tecnico, ma condizioni la portata reale della tutela, perché alcuni danni maturano prima che si arrivi alla piena nominalizzazione del soggetto (Takagi, 2022). Nel contesto IA, il rilievo aumenta perché molte decisioni ad impatto individuale sono guidate da output modellistici e profili inferenziali, invece che da record identificativi tradizionali.

La letteratura internazionale ha reso questa tensione particolarmente visibile parlando di accountability gap legato alle inferenze ad alto impatto. Il punto centrale è un divario di responsabilità e controllabilità. La protezione centrata sul dato originario e sull’accesso al record fatica quando ciò che incide sulla persona è la deduzione prodotta e usata operativamente, spesso con bassa verificabilità esterna (Wachter, Mittelstadt, 2019). Nel

quadro APPI questo non equivale a dire che manchi una disciplina, ma segnala che gli strumenti classici rischiano di intercettare solo una parte dell'effetto individualizzante.

In questa direzione si colloca anche la categoria di kojin kanren jōhō, introdotta con la riforma del 2020 e resa pienamente applicabile con l'entrata in vigore del 1° aprile 2022, con una disciplina specifica per la sua fornitura a terzi quando è prevedibile che diventi dato personale presso il destinatario (PPC, 2020; PPC, 2022b). L'intento è ridurre un'area grigia tipica dei mercati dei dati, pur senza estendere automaticamente l'intero apparato più oneroso. Resta però uno spazio di incertezza quando la trasformazione da segnale a profilo avviene lungo catene di trattamento che l'interessato non riesce a percepire o controllare.

3.5.3 Nodi critici di effettività

Una valutazione di adeguatezza non può fermarsi alle definizioni. In sistemi complessi, ciò che conta è anche la possibilità di individuare il punto di controllo e rendere effettivi rimedi e deterrenza.

La prima fragilità riguarda la frammentazione del controllo decisionale. Quando dataset, modelli e servizi sono distribuiti lungo catene tecniche, capire chi detiene la leva per intervenire diventa cruciale. Una parte dei diritti dell'interessato è pensata per contesti in cui l'operatore gestisce direttamente il dato. Quando il trattamento si sposta verso asset modellistici mediati da cloud e API, l'esercizio di quei diritti può scontrarsi con opacità contrattuali e tecniche. La disciplina sulla third-party provision resta un presidio, ma la sua efficacia dipende dalla tracciabilità reale lungo la catena e non dalla sola costruzione formale dell'adempimento.

La seconda fragilità riguarda l'enforcement e la percezione del rischio di non conformità. La revisione periodica prevista dalla riforma del 2020 ha progressivamente spostato l'attenzione su strumenti idonei a rafforzare l'effettività, includendo ipotesi come sanzioni amministrative più robuste, tra cui la discussione su un meccanismo di kachōkin, (課徴金, penalty surcharge) e su opzioni di tutela collettiva o inibitoria, anche se non tutte le ipotesi sono state trattate allo stesso modo nelle diverse fasi del dibattito (PPC, 2025).

Il documento più recente, del 9 gennaio 2026, conferma l'orientamento verso un rafforzamento selettivo della disciplina e collega il percorso di riforma al tema dell'effettività, includendo interventi su obblighi e strumenti di correzione postumi, oltre che su aree considerate a rischio (PPC, 2026). Questo elemento istituzionale è utile perché rafforza l'idea che l'adeguatezza dell'APPI sia una questione dinamica. Non riguarda solo il testo vigente, ma la capacità del sistema di aggiornare gli strumenti quando cambiano incentivi, prassi e architetture tecniche.

Accanto alla documentazione istituzionale, una parte del dibattito giuridico ha incardinato la revisione anche su questioni più teoriche con delle ricadute pratiche. I report JILIS, ad esempio, sistematizzano le linee di discussione e mettono in evidenza come la scelta degli strumenti di enforcement non sia neutra rispetto alla funzione complessiva della disciplina, soprattutto nel bilanciamento tra tutela individuale e data use (Chambers, 2025).

In conclusione, l'APPI appare adeguata solo in senso condizionato: offre un quadro generale sufficientemente flessibile per ricomprendere molti trattamenti di IA, ma resta strutturalmente esposto a zone grigie quando il rischio per i diritti deriva da inferenze, dati derivati e output generati lungo filiere distribuite. La tensione tra tutela individuale e utilità del dato, già iscritta nell'articolo 1, emerge con particolare evidenza nei sistemi di IA generativa e nei modelli di governance light-touch ricostruiti nel Capitolo 2. Su queste premesse, il Capitolo 4 analizzerà in modo sistematico le ambiguità e le criticità della regolamentazione giapponese, mostrando come tali zone grigie si traducano in problemi di enforcement, lacune normative e tensioni con la competitività economic

CAPITOLO 4 – ZONE GRIGIE E CRITICITÀ DELLA REGOLAMENTAZIONE GIAPPONESE

Nei capitoli precedenti è emersa la struttura del modello giapponese: una hard law centrata sull'APPI e parallelamente una governance dell'IA costruita attraverso soft law aggiornabile. Questa architettura light-touch risponde a una scelta di policy esplicita che mira a mantenere flessibilità regolatoria per accompagnare l'innovazione. Il presente capitolo cambia prospettiva. Dopo aver descritto il modello, lo si vuole mettere alla prova verificando come regge quando applicato agli ecosistemi informativi reali dell'IA contemporanea come produzione massiva di inferenze e profili, combinazione di basi dati eterogenee, catene tecniche frammentate e spesso transnazionali. In questi contesti la protezione dell'APPI tende a diventare meno prevedibile e più dipendente da scelte tecniche e organizzative degli operatori. Inoltre, l'allocazione delle responsabilità lungo la filiera non è sempre determinata in modo sufficientemente preciso dal diritto positivo, creando ulteriori ambiguità e criticità (Pardieck, 2024).

L'esplosione dell'IA generativa ha reso queste frizioni immediate e non più trattabili come casi marginali. All'inizio di giugno 2023, la PPC è intervenuta con un alert pubblico sull'uso dei servizi di IA generativa e, nello stesso contesto, ha pubblicato l'outline della guidance amministrativa indirizzata a OpenAI ai sensi dell'art. 147 APPI (PPC, 2023a; PPC, 2023b). Questi interventi segnalano un cambio di fase. l'IA passa da tema ad un oggetto centrale della regolazione della protezione dati. I paragrafi seguenti ricostruiscono come le categorie dell'APPI diventano contingenti nei sistemi di IA contemporanea, come questa contingenza si manifesta nei limiti di enforcement e quale ruolo gioca la soft law nell'adattamento normativo.

4.1 Zone grigie concettuali e applicative

4.1.1 Identificabilità mobile

L'APPI lega l'applicazione della disciplina all'identificabilità della persona, includendo anche l'identificazione indiretta tramite 'easy collation' con altre informazioni (APPI, art. 2). Il punto decisivo è che questa valutazione non è astratta, ma dipende dai mezzi concretamente disponibili e dalle possibilità concrete di collegamento. In un contesto IA questa impostazione introduce un'instabilità strutturale. La soglia di identificabilità è mobile, variando al variare di (a) accesso a dataset ausiliari, (b) capacità

computazionali di correlazione, (c) architettura del sistema e scelte di retention/logging (PPC, 2023a).

Primo, la disponibilità di dataset ausiliari e la data economy rendono il collegamento tra basi dati una risorsa ordinaria. Ciò che oggi appare non identificativo può diventare identificabile domani, non per mutamento dei dati in sé, ma per mutamento del contesto (nuove partnership, interoperabilità crescente). Come evidenziato nella letteratura sulla re-identificazione, l'evoluzione dell'ecosistema informativo rende instabili le garanzie dell'anonimizzazione, poiché la possibilità di collegare dataset precedentemente separati aumenta progressivamente (Sweeney, 2015). Secondo, l'evoluzione di strumenti di entity resolution e re-identificazione abbassa i costi tecnici dell'associazione. La facile collazione diventa concretamente praticabile anche per operatori che prima ne erano privi. Terzo, in sistemi IA l'identificazione può avvenire tramite inferenze. Dati come profili comportamentali, rappresentazioni interne del modello e punteggi predittivi fungono da quasi-identificatori quando collegati stabilmente a un individuo nel servizio.

Questa mobilità produce due conseguenze rilevanti. Sul piano dell'osservanza della norma, l'operatore deve compiere valutazioni conservative, ma non sempre dispone di standard tecnici pubblici che guidino l'interpretazione. Sul piano della tutela, si crea un'asimmetria informativa. L'operatore conosce la propria capacità di collegamento dati e i propri dataset, mentre l'interessato difficilmente può dimostrare che un'informazione sia in realtà identificabile nel contesto concreto. Come nota Ohm nella sua analisi critica dell'anonimizzazione, la prova della possibilità di identificazione rischia di restare nella disponibilità del soggetto regolato (Ohm, 2010). In ecosistemi complessi, questo diventa un ostacolo strutturale all'effettività della tutela.

4.1.2 Nuovi oggetti dell'IA

L'IA contemporanea produce oggetti informativi che non coincidono con record statici. Quattro classi sono particolarmente rilevanti:

(a) Output inferenziali (scoring, ranking, predizioni). Lo scoring predittivo è un valore derivato dal modello, non un dato raccolto. Dal punto di vista sostanziale può incidere più di un dato nominativo, perché orienta decisioni ad alto impatto (come potrebbero essere assunzione, credito o accesso a servizi). Il problema giuridico è duplice. Stabilire quando rientrino in personal information/personal data e stabilire se rientrino nei retained

personal data che consentono l'esercizio pieno dei diritti (PPC, 2024a). Se lo score non è conservato, o è conservato in modo non riconducibile all'interessato, il diritto resta teorico. Inoltre, la correzione incontra un ostacolo qualitativo poiché correggere uno score non equivale a correggere un dato errato. Questo richiede intervenire sulla logica del modello, sui dati di addestramento o sui parametri, degli elementi spesso opachi o proprietari. Come evidenziato da Wachter e Mittelstadt nella loro proposta di un "diritto alle inferenze ragionevoli", le inferenze generate da sistemi di IA generano un "accountability gap" poiché l'impatto sui diritti non si esaurisce nei dati originari, ma dipende dalle inferenze prodotte e usate operativamente (Wachter, Mittelstadt, 2019).

(b) Profili e rappresentazioni interne (embedding, vettori). Sistemi di raccomandazione rappresentano gli utenti tramite vettori che, pur non contenendo dati nominativi, funzionano come profili completi. L'APPI non disciplina tali rappresentazioni in modo espresso, aprendo una zona grigia: se un vettore è di fatto un profilo associato stabilmente a un individuo, trattarlo come informazione non personale riduce trasparenza e controllabilità per l'interessato (Häuselmann, Custers, 2024).

(c) Parametri di modelli e memorizzazione. I parametri appresi non sono automaticamente personal information se non esiste corrispondenza diretta con individui (PPC, 2022). Tuttavia, la letteratura su estrazione e memorization mostra che un modello può riprodurre porzioni del training set. Carlini et al. hanno dimostrato empiricamente che "da grandi modelli linguistici è possibile estrarre informazioni personali contenute nei dati di addestramento tramite interrogazioni mirate, inclusi nomi, numeri di telefono e indirizzi email" (Carlini et al., 2021, p. 2637). La linea tra parametri non personali e parametri da cui è possibile ricostruire informazioni personali può dipendere da capacità tecniche e attacchi disponibili. Ne discende una tensione. L'APPI tende a evitare qualificazioni automatiche per non bloccare l'innovazione, ma così sposta la tutela su scelte tecniche (come testing, filtraggio, minimizzazione, sicurezza) che non sempre sono tipizzate o verificabili dall'esterno.

(d) Output generativi e rischi di disclosure e inesattezza. Nei servizi generativi l'output può veicolare personal information in due modalità: riproduzione di informazioni dal training (disclosure) e generazione di contenuti plausibili, ma inesatti su individui reali. Quest'ultima ipotesi è delicata per l'APPI, perché l'informazione nasce da generazione probabilistica, spesso non persistente e la linea tra output effimero e conservato (log,

conversation history) diventa decisiva per stabilire se si attivino diritti azionabili (Kakinuma, 2023). L'alert della PPC del giugno 2023 richiama proprio questo rischio, evidenziando la necessità di verificare se l'input contenente dati personali viene riutilizzato oltre la mera generazione della risposta (PPC, 2023a).

L'IA produce quindi oggetti informativi che complicano l'applicazione di categorie costruite su dati statici. La qualificazione giuridica tende a diventare caso-specifica, dipendente da retention, collegabilità e architettura del servizio. Questo aumenta l'incertezza a posteriori e riduce la visibilità dell'interessato su ciò che esiste davvero nel perimetro del titolare (Pardieck, 2024).

4.1.3 Personal related information e filiere di data brokerage

Il legislatore giapponese ha riconosciuto che lungo la filiera la natura di un'informazione può cambiare. Ciò che per un soggetto non è personal information può diventarlo per un altro che possiede le chiavi di collegamento. La categoria di personal related information nasce per catturare i flussi della data economy (identificatori online, cookie, advertising ID, segmenti) (PPC, 2024a). Sul piano sistematico, evidenzia che la tutela non può dipendere solo dall'esistenza di un nome. la riconducibilità a una persona può essere mediata da un ecosistema di dati e capacità di collegamento (PPC, 2023).

Tuttavia, questa soluzione non elimina la zona grigia. In primo luogo, la transizione tra related e personal resta legata a valutazioni di prevedibilità ("posso ragionevolmente prevedere che diventerà personal data presso terzi") che sono difficili da accertare (Data Guidance, 2021). Secondo, molte catene reali non sono "A trasferisce a B", ma includono piuttosto intermediari, arricchimenti, scoring, riuso. Il trattamento più impattante avviene a valle, dove l'interessato ha minore visibilità. Terzo, la qualificazione non personale a monte può ridurre obblighi di trasparenza proprio nelle fasi in cui i profili vengono costruiti e raffinati.

Ne deriva un rischio tipico. La tutela si concentra sul momento in cui l'informazione è già pienamente personalizzata e usata per decidere, mentre le fasi upstream (profilazione, feature engineering, scoring) rimangono più opache. Il caso Rikunabi, che discuterò più avanti, è emblematico perché mostra come un output inferenziale, pur trattato come non personale in certi segmenti della filiera, diventi pienamente identificativo e decisivo nel punto di applicazione (in questo caso HR) (Miyashita, 2021).

4.1.4 Filiera distribuita, modelli foundation e responsabilità

L'APPI individua nel business operator il baricentro della responsabilità. La legge disciplina trasferimenti a terzi, entrustment e usi condivisi (APPI, 2003, artt. 23, 27). Queste categorie funzionano in filiere relativamente lineari. Le filiere IA contemporanee sono più complesse per almeno tre ragioni.

Primo: Foundation models e API. Un'impresa giapponese può integrare un modello estero via API, con logging lato provider e infrastrutture distribuite. In questa architettura diventa meno chiaro chi sia il soggetto in grado di garantire minimizzazione, limitazione delle finalità, controllo sulla retention, risposte alle richieste di accesso/cancellazione. Anche assumendo che l'utilizzatore resti responsabile verso i propri utenti, la sua capacità di supervisione può essere limitata da opacità tecnica e dipendenza contrattuale (Clifford Chance, 2023; Pardieck, 2024).

Secondo: Catene multi-livello e cloud. La filiera può includere sviluppatori, provider di modelli, SaaS integrator, cloud provider, sub-processor e partner di dataset. La responsabilità si disperde: ogni attore controlla un segmento, mentre nessuno ha una visione completa della filiera. Nessuno è naturalmente in grado di fornire un'informazione esaustiva all'interessato (Horibe, 2025).

Terzo: Transfrontaliero e standard di garanzia. I flussi cross-border sono frequenti con dataset di addestramento, inferenza su server esteri, logging fuori dal Giappone. L'APPI richiede misure appropriate per trasferimenti transfrontalieri, ma nei servizi IA la misura non è solo giuridica (clausole contrattuali), bensì tecnico-organizzativa (audit, controlli su retention, sicurezza, accessi, gestione incidenti, procedure di cancellazione, testing). In assenza di standard dettagliati condivisi, il requisito rischia di trasformarsi in un adempimento formalistico (PPC, 2025).

In termini di tutela, l'effetto complessivo è che l'interessato si trova di fronte a una filiera in cui: (i) non è chiaro a chi rivolgersi; (ii) ogni attore può sostenere di non essere "il" detentore dell'informazione pienamente controllabile; (iii) la ricostruzione della responsabilità richiede conoscenza tecnica e contrattuale che raramente l'interessato possiede. La zona grigia non è solo concettuale. È un problema pratico di accountability. L'APPI offre categorie astrattamente chiare, ma l'IA le rende instabili nell'applicazione. L'identificabilità diventa dipendente dal contesto tecnico e varia nel tempo; gli oggetti informativi centrali (inferenze, profili, output generativi) sfuggono al modello del record

statico; le filiere distribuite riducono la trasparenza; la qualificazione e conservazione come retained personal data finisce per decidere se i diritti restano effettivi o solo teorici. Da questa contingenza si basa il prossimo paragrafo in un quadro segnato da variabili tecniche e catene complesse, dove l'enforcement e i rimedi diventano il banco di prova della tenuta del sistema.

4.2 Problemi di enforcement e limiti applicativi

4.2.1 Poteri della PPC e struttura graduale dell'enforcement

Sul piano formale, l'APPI attribuisce alla PPC un insieme graduato di strumenti: richieste di informazioni e report, ispezioni, guidance e advice, fino a raccomandazioni e ordini, con conseguenze sanzionatorie in caso di inosservanza (APPI, 2003, artt. 40-42). La struttura privilegia la correzione cooperativa e l'adeguamento.

Questa impostazione segue una logica amministrativa: massimizzare l'adeguamento con costi contenuti (Chambers, 2025). Tuttavia, in materia di IA produce un effetto collaterale importante. Quando l'incertezza qualificatoria e la complessità tecnica sono parte del rischio, la prevalenza di interventi non coercitivi può ridurre la capacità del sistema di produrre standard chiari e replicabili. Chiudere il singolo caso non è sufficiente, occorre stabilizzare le interpretazioni su questioni ricorrenti (ad esempio profilazione inferenziale, uso di personal related information, responsabilità in filiere API-based, retention e diritti su output generativi). In contesti caratterizzati da ambiguità concettuale, l'assenza di flussi costanti di decisioni pubbliche robuste mantiene ampie aree grigie, con un effetto di deterrenza ridotto (Pardieck, 2024).

I dati di attività della PPC illustrano come l'enforcement si distribuisce concretamente. Nell'anno fiscale 2024 la PPC ha gestito un volume molto elevato di report e attività correlate agli incidenti di leakage e alle verifiche connesse. Nello specifico, secondo quanto riportato dal Japan Times sulla base del rapporto annuale della PPC, sono stati elaborati oltre 19.000 report di data breach direttamente dalla PPC, con un volume complessivo superiore ai 21.000 casi includendo le segnalazioni tramite canali amministrativi (Japan Times, 2025). Nel medesimo periodo sono stati emessi 148 report-collection orders, condotte 47 ispezioni, fornite 395 guidance/advice, rilasciata 1 raccomandazione e 0 ordini coercitivi (Chambers, 2025).

Il dato strutturale rilevante è che una parte significativa delle risorse dell'autorità è

assorbita dalla gestione amministrativa di report, consultazioni e attività correttive ordinarie. Ciò lascia meno spazio per produrre attraverso enforcement forte una standardizzazione ripetuta su questioni IA complesse. In ambiti in cui la tutela dipende da variabili tecniche come dataset, collegamento dati, logging, test di sicurezza e filtri su prompt, l'assenza di un flusso costante di decisioni pubbliche robuste mantiene ampie aree grigie (Private AI, 2025).

4.2.2 Tre limiti applicativi ricorrenti

Tre ostacoli tendono a ripresentarsi e sono direttamente collegati alle ambiguità discusse nel paragrafo precedente. Primo: l'onere di ricostruzione tecnica. Molte condotte problematiche in materia di IA non sono immediatamente osservabili, ma dipendono da come vengono collegati dataset, quali log sono conservati, quali filtri impediscono l'ingresso di dati sensibili, come si gestiscono conservazione e riuso per training. L'asimmetria informativa diventa un ostacolo operativo dove l'autorità può intervenire, ma spesso deve ricostruire a posteriori processi tecnici complessi. L'interessato, a maggior ragione, fatica a provare che un trattamento lo riguarda o a localizzare dove l'informazione esiste (Ohm, 2010).

Secondo: frammentazione e scarico di responsabilità nella filiera. In catene multi-attore ogni soggetto controlla un pezzo della pipeline. Questo aumenta il rischio che nessuno risponda pienamente alla richiesta dell'interessato. Il titolare a valle può affermare di non conoscere la logica del modello, il provider può affermare di non identificare l'interessato. L'integratore può affermare di non controllare retention o training. La conseguenza è un deficit di accountability che non dipende dalla mancanza di norme, ma dalla difficoltà di applicarle a catene in cui controllo e conoscenza sono distribuiti (Clifford Chance, 2023; Pardieck, 2024).

Terzo: prevalenza di strumenti non vincolanti e lenta produzione di standard. Q&A, alert e linee guida sono utili per adattarsi rapidamente. Tuttavia, difficilmente sostituiscono la funzione disciplinante di un corpus di decisioni coercitive ripetute su questioni ricorrenti. In un sistema che dichiara la soft law come architrave della governance, questo è un effetto prevedibile. La riduzione dell'incertezza diventa un processo progressivo e settoriale, non sempre omogenea (Yamamoto, 2020).

4.2.3 Il caso Rikunabi

Nei casi in cui l'IA emerge come oggetto regolatorio, la PPC tende a intervenire per via indiretta, riportando la questione dentro obblighi generali dell'APPI (finalità, correttezza del trasferimento, sicurezza, informative), più che colpendo direttamente l'elemento IA che genera il rischio.

Il caso Rikunabi (Recruit Career) rappresenta un esempio paradigmatico di profiling inferenziale ad alto impatto nel contesto occupazionale. Tra marzo 2018 e febbraio 2019, Recruit Career, operatore di una delle principali piattaforme giapponesi di job matching per neolaureati Rikunabi, ha sviluppato e commercializzato un servizio destinato a calcolare e vendere alle aziende clienti score predittivi sulla probabilità che ciascun candidato rifiutasse un'offerta di lavoro (Mainichi, 2019). Il caso si presenta come particolarmente rilevante perché Rikunabi domina il mercato giapponese del reclutamento universitario, con oltre 800.000 studenti registrati annualmente e una penetrazione superiore al 90% tra i candidati. La grandezza della base utenti rendeva il sistema di scoring estremamente influente sui futuri professionali dei giovani in cerca di un primo impiego.

L'architettura del servizio, denominato "Rikunabi DMP Follow", si articolava su tre attori principali: Recruit Career come gestore della piattaforma, Recruit Communications come società affiliata incaricata del calcolo degli score e 34 aziende clienti che acquistavano i profili predittivi. Il meccanismo era stato progettato con una struttura complessa che formalmente mirava ad aggirare gli obblighi di consenso previsti dall'Articolo 23 dell'APPI attraverso uno schema che gli studiosi e la Personal Information Protection Commission hanno qualificato come data laundering, ovvero un processo di trasformazione e circolazione dei dati volto a eludere le tutele normative pur mantenendo l'apparenza di conformità.

Il funzionamento del sistema era sofisticato e si basava su un doppio binario di raccolta e integrazione di informazioni. Da un lato, Recruit Career raccoglieva attraverso la piattaforma Rikunabi dati anagrafici degli utenti come nome, indirizzo email, università e facoltà di appartenenza, ma soprattutto una ricca mole di dati comportamentali generati dall'uso della piattaforma come cronologie di navigazione, le ricerche effettuate, aziende visualizzate, settori di interesse espressi, candidature inviate e precedenti rifiuti di offerte.

Tutte queste informazioni venivano associate a un identificatore univoco, il Rikunabi cookie ID, che consentiva di tracciare il comportamento degli utenti nel tempo e ricostruire profili dettagliati delle loro preferenze e strategie di ricerca.

Parallelamente, ciascuna azienda cliente raccoglieva autonomamente dati dei candidati nei propri sistemi informatici, assegnando a ogni persona un applicant ID univoco collegato a un Employer cookie ID. Per mettere in comunicazione i due dataset, le aziende invitavano i candidati a compilare un questionario web apparentemente neutro, attraverso il quale Recruit Communications raccoglieva direttamente gli Employer cookie ID e gli applicant ID, creando il ponte tecnico necessario per il successivo collegamento dei profili. A questo punto, Recruit Career trasferiva a Recruit Communications la cronologia di navigazione e i dati comportamentali degli utenti collegati ai Rikunabi cookie ID, ma volutamente privi di nomi e altri identificatori diretti che avrebbero consentito un'identificazione immediata. Questo passaggio era il cuore dello schema di pseudo-anonimizzazione. In questo modo, formalmente, Recruit Communications riceveva solo dati collegati a cookie, non a persone identificate.

La fase successiva prevedeva l'uso di tecniche di sincronizzazione cookie, mediante le quali Recruit Communications collegava i cookie Rikunabi con i cookie delle aziende, costruendo un database integrato che, pur non contenendo identificatori nominativi diretti nel proprio perimetro, consentiva comunque di isolare profili individuali stabili. Su questa base venivano addestrati modelli predittivi di machine learning, confrontando i comportamenti di candidati che nell'anno precedente avevano accettato o rifiutato offerte di lavoro. Per ciascun candidato il sistema generava uno score numerico compreso tra 0,0 e 1,0, che esprimeva la probabilità stimata di rifiuto dell'offerta, il quale successivamente veniva tradotto in una classificazione a stelle da una a cinque secondo le esigenze del cliente. Gli score venivano quindi riconsegnati alle aziende clienti associati agli applicant ID e, poiché ciascuna azienda disponeva di un proprio database interno che collegava applicant ID a identità reali, poteva immediatamente ricondurre i punteggi ai nomi dei candidati e utilizzarli operativamente nelle decisioni di selezione con estrema facilità.

Il servizio fu venduto a trentotto aziende di cui trentaquattro effettivamente utilizzarono i dati, tra cui grandi gruppi industriali come Honda, Toyota, Mitsubishi Electric, YKK, Aflac Life Insurance e Resona Holdings. Il valore commerciale complessivo

dell'operazione ammontava ad almeno 130 milioni di yen. Nel complesso furono calcolati score per 95.590 utenti, di cui 26.060 non avevano fornito un consenso valido al trasferimento dei propri dati.

Dal punto di vista giuridico, lo schema si fondava su una lettura formalistica dell'APPI. Secondo la disciplina giapponese, i cookie o identificatori generati da macchine non sono considerati dati personali se l'operatore che li tratta non può agevolmente collegarli ad altri dataset per identificare una persona nel corso ordinario della propria attività. Recruit Communications, ricevendo solo dati scollegati da nomi e identificatori diretti, non era formalmente in grado di identificare individui autonomamente e quindi, secondo una lettura strettamente letterale, non trattava tecnicamente dati personali ai sensi dell'APPI. Tuttavia, l'architettura complessiva era stata progettata sapendo che le aziende clienti avrebbero potuto facilmente reidentificare i candidati combinando gli score con i propri database interni. Questo configurava, secondo la ricostruzione della PPC, uno schema progettato deliberatamente per aggirare l'obbligo di consenso previsto dall'Articolo 23, sfruttando le zone grigie definitorie della legge.

L'indagine della PPC fu avviata nel luglio 2019, dopo che agenzie stampa rivelarono l'esistenza del servizio. Il 26 agosto 2019 l'autorità emise un'ammonizione amministrativa nei confronti di Recruit Career, accertando la violazione dell'Articolo 23, paragrafo 1, relativo alla fornitura a terzi senza consenso e dell'Articolo 20, per mancanza di adeguate misure di sicurezza sia in fase di progettazione del servizio sia nella gestione della privacy policy. Secondo quanto riportato da Miyashita nella ricostruzione del caso, la PPC concluse che l'operazione configurava servizi estremamente inappropriati, che eludevano lo spirito della legge, pur riconoscendo implicitamente che, dal punto di vista formale, l'architettura era stata costruita proprio per sfruttare le ambiguità normative (Miyashita, 2021).

L'intervento si concentrò su tre profili critici. Il primo riguardava difetti nelle misure di sicurezza in fase di progettazione. Il servizio era stato lanciato come attività di ricerca e sviluppo, con insufficiente coordinamento tra il dipartimento legale della controllata Recruit Career e quello della capogruppo Recruit Holdings senza un'adeguata verifica preventiva di conformità. Il secondo profilo riguardava la gestione della privacy policy. Nel marzo 2019, Recruit Career aveva tentato di aggiornare la privacy policy per fare

riferimento esplicitamente al servizio "Rikunabi DMP Follow", ma l'aggiornamento non fu correttamente implementato su tutte le schermate e sezioni del sito, risultando in un flusso di consenso inadeguato e incoerente che lasciava molti utenti all'oscuro delle reali finalità del trattamento. Infine, il terzo profilo riguardava la mancanza di consenso valido per 7.983 utenti. La privacy policy originaria conteneva solo una formulazione generica e vaga sull'analisi dei cookie e sulla fornitura di informazioni a clienti per attività di reclutamento ottimali, senza menzionare esplicitamente il calcolo di score predittivi né la loro vendita a terze parti.

Il 6 settembre 2019 anche il Tokyo Labour Bureau, organo del Ministero del Lavoro, emise un ammonimento separato basato sull'Employment Security Act, rilevando che la condivisione di informazioni personali violava l'obbligo di neutralità e correttezza imposto agli intermediari nei processi di collocamento, poiché favoriva unilateralmente gli interessi delle aziende a scapito di quelli dei candidati, distorcendo il mercato del lavoro e pregiudicando le pari opportunità di accesso.

Pur significativo sotto il profilo del messaggio regolatorio e della deterrenza, l'intervento della PPC ha lasciato aperte questioni fondamentali. L'autorità si è concentrata su profili procedurali e di correttezza formale quali consenso, trasparenza informativa, sicurezza organizzativa e disciplina dei trasferimenti a terzi, ma senza affrontare in modo sistematico le dimensioni del profiling algoritmico. Restano infatti irrisolte questioni strutturali: in che misura l'APPI così applicato produca obblighi standardizzabili specifici su profiling e scoring, come trasparenza sugli score e sui criteri di calcolo, diritti di contestazione e rettifica, auditing, riduzione dei bias, doveri di spiegazione. Come osservato da Takagi, queste dimensioni restano in larga parte affidate a prassi e linee guida non vincolanti, evidenziando come l'APPI possa produrre compliance procedurale senza tutela sostanziale, soprattutto quando l'impatto sui diritti deriva non dal dato identificativo originario, ma da inferenze la cui disciplina resta ai margini della norma vincolante (Takagi, 2020).

4.2.4 Il caso OpenAI

Nel giugno 2023, la Personal Information Protection Commission ha compiuto un passo senza precedenti nella regolazione dell'intelligenza artificiale generativa,

emettendo una guidance amministrativa ai sensi dell'Articolo 147 dell'APPI nei confronti di OpenAI e OpenAI OpCo, gli sviluppatori e fornitori di ChatGPT (PPC, 2023b). L'intervento arrivava in un contesto di crescente preoccupazione globale sui rischi connessi ai servizi di IA generativa, pochi mesi dopo il blocco temporaneo di ChatGPT in Italia da parte del Garante per la protezione dei dati personali e in coincidenza con il G7 di Hiroshima, dove il Giappone aveva assunto un ruolo guida nella promozione di un quadro internazionale di governance dell'IA. Il mercato giapponese rappresentava la terza fonte di traffico globale per OpenAI, con una penetrazione significativa tra utenti individuali, aziende e istituzioni pubbliche (Reuters, 2023).

Le linee guida della PPC si concentravano su due preoccupazioni principali. La prima riguardava OpenAI come fornitore del servizio. Infatti, l'autorità richiedeva che l'azienda adottasse le misure necessarie per assicurarsi di non raccogliere informazioni personali sensibili definite dall'APPI come informazioni relative a razza, credo religioso, stato sociale, storia medica e precedenti penali per finalità di machine learning senza il consenso degli interessati. Qualora tali informazioni fossero state raccolte, OpenAI era tenuta a eliminarle il prima possibile, e comunque prima che venissero processate e integrate nei dataset destinati all'addestramento dei modelli. La PPC richiedeva inoltre che la finalità di utilizzo delle informazioni personali rimanesse entro i limiti di quanto notificato agli interessati o reso pubblico (Atsumi, Sakai, 2023).

La seconda preoccupazione riguardava gli operatori economici giapponesi, le agenzie governative e gli utenti generali che utilizzavano servizi di IA generativa. La PPC sottolineava il rischio che l'inserimento di informazioni personali nei prompt potesse configurare un trattamento ulteriore rispetto alla mera generazione della risposta, soprattutto quando il fornitore riutilizzava tali input per finalità di addestramento o miglioramento del modello. Quando l'uso eccedeva la finalità originaria specificata agli interessati e avveniva senza consenso preventivo, si configurava una violazione dell'Articolo 18 dell'APPI, il quale limita il trattamento dei dati personali allo scopo necessario per il perseguimento della finalità dichiarata. L'autorità avvertiva quindi gli operatori della necessità di verificare attentamente le condizioni d'uso e le impostazioni dei servizi, assicurandosi che i dati personali inseriti non venissero utilizzati per machine learning e sottolineava anche che la responsabilità della conformità all'APPI restava in

capo agli operatori economici, non potendo essere delegata al provider estero (National Law Review, 2023).

L'intervento della PPC, pur qualificandosi formalmente come linea guida e non come sanzione vincolante, aveva una portata regolatoria significativa. La Commissione riservava esplicitamente la possibilità di adottare ulteriori misure qualora emergessero nuove preoccupazioni o mancanze nella risposta di OpenAI, lasciando aperta la porta a ispezioni on-site o, in caso di inadempimento persistente, all'imposizione di sanzioni pecuniarie previste dall'APPI (Yomiuri, 2023).

Tuttavia, l'effettività concreta della tutela dipendeva da configurazioni tecniche e organizzative che non erano tipizzate in modo puntuale dalla legge e che risultavano difficilmente verificabili quando l'infrastruttura era globale e la filiera tecnica non pienamente ispezionabile localmente. Restavano aperte diverse questioni operative che delineano con precisione le zone grigie del sistema. La prima riguardava i filtri di raccolta. Come poteva OpenAI garantire, su dataset costruiti tramite web crawling o scraping massivo di contenuti pubblici online, l'esclusione sistematica di informazioni sensibili? Soprattutto considerando che tali informazioni potevano presentarsi in forma non esplicita o contestuale e che la capacità di rilevamento automatico su corpora di centinaia di miliardi di token restava tecnicamente imperfetta. Come sottolineato da Minamoto, Oda e Kawahara, la ricerca tecnica giapponese ha affrontato la questione come un problema operativo, proponendo metodi automatizzati per rilevare e filtrare elementi potenzialmente riconducibili a special care-required personal information nei corpora destinati al pre-training, proprio perché l'esclusione manuale diventa impraticabile su larga scala (Minamoto et al., 2025).

La seconda questione critica riguardava la retention, ovvero la conservazione dei dati. OpenAI offriva agli utenti paganti la possibilità di disattivare la cronologia delle chat e di escludere i propri input per finalità di training, ma le modalità tecniche di implementazione di queste opzioni così come i tempi effettivi di cancellazione e la distinzione tra dati conservati temporaneamente per motivi di sicurezza o debugging e dati effettivamente utilizzati per addestramento non erano pienamente trasparenti né facilmente verificabili dall'esterno. Questa opacità rendeva difficile stabilire se tale opzione garantisse effettivamente l'esclusione dei dati dal ciclo di apprendimento o

semplicemente interrompesse la loro conservazione in forma accessibile all'utente.

Una terza criticità riguardava le procedure di cancellazione su richiesta. L'APPI riconosce agli interessati il diritto di richiedere la cancellazione o la sospensione dell'uso dei propri dati personali (e retained personal data), ma nei modelli di machine learning la cancellazione di un dato di addestramento non comporta automaticamente la sua rimozione dai parametri del modello già addestrato. Questo rende tecnicamente complesso, se non impossibile in molti casi, garantire una cancellazione significativa una volta che il dato è stato incorporato nel processo di apprendimento. Il problema del machine unlearning restava sostanzialmente irrisolto sia dal punto di vista tecnico sia da quello normativo, lasciando una zona grigia tra obbligo formale e possibilità materiale di adempimento (Clifford Chance, 2023).

Infine, la verificabilità dell'enforcement costituiva un nodo strutturale. La PPC non disponeva di accesso diretto ai sistemi di OpenAI, né di capacità ispettiva transfrontaliera per verificare autonomamente se e come le misure richieste fossero state effettivamente implementate. La conformità dipendeva quindi in larga misura dalla trasparenza volontaria del provider e dalla collaborazione informale tra autorità, piuttosto che da meccanismi di controllo vincolanti e verificabili in modo indipendente. Come osservato da Yamamoto nella sua analisi del quadro giapponese di regolazione dell'IA e della concorrenza, l'enforcement delle norme su piattaforme globali richiede non solo una chiarezza normativa, ma anche capacità di monitoraggio continuo del mercato, dialogo attivo con gli stakeholder e strumenti di verifica tecnica che il sistema giapponese, orientato prevalentemente a soft law e autoregolamentazione, fatica ancora a rendere pienamente operativi (Yamamoto, 2020).

Nei casi Rikunabi e OpenAI emerge un tratto comune: l'enforcement riesce a incardinare l'IA nei principi generali dell'APPI, ma fatica a trasformare il cuore tecnico del rischio in un set di obblighi chiari, standardizzabili e replicabili, capaci di ridurre stabilmente le zone grigie. Nel caso Rikunabi, il rischio si concentrava sul profiling inferenziale basato su scoring predittivi venduti a terzi senza consenso, sfruttando un'architettura di pseudo-anonimizzazione progettata per eludere formalmente gli obblighi APPI pur consentendo la reidentificazione lato cliente. Nel caso OpenAI, il rischio riguardava la memorizzazione, la riemersione e la disclosure involontaria di informazioni personali nei

modelli generativi, alimentati da dataset costruiti tramite web crawling massivo e da input utente inseriti in linguaggio naturale, con modalità di retention, filtraggio e cancellazione difficilmente verificabili dall'esterno. Queste zone grigie derivano dalla distanza strutturale tra categorie giuridiche pensate per trattamenti tradizionali basati su record statici e dinamiche tecniche caratterizzate da trasformazioni continue, inferenze non tracciabili, filiere distribuite e architetture globali difficilmente ispezionabili. In questo quadro, la tutela resta condizionata non solo dalla norma, ma dalle capacità tecniche, dalla trasparenza volontaria dei provider e dalla possibilità concreta di verificare che gli obblighi dichiarati si traducano in garanzie effettive per gli interessati.

4.2.5 Effettività dei rimedi ed evoluzione dell'enforcement

Dal punto di vista dell'effettività, il problema non è soltanto quali poteri la PPC possa esercitare sulla carta, ma che cosa l'interessato riesca davvero a ottenere quando prova ad attivare i propri diritti. L'APPI riconosce facoltà di accesso, correzione, cessazione e cancellazione, ma la praticabilità di questi diritti dipende in modo decisivo da come il titolare organizza il trattamento. In particolare, dalla riconduzione o meno delle informazioni nell'area dei retained personal data, cioè dei dati rispetto ai quali esiste un potere effettivo di intervento (APPI, 2003, art. 2). Nei contesti di intelligenza artificiale, questa premessa strutturale entra in tensione con il modo in cui l'informazione viene generata, trasformata e distribuita lungo la filiera.

Una prima linea di attrito riguarda la stessa esistenza, in forma stabile, dell'oggetto su cui far valere i rimedi. Gli output inferenziali non devono necessariamente essere conservati. Uno score può essere calcolato al momento, utilizzato per orientare un ranking o una decisione e poi non essere registrato, oppure essere memorizzato in forma che non consente più di risalire agevolmente al singolo interessato. In scenari di questo tipo, il soggetto subisce un effetto decisionale come l'esclusione da una selezione, il peggioramento di una classificazione, l'attribuzione di un profilo sfavorevole, senza poter ricostruire quale informazione abbia inciso sulla decisione né dove tale informazione sia reperibile. Il diritto esiste in astratto, ma manca il bersaglio concreto su cui indirizzarlo.

Una seconda linea di frizione deriva dalla distribuzione della conservazione lungo catene tecniche complesse. In architetture multi-attore, il titolare a valle può conservare solo il

risultato (lo score, il flag, la decisione), ma non la logica che lo ha prodotto. Il provider del modello dispone di log tecnici o di dataset di addestramento, ma non necessariamente dell'identità degli interessati. Un integratore intermedio può gestire meta-dati operativi, senza accesso ai contenuti che hanno alimentato le inferenze. Nessuno preso singolarmente controlla l'intera traiettoria del dato. In queste condizioni, anche quando un'informazione rientra formalmente nella categoria dei retained personal data, ricostruire il percorso decisionale per consentire accesso, spiegazione o sospensione dell'uso diventa, di fatto, problematico.

La terza difficoltà tocca la natura stessa dei dati inferenziali. Anche nei casi in cui lo score o il profilo siano conservati e individualizzabili, la rettifica non funziona come nel caso di un dato fattuale errato. Correggere un indirizzo o una data di nascita significa sostituire un'informazione falsa con una vera. Intervenire su una predizione implica, almeno in linea di principio, agire sulla logica del modello sulla selezione e sul peso dei dati di addestramento, o sui parametri che li rappresentano. Come osservano Häuselmann e Custers, la rettifica di dati inferiti solleva problemi concettuali perché le predizioni non sono facilmente verificabili alla stregua di un fatto passato e stati soggettivi o tratti psicologici dedotti possono non coincidere né con la realtà, né con l'autopercezione dell'interessato (Häuselmann, Custers, 2024). Il rischio è che diritti formalmente disponibili si traducano in una possibilità molto limitata di incidere su inferenze che continuano a produrre effetti.

Il quadro che ne risulta è quasi paradossale. Proprio nei punti in cui l'IA concentra il massimo impatto sulla posizione della persona, la tutela individuale tende a diventare meno azionabile. L'informazione decisiva può essere effimera, non localizzata in un unico archivio, opaca nella sua genesi o non effettivamente correggibile con i rimedi tradizionali. Come sottolineano Wachter e Mittelstadt, una protezione effettiva richiede capacità di spiegare, contestare e sottoporre a verifica gli esiti algoritmici almeno nei contesti ad alto impatto, così da trasformare le inferenze da prodotto tecnico insindacabile a oggetto di scrutinio e responsabilità (Wachter, Mittelstadt, 2019).

Queste tensioni non restano confinate nella riflessione accademica, ma iniziano a emergere anche sul piano istituzionale. Nel contesto della revisione triennale dell'APPI, la PPC ha riconosciuto che l'assetto attuale dell'enforcement, fondato in larga misura su

avvertimenti, raccomandazioni e strumenti di soft law, rischia di essere insufficiente rispetto alla scala e alla complessità dei trattamenti algoritmici (PPC, 2024b). In un Report pubblicato nel 2024, la Commissione ha messo in consultazione l'introduzione di sanzioni pecuniare amministrative per violazioni considerate particolarmente gravi, come data breach che coinvolgono oltre 1.000 soggetti, trasferimenti non autorizzati a terzi e violazioni ripetute in un arco di dieci anni, con l'obiettivo esplicito di rafforzare la funzione deterrente del sistema (Baker McKenzie, 2025). L'idea di fondo è che chi trae benefici economici da trattamenti non conformi debba esporsi a un rischio sanzionatorio più proporzionato, anche per compensare l'asimmetria tra la sofisticazione tecnica dei sistemi di IA e la relativa mitezza degli strumenti di enforcement ordinario.

In questo senso, la discussione sulle sanzioni pecuniarie non è separata dalla questione dei rimedi individuali, ma ne costituisce il rovescio istituzionale. Più i diritti di accesso, rettifica o cancellazione si scontrano con limiti strutturali legati a inferenze effimere e modelli difficilmente emendabili, più diventa cruciale che l'ordinamento disponga di leve preventive e repressive capaci di incidere sulle scelte organizzative dei titolari e dei provider. La sezione successiva analizzerà proprio questo equilibrio instabile: da un lato, un enforcement che, nella prassi quotidiana, continua a fare affidamento su linee guida e prassi interpretative aggiornabili. Dall'altro, il tentativo di introdurre elementi più robusti di responsabilizzazione economica in un sistema che rimane, per scelta, improntato a una logica light-touch.

4.3 Il paradosso del paradiso per l'addestramento

I limiti di enforcement discussi nel paragrafo precedente non sono un'anomalia, ma riflettono una caratteristica strutturale del modello giapponese, ovvero la tendenza a governare l'innovazione tramite strumenti flessibili piuttosto che attraverso interventi coercitivi capaci di fissare interpretazioni vincolanti e ripetute (METI, 2024). In questo senso l'adattamento alla tecnologia può essere letto come una risposta pragmatica al *pacing problem.* Nel caso dell'IA generativa la dinamica è più complessa. Non si tratta soltanto di un ritardo temporale del diritto, ma di una sfasatura strutturale tra categorie giuridiche, pensate per trattamenti relativamente lineari e tracciabili, e filiere basate su addestramento massivo, parametri statistici e servizi globali che producono output probabilistici.

Questa sfasatura emerge con particolare chiarezza in un punto. La gestione delle zone grigie non dipende solo dall'APPI e dalla sua interpretazione, ma anche da scelte di policy collaterali, soprattutto in materia di diritto d'autore, che pur operando su piani formalmente distinti incidono concretamente sulla disponibilità e circolazione dei dati che alimentano l'ecosistema IA (Ueno, 2021). Ne risulta un quadro in cui l'accesso ai dati è facilitato per ragioni di competitività industriale, mentre la mitigazione dei rischi privacy e di accountability tende a essere relegata a correttivi successivi, spesso di soft law (METI, 2024).

4.3.1 L'eccezione per il machine learning

Un nodo particolarmente rilevante per comprendere la traiettoria giapponese si trova fuori dall'APPI, nel Copyright Act. L'art. 30-4, introdotto con la riforma del 2018 ed entrato in vigore nel 2019, consente l'utilizzo di opere protette per finalità di "analisi delle informazioni" (*jōhō kaiseki*) senza autorizzazione diretta del titolare, a condizione che l'uso non persegua lo scopo di godimento (*enjoyment*) dell'opera (Ueno, 2021). La dottrina ha sottolineato come questa impostazione, centrata sulla distinzione tra fruizione espressiva e trattamento analitico, renda l'eccezione particolarmente ampia per attività data-driven, incluse pratiche che nella sostanza corrispondono all'addestramento di modelli su grandi corpora di testi e immagini (Ueno, 2021).

Qui bisogna prestare particolare attenzione. Il Copyright Act non autorizza il trattamento di dati personali in deroga all'APPI. Tuttavia, una disciplina così permissiva del text and data mining riduce fortemente l'attrito legale sul piano del copyright e rende praticabile su scala industriale la raccolta automatizzata (crawling/scraping) di contenuti online dove informazioni personali e contenuti autoriali risultano spesso mescolati. In altre parole, l'eccezione non sostituisce la disciplina, ma crea un corridoio di accesso ai contenuti che sposta la gestione dei rischi anche relativi alla privacy a valle, cioè nella fase di filtraggio e governance del dataset (Agency for Cultural Affairs, 2024).

Il fatto che questo equilibrio sia fragile è confermato dall'intervento interpretativo del 2024. Con il documento *General Understanding on AI and Copyright in Japan*, l'Agency for Cultural Affairs (Bunka-chō) ha chiarito che l'art. 30-4 non è un lasciapassare assoluto. La valutazione dipende dallo scopo concreto e dalle modalità d'uso, e la liceità può essere

esclusa in presenza di ingiustificato pregiudizio agli interessi del titolare, soprattutto quando l'utilizzo incide sul mercato delle opere o quando l'uso si avvicina a finalità di replica sostanziale del contenuto (Agency for Cultural Affairs, 2024). Ai fini di questa tesi, il fulcro è mettere in luce la logica di fondo: una scelta pro-innovazione (accesso ampio ai contenuti per l'analisi) richiede poi correttivi interpretativi *a posteriori* per gestire le frizioni che emergono nella pratica.

4.3.2 Dai record statici ai rischi comportamentali

Una seconda dimensione della sfasatura riguarda la natura dei rischi prodotti dai sistemi generativi. L'APPI è costruito attorno alla nozione di informazione personale e alla sua riconducibilità a un individuo specifico. Nei sistemi generativi e nelle interfacce basate su conversazione, però, una parte crescente del rischio per l'utente deriva da fenomeni che non richiedono necessariamente identificazione nominativa, come ad esempio: influenza personalizzata, sfruttamento di vulnerabilità cognitive, interazioni persuasive e contenuti sintetici ingannevoli (*dark patterns*). In questi scenari, l'impatto sull'autonomia decisionale può essere elevato anche quando il sistema opera su segnali comportamentali o su interazioni pseudonime. Un modello può imparare preferenze e debolezze attraverso lo stile di interazione e orientare scelte senza che sia tecnicamente indispensabile identificare l'utente ai sensi delle soglie tradizionali di identificabilità (European Parliament, 2021).

Per comprendere meglio possiamo ricorrere ad un confronto con la situazione europea. L'AI Act ha introdotto un perimetro di pratiche proibite che include, tra le altre, forme di manipolazione o sfruttamento di vulnerabilità (European Commission, 2021). Il Giappone, invece, non dispone oggi di un equivalente legislativo IA-centrico di pari portata che tipizzi direttamente questi rischi. La tutela resta affidata a norme indirette e a strumenti di orientamento non vincolanti, con il risultato che l'ordinamento rimane più attrezzato a gestire la circolazione di record identificativi che a presidiare in modo esplicito i rischi comportamentali e persuasivi tipici di servizi generativi e di piattaforme (METI, 2024).

Questo non significa che l'APPI sia irrilevante. Molte dinamiche restano "agganciabili" alla disciplina (come logging, riutilizzo degli input, finalità, sicurezza). Tuttavia, quando

il rischio principale consiste nella capacità del sistema di modellare e orientare comportamenti tramite interazioni e output probabilistici, la tutela fondata sul controllo individuale del dato personale tende a mostrare limiti strutturali. Il problema oltre al che cosa viene trattato, è anche il cosa il sistema riesce a fare all'utente anche con segnali deboli e senza identificazione piena (METI, 2024).

4.3.3 Frammentazione istituzionale e standardizzazione internazionale

Infine, la sfasatura si riflette anche sul piano della governance. In assenza di una legge quadro sull'IA, il sistema giapponese è segnato da una pluralità di attori con mandati diversi. il METI (e il policy network economico-industriale) promuove l'adozione dell'IA e strumenti di governance flessibili. La PPC presidia la protezione dei dati, la Bunka-chō interviene sul fronte copyright e le linee guida orizzontali, come le *AI Guidelines for Business*, rimangono strumenti di soft law, seppur influenti. Questo disallineamento produce un effetto prevedibile con l'innovazione che viene spesso accelerata da scelte regolatorie permissive (come l'ampia eccezione TDM), mentre la tutela dei diritti procede per aggiustamenti tramite documenti interpretativi successivi (Agency for Cultural Affairs, 2024).

A questa dinamica interna si affianca la dimensione internazionale. Il Giappone ha avuto un ruolo centrale nel *Hiroshima AI Process* del G7, che ha prodotto principi guida e un percorso di standardizzazione cooperativa rivolto agli sviluppatori di IA avanzata, fondato su trasparenza, gestione del rischio e responsabilità lungo il ciclo di vita (MOFA, 2025). Queste iniziative rafforzano l'immagine di una governance agile e multi-stakeholder; al tempo stesso, però, confermano il trade-off di fondo. La standardizzazione avanza soprattutto nella forma di principi e codici di condotta, diventando più complesso trasformare tali standard in obblighi giuridici uniformi e coercibili (METI, 2024).

Il risultato è un adattamento tendenzialmente reattivo. Molte regole operative si consolidano quando le pratiche industriali si sono già diffuse. Questo approccio riduce il rischio di obsolescenza normativa, ma lascia margini di incertezza per gli interessati, la cui tutela effettiva finisce spesso per dipendere dalla qualità della governance interna dei provider e dalla capacità delle autorità di esercitare una persuasione morale efficace

(METI, 2024). Qui è importante essere precisi e puntuali anche sul piano dei poteri. La PPC dispone di strumenti graduati, ma non opera con un sistema generalizzato di sanzioni amministrative pecuniarie immediate comparabile a quello di altri ordinamenti. L'architettura sanzionatoria rimane prevalentemente ancorata a meccanismi di ordine e conseguenze in caso di inosservanza, mentre proposte di rafforzamento, incluse possibili sanzioni monetarie, sono emerse proprio nella discussione di riforma recente (PPC, 2024a). In questo quadro, la dipendenza dalla cooperazione del soggetto regolato (specie quando è un provider globale) resta un punto di frizione strutturale.

4.4 Tensione tra tutela dei dati personali e competitività economica

Le criticità analizzate nei paragrafi precedenti, dalle ambiguità definitorie dell'APPI alla debolezza strutturale dell'enforcement, fino alla facilitazione dell'accesso ai dati per l'addestramento dei modelli di intelligenza artificiale, non possono essere lette come semplici lacune accidentali del sistema. Esse riflettono, piuttosto, una scelta politico-strategica consapevole. Il legislatore e il decisore pubblico giapponese hanno privilegiato la competitività economica e industriale nel settore dell'IA rispetto all'adozione di un modello di tutela della privacy rigido e fortemente vincolante.
In quest'ottica, la protezione dei dati personali non assume il ruolo di limite intrinseco allo sfruttamento informativo, come avviene nel modello europeo fondato sul riconoscimento della privacy quale diritto fondamentale. Al contrario, essa viene concepita come uno strumento funzionale alla crescita dell'economia digitale, destinato a garantire un livello minimo di fiducia sufficiente a rendere socialmente accettabile la circolazione dei dati, senza però comprimere in modo significativo la libertà di innovazione tecnologica. Il presente paragrafo ricostruisce la logica complessiva di questa impostazione.

4.4.1 Society 5.0 e Data Free Flow with Trust

L'architettura regolatoria giapponese in materia di dati e intelligenza artificiale trova il proprio fondamento nella visione strategica di Society 5.0, formalizzata dal Cabinet Office nel 5th Science and Technology Basic Plan del 2016 (Cabinet Office, 2016). In tale documento, il Giappone delinea il progetto di una super-smart society caratterizzata dalla piena integrazione tra spazio fisico e cyberspazio, resa possibile dall'impiego sistemico di intelligenza artificiale, big data e Internet of Things. All'interno

di questa visione, i dati sono concepiti come una risorsa infrastrutturale essenziale, al pari dell'energia o delle reti di trasporto. L'IA non è considerata una tecnologia emergente da contenere, bensì un fattore abilitante per la soluzione di problemi sociali strutturali, dall'invecchiamento demografico alla sostenibilità dei servizi pubblici, e un motore di crescita economica. La AI Strategy 2019 ribadisce esplicitamente l'obiettivo di rafforzare la competitività industriale del Giappone attraverso la promozione dello sviluppo e dell'implementazione sociale dell'intelligenza artificiale (Cabinet Office, 2019).

Questa impostazione interna trova una proiezione coerente sul piano internazionale nel principio del Data Free Flow with Trust (DFFT), promosso dal Giappone in occasione del G20 di Osaka nel 2019 e successivamente integrato nell'agenda del G7 (MOFA, 2020). Il DFFT mira a favorire la libera circolazione transfrontaliera dei dati quale condizione necessaria per l'innovazione globale, subordinando i flussi non a divieti generalizzati, ma alla presenza di un livello sufficiente di fiducia tra gli attori e le giurisdizioni coinvolte.

In questo quadro emerge una differenza strutturale rispetto all'approccio europeo. Mentre il GDPR concepisce la protezione dei dati come un diritto fondamentale che limita a priori la possibilità di trattamento, il modello giapponese attribuisce alla privacy una funzione prevalentemente strumentale con l'obiettivo di costruire la fiducia necessaria affinché i dati possano circolare. Tale impostazione si riflette chiaramente nell'art. 1 dell'APPI, che individua come finalità della legge la tutela dei diritti e degli interessi individuali "tenendo conto dell'utilità delle informazioni personali", ponendo protezione e sfruttamento economico su un piano di equilibrio dichiarato (APPI, art. 1). Ne deriva un assetto normativo orientato a non ostacolare l'innovazione, come abbiamo già avuto modo di discutere nei capitoli precedenti.

4.4.2 Competitività industriale e scelte normative

Letta alla luce della competizione globale nel settore dell'IA, la regolazione giapponese appare coerente con un obiettivo preciso: ridurre il costo regolatorio dell'innovazione data-driven. Le scelte analizzate nei paragrafi precedenti (dall'elasticità delle definizioni dell'APPI alla debolezza delle sanzioni, fino all'ampia eccezione per il text and data mining prevista dall'art. 30-4 del Copyright Act) si inseriscono in una strategia volta a creare un ambiente favorevole allo sviluppo e all'addestramento dei modelli di intelligenza artificiale.

Dal punto di vista politico-economico, il Giappone si colloca tra due poli dominanti. Negli

Stati Uniti, l'assenza di una disciplina federale organica sulla protezione dei dati ha consentito ai grandi operatori tecnologici di sviluppare modelli di business fondati sull'estrazione massiva di informazioni, nonostante il recente aumento del contenzioso sul training dei modelli generativi. In Cina, l'IA è sostenuta da una politica industriale fortemente interventista, che include l'accesso privilegiato ai dati e l'implementazione su larga scala dei sistemi algoritmici. In questo contesto, l'imposizione di vincoli stringenti sulla raccolta e sull'utilizzo dei dati è stata percepita dal legislatore giapponese come un potenziale svantaggio competitivo.

L'eccezione prevista dall'art. 30-4 del Copyright Act, definita in dottrina come una delle più favorevoli al machine learning a livello globale (Ueno, 2021), rappresenta un esempio emblematico di questa scelta. Facilitando l'accesso a grandi corpora di dati per finalità di addestramento, il legislatore ha ridotto drasticamente le barriere legali allo sviluppo dell'IA, accettando tuttavia una compressione delle tutele dei titolari di diritti e uno spostamento dei rischi a valle, nella fase di governance tecnica e organizzativa dei sistemi. Il trade-off è dunque esplicito: la competitività industriale e la rapidità di sviluppo vengono privilegiate rispetto alla costruzione di garanzie preventive robuste. La tutela dei dati personali viene affidata in larga misura alla responsabilità degli operatori, alla conformità volontaria e alla capacità delle autorità di orientare le pratiche attraverso linee guida e raccomandazioni, piuttosto che attraverso un apparato sanzionatorio incisivo e sistematico.

4.4.3 Il paradosso della fiducia

La strategia giapponese incontra tuttavia un limite critico proprio nell'elemento che dovrebbe sostenerla: la fiducia. Si configura così un vero e proprio paradosso della fiducia. Le stesse scelte di flessibilità e deregolamentazione adottate per favorire l'innovazione rischiano, se non adeguatamente bilanciate, di minare la legittimazione sociale dell'ecosistema data-driven.

Un segnale significativo di questa tensione emerge dall'implementazione del sistema di identificazione My Number, progettato per razionalizzare l'amministrazione pubblica e favorire l'integrazione dei dati tra enti. Nel corso del 2023, una serie di errori nella gestione delle informazioni personali (tra cui associazioni errate di dati sanitari e previdenziali) ha attirato ampia attenzione mediatica e determinato ispezioni da parte della Personal Information Protection Commission (Mainichi, 2023). Al di là delle

specifiche responsabilità tecniche, tali episodi hanno rafforzato la percezione pubblica di fragilità nella gestione dei dati centralizzati. Avremo modo di affrontare più nel dettaglio il sistema MyNumber nel corso del prossimo capitolo.

Analoghe dinamiche si riscontrano nel settore privato. I casi analizzati nel 4.2, come quello di Rikunabi o le incertezze legate all'uso dei dati personali nei servizi di IA generativa, mostrano come l'ampiezza delle zone grigie normative, combinata con un enforcement prevalentemente persuasivo, possa tradursi in pratiche opache e difficilmente contestabili dagli interessati. La risposta della PPC, incentrata su guidance e pressione morale, favorisce l'adeguamento cooperativo ma fatica a produrre standard vincolanti consolidati su questioni ricorrenti, quali la profilazione inferenziale o il riutilizzo dei dati per l'addestramento dei modelli. La conseguenza diretta è la creazione delle zone grigie.

Il rischio sistemico è che, in assenza di tutele percepite come solide ed effettive, i cittadini sviluppino una resistenza crescente alla condivisione dei propri dati, impoverendo l'ecosistema informativo necessario alla realizzazione di Society 5.0. Se la fiducia viene meno, anche il principio del Data Free Flow with Trust perde la propria base di legittimazione. È in questa prospettiva che si collocano le recenti riflessioni della PPC, espresse nel Interim Report del 2024, sulla necessità di rafforzare la deterrenza attraverso l'introduzione di sanzioni amministrative pecuniarie per le violazioni più gravi, al fine di ancorare la conformità a incentivi economici più chiari (PPC, 2024b).

Per concludere, possiamo dire che il modello giapponese appare caratterizzato da un equilibrio instabile. Da un lato, esso ha consentito al Paese di posizionarsi come un contesto favorevole allo sviluppo dell'intelligenza artificiale, mantenendo elevata flessibilità nell'uso dei dati. Dall'altro, l'esperienza concreta mostra che la fiducia degli interessati non può essere presunta, ma deve essere continuamente costruita attraverso garanzie percepite come credibili. Questa tensione si manifesta in modo particolarmente evidente nel sistema My Number, che rappresenta al contempo il progetto più ambizioso di integrazione dei dati personali e uno dei principali banchi di prova della sostenibilità del modello giapponese. Il Capitolo 5 analizzerà tale caso applicativo in dettaglio, mostrando come le zone grigie teoriche emerse finora si traducano in problemi concreti di governance e accettazione sociale.

CAPITOLO 5 – DUE CASI APPLICATIVI: MY NUMBER E BLOCKCHAIN

I capitoli precedenti hanno ricostruito il quadro giuridico e istituzionale della tutela dei dati personali e della governance dell'innovazione digitale in Giappone, mettendo in luce un tratto ricorrente ovvero la preferenza per un impianto leggero nei vincoli prescrittivi e denso negli strumenti di accompagnamento, con un ruolo centrale della Personal Information Protection Commission nel dare concretezza all'APPI attraverso interpretazioni e prassi (PPC, 2024a). La conseguenza, emersa soprattutto nel Capitolo 4, è che molte frizioni non dipendono soltanto da vuoti normativi, ma dal modo in cui il diritto viene chiamato a reggere catene operative complesse, spesso distribuite, dove la tutela effettiva dipende dalla qualità dell'implementazione, dalla chiarezza di chi detiene la responsabilità e dalla capacità dei controlli di scalare.

Questo capitolo vuole passare dal lato teorico ad uno più concreto, attraverso due casi che sono diversi tecnicamente ma comparabili giuridicamente perché trasformano il dato personale in infrastruttura. Il primo è My Number, cioè l'architettura nazionale che assegna un identificatore individuale e organizza, entro limiti legali, l'interoperabilità fra basi di dati pubbliche oggi sempre più intrecciata con l'identità digitale quotidiana tramite la My Number Card, l'autenticazione online e i servizi di portale (Digital Agency, 2025). Il secondo è l'insieme di sperimentazioni e proposte blockchain in ambito pubblico (come identità e certificazioni), spesso presentate come risposta tecnica alla crisi di fiducia verso sistemi centrali o come modo per rendere verificabili i flussi informativi.

Il punto di contatto fra i due casi è la collocazione della fiducia. My Number presuppone fiducia nella capacità dello Stato di definire controlli e responsabilità lungo una rete amministrativa complessa. Molte architetture blockchain spostano parte di quella fiducia su meccanismi crittografici e su registri verificabili, ma al prezzo di nuove tensioni con categorie giuridiche classiche (come individuazione del titolare e governance del sistema). In questa prospettiva, i due casi funzionano come test complementari: My Number rende immediato il problema della tutela quando l'identificazione stabile è il presupposto del coordinamento; la blockchain rende evidente cosa accade quando il dato, o la sua prova, tende all'immodificabilità e la governance è distribuita.

Ai fini della tesi, il punto di interesse è la possibilità di preservare fiducia e legittimazione sociale in una strategia che vuole promuovere circolazione del dato e digitalizzazione dei servizi senza perdere la dimensione "with Trust" (v. 2.2–2.3), quando l'identità digitale diventa condizione ordinaria di accesso a welfare, sanità e procedure amministrative.

5.1 Struttura del sistema My Number

My Number (kojin bangō, 個人番号) nasce con un obiettivo dichiaratamente pratico, quello di ridurre la frammentazione amministrativa e rendere più efficienti e controllabili i procedimenti in cui l'identità del soggetto è la chiave per erogare prestazioni o accertare degli obblighi. Brevemente, il sistema assegna a ciascun residente un numero individuale a dodici cifre e ne consente l'uso solo entro un perimetro legale tipizzato. Il numero, infatti, non è pensato come documento a sé stante, ma come strumento di collegamento che permette agli enti pubblici autorizzati di verificare informazioni già detenute da altre amministrazioni, riducendo quindi richieste di certificazioni ripetute e la dipendenza da allegati cartacei (Digital Agency, 2025). In altre parole, l'architettura mira a far sì che, quando il cittadino richiede un beneficio o completa una procedura, l'amministrazione possa confermare requisiti e dati necessari tramite scambi informativi controllati, piuttosto che scaricare sull'utente l'onere di provare ogni volta informazioni che lo Stato già possiede in un altro segmento della macchina pubblica (Board of Audit of Japan, 2016).

La base normativa è *l'Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures* (Act No. 27 del 2013, comunemente "My Number Act"), che definisce l'identificatore, disciplina le condizioni di trattamento e introduce un regime speciale rispetto alla disciplina generale della protezione dei dati (My Number Act, 2013). Proprio l'esistenza di una legge speciale segnala che il legislatore considera l'identificatore nazionale un punto di rischio qualitativamente diverso rispetto al trattamento ordinario di personal information. L'identificatore stabile tende naturalmente a spingere verso riusi e interconnessioni crescenti, rendendo necessario valutare la tutela non solo sul piano del singolo adempimento, ma anche sul terreno degli effetti sistemici di interoperabilità (Crabtree et al., 2018).

Per comprendere cosa fa My Number nella pratica, conviene distinguere tre livelli che

interagiscono fra loro. Il primo livello è l'identificatore. Il My Number in senso stretto è il numero individuale che viene richiesto in molte situazioni della vita amministrativa (come lavoro, prestazioni, procedure fiscali, eventi rilevanti come nascita e assistenza per persone non autosufficienti e anche contesti emergenziali), perché consente di collegare l'operazione a una persona in modo univoco (Digital Agency, 2025). Nel corso di questa tesi, abbiamo visto come nei trattamenti normali l'identificabilità è spesso una soglia mobile (v. 4.1), mentre in My Number l'identificabilità è incorporata nel design stesso del sistema e la minimizzazione non può essere letta come semplice riduzione dei campi informativi, ma piuttosto deve essere ripensata come governo dell'interoperabilità e dei punti di accesso.

Il secondo livello è la My Number Card, cioè la smart card che rende l'identità digitale utilizzabile in modo operativo. La card ha una funzione ibrida: da un lato è documento di identificazione con fotografia, utilizzabile come strumento di verifica dell'identità in contesti che lo richiedono. Dall'altro include, nel chip IC, componenti e certificati della Public Key Infrastructure pubblica (JPKI), che consentono autenticazione online e firma elettronica per procedure digitali (Nippon.com, 2023). Questo passaggio è decisivo per capire perché My Number, pur nato come leva di efficienza amministrativa, sia diventato negli anni un'infrastruttura di vita quotidiana. Infatti, la card oltre a rappresentare una comodità, crea anche la condizione tecnica per spostare servizi e procedure sul canale digitale, riducendo di fatto l'uso del numero in chiaro e concentrando il rischio su credenziali, certificati, procedure di rilascio, gestione delle eccezioni, revoche e rinnovi.

Il terzo livello è la dimensione di sistema, cioè l'insieme delle piattaforme e dei canali che permettono scambio informativo e interazione con l'utente. Da una parte c'è il portale (MyNaPortal) come interfaccia per servizi e comunicazioni, dall'altra c’è la rete di coordinamento fra amministrazioni che consente la verifica di informazioni e lo scambio entro perimetri autorizzati. Bisogna però fare un chiarimento fondamentale. My Number non coincide con un archivio unico onnicomprensivo dove tutto confluisce automaticamente. Le informazioni sostanziali (fisco, pensioni, sanità, assistenza locale) rimangono nelle banche dati degli enti competenti, ciò che cambia è la capacità di allineare e verificare dati tramite meccanismi di coordinamento informativo e procedure standardizzate (Board of Audit of Japan, 2016). Parlando di tutela, questo significa che al

rischio classico di una violazione centralizzata si aggiunge anche quello di errori o incongruenze replicabili lungo la catena di implementazione, quando molte amministrazioni (sia centrali che locali) devono applicare standard tecnici e regole giuridiche in modo coerente.

Questo suo aspetto di rete consente di leggere My Number come un caso limite per le categorie dell'APPI. In un sistema con molti nodi, l'accountability tende a diventare opaca per l'utente. Questo perché la responsabilità è formalmente distribuita fra chi gestisce infrastruttura e standard, chi gestisce i dati sostantivi e chi opera localmente, ma la percezione sociale, soprattutto quando qualcosa va storto, resta unitaria ("lo Stato"). Ed è proprio questa frizione che la letteratura empirica collega al tema della fiducia: un'identità digitale nazionale può funzionare sul piano tecnico e legale, ma rimanere fragile sul piano politico-sociale se la popolazione percepisce opacità nell'uso dei dati o inefficacia dei rimedi (Crabtree et al., 2018). La riflessione è particolarmente pertinente per il Giappone, dove l'accettazione di My Number è stata storicamente intrecciata a preoccupazioni per la sorveglianza e per l'estensione incrementale degli usi nel tempo. A questo si aggiungono anche degli incidenti che avremo modo di affrontare successivamente.

5.1.1 Presidi giuridici ed evoluzione del sistema

Sul piano strettamente giuridico, il My Number Act costruisce un perimetro di liceità tipizzato e insieme un regime rafforzato per ciò che ruota attorno al My Number. L'uso del numero individuale è consentito solo per finalità determinate dalla legge, tradizionalmente ricondotte ai grandi ambiti di sicurezza sociale, tassazione e gestione dei disastri (My Number Act, 2013, art. 9). La logica è prevenire che l'identificatore diventi a scopo generalizzato. L’idea di fondo è impedire che la pubblica amministrazione o soggetti terzi estendano l'uso al di fuori delle ipotesi previste. Coerentemente, la disciplina sulle "specific personal information" (informazioni personali che includono il numero) è più stringente e le linee guida della PPC dettagliano, per operatori sia pubblici che privati, forme cautelari come regole sulla comunicazione e sulla gestione dei casi di violazione o uso improprio (PPC, 2024a).

Il regime sanzionatorio, inoltre, è più severo rispetto a quanto ci si aspetterebbe in un trattamento ordinario, proprio perché il danno potenziale non si limita ad essere

individuale ma è sistemico. L'uso indebito del numero o la comunicazione non autorizzata di specific personal information può aprire la strada a riusi e interconnessioni non controllate (My Number Act, 2013). Anche qui, tuttavia, un elemento rilevante è la sua capacità di incidere su comportamenti e prassi in un contesto in cui la vulnerabilità può derivare non da malafede, bensì da errori procedurali, mancanza di correlazione fra registri, integrazioni con altri sistemi e divergenze applicative fra gli enti che lo utilizzano.

A partire dal 2020, il sistema è stato progressivamente inserito in un'accelerazione più ampia della digitalizzazione amministrativa, culminata nell'istituzione della Digital Agency e nella spinta a utilizzare la My Number Card come infrastruttura di accesso a servizi digitali (Digital Agency, 2025). Un passaggio emblematico è l'integrazione sanitaria: la transizione verso l'uso della My Number Card come strumento principale di verifica dell'assicurazione sanitaria è stata accompagnata da misure transitorie e da un calendario che, pur non eliminando immediatamente tutte le alternative, ha ridotto la natura opzionale dell'identità digitale nei servizi essenziali (MHLW, 2024). È un cambio molto importante. Quando l'identità digitale diventa requisito ordinario per la fruizione di prestazioni fondamentali, la tolleranza sociale verso errori e ambiguità diminuisce e la questione della fiducia si sposta dal livello retorico (innovazione, efficienza) al livello operativo.

Quantitativamente parlando, la diffusione della My Number Card è cresciuta rapidamente. Secondo dati ufficiali della Digital Agency, a gennaio 2026 le carte emesse superavano i 100 milioni, pari a circa l'80% della popolazione (Digital Agency, 2026). La stessa crescita, però, non risolve automaticamente il problema della fiducia. L'adozione formale di un'infrastruttura può coesistere con una percezione di fragilità se il sistema sperimenta errori replicabili o se l'espansione degli usi viene percepita come un ampliamento non pienamente controllabile. La discussione giuridica sul rapporto fra My Number Act, registri di base (come il koseki e il resident registry) e protezione della persona mostra che la posta in gioco non è soltanto l'efficienza, ma l'equilibrio fra interoperabilità e limiti sostanziali (Crabtree et al., 2018).

Questi elementi consentono di isolare il punto su cui My Number stressa il modello giapponese: la tutela non dipende solo dall'architettura normativa, ma dalla capacità di farla vivere lungo una rete amministrativa complessa, dove errori di registrazione e di

allineamento possono propagarsi e dove la responsabilità tende a frammentarsi diventando difficilmente verificabile. È precisamente in questa distanza fra disegno giuridico e struttura operativa che si colloca un confronto con il caso della blockchain, dove è fondamentale la possibilità di rendere verificabili i passaggi in cui oggi la fiducia è affidata soprattutto a procedure e coordinamento istituzionale.

5.2 Criticità e Limiti del My Number

Le criticità che hanno investito My Number nel 2023 e nel 2024 non sono riducibili a una somma di episodi contingenti. Il punto centrale è di natura infrastrutturale, infatti un sistema di identità amministrativa nazionale diventa vulnerabile quando subisce attacchi esterni e anche quando la qualità del dato e l'uniformità delle prassi operative non reggono la scala dell'interoperabilità. In un'architettura che abilita collegamenti tra registri e procedure eterogenei l'errore tende a replicarsi, non perché vi sia necessariamente un intento illecito, ma perché la stessa catena tecnico-organizzativa che rende possibile l'efficienza moltiplica l'impatto di possibili imperfezioni (Board of Audit of Japan, 2016).

Questo spiega perché, nel caso My Number, la frizione principale invece di coincidere con l'uso illecito in senso stretto coincida spesso con l'uso formalmente lecito ma operativamente fallibile. Errori di collegamento tra registri, procedure di verifica non uniformi, gestione disomogenea delle eccezioni, integrazioni imperfette con sistemi legacy e passaggi manuali non sufficientemente robusti. Ed è anche la ragione per cui, sul piano politico-sociale, una quota percentualmente contenuta di errori può generare un "trust shock". Quando l'identità digitale entra stabilmente in sanità e welfare, cresce drasticamente la sensibilità pubblica verso qualunque ambiguità nella catena di identificazione.

5.2.1 Incidenti, "trust shock" e risposta istituzionale

Gli episodi emersi nel 2023 hanno un tratto comune quello di mostrare come vulnerabilità ordinarie (ad esempio procedure di sportello od operazioni di registrazione) possano produrre effetti sistemici quando l'identità funge da chiave di coordinamento. In un'infrastruttura identitaria, ciò che altrove resterebbe un errore locale diventa un problema pubblico perché incide sulla certezza dell'identificazione e, dunque, sulla

fiducia nella correttezza della decisione amministrativa che si appoggia a quel collegamento.

Un primo nucleo di criticità ha riguardato il programma di incentivi MyNaPoint. La Digital Agency ha riportato 172 casi di collegamento errato relativi a MyNaPoint, distribuiti in 131 enti locali, riconducibili a carenze procedurali. Si trattano, in particolare, di pratiche operative non sufficientemente rigorose nell'uso dei terminali e nella gestione delle operazioni di registrazione. L'interesse giuridico è che se l'aggancio tra identità e procedura può risultare errato in un passaggio amministrativo standard, il rischio riguarda la robustezza delle prassi operative che implementano le regole.

Il secondo incidente ha coinvolto l'uso della My Number Card come strumento collegato ai servizi sanitari (myna insurance card). Nello stesso documento di luglio 2023, la Digital Agency ha indicato 7.312 casi di collegamento errato relativi alla componente sanitaria (alla data di riferimento del report) e ha riportato anche casi di effettiva visualizzazione di informazioni non pertinenti (come, ad esempio, informazioni sui farmaci) pari a 10. Indipendentemente dalla frequenza, questi eventi producono un impatto qualitativamente diverso perché toccano dati percepiti come ad alta sensibilità e investono un servizio essenziale, nel quale l'utente si aspetta certezza del matching e prevedibilità dei rimedi.

Accanto a tali criticità, nel 2023 ci sono ulteriori casi che, pur meno simbolici della sanità, mostrano la natura trasversale del problema. La registrazione errata del conto per la ricezione di fondi pubblici è stata quantificata in 940 casi, inoltre si sono verificati episodi legati all'emissione di certificati tramite convenience store (ad esempio certificati rilasciati erroneamente), con 14 casi di emissione errata e 50 casi di input errato. Nel complesso, questi elementi sottolineano la stessa cosa. Non si tratta di un singolo punto debole, bensì di un insieme di frizioni generate dall'interazione tra processi amministrativi distribuiti, passaggi manuali e standard applicati in modo non perfettamente uniforme.

Di fronte a questa sequenza, la risposta istituzionale non si è limitata alla comunicazione. Il governo ha impostato una reazione centrata su contromisure operative immediate e una strategia di verifica massiva volta a recuperare credibilità tramite un controllo sistematico dei collegamenti tra registri. In questa cornice si colloca la My Number Information Total

Inspection (Sōtenken, 総点検), il cui quadro complessivo è stato formalizzato dalla Digital Agency nella documentazione della riunione del 12 dicembre 2023.

Il dato più rilevante è che la Total Inspection ha interessato 82,08 milioni di record (somma di quattro grandi ambiti) e ha identificato 8.351 casi di collegamento errato (0,01%). La stessa fonte fornisce una scomposizione che consente di evitare formule vaghe: 5.645 casi relativi ai supporti alla disabilità; 1.142 relativi alle informazioni di eleggibilità dell'assicurazione sanitaria; 1.186 relativi al conto per la ricezione di fondi pubblici; 378 relativi alle pensioni. Oltre al totale, è rilevante la scelta di policy implicita. Infatti, quando l'errore è scalabile la reazione tende a essere un'azione di gestione della qualità su larga scala invece che centrato su singoli abusi.

Cronologia essenziale del sistema My Number (2013–2024)

- 2013: approvazione del My Number Act (Act No. 27 of 2013), con introduzione dell'identificatore e perimetro d'uso tipizzato.
- 2016: entrata a regime dell'operatività del sistema nelle procedure amministrative (Board of Audit of Japan, 2016).
- 2021: istituzione della Digital Agency, con mandato di coordinamento della trasformazione digitale e della componente infrastrutturale collegata a My Number.
- 2023: emergono errori di collegamento e incidenti ad alta visibilità e vengono rese pubbliche le contromisure (Digital Agency, 2023).
- 2023: avvio e consolidamento della Total Inspection. Al 12 dicembre 2023 risultano 82,08 milioni di record verificati e 8.351 casi di collegamento errato, con pubblicazione della scomposizione per ambiti (Digital Agency, 2023).
- 2024: la transizione sanitaria riduce la natura opzionale dell'integrazione fra My Number Card e assicurazione sanitaria, aumentando la sensibilità pubblica verso la resistenza operativa (MHLW, 2024).

Quella che emerge chiaramente da questa cronologia è che l'accelerazione successiva alla creazione della Digital Agency non è un dettaglio. Con l'infrastruttura identitaria che viene spinta verso un uso quotidiano in servizi essenziali, la gestione dell'errore diventa questione di legittimazione pubblica.

5.2.2 Responsabilità e rimedi

Sul piano normativo, My Number è circondato da un regime più rigoroso del trattamento ordinario con finalità tipizzate e regole speciali per le informazioni che includono l'identificatore (specific personal information), divieti sulla raccolta e comunicazione non autorizzata, e un apparato sanzionatorio dedicato (My Number Act, 2013). Tuttavia, le criticità del 2023 mostrano che una porzione rilevante del rischio si collocano nel perimetro della correttezza sostanziale del trattamento. Emergono tre fragilità di governance principali:

- La responsabilità formalmente distribuibile, con accountability socialmente unitaria. L'utente percepisce l'infrastruttura come unitaria ("lo Stato"), ma in realtà la catena concreta include molti più strati. Ci sono enti che gestiscono basi dati sostantive (come sanità, previdenza, fiscalità), altri enti locali che operano registrazioni e verifiche, soggetti tecnici che implementano interfacce e integrazioni e solo infine un livello di coordinamento centrale. Questa distribuzione rende più complesso definire la responsabilità quando l'errore nasce dall'interazione tra nodi diversi e non da un singolo abuso. Ne deriva che, in termini di rimedi, la domanda cruciale diventa chi può correggere, con quali tempi e come garantire che la correzione abbia effetto coerentemente lungo tutti i collegamenti, evitando che l'errore riemerga in un altro passaggio o servizio.

- I rimedi amministrativi sono efficaci solo se scalabili. La Total Inspection rappresenta una risposta istituzionale orientata alla scalabilità con verifiche massive e identificazione dei collegamenti errati che portano alla sospensione della visualizzazione di informazioni potenzialmente inesatte (Digital Agency, 2023). Tuttavia, misure di questo tipo somigliano a un modello di gestione della qualità che funzionano solo se diventano continuative e standardizzate con supporto di controlli automatizzabili, mentre perdono efficacia se restano interventi straordinari attuati solo dopo che è avvenuto l'incidente.

- Il ruolo della PPC non sempre è efficace. La Personal Information Protection Commission rimane l'attore chiave per dare concretezza agli obblighi tramite linee guida e Q&A, incluse indicazioni sul trattamento delle "specific personal information". Tuttavia, in un'infrastruttura identitaria, le linee guida risultano più incisive quando devono orientare comportamenti diffusi, ma diventano meno determinanti quando servono

standard tecnici realmente vincolanti. Il che significa che la PPC può presidiare il quadro di regole e intervenire sulle prassi, ma la resilienza operativa dipende da come tali regole vengono tradotte in procedure.

5.2.3 Dinamiche strutturali

Per comprendere perché My Number abbia generato un "trust shock" pur in presenza di un tasso complessivo di errori contenuto (0,01% nella Total Inspection), occorre spostare l'attenzione dal singolo incidente a tre dinamiche strutturali.

- L'interoperabilità come moltiplicatore del rischio. Il disegno di My Number non coincide con un unico archivio, infatti i dati restano distribuiti nelle amministrazioni competenti, mentre identificatore e meccanismi di coordinamento abilitano verifiche e scambi. Proprio questa rete, però, fa sì che l'errore non sia isolato. Se una prassi di registrazione o un flusso di abbinamento è difettoso, può produrre una serie di casi simili, perché la medesima regola operativa viene applicata su scala nazionale. L'errore diventa quindi scalabile perché lo è la procedura stessa.

- Il trade-off tra accelerazione dell'adozione e maturità operativa. La spinta alla digitalizzazione aumenta i benefici, ma riduce tolleranza per l'errore. Quando l'identità digitale diventa parte del rapporto quotidiano con servizi essenziali, la soglia di accettabilità si abbassa. L'utente non valuta più My Number come innovazione in corso di sviluppo, ma come infrastruttura da cui dipendono prestazioni e diritti. In questo passaggio di scala, eventuali errori diventano socialmente intollerabili, anche se rari, perché colpiscono l'identità come chiave dell'accesso.

- La fiducia è una variabile operativa. Un contributo utile è dalla percezione del rischio privacy e adozione di servizi digitali. In uno studio basato su survey, Ōiso, Ida e Kuroda analizzano la relazione tra il rischio percepito e probabilità di adozione per vari servizi, includendo esplicitamente la My Number Card. Il risultato è che la percezione del rischio e la fiducia incidono sull'adozione, con la comunicazione pubblica degli incidenti accompagnata dalle misure di risposta e prevenzione che può influenzare la dinamica della fiducia. In questa prospettiva, la Total Inspection e la pubblicazione dei risultati possono essere lette come una strategia di recupero della credibilità rendendo visibili errori e contromisure per ridurre l'incertezza percepita e stabilizzare l'adozione (Ōiso et

al., 2024).

Per riassumere, le criticità di My Number non provano automaticamente l'inadeguatezza del My Number Act o dell'APPI. Mostrano però dove si colloca un punto debole tipico delle infrastrutture identitarie nel modello giapponese ovvero la distanza tra architettura normativa e resilienza operativa. Quando l'identità è infrastruttura, la tutela dipende anche dalla capacità di rendere affidabili e verificabili i passaggi di implementazione lungo una rete amministrativa complessa, in cui errori di registrazione e di allineamento possono propagarsi e frammentare la responsabilità.

È su questa stessa distanza che si innesta il caso blockchain come proposta di diversa collocazione della fiducia, con costi giuridici propri che richiedono un esame rigoroso.

5.3 Blockchain e identità digitali

Le criticità emerse tra il 2023 e il 2024 per My Number (v. 5.2) hanno chiarito che la vulnerabilità non riguarda solo l'attacco informatico o con l'uso fuori dallo scopo, ma ha anche sottolineato che l'errore ordinario diventa sistemico perché si propaga lungo catene di interoperabilità. A partire da questo contesto, la blockchain entra nel dibattito pubblico giapponese come insieme di scelte architetturali finalizzate a rafforzare verificabilità e tracciabilità di passaggi specifici come, ad esempio, il rilascio e la validità di attestazioni, l'integrità di registri per la prova temporale di eventi, riducendo la dipendenza da verifiche manuali e da circuiti amministrativi non sempre trasparenti. Oltre al mettere i dati personali su blockchain, parliamo anche dell'adozione di modelli DID/VC (Decentralized Identifiers / Verifiable Credentials) e di un paradigma di Trusted Web che può usare registri distribuiti. (Cabinet Secretariat, 2023).

5.3.1 Struttura della blockchain

Iniziamo parlando di cos'è e come funziona lo strumento che è blockchain. Sul piano tecnico, una blockchain è una famiglia di sistemi di registro distribuito (distributed ledger) in cui una rete di nodi mantiene, secondo regole condivise, una cronologia di transazioni o eventi. Ha due caratteristiche principali che spiegano perché questa tecnologia venga proposta, a seconda dei casi, per criptovalute, supply chain, certificazioni e anche servizi pubblici. Queste caratteristiche sono l'integrità verificabile

delle registrazioni e la possibilità di coordinare attori che non vogliono affidarsi a un unico database controllato da un soggetto centrale (Yaga et al., 2018; Böhme et al., 2015).

Dal punto di vista della struttura dei dati, le informazioni vengono raggruppate in blocchi. Ogni blocco incorpora un valore crittografico chiamato hash che dipende dal suo contenuto. Il blocco successivo include, a sua volta, l'hash del blocco precedente. Questa concatenazione permette che nel caso in cui un blocco passato venisse alterato, cambierebbe il suo hash e di conseguenza la catena risulterebbe incoerente e quindi riconoscibile come manomessa. Più che a rendere impossibile l'alterazione, serve a renderla evidente e onerosa, a seconda delle regole di consenso adottate e del tipo di rete (Yaga et al., 2018).

La blockchain, tuttavia, non è solo un formato di memorizzazione. È anche un insieme di procedure che consente ai nodi di concordare quale sia la versione valida del registro e in quale ordine aggiungere nuovi blocchi. Nei sistemi permissionless (aperti), come ad esempio Bitcoin, l'accordo è legato a meccanismi economico-computazionali definiti proof-of-work, che rendono costosa la riscrittura della storia delle transazioni. Questo modello fa sì che nessun attore controlli stabilmente la maggioranza della capacità rilevante (Nakamoto, 2008). Nei sistemi permissioned (a partecipazione controllata), più diffusi in contesti pubblici, gli equilibri cambiano con l'affidabilità che dipende in misura maggiore dalla governance decisa in precedenza e in misura minore dagli incentivi economici di una rete aperta (Yaga et al., 2018). Scegliere la decentralizzazione in ambito pubblico rappresenta una variabile strutturale che incide su accountability e gestione del rischio.

Un ulteriore livello è la crittografia a chiave pubblica. Nella maggior parte delle architetture blockchain, l'autorizzazione a compiere operazioni è basata su coppie di chiavi pubblica/privata e firme digitali. La firma prova che chi controlla la chiave privata ha autorizzato una transazione o una dichiarazione, con l'idea di spostare una parte della fiducia su verifiche crittografiche e non solo su registrazioni custodite in un database centrale (Yaga et al., 2018). Infine, in alcune piattaforme è possibile eseguire codice sulla rete sotto forma di smart contract ovvero programmi che applicano regole e registrano stati (ad esempio validità, revoca, timestamp), producendo effetti verificabili dai partecipanti. Tuttavia, nei servizi pubblici lo smart contract opera come registro di stato

o come meccanismo di prova, mentre dati personali e valutazioni sostanziali restano in ambienti governabili off-chain (Buterin, 2014).

Inoltre, non bisogna dimenticare che la blockchain nasce con le criptovalute e poi si estende ad altri usi. Bitcoin è il primo caso di successo, il quale combina un registro distribuito, proof-of-work e incentivi economici per evitare la doppia spesa senza un'autorità centrale (Nakamoto, 2008). Da lì, la tecnologia si amplia: criptovalute e pagamenti; tokenizzazione; finanza decentralizzata; NFT; prove temporali; supply chain; certificazioni. Dal punto di vista giuridico, questo comporta che blockchain non è una categoria unica. Cambiano drasticamente rischi e compatibilità con la protezione dei dati a seconda che la rete sia pubblica o permissioned e, soprattutto, a seconda che i dati personali siano registrati on-chain o restino off-chain (Yaga et al., 2018). In Giappone, inoltre, le attività collegate alle criptovalute e i crypto-assets ricadono in un quadro regolatorio specifico nella disciplina dei servizi di pagamento, cioè il Payment Services Act del 2009.

Nel caso dell'utilizzo della blockchain nei servizi pubblici, all'immutabilità si aggiunge anche come progettare verificabilità e correzione senza trasformare l'infrastruttura in un sistema rigido o incompatibile con rettifica e aggiornamento.

5.3.2 I registri di fiducia

Nel dibattito contemporaneo sull'identità digitale, l'asse si è spostato dalla blockchain intesa come registro universale alla blockchain come infrastruttura di supporto per identificatori e credenziali verificabili. In questo contesto, gli standard W3C definiscono l'ordine e aiutano ad evitare equivoci.

Il W3C definisce i Decentralized Identifiers (DID) come identificatori progettati per essere gestiti dal controller tramite metodi crittografici, senza richiedere necessariamente un identity provider unico e centralizzato (W3C, 2022). L'aspetto tecnicamente e giuridicamente rilevante è che il DID non impone una tecnologia specifica. Può appoggiarsi a blockchain, ma anche a registri non-blockchain o a soluzioni ibride. DID è un modello di identificazione che può, in alcuni casi, essere supportato da un registro distribuito. Le Verifiable Credentials (VC) sono, invece, attestazioni firmate digitalmente (ad esempio "è iscritto a X", "possiede il requisito Y") che un soggetto può conservare e

presentare a terzi in modo verificabile, senza che il verificatore debba interrogare ogni volta la base dati originaria (W3C, 2025). Questa impostazione favorisce minimizzazione e selettività informativa perché presenta la prova di uno status e non l'intero dossier personale. In concreto, però, richiede governance per processi di revoca, aggiornamento e chiarimento dei ruoli lungo la catena di emissione e verifica.

Dal punto di vista del design, le implementazioni realistiche per servizi pubblici tendono a evitare la scrittura di dati personali on-chain. Più spesso l'architettura combina componenti off-chain e on-chain in modo che le informazioni personali restino in ambienti governabili, mentre il registro ospita prove di integrità o temporalità (hash, timestamp) oppure pubblica stati (valida/non valida, revocata/non revocata) di una credenziale senza includerne il contenuto. È precisamente questa combinazione tra elementi off-chain e on-chain che permettono la verificabilità con l'esigenza di correggere errori e aggiornare informazioni senza inseguire la cancellazione di dati su un registro replicato (Yaga et al., 2018)

Queste premesse consentono di interpretare meglio il concetto di Trusted Web dove l'obiettivo non è sostituire My Number con una blockchain, ma costruire strati di fiducia verificabile per funzioni specifiche, lasciando i dati personali in domini di controllo più tradizionali.

5.3.3 Trusted Web

Nel caso giapponese, emerge una cornice che collega circolazione del dato, fiducia e verificabilità. Il riferimento più diretto è la Trusted Web initiative, sviluppata nell'ambito delle politiche sul digital market e sulla trasformazione digitale, che propone un'architettura per rendere più affidabili scambi e attestazioni nel web e registrazioni verificabili di eventi, mantenendo un'impostazione dichiaratamente neutrale (Cabinet Secretariat, 2023). La neutralità, in questo caso, consente di includere registri distribuiti come opzione per audit e proof-of-integrity, senza trasformare la blockchain in un contenitore di dati personali.

Dentro questa traiettoria, un secondo snodo importante è l'avvio di iniziative istituzionali specifiche sulle VC. La Digital Agency ha avviato nel 2025 un lavoro esplicito sulla governance delle credenziali verificabili. La documentazione resa pubblica colloca la

prima riunione nel marzo 2025 e inquadra l'obiettivo in termini di affidabilità e criteri di utilizzo nelle procedure amministrative (Digital Agency, 2025). Anche qui, dobbiamo sottolineare il trade-off reso evidente da My Number: ridurre errori scalabili e passaggi manuali attraverso prove verificabili, senza introdurre un nuovo identificatore e senza creare irreversibilità ingestibili.

Possiamo dire che la traiettoria giapponese appare orientata a un uso sobrio della blockchain: usa come supporto e non come deposito di identità. Le VC vengono usate come strumento per attestare requisiti e status, ma sempre con governance e standard come presupposti. Quando il problema principale è la resilienza operativa e la fiducia nella catena, la risposta più che inasprire i divieti, è quella progettare controlli verificabili e scalabili.

5.3.4 Compatibilità con APPI e My Number

L'integrazione di componenti blockchain/DID/VC nei servizi pubblici non produce automaticamente maggiore tutela, ma sposta la tutela su nuove scelte architetturali. I nodi principali, letti attraverso APPI e attraverso il My Number Act, possono essere ricondotti a quattro profili che richiedono, ciascuno, scelte di design coerenti.

Il primo profilo riguarda la responsabilità giuridica lungo la catena. Nel modello VC, coloro che inseriscono, detengono e verificano sono ruoli funzionali diversi che non riconducono automaticamente su un unico titolare del trattamento. In un servizio pubblico possono essere enti diversi ed inoltre entrano in gioco soggetti tecnici (come fornitori e gestori) che incidono su trattamento e sicurezza. Il rischio, sul piano della legittimazione, è simile a quello emerso per My Number ovvero responsabilità distribuita e accountability percepita come unitaria. La differenza è che qui la catena include anche regole crittografiche e registri di stato, ma la complessità aumenta invece di diminuire (Cabinet Secretariat, 2023; W3C, 2025).

Il secondo profilo riguarda minimizzazione e limitazione della finalità. Le VC consentono, almeno in teoria, di presentare solo ciò che serve ("ha il requisito X") senza trasferire l'intero set informativo, il che rappresenta un vantaggio immediato in termini di minimizzazione. Tuttavia, un'identità o una credenziale riutilizzabile può diventare un

identificatore di fatto se viene presentata in molti contesti senza cautele anche senza contenuto sensibile, poichè la ripetizione può generare correlazione e ricostruzione di pattern. Per un ordinamento già sensibile a questo rischio, la progettazione deve prevedere una riduzione dei metadati osservabili e misure che impediscano che l'ecosistema VC diventi, per accumulo di usi, una chiave universale (W3C, 2025).

Il terzo profilo riguarda rettifica, aggiornamento e cancellazione. Il conflitto classico fra blockchain e protezione dei dati riguarda l'immutabilità, ma nel pubblico l'uso più plausibile non è mettere dati personali on-chain, bensì pubblicare prove e stati e mantenere off-chain i contenuti. In questo modo la correzione richiede che lo stato della credenziale venga aggiornato e che il verificatore sia obbligato a controllare tale stato piuttosto di una rimozione. È un meccanismo coerente con quanto detto precedentemente: se l'errore scala, serve un modo strutturale e uniforme di correggere e propagare la correzione lungo tutta la catena (Yaga et al., 2018).

Il quarto profilo riguarda trasferimenti e superficie di rischio. Anche se non si scrivono dati personali in chiaro, un registro pubblico globale può esporre metadati osservabili e replicati fuori giurisdizione. Da qui la tendenza, nelle architetture istituzionali, a preferire soluzioni permissioned o comunque governate, dove l'on-chain sia limitato a ciò che è strettamente necessario per auditabilità e dove lo scambio di VC sia progettato per evitare riusi incontrollati. La Trusted Web initiative riflette questa cautela e registra l'esigenza di verificabilità e tracciabilità, insistendo sulla neutralità tecnologica e sulla necessità di un design che non trasformi l'infrastruttura di fiducia in un nuovo vettore di rischio (Cabinet Secretariat, 2023).

Possiamo riassumere dicendo che la blockchain non appare, nel percorso giapponese, come soluzione a My Number, ma come possibile risposta a un problema specifico emerso con chiarezza negli incidenti del 2023 e del 2024: rendere verificabili e scalabili alcuni passaggi critici senza affidarsi esclusivamente a controlli a posteriori e a catene amministrative eterogenee. I sistemi My Number e Blockchain hanno due modi diversi di collocare la fiducia, ma rispondono allo stesso problema.

5.4 Confronto tra My Number e Blockchain

Il filo che collega i due casi analizzati fin qui è di tipo istituzionale. My Number e le traiettorie giapponesi su registri di fiducia rispondono alla stessa domanda di fondo, resa più urgente dagli incidenti del 2023–2024. Come si mantiene affidabile una catena decisionale pubblica quando l'identità digitale diventa la chiave ordinaria per l'accesso a prestazioni e procedure? Soprattutto se la qualità del dato e dei collegamenti non può più essere data per scontata (v. 5.2–5.3). La differenza decisiva riguarda dove viene collocata la fiducia e, di conseguenza, quale tipo di fallimento tende a emergere per primo.

Da un lato, My Number è un'infrastruttura di coordinamento amministrativo fondata su finalità tipizzate e su una rete di soggetti pubblici che scambiano e verificano informazioni attraverso sistemi standardizzati. L'Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures nasce per rendere possibile la verifica incrociata di informazioni appartenenti a domini diversi e, al contempo, per introdurre restrizioni sulle specific personal information, riconoscendo implicitamente che un identificatore stabile produce rischi qualitativamente diversi rispetto a trattamenti ordinari (My Number Act, 2013).

Dall'altro lato, l'ecosistema blockchain non propone necessariamente un'alternativa anti-statale, né una sostituzione di My Number. Nelle declinazioni più compatibili con il percorso giapponese, il punto è rendere verificabili alcune proprietà chiave dei flussi informativi, tali integrità, provenienza, validità e revoca delle attestazioni. In questa prospettiva, registri distribuiti possono diventare una componente dell'architettura di fiducia, ma non il luogo dove risiede il dato vero e proprio. Il baricentro si sposta su prove verificabili e su regole di governance per lo scambio di credenziali (Digital Agency, 2025).

5.4.1 Collocamento della fiducia

Nel modello My Number, la fiducia poggia sul disegno giuridico e sulla capacità dell'apparato pubblico di farlo vivere lungo una rete estesa. In termini funzionali, il sistema punta a rendere controllabile l'interoperabilità. Si accetta che un'identità stabile sia lo strumento più efficiente per allineare banche dati e procedimenti, ma si cerca di governarne l'effetto moltiplicatore attraverso un perimetro d'uso definito dalla legge, regole speciali sulla circolazione del numero e delle informazioni che lo includono, e una

catena di responsabilità che resta pubblica (My Number Act).

In questo contesto l'affidabilità non dipende solo dal divieto di utilizzare il sistema fuori dallo scopo per il quale è stato creato. Dipende anche da condizioni operative che spesso non sono visibili nella norma, ma determinano la tutela concreta: accuratezza dei registri, correttezza del matching, uniformità delle procedure nei punti di frontiera (sportelli, enti locali, strutture sanitarie), qualità degli standard tecnici e capacità di audit. Gli incidenti del 2023–2024 hanno mostrato che, anche quando il trattamento è formalmente lecito, l'errore può diventare sistemico perché la procedura è scalabile quanto lo è l'interoperabilità. Ne deriva una fragilità tipica delle reti amministrative complesse dove l'accountability è distribuita nella catena applicativa, ma la percezione pubblica rimane unitaria. Se un errore consente di visualizzare informazioni sanitarie altrui, per l'utente non fallisce un singolo ufficio, fallisce "lo Stato".

Nell'ecosistema blockchain, la fiducia tende invece a essere spostata su prove verificabili e su meccanismi che rendono più difficile, o comunque più evidente, la manipolazione a posteriori. Un registro distribuito e crittografie possono offrire integrità verificabile e coordinamento senza dipendere da un unico database controllato da un singolo attore (Yaga et al., 2018). In concreto, questo non elimina l'istituzione, cambia solo la modalità del controllo. Accanto alla fiducia procedurale, viene introdotta una fiducia controllabile, quella sulla catena.

Gli standard W3C formalizzano bene questa tensione. Il DID è un identificatore progettato per essere gestito dal controller tramite metodi crittografici, senza presupporre per definizione un identity provider centrale, le Verifiable Credentials invece sono attestazioni firmate digitalmente che un holder può presentare a un verificatore (verifier), riducendo la necessità di interrogare ogni volta la base dati originaria (W3C, 2025). In ottica APPI, questa minimizzazione riduce i campi e implica una progettazione di scambi basati su requisiti e prove, con minore esposizione di dati non necessari.

Tuttavia, questo spostamento ha un costo, poiché la fiducia tecnica richiede governance. Se la catena si fonda su attestazioni, chiavi e registri di stato, diventa essenziale stabilire chi definisce gli schemi delle credenziali, chi controlla la qualità dell'emissione, come si gestisce la revoca, come si evitano correlazioni tra presentazioni ripetute, quale

infrastruttura garantisce risoluzione e controllo dello stato. Non dobbiamo sorprenderci che il percorso giapponese più coerente con un uso pubblico delle VC assuma la forma di un lavoro istituzionale sulla governance, più che di un'adozione della blockchain come registro generalista (Digital Agency, 2025).

5.4.2 Rischi speculari

Il confronto diventa più chiaro se si osserva come cambiano i rischi dominanti, cioè quelli che tendono a emergere anche in assenza di malafede.

Nel caso My Number, il rischio caratteristico è che l'identificatore stabile agisca da leva verso riusi incrementali. La legge speciale nasce proprio per evitare che l'identificatore diventi a scopo generico e per impedire che la protezione sia affidata soltanto a consenso e trasparenza, strumenti strutturalmente deboli quando l'infrastruttura diventa condizione ordinaria di accesso a servizi essenziali come ad esempio quelli sanitari. Tuttavia, la vulnerabilità più delicata riguarda lo slittamento amministrativo dei casi d'uso e, soprattutto, l'errore di collegamento che si propaga lungo la rete. Il sistema può rispettare formalmente confini di finalità e di competenza, ma se la catena produce collegamenti e visualizzazioni errate, l'effetto sulla fiducia pubblica è immediato perché l'identità è la premessa di ogni trattamento successivo (v. 5.2).

Nel modello DID/VC, l'equivalente funzionale passa dalla correlazione e dalla ri-identificazione di fatto. La promessa delle credenziali è selettività informativa, ma se lo stesso identificatore, la stessa credenziale o gli stessi metadati sono osservabili ripetutamente in contesti diversi, è possibile ricostruire pattern e legami tra eventi anche senza accedere al contenuto sensibile dell'attestazione. È un rischio esplicitamente richiamato negli standard e che impone scelte di design, come identificatori contestuali che limitino la tracciabilità delle presentazioni (W3C, 2025). In termini di compatibilità con My Number, qualsiasi sistema di credenziali pubbliche che finisse per funzionare come identificatore trasversale, anche senza chiamarsi numero nazionale, riprodurrebbe sotto altra forma lo stesso problema politico-sociale che accompagna My Number sin dall'origine. Un secondo asse riguarda la capacità di correggere gli errori. Nella governance pubblica tradizionale, correggere significa modificare un record, aggiornare un registro, riallineare basi dati. Il problema, come mostra My Number, è far sì che la

correzione si propaghi in modo coerente lungo la catena, senza lasciare copie incoerenti e senza aprire nuove frizioni amministrative (v. §5.2). Nel mondo blockchain, l'immutabilità è spesso presentata come pregio, ma dal punto di vista della protezione dei dati può diventare un vincolo se interpretata come registrazione irreversibile di contenuti personali. Per questa ragione, le configurazioni realistiche in ambito pubblico tendono a evitare dati personali on-chain e a concentrare l'on-chain su prove e stati, in modo che la correzione si traduca in revoca o aggiornamento dello stato di validità, mantenendo governabili off-chain i contenuti sostantivi (W3C, 2025). Questo può rispondere, almeno in astratto, a ciò che abbiamo introdotto nel paragrafo precedente. Se l'errore scala, la correzione deve essere scalabile e verificabile lungo tutta la catena, ma ciò vale soltanto se l'obbligo di controllare lo stato è incorporato nelle procedure dei verificatori e se la governance dell'infrastruttura è definita in modo non ambiguo. Un terzo asse riguarda i confini regolatori e il modo in cui l'ordinamento incanala la tecnologia. My Number ha beneficiato di una scelta legislativa esplicita fin dall'inizio con il My Number Act. Nel caso blockchain, l'esperienza giapponese mostra invece una biforcazione netta. Quando si parla di crypto-assets e mercati, la blockchain entra in una disciplina settoriale come quella dei servizi di pagamento, che tratta gli asset crittografici come oggetto regolatorio e non come semplice tecnologia neutra. Ricordiamo infatti che il Giappone è uno dei paesi con una delle governance più chiare riguardo le cryptovalute. Quando invece si parla di fiducia digitale e servizi pubblici, l'orientamento più credibile è quello di una governance tecnico-istituzionale compatibile con APPI, che eviti la costruzione di un'identità parallela generalista e che privilegi l'uso di attestazioni verificabili in contesti determinati (Digital Agency, 2025).

Questo confronto va letto come tra due modi di ottenere affidabilità in un ecosistema complesso. My Number affida l'affidabilità a legalità tipizzata e coordinamento amministrativo, mentre DID/VC la affidano a prove verificabili e a un disegno che può ridurre la circolazione del dato, ma che richiede una governance rigorosa di standard, ruoli e responsabilità. Nessuna delle due architetture è in realtà superiore all'altra. My Number diventa fragile quando l'errore scalabile mina la fiducia nella catena pubblica, le architetture basate su credenziali diventano fragili quando la governance non impedisce correlazione e quando revoca e stati di validità non sono integrati in obblighi procedurali e controlli effettivi.

In questa prospettiva, il confronto vuole sottolineare che un'identità digitale pubblica affidabile richiede sia un perimetro legale chiaro (con finalità tipizzate e responsabilità decise), sia meccanismi tecnici che rendano verificabili e correggibili gli errori nei punti di maggiore rischio (collegamenti tra registri e propagazione di correzioni). Il lavoro giapponese sulla governance delle Verifiable Credentials sembra muoversi in questa direzione, senza decentralizzare l'identità come fine, ma rendendo più robusta la catena di fiducia, introducendo verificabilità dove l'errore amministrativo ordinario rischia di diventare sistemico (Digital Agency, 2025). Per il Giappone, la lezione non impone una scelta tra My Number e blockchain, ma suggerisce di aumentare la dei passaggi critici tramite standard procedurali più solidi e registri di stato che consentano di verificare integrità e validità delle operazioni, senza replicare on-chain dati personali né creare un nuovo identificatore trasversale.

5.5 SPID come terza via

Il confronto con SPID ci viene in aiuto per capire meglio il concetto di fiducia e di come conti come un ordinamento costruisce la fiducia nella filiera che identifica le persone e fa circolare dati tra organizzazioni. Le infrastrutture d'identità non sono semplici strumenti di accesso, servono a stabilire quali collegamenti siano facili, quali controlli siano scalabili e quali errori possano propagarsi come input in processi automatizzati. Questa lettura infrastrutturale è coerente con la letteratura che analizza i sistemi d'identità come dispositivi socio-tecnici. Il rischio non dipende solo dalla tecnologia, ma dall'intreccio tra architettura, governance e aspettative pubbliche (Whitley, Hosein, 2010)

Nel modello italiano, SPID nasce precisamente come strato di autenticazione federata. L'utente ottiene credenziali presso un soggetto accreditato (Identity Provider) e le utilizza per accedere ai servizi (service provider) secondo regole tecniche e organizzative comuni. La base normativa è incardinata nel Codice dell'Amministrazione Digitale (D.Lgs. 82/2005, art. 64) e nel DPCM 24 ottobre 2014, che definisce caratteristiche, ruoli e requisiti del sistema pubblico di identità digitale (CAD, 2005; Presidenza del Consiglio dei Ministri, 2014). SPID standardizza soprattutto la relazione di accesso (chi sei/ puoi entrare), non la sincronizzazione sostanziale dei registri amministrativi sottostanti.

Questa scelta architetturale cambia immediatamente il legame tra identità e automazione. Un'identità che abilita interoperabilità profonda tra enti (come My Number) tende a creare un data layer riusabile per verifiche incrociate e, in prospettiva, per servizi proattivi e decisioni data-driven. Questo lo espone a rischi sistemici quando l'errore di collegamento diventa replicabile lungo catene operative eterogenee (v. 5.2). SPID, invece, lascia più visibile la frammentazione dei registri. L'accesso è unificato, ma il patrimonio informativo resta distribuito e meno naturalmente integrabile in dataset uniformi. Questo porta ad un trade-off di tipo strutturale, dove l'automazione massiva e riuso dei dati sono meno immediati, ma c'è anche minore probabilità che un errore di collegamento identitario si propaghi automaticamente tra domini diversi, contaminando più procedure e più basi dati (Whitley, Hosein, 2010).

Proprio perché SPID non nasce per coordinare a valle i dati tra amministrazioni, le vulnerabilità dominanti si spostano. La fiducia si concentra su due snodi: identity proofing/enrollment (quanto è robusta la verifica iniziale dell'identità) e autenticazione (quanto sono resilienti credenziali, canali e procedure). Questa ricollocazione del rischio permette di distinguere enrollment, autenticazione e federazione e e a capire dove si formano gli errori e come possono essere sfruttati o amplificati (Yaga et al., 2018). In questo senso, SPID la colloca la fiducia negli intermediari accreditati e nei controlli su processi e standard, riducendo la dipendenza da un collegamento identitario unico. L'evoluzione tecnica del sistema conferma questa impostazione. L'attenzione italiana si è concentrata nel tempo anche su standard di integrazione e federazione più moderni, fra cui OpenID Connect, con documenti di indirizzo e regole tecniche che mirano a garantire interoperabilità e sicurezza del layer di autenticazione (AgID, 2021). Si rafforzano i meccanismi di accesso e scambio di asserzioni d'identità, non si costruisce automaticamente un meccanismo di allineamento sostanziale dei registri amministrativi.

Il nesso con l'IA diventa più chiaro se si guarda alla catena causale degli errori. Nei sistemi che alimentano automazione e decisioni algoritmiche, il fulcro è la qualità del dato e correttezza dell'attribuzione. La letteratura sui pericoli in machine learning insiste sul fatto che danni e discriminazioni possono nascere a monte, prima del modello, quando i dati sono incompleti, distorti o attribuiti in modo errato (Suresh, Guttag, 2019). In un'infrastruttura identitaria orientata all'interoperabilità, l'errore di collegamento non

resta un errore amministrativo isolato, diventando un errore di input che può essere riusato e replicato in processi automatizzati. È un punto analogo a quello dei sistemi data-driven che possono produrre impatti disparati nonostante una legalità formale del trattamento, perché gli effetti emergono dalla combinazione tra dati e contesto d'uso (Selbst et al., 2019).

Possiamo quindi utilizzare SPID come controllo comparativo, perché ci mostra cosa cambia quando l'identità digitale non è progettata come chiave di interoperabilità. Se il sistema non tende a unificare i registri, la probabilità di contaminazione orizzontale da errori di collegamento diminuisce. Al tempo stesso, diventa più difficile costruire in modo automatico dataset amministrativi omogenei e riusabili per l'IA pubblica. In altre parole, SPID attenua alcuni rischi per design, ma sposta l'attenzione su altri rischi come compromissione credenziali, errori di proofing, incidenti sugli intermediari, e più in generale vulnerabilità tipiche degli ecosistemi federati (Whitley, Hosein, 2010). Questa è la stessa logica che abbiamo già osservato con la differenza fra enforcement classico e resilienza operativa.

Con blockchain, invece, abbiamo visto l'idea di far circolare attributi verificabili invece di dossier completi, riducendo la necessità di interrogare continuamente basi dati originarie. In astratto, questo rafforza minimizzazione e controllo contestuale, in pratica, introduce una domanda di governance su revoca, aggiornamento e correlazione (W3C, 2025). Parlando di IA, un'architettura basata su attributi granulari può ridurre l'eccesso informativo e la profilazione involontaria, ma solo se la filiera di attestazione e status è governata in modo rigoroso (Selbst et al., 2019). Quindi SPID rappresenta una sorta di terza via che standardizza l'accesso, ma non l'attribuzione selettiva e verificabile di attributi riusabili.

In questa prospettiva, l'evoluzione europea verso il portafoglio di identità digitale mostra una convergenza. Il legislatore europeo ha rafforzato il quadro normativo per un'identità digitale che supporti anche attributi e attestazioni, non solo autenticazione. La riforma eIDAS (European Union 2024/1183) mira a rendere disponibile un'identità digitale utilizzabile in un ampio spettro di servizi, con un impianto che riconosce esplicitamente il tema del controllo e della protezione dei dati in un ecosistema transfrontaliero. (European Union 2024/1183, 2024). La letteratura più recente, pur con accenti diversi,

tende a leggere questa traiettoria come un tentativo di combinare interoperabilità e minimizzazione tramite portafogli digitali e credenziali, spostando parte della fiducia su attestazioni e verifiche più standardizzate (European Union, 2024a).

L'Italia si inserisce in questa dinamica con il Sistema IT-Wallet, che esplicitamente si collega al quadro europeo e introduce un livello ulteriore rispetto a SPID che implementa gestione di documenti e attestazioni in forma digitale, con problemi di validità, aggiornamento e governance che richiamano da vicino i temi discussi per VC e registri di stato. La documentazione istituzionale italiana colloca IT-Wallet nel quadro eIDAS 2.0 e richiama anche il fondamento interno nel CAD (art. 64), chiarendo che l'obiettivo è costruire un'infrastruttura nazionale coerente con i progetti europei sul wallet (Dipartimento per la trasformazione digitale, 2025). Questo progetto ci interessa particolarmente, perché mostra la tendenza a separare sempre più identità come accesso e attributi verificati, con un impatto diretto su come l'IA pubblica può (o non può) essere alimentata con dati verificabili, ma minimizzati.

My Number mette a fuoco la fragilità di un'identità-infrastruttura quando l'errore operativo ordinario diventa sistemico e l'accountability si disperde in una rete ampia. DID/VC mostrano come l'affidabilità possa essere ripensata come verificabilità di attributi e stati, ma richiedono una governance stringente per evitare correlazione e zone grigie su revoca e responsabilità. SPID mostra invece cosa accade quando l'identità digitale resta soprattutto un layer di accesso federato dove l'automazione data-driven su scala nazionale è meno naturale, ma alcuni rischi di propagazione orizzontale degli errori identitari sono attenuati perché l'architettura non nasce per collegare registri eterogenei.

Possiamo chiudere dicendo che non si governa l'IA ignorando la filiera dei dati. La correttezza algoritmica non si decide solo nel modello o nella regola astratta di trasparenza, ma nella capacità dell'infrastruttura di garantire attribuzione corretta, aggiornamento e rettificabilità prima che l'informazione diventi input in processi automatizzati. La ricerca sui danni in ML è chiara nel collocare molte fonti di danno a monte nelle fasi di produzione dei dati, categorizzazione, etichettatura, nelle scelte di pipeline e nelle asimmetrie istituzionali che determinano che cosa conta come segnale (Selbst et al., 2019). Quando l'identità digitale opera come chiave di interoperabilità, un errore di collegamento può trasformarsi in esclusione indebita, attribuzione errata o

decisione automatizzata viziata anche senza alcuna malafede e anche in presenza di un trattamento formalmente lecito. Il principio di accuratezza, che nel diritto della protezione dei dati è spesso letto come obbligo procedurale, diventa qui un requisito infrastrutturale poiché senza accuratezza e controllabilità a monte, l'IA tende ad amplificare l'errore (Selbst et al., 2019).

Per il Giappone, in un contesto orientato a servizi proattivi e automazione amministrativa, la fiducia non si costruisce soltanto con linee guida sugli algoritmi, ma rendendo robusta la catena identitaria e i meccanismi di collegamento e aggiornamento dei dati che alimentano l'automazione. Questo non implica imitare SPID né adottare blockchain come soluzione unica. Implica riconoscere che, quando l'identità diventa infrastruttura di interoperabilità, deve essere governata come componente critica: standard operativi uniformi, ruoli chiari, controlli scalabili, e strumenti che rendano l'errore non solo individuabile, ma anche correggibile e verificabile lungo tutta la catena. L'IA pubblica sicura si fonda dall'identità e dalla qualità del dato che l'amministrazione decide di rendere interoperabile, con la sua governance.

CONCLUSIONI

Questa tesi ha indagato in che misura l'Act on the Protection of Personal Information (APPI) riesce a intercettare i rischi connessi all'uso dell'intelligenza artificiale in Giappone. Inoltre, sono stati presi in analisi quali limiti strutturali emergono quando tecnologie basate su apprendimento automatico, inferenza e generazione di contenuti entrano in contatto con categorie normative costruite in un contesto diverso. Il lavoro svolto nei cinque capitoli dimostra che la questione non è stabilire se l'APPI si applichi all'IA. È capire quando la tutela riesce a essere effettiva nella pratica, lungo filiere distribuite e per interessati che spesso non hanno piena visibilità. Il quadro che emerge è netto. L'APPI resta il riferimento anche nell'era dell'IA perché incide su finalità, trasferimenti, outsourcing, sicurezza e diritti. La sua capacità di garantire una tutela stabile si indebolisce però proprio dove l'IA contemporanea concentra valore e rischio, ovvero nelle inferenze statistiche, negli output generativi, nella gestione di filiere multi-attore e nell'interoperabilità tra basi dati. L'APPI regge come cornice generale, ma perde presa quando il rischio si sposta dal singolo atto di trattamento al comportamento del sistema e della filiera che lo alimenta. Il sistema intercetta bene i trattamenti tradizionali, riconducibili a dati conservati, finalità esplicite e responsabilità chiare. Fatica invece a governare ciò che l'IA fa ai dati attraverso trasformazioni, riusi e apprendimento.

Questo risultato va letto insieme alla scelta giapponese di governance light-touch. Il ricorso esteso a strumenti di soft law permette aggiustamenti rapidi e riduce il rischio di norme che invecchiano troppo in fretta. La flessibilità, tuttavia, ha un costo e molte garanzie finiscono per dipendere da variabili operative che, in un contesto algoritmico, determinano di fatto il livello di protezione. Retention, logging, scelte architetturali sui dataset, policy di riuso e standard interni di test non sono dettagli tecnici, ma fattori che decidono se un rischio viene prevenuto o soltanto gestito a posteriori. Quando questi elementi non si traducono in criteri pubblici e verificabili, la tutela diventa meno prevedibile per gli interessati e più esposta a soluzioni negoziate tra autorità e operatori.

L'analisi evidenzia tre punti che spiegano perché le zone di incertezza siano strutturali. Il primo riguarda la soglia di applicazione dell'APPI, fondata sull'identificabilità e sulla possibilità di collegare un'informazione a un individuo. Nel contesto algoritmico questa soglia si sposta continuamente, perché dipende da dataset

ausiliari disponibili, capacità di correlazione, partnership tecniche e interoperabilità tra sistemi. Un'informazione oggi non identificativa può diventarlo domani senza che cambi il dato in sé, semplicemente perché cambia l'ecosistema che lo rende collegabile. Chi gestisce sistemi complessi conosce la propria capacità di collegamento e le condizioni che la rendono possibile, ma chi ne è oggetto non può valutarne appieno portata e implicazioni. Questa asimmetria sposta la tutela dal tipo di dato al contesto tecnico e rende più difficile per l'interessato attivare diritti in modo davvero informato.

Un secondo punto riguarda gli oggetti informativi che l'IA produce. Punteggi predittivi, profili vettoriali, rappresentazioni interne ai modelli e output probabilistici non si comportano come record statici in un database. L'APPI può incidere su questi fenomeni attraverso definizioni e obblighi generali, ma la tutela effettiva dipende spesso da una condizione molto concreta. L'informazione viene conservata in modo tracciabile e riconducibile all'interessato, rientrando così nei retained personal data, oppure resta effimera, frammentata o non tracciabile. Se manca una conservazione riconducibile, o se la catena di custodia è spezzata lungo la filiera, il diritto rischia di restare formale. La generazione probabilistica è un problema giuridico, poiché cambia il tipo di errore e la possibilità di correggerlo.

Il terzo punto riguarda le filiere distribuite. Le categorie classiche dell'APPI, come trasferimento a terzi e outsourcing, funzionano quando la catena è lineare e il controllo è concentrato. Con foundation model, API globali e servizi cloud, la responsabilità tende a disperdersi. L'operatore a valle può non controllare retention e training, il provider può non identificare l'interessato, l'integratore può non avere visibilità sui dataset utilizzati. Questa frammentazione diventa un problema pratico di accountability. Quando l'interessato richiede accesso, cancellazione o chiarimenti su finalità e riusi, nessun nodo della catena dispone naturalmente di tutte le informazioni necessarie per rispondere in modo completo e verificabile.

Le zone grigie individuate nel corso della tesi sono un prodotto strutturale dell'architettura complessiva del sistema giapponese e questo si riflette anche nell'enforcement. La Personal Information Protection Commission opera prevalentemente in chiave cooperativa, coerentemente con un ordinamento che mira a massimizzare l'adeguamento volontario riducendo attriti amministrativi. Nel settore IA

questa impostazione, però, produce un effetto collaterale. Questo perché la tutela avrebbe bisogno di interpretazioni ripetute e standardizzate su questioni ricorrenti, mentre l'uso prevalente di strumenti non vincolanti e la pressione operativa riducono lo spazio per fissare criteri tecnici stabili. Ciò che dovrebbe diventare una regola replicabile rischia di restare una soluzione negoziata caso per caso.

I casi concreti analizzati rendono questo quadro più visibile. Rikunabi ha mostrato come la circolazione di inferenze predittive ad alto impatto sollevi problemi di qualificazione giuridica e di opacità nelle fasi upstream, dove profili e score vengono costruiti prima di arrivare al punto decisionale. L'intervento amministrativo nei confronti di OpenAI ha evidenziato un altro limite. Quando il rischio è incorporato nella struttura del servizio e l'operatore ha dimensione globale, la segnalazione può indicare una direzione, ma difficilmente trasforma da sola prassi interne in obblighi standardizzati. Diventa allora centrale la traducibilità delle garanzie in controlli verificabili. Se la tutela dipende da filtri, governance dei dataset e policy di riuso dei prompt, servono capacità di audit, obblighi procedurali chiari e maggiore visibilità su aspetti che oggi restano per lo più interni ai provider.

Il sistema My Number aggiunge una dimensione ulteriore perché collega la protezione dei dati alla tenuta di un'infrastruttura pubblica di identificazione e interoperabilità. Gli incidenti che si sono verificati nel 2023 hanno mostrato che la fragilità non nasce soltanto dall'abuso intenzionale, ma anche dall'errore scalabile. I collegamenti errati tra identità e dati sanitari hanno avuto un impatto significativo perché hanno coinvolto informazioni percepite come altamente sensibili. L'utente, di fronte a un errore di abbinamento, percepisce un fallimento unitario dell'infrastruttura pubblica, senza distinguere di quale componente sia effettivamente colpa. Il risultato che emerge è che la fiducia è una variabile regolatoria, non un effetto automatico della legge. In una governance orientata all'innovazione, una crisi di fiducia riduce la legittimazione sociale e, senza legittimazione, la circolazione dei dati diventa politicamente fragile.

Il confronto con blockchain e credenziali verificabili chiarisce che il modo in cui si colloca la fiducia nell'architettura modifica i rischi dominanti. Spostare la verificabilità su prove crittografiche può ridurre l'esposizione di dati non necessari, ma introduce nuove domande di governance su revoca, correlazione e gestione degli errori. Non esiste un

modello superiore in assoluto. Esistono compromessi strutturali. La protezione dei dati, infatti, dipende dalla progettazione della filiera e dall'incorporazione di controlli verificabili.

Questa ricerca vuole mostrare che nel trade-off tra innovazione e protezione, bisogna capire dove e come la protezione diventa effettiva. Non basta che la norma riconosca diritti sulla carta. I diritti devono agganciarsi a oggetti accessibili, correggibili e tracciabili lungo la filiera, dove l'errore deve essere individuabile e la correzione deve essere scalabile. La responsabilità non può dissolversi tra attori che controllano solo frammenti del processo. Quando queste condizioni mancano, la tutela si riduce a un insieme di aspettative formali e il sistema giapponese rischia di ottenere l'opposto di ciò che intende perseguire, cioè una perdita di fiducia che rende più fragile, non più forte, la strategia di crescita digitale.

Guardando avanti, il modello giapponese si trova di fronte a scelte non rinviabili. La flessibilità del light-touch resta un vantaggio solo se accompagnata da meccanismi che trasformino le best practice in standard verificabili, almeno per categorie di trattamenti ad alto rischio. Questo richiede un rafforzamento delle competenze tecniche della PPC e linee guida operative più dettagliate, capaci di chiarire cosa è richiesto in concreto su retention sicura, logging adeguato, audit replicabili e correzione effettiva degli errori. Serve inoltre maggiore chiarezza sui ruoli lungo la filiera algoritmica, così che sviluppatori, integratori, provider e utilizzatori conoscano gli obblighi minimi rispetto a informativa, gestione delle richieste degli interessati e responsabilità in caso di errore. Quando i trattamenti coinvolgono operatori globali e infrastrutture distribuite, l'efficacia degli strumenti cooperativi tende a ridursi. Diventano più importanti forme di cooperazione internazionale e clausole operative standardizzate che rendano concretamente estendibili le garanzie richieste dall'APPI anche oltre confine. Un coordinamento più solido tra PPC, autorità di settore e ministeri competenti può ridurre i rischi di frammentazione senza snaturare l'assetto plurale della governance giapponese. Allo stesso tempo, procedure di consultazione più robuste sugli orientamenti interpretativi possono rafforzare legittimazione e prevedibilità, senza compromettere la velocità di adattamento.

Il caso giapponese offre una lezione che va oltre i confini nazionali. La soft law non è

un'assenza di regole, ma un modo diverso di produrle, che richiede capacità amministrativa e meccanismi credibili di monitoraggio continuo. Il Giappone ha costruito un sistema che privilegia adattabilità e cooperazione. La sfida per il futuro non è difendere il modello in astratto, ma dimostrare che può produrre tutela effettiva proprio dove valore e rischio si generano in modo distribuito, opaco e transnazionale. È su questo terreno che si gioca la sostenibilità dell'equilibrio tra promozione dell'innovazione e protezione dei diritti fondamentali.

BIBLIOGRAFIA

Agency for Cultural Affairs (Bunkachō) 文化庁. (2024). AI to chosakuken ni kansuru ippanteki rikai [AIと著作権に関する一般的な理解 – Comprensione generale su IA e diritto d'autore in Giappone]. Agency for Cultural Affairs. https://www.bunka.go.jp/seisaku/chosakuken/pdf/93903601_01.pdf (ultimo accesso: 15/02/2026)

Agenzia per l'Italia Digitale (AgID). (2021). SPID - Sistema Pubblico di Identità Digitale

. AgID. https://www.agid.gov.it/it/piattaforme/spid (ultimo accesso: 15/02/2026)

AI CERTS (Foundation for Data Privacy & Protection). (2025, November 28). Japan's National Policy Drives Unified AI Governance by 2025. AI CERTS Analysis Platform. https://www.aicerts.ai/news/japans-national-policy-drives-unified-ai-governance-by-2025/ (ultimo accesso: 15/02/2026)

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248). European Commission. https://ec.europa.eu/newsroom/article29/items/611236 (ultimo accesso: 15/02/2026)

Article 29 Data Protection Working Party. (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01). European Commission. https://ec.europa.eu/newsroom/article29/items/612053 (ultimo accesso: 15/02/2026)

Ashmore, Rob, Calinescu, Radu & Paterson, Colin. (2021). Assuring the machine learning lifecycle: Desiderata, methods, and challenges. *ACM Computing Surveys*, 54(5), 1–39. https://doi.org/10.1145/3453444

Atsumi & Sakai. (2023, June 6). Japan's PPC Issues Guidance to OpenAI on Personal Information Protection. Atsumi & Sakai Legal Update. https://www.aplawjapan.com/publications/20230608 (ultimo accesso: 15/02/2026)

Baker McKenzie. (2025). Japan: Discussions for the amendment of the data privacy law https://connectontech.bakermckenzie.com/japan-discussions-for-the-amendment-of-

the-data-privacy-law/ (ultimo accesso: 15/02/2026)

Baker McKenzie. (2025). Japan's AI Bill Advances Toward Enactment. https://connectontech.bakermckenzie.com/japans-ai-bill-advances-toward-enactment/ (ultimo accesso: 15/02/2026)

Barocas, Solon & Selbst, Andrew D. (2016). Big Data's Disparate Impact. *California Law Review*, 104, 671–743. https://www.cs.yale.edu/homes/jf/BarocasSelbst.pdf (ultimo accesso: 15/02/2026)

会計検査院 [Board of Audit of Japan]. (2016). Kuni no gyōsei kikan tō ni okeru shakai hoshō–zei bangō seido no dōnyū ni kakaru jōhō shisutemu no seibi tō no jōkyō ni tsuite

[国の行政機関等における社会保障・税番号制度の導入に係る情報システムの整備等の状況について – Stato della predisposizione dei sistemi informativi per l'introduzione del sistema numero sociale e fiscale presso le amministrazioni statali]. https://report.jbaudit.go.jp/org/h28/ZUIJI8/2016-h28-Z8001-0.htm (ultimo accesso: 15/02/2026)

Böhme, Rainer, Christin, Nicolas, Edelman, Benjamin & Moore, Tyler. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2), 213–238. https://doi.org/10.1257/jep.29.2.213

British Institute of International and Comparative Law (BIICL). (2025). Bridging Soft and Hard Law in AI Governance. BIICL Research Paper. https://www.biicl.org/blog/121/bridging-soft-and-hard-law-in-ai-governance (ultimo accesso: 15/02/2026)

Burrell, Jenna. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12. https://doi.org/10.1177/2053951715622512

Buterin, Vitalik. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper. https://ethereum.org/en/whitepaper/ (ultimo accesso: 15/02/2026)

Cabinet Office 内閣府. (2016). Dai 5-ki kagaku gijutsu kihon keikaku

[第5期科学技術基本計画 – Quinto piano di base per la scienza e la tecnologia]. Government of Japan. https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf (ultimo accesso: 15/02/2026)

Cabinet Office 内閣府. (2017). Society 5.0 senryaku bunsho [Society 5.0戦略文書 – Documento strategico Society 5.0]. Government of Japan. https://www8.cao.go.jp/cstp/society5_0/index.html (ultimo accesso: 15/02/2026)

Cabinet Office, AI Policy Study Group 内閣府AI政策検討会. (2025). AI governance policy interim report [AI統治政策中間報告 – Rapporto intermedio sulla politica di governance dell'IA]. Government of Japan. https://www8.cao.go.jp/cstp/ai/interim_report_en.pdf (ultimo accesso: 15/02/2026)

Cabinet Office, Science and Technology Strategy Division 内閣府科学技術政策担当. (2019). AI senryaku 2019 [AI戦略2019 – Strategia IA 2019]. Government of Japan. https://www8.cao.go.jp/cstp/ai/aistratagy2019.pdf (ultimo accesso: 15/02/2026)

Cabinet Secretariat 内閣官房. (2022, August). Trusted Web White Paper Ver. 2.0 (Executive Summary) [トラステッドウェブ ホワイトペーパー ver.2.0概要]. Government of Japan. https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/trustedweb_gaiyou.pdf (ultimo accesso: 15/02/2026)

Cabinet Secretariat 内閣官房. (2025). Dejitaru shakai no jitsugen ni muketa jūten keikaku [デジタル社会の実現に向けた重点計画 – Piano prioritario per la realizzazione della società digitale]. Government of Japan. https://www.cas.go.jp/jp/seisaku/digital_denen/ (ultimo accesso: 15/02/2026)

Carlini, Nicholas et al. (2021). Extracting Training Data from Large Language Models. In Proceedings of the 30th USENIX Security Symposium, 2633–2650. https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting (ultimo accesso: 15/02/2026)

Center for Strategic and International Studies (CSIS). (2025, February). New Government Policy Shows Japan Favors a Light-Touch AI Regulation. CSIS Analysis. https://www.csis.org/analysis/new-government-policy-shows-japan-favors-light-touch-ai-regulation (ultimo accesso: 15/02/2026)

Chambers and Partners. (2025). Data Protection & Privacy: Japan. Chambers Global Practice Guides. https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/japan (ultimo accesso: 15/02/2026)

Citadel AI. (2024, June 25). Japan's AI Guidelines for Business 2024. Citadel AI Blog. https://citadel-ai.com/blog/2024/06/25/ai-guideline-for-business-2024/ (ultimo accesso: 15/02/2026)

Clifford Chance. (2023). JAPANESE LAW ISSUES SURROUNDING GENERATIVE AI. Clifford Chance Briefing. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/10/japanese-law-issues-surrounding-generative-ai-chatgpt-bard-and-beyond.pdf (ultimo accesso: 15/02/2026)

Codice dell'Amministrazione Digitale (CAD). (2005). Decreto legislativo 7 marzo 2005, n. 82. Gazzetta Ufficiale della Repubblica Italiana. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82 (ultimo accesso: 15/02/2026)

Crabtree, Andy et al. (2018). Building accountability into the Internet of Things: the IoT Databox model. *Journal of Reliable Intelligent Environments*, 4(1), 39–55. https://doi.org/10.1007/s40860-018-0054-5

Data Guidance. (2021). Japan: Amended APPI guidelines. Data Guidance Opinion. https://www.dataguidance.com/opinion/japan-amended-appi-guidelines (ultimo accesso: 15/02/2026)

Derrida Debacker Group (DDG). (2025, January 9). Japan's 2025 AI Promotion Act: Structuring Innovation Through Soft Regulation. DDG Legal Analysis. https://www.ddg.fr/actualite/japans-2025-ai-promotion-act-structuring-innovation-through-soft-regulation (ultimo accesso: 15/02/2026)

Digital Agency デジタル庁. (2023). Mainanbā jōhō sōtenken honbu (dai 5-kai) [マイナンバー情報総点検本部（第5回）– Quinta riunione del quartier generale per la verifica complessiva delle informazioni My Number]. Digital Agency. https://www.digital.go.jp/councils/mynumber-all-check/368a251f-02a6-48a5-9125-1e3f138d6b9d (ultimo accesso: 15/02/2026)

Digital Agency デジタル庁. (2025). Mainanbā (kojin bangō) seido・Mainanbā kādo [マイナンバー（個人番号）制度・マイナンバーカード – Sistema My Number (numero personale) e My Number Card]. Digital Agency. https://www.digital.go.jp/policies/mynumber/ (ultimo accesso: 15/02/2026)

Digital Agency デジタル庁. (2026). *My Number kādo fukyū jōkyō dasshu bōdo* [マイナンバーカード普及状況ダッシュボード – My Number Card Penetration Dashboard]. Digital Agency. https://www.digital.go.jp/en/resources/govdashboard/mynumber_penetration_rate (ultimo accesso: 15/02/2026)

Dipartimento per la trasformazione digitale. (2025). Sistema IT-Wallet: il sistema di portafoglio digitale italiano. Presidenza del Consiglio dei Ministri. https://innovazione.gov.it/progetti/sistema-it-wallet/ (ultimo accesso: 15/02/2026)

European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). COM(2021) 206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (ultimo accesso: 15/02/2026)

European Parliament. (2021). Artificial Intelligence Act. European Parliamentary Research Service (EPRS Briefing, 698792). https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (ultimo accesso: 15/02/2026)

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj (ultimo accesso: 15/02/2026)

European Union. (2024a). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0). Official Journal of the European Union, L 2024/1183. https://eur-lex.europa.eu/eli/reg/2024/1183/oj (ultimo accesso: 15/02/2026)

European Union. (2024b). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj (ultimo accesso: 15/02/2026)

Gyōsei tetsuzuki ni okeru tokutei no kojin o shikibetsu suru tame no bangō no riyō tō ni kansuru hōritsu [Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures – My Number Act]
行政手続における特定の個人を識別するための番号の利用等に関する法律. (2013). Hōritsu dai nijūnana gō [法律第二十七号 – Legge n. 27 del 2013]. https://elaws.e-gov.go.jp/document?lawid=425AC0000000027 (ultimo accesso: 15/02/2026)

Hasan, Md. Kamrul, Habib, Ahasan, Islam, S. M. Sarowar & Pandey, Bipin. (2023).

Häuselmann, Andreas & Custers, Bart. (2024). The Right to Rectification and Inferred Personal Data. *European Journal of Law and Technology*, 15(3). https://ejlt.org/index.php/ejlt/article/download/1004/1097/4491 (ultimo accesso: 15/02/2026)

Horibe Masao 堀部政男. (2025). Nihon ni okeru puraibashī・kojin jōhō hogo no rekishi no ichidan [日本におけるプライバシー・個人情報保護の歴史の一端 – Alcuni aspetti della storia della privacy e della protezione dei dati personali in Giappone]. Nippon DPO Kyōkai dai 37-kai kojin jōhō hogo seminar shiryō [日本DPO協会第37回個人情報保護セミナー資料]. https://dpo.or.jp/wp-content/uploads/2025/07/日本DPO協会第37回個人情報保護セミナー20250417資料-0415.pdf (ultimo accesso: 15/02/2026)

Japan Network Security Association (JNSA) 日本ネットワークセキュリティ協会. (2025). 生成AI活用の光と影：リスクと制度対応 [Luci e ombre dell'uso di IA generativa: rischi e risposte regolatorie]. JNSA Press, 55, 10–15. https://www.jnsa.org/jnsapress/vol55/2_kikou_3.pdf (ultimo accesso: 15/02/2026)

Japan Times. (2025, January 15). PPC Reports Record Number of Data Breach Notifications in FY2024. *The Japan Times*. https://www.japantimes.co.jp/news/2025/01/15/japan/ppc-data-breach-notifications/ (ultimo accesso: 15/02/2026)

Kakinuma Taichi 柿沼太一. (2023). Seisei AI no riyō gaidorain sakusei no tame no tebiki [生成AIの利用ガイドライン作成のための手引き – Guida alla redazione di linee guida per l'utilizzo dell'IA generativa]. STORIA hōritsu jimusho 公式ブログ [STORIA法律事務所 – Blog ufficiale]. https://storialaw.jp/blog/9414

Kōjin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information – APPI] 個人情報の保護に関する法律. (2003). Hōritsu dai gojūnana gō [法律第五十七号 – Legge n. 57 del 2003]. https://elaws.e-gov.go.jp/document?lawid=415AC0000000057 (ultimo accesso: 15/02/2026)

Kōjin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information – APPI, versione emendata] 個人情報の保護に関する法律. (2022). Personal Information Protection Commission. https://laws.e-gov.go.jp/law/415AC0000000057 (ultimo accesso: 15/02/2026)

Kōjin jōhō no hogo ni kansuru hōritsu shikō rei [Decreto attuativo della legge sulla protezione delle informazioni personali] 個人情報の保護に関する法律施行令. (2003). Seirei dai gohyaku nana gō [政令第五百七号 – Decreto governativo n. 507 del 2003]. https://elaws.e-gov.go.jp/document?lawid=415CO0000000507 (ultimo accesso: 15/02/2026)

Mainichi Shimbun 毎日新聞. (2019, August 27). Kigyō no dēta katsuyō, towareru jōhō hogo – Rikunabi mondai ni “hyōzan no ikkaku”
[企業のデータ活用、問われる情報保護　リクナビ問題に「氷山の一角」 – Uso dei dati da parte delle imprese e tutela delle informazioni: il caso Rikunabi come “punta dell’iceberg”]. Mainichi Shimbun. https://mainichi.jp/articles/20190827/k00/00m/020/270000c (ultimo accesso: 15/02/2026)

Mainichi Shimbun 毎日新聞. (2023, May 23). Mainanbā ni betsu nin kōza o goroku ga aitsugu – Kōno-shi, sōtenken no jisshi o happyo
[マイナンバーに別人口座を誤登録が相次ぐ　河野氏、総点検の実施を発表 – Registrazioni errate di conti bancari di altre persone collegate al My Number: Kōno annuncia una verifica complessiva]. Mainichi Shimbun. https://mainichi.jp/articles/20230523/k00/00m/040/243000c (ultimo accesso: 15/02/2026)

METI (Ministry of Economy, Trade and Industry) 経済産業省. (2021). AI gensoku jissen no tame no gabananansu gaidorain
[AI原則実践のためのガバナンス・ガイドライン – Linee guida di governance per l'attuazione dei principi dell'IA]. METI.

https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_1.pdf (ultimo accesso: 15/02/2026)

METI (Ministry of Economy, Trade and Industry) 経済産業省. (2024). AI gaidorain for Business Ver. 1.0 [AIガイドライン for Business Ver. 1.0 – Linee guida IA per le imprese, versione 1.0]. METI. https://www.meti.go.jp/press/2024/04/20240419004/20240419004.html (ultimo accesso: 15/02/2026)

METI (Ministry of Economy, Trade and Industry) 経済産業省. (2025). AI Guidelines for Business Ver. 1.01 [AIガイドライン for Business Ver. 1.01 – Linee guida IA per le imprese, versione aggiornata]. METI. Recuperato da https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20241226_1.pdf (ultimo accesso: 15/02/2026)

MHLW (Ministry of Health, Labour and Welfare) 厚生労働省. (2024). Maina hokenshō no riyō ni tsuite [マイナ保険証の利用について – Sull'uso della tessera sanitaria collegata a My Number]. MHLW. https://www.mhlw.go.jp/stf/newpage_08277.html (ultimo accesso: 15/02/2026)

MIC (Ministry of Internal Affairs and Communications) 総務省. (2020). AI nettowāku shakai suishin kaigi hōkokusho [AIネットワーク社会推進会議報告書 – Rapporto della Conferenza per la promozione della società IA in rete]. MIC. https://www.soumu.go.jp/main_content/000698163.pdf (ultimo accesso: 15/02/2026)

Minamoto Rei 源怜維, Oda Yusuke 小田悠介 & Kawahara Daisuke 河原大輔. (2025). Daikibo gengo moderu no jizen gakushū-yō kōpasu ni okeru yō hairyo kojin jōhō no kenshutsu
[大規模言語モデルの事前学習用コーパスにおける要配慮個人情報の検出 – Rilevamento di informazioni personali sensibili nei corpora di pre-addestramento di modelli linguistici di grandi dimensioni]. Gengo shori gakkai nenji taikai ronbunshū [言語処理学会第31回年次大会論文集 – Proceedings of the 31st Annual Meeting of the Association for Natural Language Processing], 31, P7-19. https://www.anlp.jp/proceedings/annual_meeting/2025/pdf_dir/P7-19.pdf

Miyashita Hiroshi 宮下紘. (2021). Hito no kanjō o yusaburu AI gijutsu no hōteki kadai to wa [人の感情をゆさぶるAI技術の法的課題とは – Le questioni giuridiche delle tecnologie AI che influenzano le emozioni umane]. JST RISTEX HITE Project Interview. https://www.jst.go.jp/ristex/hite/topics/464.html (ultimo accesso: 18/02/2026)

MOFA (Ministry of Foreign Affairs of Japan) 外務省. (2020). DFFT: Data Free Flow with Trust to wa [DFFT：Data Free Flow with Trustとは – Che cos'è il Data Free Flow with Trust]. MOFA. https://www.mofa.go.jp/mofaj/files/100167362.pdf (ultimo accesso: 15/02/2026)

MOFA (Ministry of Foreign Affairs of Japan) 外務省. (2025). AI ni kakaru kokusai gabanansu no kouchiku: Hiroshima AI Process no gaiyō [AIに係る国際ガバナンスの構築：広島AIプロセスの概要 – Costruire una governance internazionale dell'AI: sintesi del Hiroshima AI Process]. 外務省. https://www.mofa.go.jp/mofaj/ecm/st/pagew_000001_01551.html (ultimo accesso: 18/02/2026)

Mühlhoff, Rainer & Ruschemeier, Hannah. (2024). Regulating AI with purpose limitation for models. AI Law and Regulation. Manuscript/early view. https://rainermuehlhoff.de/media/publications/m%C3%BChlhoff_ruschemeier_2024_regulating_ai_with_purpose_limitation_for_models.pdf

Nakamoto, Satoshi. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf (ultimo accesso: 15/02/2026)

National Law Review. (2023, July 5). Japan Issues Warning About Personal Data Use in Generative AI Services. The National Law Review, Vol. XIII, No. 186. https://natlawreview.com/article/japanese-privacy-regulator-cautioned-businesses-regarding-issues-relating-to (ultimo accesso: 15/02/2026)

Nippon.com. (2023, July 7). Only fraction of Japanese residents use My Number ID card for health insurance. Nippon.com. https://www.nippon.com/en/japan-data/h01482/ (ultimo accesso: 18/02/2026)

OECD (Organisation for Economic Co-operation and Development). (2019). Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-

LEGAL-0449 (ultimo accesso: 15/02/2026)

OECD (Organisation for Economic Co-operation and Development). (2024). Explanatory Memorandum on the Updated OECD Definition of an AI System. OECD Digital Economy Papers, No. 354. https://doi.org/10.1787/623da898-en

OECD (Organisation for Economic Co-operation and Development). (2024). Governing with Artificial Intelligence. OECD Public Governance Policy Papers. https://www.oecd.org/en/publications/governing-with-artificial-intelligence_26324bc2-en.html (ultimo accesso: 18/02/2026)

Ohm, Paul. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57, 1701–1777. https://epic.org/wp-content/uploads/privacy/reidentification/ohm_article.pdf (ultimo accesso: 15/02/2026)

Ōiso Naoki 大磯直樹, Ida Takanori 依田高典 & Kuroda Masahiro 黒田昌裕. (2024). Kojin no puraibashī ishiki-tō to dejitaru sābisu riyō ni kansuru jisshō bunseki [個人のプライバシー意識等とデジタルサービス利用に関する実証分析 – Analisi empirica della consapevolezza della privacy e dell'uso di servizi digitali]. 公共選択研究 [Kōkyō sentaku kenkyū – Public Choice Studies], 80, 1–26. CiNii Research: https://cir.nii.ac.jp/crid/1390853829701199744

Pardieck, Andrew M. (2024). Privacy Matters: Data Breach Litigation in Japan. *Washington International Law Journal*, 33(1), 1–52. https://digitalcommons.law.uw.edu/wilj/vol33/iss1/3/ (ultimo accesso: 15/02/2026)

Pasquale, Frank. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge (MA), Harvard University Press.

Personal Information Protection Commission (PPC) 個人情報保護委員会. (2020). Kojin kanren jōhō no daisansha teikyō ni kansuru gaidorain [個人関連情報の第三者提供に関するガイドライン – Linee guida sulla fornitura a terzi delle informazioni correlate a persone]. PPC. https://www.ppc.go.jp/personalinfo/legal/guidelines_anonymous/ (ultimo accesso: 15/02/2026)

Personal Information Protection Commission (PPC) 個人情報保護委員会. (2022a). Q1-8: Fukusūnin no kojin jōhō o kikai gakushū no gakushū-yō dētasetto toshite mochīte seisei shita gakushū-zumi paramēta wa, kojin jōhō ni atarimasu ka?

[Ｑ１－８：複数人の個人情報を機械学習の学習用データセットとして用いて生成した学習済みパラメータは、個人情報に当たりますか。– Q1-8: I parametri addestrati generati usando dati personali di più persone rientrano nella nozione di “informazioni personali”?]. In: 「個人情報の保護に関する法律についてのガイドライン」に対するQ&A. PPC. https://www.ppc.go.jp/all_faq_index/faq1-q1-8/ (ultimo accesso: 18/02/2026)

Personal Information Protection Commission (PPC) 個人情報保護委員会 (2022b), Reiwa 2-nen kaisei kojin jōhō hogo hō ni tsuite [令和2年 改正個人情報保護法について – Sulla riforma 2020 della legge sulla protezione delle informazioni personali], Personal Information Protection Commission, https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/ (ultimo accesso: 15/02/2026).

Personal Information Protection Commission (PPC) 個人情報保護委員会 (2023a, 2 giugno), Seisei AI sābisu no riyō ni kansuru chūikanki tō [生成AIサービスの利用に関する注意喚起等 – Avviso sull’uso dei servizi di IA generativa e altre misure], Personal Information Protection Commission. https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf (ultimo accesso: 15/02/2026).

Personal Information Protection Commission (PPC) 個人情報保護委員会 (2023b, 2 giugno), OpenAI ni taisuru chūikanki no gaiyō [OpenAIに対する注意喚起の概要 – Sintesi dell’avviso rivolto a OpenAI], in: Seisei AI sābisu no riyō ni kansuru chūikanki tō [生成AIサービスの利用に関する注意喚起等], Allegato 2, Personal Information Protection Commission. https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/ (ultimo accesso: 15/02/2026).

Personal Information Protection Commission (PPC) 個人情報保護委員会. (2024a). Kojin jōhō hogo hō gaidorain (tsūsoku hen) [個人情報保護法ガイドライン（通則編）– Linee guida sulla legge per la protezione delle informazioni personali – Regole generali]. PPC. https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/ (ultimo accesso: 15/02/2026)

Personal Information Protection Commission (PPC) 個人情報保護委員会 (2024b, 27 giugno), Kojin jōhō hogo hō iwayuru san nen goto minaoshi ni kakaru kentō no chūkan seiri [個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理 – Intermediazione delle valutazioni sulla “revisione triennale” della legge sulla protezione delle informazioni personali], Personal Information Protection Commission. https://www.ppc.go.jp/files/pdf/240627_02_houdou_betten1.pdf (ultimo accesso: 15/02/2026).

Personal Information Protection Commission (PPC). (2024c). AI 利用と個人情報の関係の考察 [Discussion on the legal nature of personal data in the AI era]. PPC Discussion Materials, 3 aprile 2024. https://www.ppc.go.jp/files/pdf/240403_shiryou-1-2.pdf (ultimo accesso 21/02/2026)

Personal Information Protection Commission (PPC) 個人情報保護委員会 (2025), Kojin jōhō no hogo ni kansuru hōritsu ni tsuite no gaidorain (gaikoku ni aru daisansha e no teikyō hen) [個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編） – Linee guida sulla legge in materia di protezione delle informazioni personali (fornitura a terzi situati all’estero)], Personal Information Protection Commission. https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/ (ultimo accesso: 15/02/2026).

Personal Information Protection Commission (PPC). (2026). Kojin jōhō hogo hō iwayuru san nen goto minaoshi no seido kaisei hōshin [個人情報保護法 いわゆる3年ごと見直しの制度改正方針 — System Reform Policy under the Triennial Review of the Act on the Protection of Personal Information]. https://www.ppc.go.jp/files/pdf/01-1_seidokaiseihousin.pdf (ultimo accesso 20/02/2026).

Presidenza del Consiglio dei Ministri (2014), Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014: Definizione delle caratteristiche del sistema pubblico per la gestione dell’identità digitale di cittadini e imprese (SPID), Gazzetta Ufficiale della Repubblica Italiana, Serie Generale n. 285 del 9 dicembre 2014.

https://www.gazzettaufficiale.it/eli/id/2014/12/09/14A09376/sg (ultimo accesso: 15/02/2026).

Private AI (2025, 11 febbraio), What the International AI Safety Report 2025 has to say about privacy risks from general-purpose AI, Private AI Blog. https://www.private-ai.com/en/blog/ai-safety-report-2025-privacy-risks (ultimo accesso: 15/02/2026).

Reuters (2023, 2 giugno), Japan privacy watchdog warns ChatGPT-maker OpenAI on user data, Reuters Technology. https://www.reuters.com/technology/japan-privacy-watchdog-warns-chatgpt-maker-openai-data-collection-2023-06-02/ (ultimo accesso: 15/02/2026).

Selbst, Andrew D., Boyd, Danah, Friedler, Sorelle A., Venkatasubramanian, Suresh & Vertesi, Janet. (2019). Fairness and Abstraction in Sociotechnical Systems. In Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT '19), 59–68. https://doi.org/10.1145/3287560.3287598

Suresh, Harini & Guttag, John. (2019). A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle. In Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '21). https://doi.org/10.1145/3465416.3483305

Sweeney, Latanya. (2015, September 28). Only You, Your Doctor, and Many Others May Know. Technology Science. https://techscience.org/a/2015092903/ (ultimo accesso: 15/02/2026)

Takagi Hiromitsu 高木浩光. (2020). Kojin jōhō hogo kara kojin dēta hogo e: Min'kan bumon to kōteki bumon no kitei tōgō ni muketa kentō (4)
[個人情報保護から個人データ保護へ――民間部門と公的部門の規定統合に向けた検討⑷ – Dalla protezione delle informazioni personali alla protezione dei dati personali: verso l'integrazione delle norme tra settore privato e pubblico (4)]. *Jōhō Hōsei Kenkyū* [情報法制研究 – *Journal of Law and Information System*], 7, 78–102. https://doi.org/10.32235/alis.7.0_78

Takagi Hiromitsu 高木浩光. (2022). Takagi Hiromitsu-san ni kiku, kojin dēta hogo no shinzui: Ima tokimekasareru hanseiki no keii to konran
[高木浩光さんに訊く、個人データ保護の真髄――いま解き明かされる半世紀の経緯と混乱 – Intervista: l'essenza della protezione dei dati personali, tra

mezzo secolo di evoluzione e confusione]. *Jōhō Hōsei Repōto* [情報法制レポート – *Information Law Report*], 3, 47–99. https://doi.org/10.57332/jilis.3.0_47

Takagi Hiromitsu 高木浩光. (2025). Kojin jōhō hogo kara kojin dēta hogo e (10): Hō mokuteki ni motozuku seido minaoshi no kentō [個人情報保護から個人データ保護へ⑽――法目的に基づく制度見直しの検討 – Revisione del sistema basata sulle finalità della legge (10)]. *Jōhō Hōsei Kenkyū* [情報法制研究 – *Journal of Law and Information System*], 17, 57–73. https://doi.org/10.32235/alis.17.0_057

Ueno Tatsuhiro 上野達弘. (2021). Jōhō kaiseki to chosakuken: "Kikai gakushū paradaisu" toshite no Nihon [情報解析と著作権――「機械学習パラダイス」としての日本 – Analisi informativa e diritto d'autore: il Giappone come "paradiso del machine learning"]. *Jinkō Chinō* [人工知能], 36(6), 745–749. https://doi.org/10.11517/jjsai.36.6_745

Ushijima & Partners. (2023). Generative AI and the Protection of Personal Information under the Japanese Law. Client Alert. https://www.ushijima-law.gr.jp/client-alert_seminar/client-alert/ppc_generativeai/ (ultimo accesso: 15/02/2026)

Villasenor, John. (2024). Artificial Intelligence, Trade Secrets, and the Challenge of Transparency. North Carolina Journal of Law & Technology, 25(3), 495–556. https://journals.law.unc.edu/ncjolt/wp-content/uploads/sites/4/2024/04/Villasenor-Final.pdf (ultimo accesso: 19/02/2026).

Wachter, Sandra & Mittelstadt, Brent. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2019(2), 494–620. https://journals.library.columbia.edu/index.php/CBLR/article/download/3424/1370/5776 (ultimo accesso: 15/02/2026)

Wallach, Wendell, Reuel, Anka & Kaspersen, Anja. (2023). Soft Law Functions in the International Governance of AI. Carnegie Council for Ethics in International Affairs. https://lsi.asulaw.org/softlaw/wp-content/uploads/sites/7/2023/12/Wallach-et-al_Soft-Law-Functions-in-the-International-Governance-of-AI.pdf (ultimo accesso: 19/02/2026).

Whitley, Edgar A. & Hosein, Gus. (2010). Global Identity Policies and Technology: Do

we Understand the Question? *Global Policy*, 1(2), 209–215. https://doi.org/10.1111/j.1758-5899.2010.00028.x

World Wide Web Consortium (W3C). (2022). Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. W3C Recommendation. https://www.w3.org/TR/did-core/ (ultimo accesso: 15/02/2026)

World Wide Web Consortium (W3C). (2025). Verifiable Credentials Data Model v2.0. W3C Recommendation. https://www.w3.org/TR/vc-data-model-2.0/ (ultimo accesso: 15/02/2026)

Yaga, Dylan, Mell, Peter, Roby, Nik & Scarfone, Karen. (2018). Blockchain Technology Overview. National Institute of Standards and Technology (NIST), NISTIR 8202. https://doi.org/10.6028/NIST.IR.8202

Yamamoto Tatsuhiko 山本龍彦. (2020). Jikojōhō kontorōru ken no genkai to dejitaru shakai [自己情報コントロール権の限界とデジタル社会 – I limiti del diritto al controllo delle informazioni personali nella società digitale], in: Trust MF, AI jidai ni okeru pāsonaru dēta no hōteki seishitsu [AI時代におけるパーソナルデータの法的性質 – Natura giuridica dei dati personali nell'era dell'IA], Trust MF. https://trust-mf.or.jp/pdf/other/paper/2024_02.pdf (ultimo accesso: 19/02/2026).

Yomiuri Shimbun 読売新聞. (2023, June 3). Kojin jōhō hogo i, OpenAI ni gyōsei shidō [個人情報保護委、OpenAIに行政指導 – La PPC emette orientamento amministrativo verso OpenAI]. *Yomiuri Shimbun*. https://www.yomiuri.co.jp/national/20230603-OYT1T50123/ (ultimo accesso: 15/02/2026)

Zuboff, Shoshana. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, PublicAffairs.