Università
Ca'Foscari
Venezia

Corso di Laurea Magistrale in

Lingue, Economie e Istituzione dell'Asia e dell'Africa Mediterranea

Ordinamento ex D.M. 270/2004

Tesi di Laurea

Il trasferimento di dati personali in Giappone

Dalla nascita del concetto di privacy all'adeguamento con la normativa europea

Relatore
Prof. Giorgio Fabio Colombo

Correlatore
Prof. Marco Zappa

Laureando
Lorenzo Ignesti
Matricola 846457

Anno Accademico
2024 / 2025

Ringraziamenti

Alla mia famiglia,
perché mi ha sostenuto incondizionatamente

Agli amici di una vita,
perché hanno reso indimenticabili questi anni

要旨

この論文は、日本の「個人情報保護法」（APPI）における個人データの移転に関する規定を検討し、欧州連合の規制との類似点と相違点を明らかにすることを目的としている。

現代社会では、多国籍企業やクラウドサービス、オンラインプラットフォームの間で、データが常に国境を越えて移動している。このようなデータの国際的な移転の増加は、人々の権利やプライバシーを守るために重要な課題を生んでいる。そのため、各国は基本的人権を尊重しつつ、国際的なルールに沿った法整備を進める必要がある。特に日本は、技術の進歩のみならず法制度の継続的な改善にも注力している点が注目される。実際、「個人情報保護法」は何度も改正されており、文化の違いがあっても、「EU 一般データ保護規則」（GDPR）に合わせようとする意志が見られる。長い交渉の結果、日本は 2019 年に EU から「十分性認定」を受けた。

第一章では、プライバシーの歴史的変遷と日本の社会文化的背景を説明し、「宴の後」と呼ばれる判例を通して、日本におけるプライバシーに関する誤解を明らかにする。また、ヨーロッパやアジアにおける最も重要な国際協定についても解説する。

第二章では、元の法律と 2015 年の改正を中心に、日本の個人情報保護法の内容や運用について詳しく見ていく。特に越境データの扱いや個人情報保護委員会について考察する。

第三章では、1990 年代から現在に至るまでの日本と欧州連合の関係や協定について述べ、両国のデータ保護法の類似点と相違点を比較する。また、近年日本で行われた最新の変更点と、技術の進歩に対応するために導入が検討されている提案についても述べる。

本研究でわかったことは、日本のプライバシー保護や個人情報保護の歴史や社会の背景、法律の変化は、デジタル社会の問題に対応するために常に改良されてきたということです。

日本の法律は、OECD のガイドラインや条約第 108 号をもとにしたものから、よりヨーロッパの制度に近い形に変わりました。2015 年の改正では、「個人情報保護委員会」（PPC）の設置、匿名情報や機微情報のルールの強化、そして罰則の厳しくなることが主な変更点でした。

その後、三年間の見直しとデジタル改革により、公共部門と民間部門の規制が強化され、監督も強化された。機密情報管理、透明性、説明責任も改善された。

しかし、これらの取り組みにはまだ EU の規則との違いが残っている。現在の APPI は、GDPR と比べて個人の権利が十分に守られておらず、「データポータビリティ権利」や「反対権利」、「忘れられる権利」といった重要な権利が欠けている。また、自動プロファイリングに関する規制はまだ十分に整備されておらず、未成年者の保護やプライバシー影響評価の面でも改善が必要である。罰則についても、GDPR ほど厳しくなく、勧告や是正措置に頼る傾向が強い。

さらに、子どものデータ処理や「個人情報取扱責任者」（RDP）、「プライバシー影響評価」（PIA）に関する規定にも不十分な点がある。制裁については、最近厳しくな

ってきたが、依然として、日本の規制は EU の GDPR に比べて厳しさが足りず、主に勧告や改善措置が優先されている。データ移転に関しては、日本はこれまでに大きく進歩し、EU とほぼ同等の水準に達したものの、オプトアウト制度に裁量の余地が多く、個人の信頼を損なう可能性がある。また、適合性認定がない場合の十分な対策もまだ整備されていない。最後に、司法協力や公開記録に関するデータ移転は、PPC の規定に含まれていない点が課題である。

日本と EU の基準の違いは、それぞれの文化的な違いにも関係していると考えられる。西洋とは違って、日本ではプライバシーを個人ではなく集団を守るものとして重視しているため、完全な規範の統一は難しい状況にある。しかし、これまで直面してきた課題を踏まえ、日本は個人情報保護の規制において国際社会の重要なパートナーだと私は考えている。将来的には、新しい提案がこのギャップをさらに埋め、革新と伝統の調和を図ることが求められるだろう。

Indice

要旨 **1**

Introduzione **6**

Capitolo 1. Evoluzione del diritto sulla protezione dei dati personali in Giappone . **8**

1.1. Dalla *privacy* delle informazioni al "dato personale" 8

1.2. La riservatezza nella cultura giapponese 11

1.2.1. La privacy nei tribunali: il caso "Utage no ato" 13

1.3. Gli strumenti internazionali per il trasferimento dei dati 16

1.3.1. Linee Guida OCSE e Convenzione 108 17

1.3.2. Gli accordi di libero scambio tra Giappone e Asia 19

1.3.3. Asian-Pacific Economic Cooperation 21

Capitolo 2. Il traffico di dati nella normativa giapponese **23**

2.1. Contesto storico 23

2.2. La prima legge giapponese sulla protezione dei dati personali (APPI) 24

2.2.1. Struttura normativa 26

2.2.2. Definizioni e applicazioni 28

2.2.3. Autorità regolatorie e sanzioni 29

2.3. La Riforma del 2015 30

2.3.1. Le nuove definizioni 32

2.3.2. La Commissione per la Protezione dei Dati Personali 34

2.3.3. Le conseguenze del "caso Benesse" 36

2.3.4. Trasmissione dei dati personali a Paesi esteri 38

2.3.5. Promozione del sistema CBPR 40

2.4. Il diritto all'oblio 42

Capitolo 3. Giappone ed Europa sul trasferimento di dati: accordi e divergenze .. 45

3.1. Il Regolamento europeo (GDPR): tra passato e presente 45

3.2. Gli accordi di libero scambio 51

3.3. La decisione di adeguatezza 52

3.4. Le Norme Supplementari 55

3.4.1. I diritti dell'interessato 56

3.4.2. Gli obblighi per il titolare del trattamento 57

3.4.3. Il "dato pseudonimizzato" 58

3.4.4. Estensione dell'ambito di applicazione extraterritoriale e novità sul trasferimento transfrontaliero 59

3.4.5. Il "caso Rikunabi" e il potenziamento delle sanzioni 60

3.5. Questioni in sospeso 62

3.6. Ultimi sviluppi 63

Conclusioni 70

Bibliografia 73

Fonti giurisprudenziali 87

Sitografia 89

Introduzione

"*Storicamente la privacy era quasi implicita, perché era difficile trovare e raccogliere informazioni. Ma nel mondo digitale, che si tratti di fotocamere o satelliti o semplicemente di ciò su cui si fa clic, è necessario disporre di regole più esplicite […]*". Le parole di Bill Gates colgono in pieno la sfida che ci pone l'era digitale: un'epoca in cui il traffico di dati personali è una risorsa vitale che sostiene il funzionamento dell'economia globale. Il flusso di informazioni tra le aziende multinazionali, i servizi cloud e le piattaforme online scorre senza sosta attraverso i confini nazionali, creando un sistema interconnesso e complesso. Questo scenario apre a nuove opportunità di crescita economica, ma al contempo solleva problematiche riguardo alla sicurezza e alla protezione della *privacy* degli individui. Oggi tutti i Paesi hanno la responsabilità di emanare delle leggi sulla protezione dei dati personali conformi alle normative internazionali, che pongano al centro i diritti fondamentali dell'uomo.

Alla luce di questo, il Giappone diventa un eccellente caso di studio, non tanto per la sua posizione di leader tecnologico, quanto per l'attitudine verso il continuo perfezionamento normativo. Infatti, le numerose revisioni dell'*Act on the Protection of Personal Information* (APPI) [1] testimoniano, nonostante le marcate divergenze socioculturali, la volontà di perseguire un modello condiviso a livello globale. In questo senso, il raggiungimento della decisione di adeguatezza con l'Unione Europea offre uno spunto didattico di come il processo di mediazione richieda un attento "*studio degli ordinamenti stranieri interessati*"[2].

Da qui nasce l'interesse per questa ricerca, che sarà dedicata allo studio giuridico e giurisprudenziale dell'APPI in relazione al trasferimento di dati personali, offrendo una panoramica delle disposizioni e della sua evoluzione normativa, con particolare attenzione all'analisi del processo che ha portato al riconoscimento della reciproca equivalenza con la normativa europea.

Il primo capitolo sarà rivolto agli sviluppi storici e legislativi che hanno segnato l'affermazione della *privacy* come diritto autonomo, passando dalla concezione

[1] Le leggi sono riportate nella trascrizione inglese, poiché è la nomenclatura comunemente adottata nella letteratura specialistica internazionale.
[2] F. SERINI (2022), *La protezione dei dati personali tra Giappone e Unione europea*, Roma, Aracne, p. 17.

tradizionale alla moderna definizione giuridica di "dato personale". Inizialmente, verrà trattata la prospettiva giapponese dal punto di vista socioculturale, sfatando, attraverso l'esame di un caso giurisprudenziale emblematico, il mito secondo cui non esiste il concetto di *privacy* in Giappone. Nei paragrafi successivi invece ci concentreremo sul contesto internazionale, illustrando gli strumenti e gli accordi multilaterali che hanno accompagnato il Giappone nella regolamentazione del commercio internazionale dei dati personali, tra cui le Linee Guida OCSE, la Convenzione 108, e gli accordi di libero scambio nell'area Asia-Pacifico (APEC).

Il secondo capitolo aprirà con la ricostruzione del contesto storico che ha portato all'adozione della prima legge sulla protezione dei dati giapponese, delineando il quadro istituzionale di riferimento che verrà modificato in parte nella successiva riforma del 2015. Nello studio di quest'ultima approfondiremo le principali novità introdotte, come la creazione della Commissione per la Protezione dei Dati Personali (PPC) e l'adozione di misure più rigorose in risposta agli scandali di fughe di dati. Tuttavia, l'attenzione sarà riservata alla nuova disciplina sul trasferimento transfrontaliero dei dati e alla promozione dei sistemi progettati per garantirne il corretto trattamento.

Il terzo e ultimo capitolo verterà sui rapporti e sugli accordi tra il Giappone e l'Unione Europea che sono intercorsi dagli anni '90 fino a oggi. L'argomentazione prenderà forma mediante l'analisi comparata delle rispettive normative in materia di protezione dei dati, fondamentale nell'elaborazione della decisione di adeguatezza del gennaio 2019. Si evidenzieranno quindi le convergenze e le divergenze tra i due sistemi legislativi, nonché le ultime revisioni che sono state recentemente introdotte dal governo giapponese per adattarsi all'incessante progresso tecnologico globale.

Le considerazioni finali saranno utili per fornire un quadro completo dei risultati ottenuti dalla ricerca storica, giuridica e giurisprudenziale dei due ordinamenti. In chiusura, si cercherà di individuare quali sono gli ambiti giuridici su cui il governo giapponese dovrà intervenire nei prossimi anni, affinché possa consolidare la propria posizione pionieristica nel campo del trasferimento internazionale dei dati personali.

Capitolo 1

Evoluzione del diritto sulla protezione dei dati personali in Giappone

1.1. Dalla *privacy* delle informazioni al "dato personale"

Nella natura dell'essere umano è sempre esistito l'impulso naturale di proteggersi dai pericoli dell'ambiente circostante, che si trattassero del freddo o degli attacchi degli animali selvatici. Nel suo modello piramidale dei bisogni fondamentali, Maslow colloca, subito dopo i bisogni fisiologici, il bisogno di sicurezza, poiché senza di esso non è possibile garantire la sopravvivenza[3].
Partendo da questa riflessione, l'esigenza di protezione non si esaurisce nella dimensione fisica, ma può essere estesa anche alla difesa dell'identità e del proprio spazio personale. La tutela della sfera privata è quindi intrinseca alla natura umana, ma, a seconda del contesto storico e sociale, ha assunto interpretazioni e forme diverse[4]. Il confine di demarcazione tra pubblico e privato si è adattato ai cambiamenti della società. La *privacy*, come la intendiamo oggi, non è un concetto statico, bensì il frutto di un lungo processo di evoluzione sociale, giuridica e tecnologica.

Facendo un passo indietro nella storia, nell'Antica Grecia si riteneva che la partecipazione costante alla vita della *polis* fosse un dovere di ogni uomo. Tuttavia, *"senza una casa un uomo non poteva partecipare agli affari della città, perché in essa non aveva un luogo che fosse propriamente suo"*[5]. Così in cambio del suo contributo negli affari pubblici, la città-stato garantiva la tutela dei confini della proprietà e riconosceva a ogni cittadino la

[3] A. MASLOW (1954), *Motivation and personality*, New York; cit. in M. IASELLI, S. GORLA (2015), *Storia della Privacy*, Lex et Ars, Roma, p. 9.
[4] M. OROFINO (2018), *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, a cura di L. PANELLA, Editoriale Scientifica, p. 9.
[5] S. NIGER (2006), *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Le Monografie di Contratto e Impresa, Padova, p. 2.

possibilità di possedere una sfera privata (*oíkos*), anche se limitata esclusivamente "*all'espletamento dei propri bisogni personali e delle proprie necessità*"[6].
Nel Medioevo l'influenza della religione cristiana e della struttura gerarchica feudale contribuì alla formazione di una struttura sociale in cui la collettività prevaleva sull'individualità. Le persone vivevano in comunità ristrette, come villaggi rurali o feudi, dove l'affermazione personale era sacrificata in favore del bene familiare e l'identità era definita dalle caratteristiche del gruppo sociale di cui si faceva parte. Il privato non era inteso come nei termini moderni, ma rappresentava un elemento di appartenenza, un luogo dove trovare sicurezza e protezione all'interno della collettività[7].

Con la caduta del feudalesimo e l'emergere della classe media invece si affermò una concezione di *privacy* più vicina a quella moderna. La borghesia iniziò ad accumulare risorse economiche sufficienti per aspirare a quel senso di intimità che fino ad allora era concesso solo a pochi. Da un lato, socialmente la *privacy* divenne "*l'acquisizione di un privilegio da parte di un gruppo*"[8], un simbolo di status che distingueva questa classe sociale dalle altre e che le conferiva il diritto esclusivo di possedere uno spazio riservato; dall'altro, la separazione tra pubblico e privato si fece talmente marcata da generare la paura che le "*proprie convinzioni più intime*"[9] potessero essere svelate. Nacque quindi la necessità di istituire una regolamentazione giuridica che proteggesse non solo gli spazi fisici, ma anche le opinioni e i pensieri.

Fu proprio nell'età d'oro della borghesia, precisamente nel 1890, che due giovani avvocati statunitensi, Samuel Warren e Louis Brandeis, pubblicarono il famoso articolo intitolato *"The Right to Privacy"*, in cui sostenevano l'urgenza di preservare i sentimenti e le emozioni dalla divulgazione non autorizzata delle informazioni, ritenuta una violazione della personalità stessa[10]. Del resto, in quel periodo, la carta stampata era diventata il mezzo di comunicazione più in voga e spesso i contenuti si concentravano su argomenti sensazionalistici come scandali e pettegolezzi[11].

---

[6] F. FABRIS (2009), *Il diritto alla privacy tra passato, presente e futuro*, Trieste, Tigor, pp. 94.
[7] L. C. TESSORE (2024), *Diritto alla privacy: dalle origini ai giorni nostri*, Studio Cataldi, https://www.studiocataldi.it/articoli/47042-diritto-alla-privacy-dalle-origini-ai-giorni-nostri.asp
[8] M. IASELLI, S. GORLA (2015), *op., cit.*, p. 27.
[9] M. OROFINO (2018), *op. cit.*, p. 10.
[10] S. WARREN, L. BRANDEIS (1890). *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, p. 197.
[11] D. J. SOLOVE (2006), *A Brief History of Information Privacy Law*, Proskauer On Privacy, PLI, p. 10.

I due giuristi si affidarono dunque all'adattabilità del *common law* per riconoscere in esso un nuovo diritto autonomo, distinto sia dal diritto alla proprietà che dal diritto alla riservatezza delle comunicazioni interpersonali[12], definito come "*the right to be let alone*". Le riflessioni teoriche di Warren e Brandeis hanno avuto un impatto tale da essere considerate il *"più grande contributo alla privacy"*[13], specialmente in considerazione degli sviluppi imminenti che avrebbero segnato l'era tecnologica, un periodo in cui la dimensione privata è costantemente messa alla prova.

Oggi la nozione stessa di *privacy* deve essere reinterpretata in una chiave contemporanea, come diritto di ogni individuo di gestire la circolazione delle proprie informazioni personali[14]. Questa ridefinizione è principalmente dovuta alla diffusione dei computer, la cui innovazione risiede nell'elaborare grandi volumi di informazioni della rete, che vengono immagazzinati nelle cosiddette "banche dati". Attraverso l'accesso a queste, è possibile conoscere aspetti privati di una persona, come le abitudini di consumo, le relazioni sociali, la situazione finanziaria, i siti web visitati più frequentemente o persino i dati sanitari personali[15]. Queste pratiche, seppur giustificate dalla volontà di migliorare la gestione amministrativa, possono comportare usi impropri, con derive più estese e pericolose rispetto a quelle che si verificavano con le documentazioni cartacee.
Dunque, diventa necessario tutelare i dati personali condivisi online, monitorarne la circolazione e, se necessario, revocarne il consenso e richiederne la cancellazione. Entriamo in nuova realtà in cui il "dato" diventa l'elemento centrale, un bene di scambio per accedere ai servizi digitali e, in sostanza, per essere parte attiva dell'ecosistema della rete[16].
Alla luce di ciò, il tradizionale diritto del "*right to be let alone*" lascia spazio al più dinamico diritto alla protezione dei dati personali: uno strumento flessibile che si adatta alle sfide

---

[12] A. BALDASSARRE (1974), *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, Roma; cit. in M. OROFINO (2018), *op. cit.*, p. 11.
[13] D. J. SOLOVE, P. M. SCHWARTZ (2021), *Information Privacy Law*, Wolters Kluwer Law & Business, New York; cit. in P. GUARDA, G. BINCOLETTO (2023), *Diritto comparato della privacy e della protezione dei dati personali*, Milano, Ledizioni, p. 19.
[14] A. WESTIN (1967), *Privacy and freedom*, New York, Atheneum; cit. in Y. ORITO, K. MURATA, (2005), *Privacy Protection in Japan: Cultural Influence on the Universal Value*, Electronic proceedings of Ethicomp, p. 2.
[15] F. FABRIS (2009), *op., cit.*, p. 97.
[16] A. ALONGI, F. POMPEI (2021), *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*, Cyber-Security-Defense, pp. 25-26.

della società contemporanea, regolando le modalità di raccolta, di trattamento e di trasferimento dei dati.
Non è mai accaduto nella storia del diritto che lo sviluppo tecnologico richiedesse una tale rapidità di adattamento; in tempi brevi, ogni paese si è ritrovato a dover aggiornare le proprie normative[17]. Tra tutti, nonostante le differenze culturali e giuridiche, il Giappone ha dimostrato una straordinaria capacità di coniugare tradizione e modernità, rispondendo tempestivamente alle sfide poste dalla globalizzazione e dalla cooperazione internazionale.

1.2. La riservatezza nella cultura giapponese

In ogni sistema legale, le leggi sulla *privacy* mirano a riflettere le pratiche sociali e i valori di quella cultura. Pertanto, è essenziale considerare lo sviluppo storico e culturale che sta alla base delle legislazioni, soprattutto quando si tratta di cooperazione transfrontaliera[18].
Nel caso del Giappone, la riservatezza è tradizionalmente considerata una questione di rispetto e armonia sociale. Il sociologo Doi Takeo evidenzia come questo equilibrio sia sostenuto da due concetti: *amae* (甘え) ed *enryo* (遠慮)[19]. Insieme esprimono la convenzione sociale secondo cui è importante moderare le parole per non rivelare i propri sentimenti, contribuendo così a mantenere l'armonia all'interno del gruppo. In altre parole, una persona potrebbe temere che, esprimendosi senza riserve, possa essere visto come invadente e scortese[20].
Un esempio concreto si poteva osservare nelle case giapponesi tradizionali di epoca Meiji (1852-1912): gli spazi erano divisi da porte scorrevoli di carta (*shōji* 障子), che rendevano facile ascoltare le conversazioni delle persone accanto. In tali situazioni, gli interlocutori erano costretti ad affidarsi all'indiscrezione di chi ascoltava, e a sua volta l'ascoltatore

---

[17] R. PAGANO (1986), *La tutela dei dati personali. Evoluzione delle legislazioni europee e stato del dibattito,* Informatica e diritto, p.70.
[18] H. MIYASHITA (2011), *The evolving concept of data privacy in Japanese law*, International Data Privacy Law, Vol. 1, No. 4, p. 229.
[19] Letteralmente *amae* significa "indulgenza", dal verbo *amaeru* "fare affidamento sugli altri"; *enryo* significa "riserbo". Per approfondimenti si veda T. DOI (1973), *The anatomy of dependence,* trad. di J. BESTER, Kodansha International.
[20] Y. ORITO, K. MURATA (2008), *Rethinking the concept of the right to information privacy: a Japanese perspective, Journal of Information, Communication and Ethics in Society, Vol. 6, No. 3, p. 239.*

adottava un comportamento di riserbo, *"as-if"*[21] non avesse mai sentito. Nella metà del Novecento, l'antropologa e scrittrice americana Ruth Benedict esaminò questa dinamica sociale nella sua opera "Il crisantemo e la spada". L'autrice affermava che la poca *privacy* presente nelle comunità giapponesi rendeva inevitabile che "il mondo" venisse a conoscenza di tutto ciò che una persona faceva, con il rischio di escluderla qualora il suo comportamento non fosse stato approvato dagli altri. Inoltre, questa interpretazione era rafforzata anche dall'assenza di un termine equivalente a *"privacy"* nel vocabolario linguistico tradizionale, inducendo altri studiosi a credere nel mito occidentale secondo cui tra i giapponesi mancasse il concetto di intimità[22].

La validità delle conclusioni di Benedict deve essere però valutata con un approccio critico, considerando i limiti metodologici e interpretativi che hanno caratterizzato la sua ricerca. Le osservazioni condotte non erano fonte di un'esperienza diretta, bensì di studi generalizzati e interviste con giapponesi emigrati negli Stati Uniti durante la Seconda guerra mondiale. In Giappone, questo genere letterario è noto come *Nihonjinron* (日本人論 "teorie sui giapponesi"), ovvero quelle ricerche che trattano le caratteristiche del popolo giapponese e della sua cultura. Questi scritti sono spesso impiegati a supporto visioni nazionalistiche, che presentano la cultura giapponese come unica e definita. Per questa ragione, il termine viene spesso utilizzato in senso negativo, per indicare spiegazioni onnicomprensive e troppo semplificate, che sembrano racchiudere il Giappone in un'unica definizione[23].

Dal punto di vista lessicale, è opportuno osservare che il termine inglese "*privacy*", trascritto nel sillabario per le parole straniere (*katakana*) come "*puraibashī*", è stato introdotto solo successivamente. Ciò potrebbe aver fatto presumere che la percezione della riservatezza non fosse un concetto comune all'epoca; tuttavia, affermare che

---

[21] Convenzione giapponese. Consiste nel non rivelare informazioni ascoltate involontariamente, comportandosi "come se" non fossero mai state udite, per mantenere l'armonia e il rispetto reciproco. Si veda M. MIZUTANI, J. DORSEY, J. MOORE (2004), *The internet and Japanese conception of privacy*, Ethics and Information Technology, Vol. 6, pp. 121, 124.

[22] Ad es. in M. ITOH (1964), *Issues in the "After the Banquet" Decision*, trad. di C. J. BRADSHAW, Jurist, No. 309, 1964, pp. 47-51; cit. in A. ADAMS, K. MURATA, Y. ORITO (2009), *The Japanese Sense of Information Privacy*, AI & Soc, Vol. 24, p. 327. L'autore scrive: *"[...]in our country (Japan), where a sense of respect for the private life of the individual is lacking,[...]"*.

[23] P. KENT (1999), *Japanese perceptions of the "Chrysantemum and the Sword"*, Dialectical Anthropology, Vol. 24, No. 2, p. 182.

qualcosa non possa esistere semplicemente perché non è rappresentato da una parola specifica sarebbe un grave eccesso di semplificazione[24]. In merito a ciò, Adams, Murata e Orito hanno suggerito un'interpretazione diversa: non solo era una nozione ben presente, ma proprio i comportamenti sopra descritti riflettevano una profonda comprensione della *privacy* delle informazioni, come dimostrato dalla rapidità con cui la società giapponese è passata da un sistema fondato su queste norme sociali a uno in cui si è affermata una forte protezione legale[25].

1.2.1. *La privacy nei tribunali: il caso "Utage no ato"*

Il sistema giudiziario giapponese è strutturato in un'organizzazione di tribunali articolata su tre gradi di giudizio. Al vertice vi è la Corte Suprema (*Saikō Saibansho*, 最高裁判 所), seguita da 8 Corti d'Appello, o Alte Corti (*Kōtō Saibansho*, 高等裁判所), 50 Tribunali distrettuali (*Chihō Saibansho*, 地方裁判所), 50 Tribunali di famiglia (*Katei Saibansho*, 家庭裁判所) e 438 Tribunali semplici (*Kan'i Saibansho*, 簡易裁判所).

I Tribunali distrettuali rappresentano il primo grado di giudizio e si occupano dei casi di materia civile e penale che si verificano all'interno della giurisdizione di competenza. A loro rispondono direttamente i Tribunali semplici, ovvero quelle corti che seguono soprattutto i casi civili di minore entità e i reati lievi, che solitamente non prevedono pene detentive. Mentre i Tribunali di famiglia, come si deduce dal nome, sono adibiti alle questioni familiari, ereditarie e di giustizia minorile.

Le Alte Corti che stanziano nelle città di Tokyo, Osaka, Fukuoka, Hiroshima, Sapporo, Nagoya, Takamatsu e Sendai costituiscono il secondo grado di giudizio e gestiscono i casi che provengono dalle corti inferiori.

Infine, la Corte Suprema con sede a Tokyo è l'organo di terzo grado, a cui spetta l'importante compito di esaminare in appello i provvedimenti presi dalle Alte Corti e di controllare la costituzionalità delle leggi. Il Presidente della Corte viene nominato

[24] M. MIZUTANI, J. DORSEY, J. MOORE (2004), *op. cit.*, p. 122.
[25] A. ADAMS, K. MURATA, Y. ORITO (2009), *op. cit.*, pp. 329, 336.

dall'Imperatore e sceglie i 14 giudici, i quali vengono riconfermati tramite un giudizio popolare nelle elezioni generali della Camera dei Rappresentanti[26].

La prima decisione delle corti giapponesi che riconobbe il diritto alla *privacy* riguardò un caso giudiziario di grande clamore avvenuto nel 1964. Il procedimento legale fu intentato da Arita Hachirō, Ministro degli Esteri per tre mandati e candidato senza successo alla carica di Governatore di Tokyo nel 1959, contro Mishima Yukio[27], autore del romanzo "Dopo il banchetto" (*Utage no Ato* 宴の後), pubblicato nel 1960. La storia si basava sulla rielaborazione di elementi privati della vita di Arita, inclusi il divorzio e le relazioni personali. Da quanto affermato dal politico, la pubblicazione dell'opera e la conseguente violazione della sua *privacy* gli avevano provocato un grave stress emotivo, soprattutto per le descrizioni riguardanti il suo complicato rapporto con la moglie e le loro interazioni intime in camera da letto[28].

Il nodo centrale verteva sul riconoscimento del diritto alla *privacy* nella normativa giapponese. Sebbene la Costituzione del Giappone (*Nihonkoku Kenpō* 日本国憲法)[29] non contemplasse una disposizione specifica a riguardo, la Corte Distrettuale di Tokyo interpretò, alla luce dell'articolo 13 della Costituzione, l'articolo 709 del Codice civile come un riconoscimento implicito del diritto alla *privacy*, quale interesse giuridicamente protetto. Pertanto, la sua mancata osservanza consentiva di richiedere un intervento giuridiziale a tutela del diritto leso[30]. A tal proposito, la Corte si pronunciò così:

> L'articolo 13 della Costituzione del Giappone afferma chiaramente che tutti i cittadini devono essere rispettati come individui e che il loro diritto al perseguimento della felicità costituisce l'obiettivo supremo della politica nazionale. Poiché il rispetto della *privacy* non è altro che

[26] A. ORTOLANI (2011), *Giappone (diritto moderno)*, Digesto delle discipline privatistiche, Torino, pp. 445-446.
[27] Pseudonimo di Hiraoka Kimitake (1925-1970), fu uno scrittore giapponese di fama internazionale.
[28] T. SUGANO (1970), *Privacy in Japan,* The Comparative and International Law Journal of Southern Africa, Vol. 3, No. 2, p. 225.
[29] Costituzione del Giappone. Promulgata il 3 novembre 1946 e in vigore dal 3 maggio 1947, prese il posto della prima Costituzione (*Dainippon teikoku kenpō* 大日本帝国憲法) del periodo Meiji. Si tratta della Carta costituzionale più longeva al mondo e stabilisce i principi della democrazia, dei diritti umani e del pacifismo.
[30] L'articolo stabilisce: "Una persona che con dolo o colpa viola i diritti o gli interessi altrui, protetti dalla legge, è tenuto a risarcire i danni che ne conseguono". Occorre precisare che il testo originale citava solo la violazione di un diritto; la tutela degli interessi protetti dalla legge fu successivamente aggiunta con la riforma linguistica del 2005. Si veda A. ORTOLANI (2011), *op., cit.,* pp. 441-442. Il Codice civile attuale è reperibile al sito: https://www.japaneselawtranslation.go.jp/en/laws/view/3494

> l'affermazione della dignità individuale e la realizzazione del diritto dell'individuo al perseguimento della felicità, si deve intendere che, quando viene ostacolato tale diritto da un'effettiva violazione della sua privacy, lo Stato è tenuto a fornire tutte le agevolazioni al cittadino, al fine di eliminare tale violazione e ricevere il risarcimento del danno. L'interpretazione e l'applicazione dell'articolo 709 del Codice civile devono essere fatte in questa prospettiva[31].

La Corte giunse alla conclusione che, con la pubblicazione del romanzo, i convenuti avevano esposto il querelante all'attenzione pubblica, provocandogli un forte disagio psicologico e violando intenzionalmente la sua *privacy*[32]. In virtù della decisione, gli imputati furono condannati a un risarcimento di 800.000 yen. Mishima impugnò la decisione e portò il caso all'Alta Corte di Tokyo ma, a causa della sua morte prematura di Arita, la vicenda si concluse con un accordo con i familiari, che acconsentirono alla vendita del romanzo.
Da quel momento in poi, la sentenza incoraggiò i tribunali a prendere in considerazione più seriamente le violazioni della *privacy*.

In un'altra causa legale, anche la Corte Suprema riconobbe l'ammissibilità della violazione del diritto alla *privacy* ai sensi dell'art. 13. Le circostanze riguardavano la manifestazione non autorizzata degli studenti dell'Università Ritsumeikan di Kyoto del 1965, durante la quale un poliziotto fotografò alcuni manifestanti in prima fila senza il loro consenso[33]. Al momento dell'udienza, le fotografie furono utilizzate per confermare la partecipazione degli imputati all'evento, ma uno di loro contestò l'acquisizione delle immagini, ritenendola una lesione ai suoi diritti. Sebbene la Corte respinse questa difesa, il giudice dispose che la fotografia di un cittadino senza giustificazione ad opera di un agente di polizia costituiva una trasgressione dell'articolo 13 della Costituzione[34].
Non ci sono dubbi che la *privacy* delle persone ritratte fosse l'elemento principale del caso dato che le fotografie mostravano informazioni personali sufficienti a identificarle.

---

[31] TRIBUNALE DISTRETTUALE DI TOKYO, *Shōwa sanjūkyūnen kyūgatsu nijūhachinichi hanketsu* (Sentenza del 28 settembre 1964), Kakyū Saibansho Minji Hanreishū, Vol. 15, No. 9, p. 2317.
[32] T. SUGANO (1970), *op. cit.*, p. 226.
[33] G. GREENLEAF (2014), *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford University Press, p. 230.
[34] Ciononostante, se invece la fotografia fosse stata scattata per preservare delle prove di crimine in corso o recentemente avvenuto, in tal caso non avrebbe infranto la Carta costituzionale, anche senza consenso o mandato. CORTE SUPREMA DEL GIAPPONE, *Shōwa yonjūyon'nen jūnigatsu nijūyon'nichi hanketsu* (Sentenza del 24 dicembre 1969), Keishū, Vol. 23, No. 12, p. 1625.

Tuttavia, è interessante notare che questa interpretazione rientra nella definizione moderna di "dato personale", nonostante si tratti di un caso molto precedente all'entrata in vigore della normativa sulla protezione dei dati[35]. Difatti, nei regolamenti come il GDPR in Europa o la legge APPI in Giappone, questo termine è definito come qualsiasi informazione che possa identificare direttamente o indirettamente una persona. Ciò include dati ovvi, come nome e cognome ma anche informazioni meno immediate, come numeri identificativi, dati relativi alla posizione e, appunto, fotografie.

1.3. Gli strumenti internazionali per il trasferimento dei dati

Lo sviluppo e la diffusione dei sistemi informatici dagli anni '70 in poi segnarono l'inizio di una rivoluzione tecnologica che avrebbe trasformato radicalmente il modo in cui i dati venivano creati, gestiti e condivisi. Le varie autorità nazionali si accorsero dell'esigenza di rivedere le proprie normative sulla *privacy*, dal momento che l'ampio impiego di queste nuove tecnologie nelle pubbliche amministrazioni sollevava timori tra la popolazione riguardo al potenziale rischio di un controllo esteso e invasivo da parte degli Stati[36].
Mentre in Giappone alcune amministrazioni locali iniziarono a adottare una serie di misure come le Ordinanze sul Consiglio di gestione dei sistemi di calcolo elettronico nella città di Tokushima, (*Tokushimashi denshi keisan soshiki unei shingikai jōrei* 徳島市電子計算組織運営審議会条例, 1973) e Kunitachi (*Kunitachishi denshi keisan soshiki no unei ni kansuru jōrei* 国立市電子計算組織の運営に関する条例, 1975)[37], in Europa si cominciò a discutere sulla regolazione del libero flusso di dati oltre i confini nazionali.

Già nel 1968, il Comitato dei ministri del Consiglio d'Europa avviò un dibattito sul grado di tutela della riservatezza nei vari stati europei. L'obiettivo era valutare l'impatto delle crescenti innovazioni tecnologiche sulla protezione dei dati personali, in un contesto privo

[35] R. WALTERS, L. TRAKMAN, B. ZELLER (2019), *Data Protection Law. A Comparative Analysis of Asia-Pacific and European Approaches*, Springer, p. 242.
[36] F. SERINI (2022), *op., cit.*, p. 81.
[37] G. GREENLEAF (2014), *op. cit.*, p. 231.

di direttive uniformi per i membri della Comunità europea[38]. I risultati evidenziarono un panorama normativo disomogeneo, caratterizzato da notevoli differenze tra le legislazioni nazionali.

Inoltre, la trasformazione digitale rivelò una serie di complessi interessi politici, soprattutto nel commercio internazionale, dove il trattamento e la condivisione dei dati acquisivano sempre maggiore valore nell'economia mondiale. Dunque, i governi e le organizzazioni internazionali si trovarono costretti a considerare seriamente l'adozione di disposizioni giuridiche per definire un quadro comune a livello globale. Con questa volontà, nel 1980 furono adottate le *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* dell'OCSE[39] e la Convenzione 108 del Consiglio d'Europa.

1.3.1. *Linee Guida OCSE e Convenzione 108*

Le linee guida OCSE del 1980 furono le prime a porre l'attenzione sul libero trasferimento internazionale di dati personali, stabilendo dei principi non vincolanti che promuovevano la protezione della *privacy* e delle libertà individuali, e fornivano raccomandazioni utili alla cooperazione tra i Paesi membri. Assieme alla Convenzione 108, furono il primo strumento internazionale a definire le nozioni di "dato di carattere personale", "detentore di una collezione di dati", e per la prima volta menzionarono i "flussi transfrontalieri di dati personali", definendoli *"movements of personal data across national borders"*[40].

Nello specifico il paragrafo 15 esortava i Paesi membri a considerare gli effetti che le operazioni di trattamento e la riesportazione dei dati personali avrebbero avuto sugli altri Stati. In altre parole, raccomandava di redigere delle normative che non fossero in contrasto con quelle di altri Paesi, promuovendo invece un trattamento dei dati compatibile e conforme alle altre leggi. A tal proposito, il paragrafo successivo invitava a

---

[38] A. ALONGI, F. POMPEI (2021), *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*, Cyber-Security-Defense, p. 238.

[39] Organizzazione per la Cooperazione e lo Sviluppo Economico, è un'organizzazione internazionale fondata nel 1961 che promuove politiche volte a migliorare il benessere economico e sociale a livello globale.

[40] OCSE (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* pp. 11, 13. Il "dato di carattere personale" si riferisce a "ogni informazione concernente una persona fisica identificata o identificabile (persona interessata)"; il "detentore di una collezione di dati" sta per "la persona fisica o giuridica, la pubblica autorità, il servizio o qualsiasi altro organismo che, secondo la legge nazionale, è competente a decidere quale debba essere la finalità dello schedario automatizzato, quali categorie di dati a carattere personale debbano essere registrate e quali operazioni debbano essere loro applicate".

adottare tutte le misure ragionevoli e appropriate per garantire che i flussi di dati, inclusi quelli attraverso un Paese membro, avvenissero in modo sicuro e costante.
Il paragrafo 17 sottolineava quanto fosse importante non porre restrizioni ai flussi transfrontalieri tra i Paesi, salvo nei casi in cui uno di essi non rispettasse adeguatamente le linee guida o se la riesportazione dei dati rischiasse di eludere la legislazione sulla *privacy* del Paese da cui proveniva. Inoltre, consentiva di imporre delle restrizioni su categorie specifiche di dati personali qualora la legislazione nazionale prevedesse norme particolari per tali dati e il Paese destinatario non offrisse una protezione equivalente.
Infine, l'ultimo paragrafo dissuadeva dall'elaborazione di politiche o pratiche che facessero da ostacolo alla corretta trasmissione dei dati, garantendo al contempo il rispetto delle libertà individuali e della *privacy*. Lo scopo delle linee guida era dunque quello di istituire un sistema normativo omogeneo per regolare il trattamento e l'esportazione dei dati tra i Paesi membri, indispensabile per favorire lo sviluppo economico, la cooperazione internazionale e l'innovazione tecnologica.

Sebbene perseguisse lo stesso intento, la Convenzione di Strasburgo (n. 108) adottava un criterio più vincolante e stabiliva disposizioni legalmente impegnative per gli Stati firmatari. In riferimento alla circolazione internazionali, il capitolo 3 vietava ai Paesi partecipanti di bloccare o subordinare a specifiche autorizzazioni il trasferimento transfrontaliero dei dati[41]. Tuttavia, come stabilito dal terzo comma dell'art. 12, vi erano due eccezioni:

> a) se la legislazione dello Stato trasferente imponeva regolamenti specifici per alcune categorie di dati personali o per i casellari automatizzati che li conteneva, in ragione della natura degli stessi, salvo che lo Stato destinatario non garantisse una protezione equivalente;
> b) se il trasferimento avveniva verso un Paese non contraente attraverso un altro Paese membro, al fine di evitare che il trasferimento eludesse la legislazione o le garanzie dello Stato trasferente del flusso di dati.

[41] CONSIGLIO D'EUROPA (1981), *Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* (Convenzione n. 108), Strasburgo, pp. 4-5.

Il Giappone ha aderito al trattato nel 2002 come membro non europeo, ma non ha tuttora completato il processo di ratifica; ciò significa che, pur essendo un firmatario, non è giuridicamente obbligato a conformarsi alle sue disposizioni.
In ogni caso, entrambi i trattati costituiscono i pilastri del diritto alla protezione dei dati personali giapponese, poiché sono anche il modello da cui i governi locali si sono ispirati per elaborare l'*Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs* (*Gyōsei kikan no hoyūsuru denshi keisanki shori ni kakaru kojin jōhō no hogo ni kansuru hōritsu* 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律, 1988)[42].

Nonostante questa legge rappresentasse un importante passo avanti per la protezione dei dati personali nel settore pubblico, escludeva completamente il settore privato. È probabile che questa lacuna legislativa non fosse ritenuta urgente, poiché la principale preoccupazione dell'epoca era rivolta alla crescente quantità di dati personali gestiti dagli enti governativi, i quali utilizzavano numeri di riferimento digitali per associare ogni dato a una persona, incrociando i numeri di identificazione con i registri cartacei[43].

1.3.2. *Gli accordi di libero scambio tra Giappone e Asia*

Nel corso della sua storia, il Giappone ha partecipato attivamente a diverse organizzazioni e ha stipulato vari accordi commerciali per promuovere la libera circolazione dei dati, principalmente attraverso il *General Agreement on Tariffs and Trade* (GATT) e l'Organizzazione Mondiale del Commercio (OMC). Tuttavia, fino agli anni 2000, il suo ruolo nei dibattiti sugli Accordi di Libero Scambio (FTA) in Asia era rimasto marginale, finché non cominciò a perseguire una politica più diversificata, orientata alla liberalizzazione bilaterale e plurilaterale, vale a dire tra due o più paesi selezionati[44]. Questo nuovo approccio prese piede nel novembre del 2002 quando Singapore propose la creazione di un gruppo di studio composto da funzionari governativi, imprenditori e accademici per esaminare i contenuti di un possibile accordo bilaterale e il suo impatto

[42] Y. SUDA (2020), *Japan's Personal Information Protection Policy Under Pressure, Asian Survey: The Japan-EU Data Transfer Dialogue and Beyond*, Vol. 60, No. 3, p. 513.
[43] A. ADAMS, K. MURATA, Y. ORITO (2010), *The Development of Japanese Data Protection*, Policy & Internet, Vol. 2, No. 2, p. 117.
[44] S. URATA (2007), *Japan's FTA Strategy and Free Trade Area of Asia Pacific (FTAAP)*, PECC/ABAC Joint Study on Free Trade Area of the Asia Pacific, p. 1.

sulle rispettive economie[45]. Dopo una serie di negoziati, i primi ministri formalizzarono l'intesa che portò all'entrata in vigore del *Japan-Singapore Economic Partnership Agreement* (JSEPA).
Questo fu il primo di una serie di accordi bilaterali con i paesi dell'*Association of Southeast Asian Nations* (ASEAN)[46], che culminarono con il raggiungimento di una cooperazione economica tra il Giappone e l'ASEAN stessa. Ciò includeva anche negoziazioni per gli FTA, che iniziarono nel 2005 e si conclusero con la firma dell'Accordo di Partenariato Economico Giappone-ASEAN (AJCEP) nel 2008. L'intento era rafforzare i legami economici, politici e strategici, migliorare l'ambiente degli affari nella regione e proteggere i diritti di proprietà intellettuale a favore delle imprese giapponesi[47].

Come parte della sua politica commerciale plurilaterale, il Giappone ha aderito nel 2017 al CPTPP (*Comprehensive and Progressive Agreement for Trans-Pacific Partnership*), un accordo che coinvolge paesi provenienti da diverse regioni, dall'Asia all'Oceania fino alle Americhe[48]. Il CPTPP è una versione rivisitata del TPP (*Trans-Pacific Partnership*), che, in seguito all'abbandono degli Stati Uniti, ha cambiato nome ma ha mantenuto lo stesso impegno: creare un modello commerciale più adatto al contesto globale contemporaneo rispetto agli accordi tradizionali dell'OMC[49].

Nel contesto degli scambi transfrontalieri, l'art. 14.11 inerente al *"Cross-Border Transfer of Information by Electronic Means"* imponeva che ogni parte consentisse il flusso di dati elettronici tra i paesi membri, per fini aziendali. Questo permetteva una certa flessibilità nell'utilizzo di misure per raggiungere i legittimi obiettivi, come evitare discriminazioni arbitrarie o ingiustificate, o restrizioni mascherate sul commercio, purché tali misure non eccedessero quelle necessarie per raggiungere l'obiettivo prefissato[50].

---

[45] *Ivi*, p. 2.
[46] Organizzazione regionale che promuove la cooperazione economica, politica e culturale tra dieci paesi del Sud-Est asiatico: Indonesia, Malesia, Filippine, Singapore, Thailandia, Brunei, Vietnam, Laos, Myanmar, Cambogia. Il Giappone non ne fa parte, ma mantiene una stretta collaborazione attraverso partenariati economici e strategici.
[47] S. URATA (2007), *op. cit.,* p. 4.
[48] Attualmente include 12 paesi: Giappone, Malesia, Singapore, Brunei, Vietnam, Australia, Nuova Zelanda, Canada, Messico, Cile e Perù e Regno Unito.
[49] M. BURRI (2022), *Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions: Implications for the Future EU-ASEAN Agreement*, Legal Issues of Economic Integration, No. 49, p. 154.
[50] Il capitolo 14 dell'accordo è disponibile in inglese nel sito dell'Ufficio del Gabinetto giapponese al link: https://www.cas.go.jp/jp/tpp/tppinfo/kyotei/tpp_text_en/pdf/14.Electronic_Commerce.pdf

1.3.3. *Asian-Pacific Economic Cooperation*

Dopo aver esaminato il ruolo che hanno assunto gli accordi di libero scambio nell'incentivare il trasferimento transfrontaliero di dati, è indispensabile ampliare lo sguardo verso le iniziative regionali che hanno contribuito a plasmare il panorama economico dell'area Asia-Pacifico.

In questo senso, l'impegno del Giappone non si limita agli accordi bilaterali o plurilaterali, ma si estende anche a progetti multilaterali, come la fondazione dell'*Asian-Pacific Economic Cooperation* (APEC).

Concepito nel 1989 come un gruppo informale di dialogo tra ministri e alti funzionari di dodici Paesi, l'APEC si è gradualmente trasformato in un organismo intergovernativo di grande rilevanza, soprattutto con l'introduzione nel 1993 del *"Economic Leaders' Meeting"*, l'incontro annuale tra i leader economici. Questa cooperazione tra economie della regione Asia-Pacifico aveva l'ambizioso obiettivo di promuovere il libero scambio e gli investimenti entro il 2010 per le economie sviluppate ed entro il 2020 per quelle in via di sviluppo[51].

A differenza dell'Organizzazione Mondiale del Commercio e di altri organismi commerciali multilaterali, l'APEC non impone obblighi legali ai suoi partecipanti né dispone di istituzioni formali oltre ai regolari incontri. Inoltre, le decisioni vengono prese per consenso e gli impegni sono assunti su base volontaria[52].

Le sue fondamenta si basano su principi che si erano rivelati efficaci nella promozione della cooperazione regionale all'interno dell'ASEAN, tra cui la trasparenza nelle politiche, l'uguaglianza nei benefici di tutti i partecipanti e l'evoluzione basata sul consenso, con un approccio graduale, sostenibile e pragmatico alla cooperazione[53].

Dopo il *Leaders' Meeting* del 2004 in Cile, con la supervisione dell'*Electronic Commerce Steering Group Privacy Subgroup* (ECSG), l'APEC ha adottato il *"Privacy Framework"*. Pur ispirandosi alle Linee guida dell'OCSE, il *Framework* non pone l'accento sulla tutela della *privacy*, ma sull'importanza del commercio globale e del libero flusso di dati. Attraverso

---

[51] L'APEC conta attualmente 21 economie membri. Per approfondimenti si veda APEC (2019). *APEC at 30: A Region in Constant Change*, APEC Regional Trends Analysis, Singapore.

[52] J.G. TAN (2008), *A Comparative Study of the APEC Privacy Framework*: *A new voice in the data protection dialogue*?, Asian Journal of Comparative Law, Vol. 3, p. 21.

[53] P. DRYSDALE (1988), *International Economic Pluralism: Economic Policy in East Asia and the Pacific*, Allen and Unwin, Sydney; cit. in APEC (2019), *op. cit.*, p. 1.

un insieme di principi intendeva rafforzare la protezione dei dati nell'area Asia-Pacifico, favorendo la crescita del commercio elettronico. Questo modello è orientato verso una protezione della *privacy* coerente, piuttosto che uguale. In tal modo si bilanciano le esigenze di privacy con gli interessi commerciali e sociali, riconoscendo anche le differenze culturali e le altre peculiarità presenti nelle diverse economie[54].

Fin da subito questa novità è stata oggetto di alcune osservazioni negative, tra cui quella di Greenleaf, che l'ha descritto come una versione semplificata dell'OCSE[55]. Secondo l'autore le debolezze del *Framework* non derivavano solo dal fatto che gli standard del 1980 rappresentavano un punto di partenza inadeguato, ma anche dalla presenza di gravi lacune. Una delle quali riguardava l'assenza di disposizioni relative al trasferimento dei dati verso Paesi non appartenenti all'APEC[56].

Bisogna precisare che nell'Annex 1 del documento erano già presenti delle indicazioni per il futuro, ovvero: la volontà di condividere informazioni tra le economie membri dell'APEC in modo rapido, sistematico ed efficiente; la cooperazione tra le autorità responsabili delle indagini e dell'applicazione delle norme sulla *privacy*; e l'impegno a sostenere lo sviluppo e il riconoscimento dei *"cross-border privacy codes"*[57] nell'intera regione APEC[58].

Queste proposte furono concretizzate solo nel settembre del 2005 con la revisione finale, nella quale venne integrata una sezione specifica dedicata all'esportazione dei dati. A differenza degli strumenti internazionali precedenti però non erano previste alcune limitazioni in materia. Di conseguenza, è stato essenziale implementare un sistema di regole responsabile dei trasferimenti all'interno dell'APEC *Privacy Framework*, chiamato *Cross Border Privacy Rules System* (CBPR), al fine di garantire la protezione dei dati personali di un individuo indipendentemente dal luogo in cui tali dati venissero trasferiti o consultati[59]. Questo progetto ha preso il nome di *"Data Privacy Pathfinder".*

---

[54] È stato aggiornato nel 2015, ma i principi di base sono rimasti invariati. APEC (2015), *APEC Privacy Framework*, Digital Economy Steering Group, pp. 2-4.

[55] G. GREENLEAF (2003), *The APEC privacy initiative: "OECD Lite" for the Asia-Pacific?,* Privacy Law and Business, Vol. 71, pp. 16-18.

[56] J.G. TAN (2008), *op. cit.*, p. 26.

[57] Si riferisce ai codici di condotta o alle linee guida adottate da organizzazioni per garantire la protezione della *privacy* dei dati personali quando questi vengono trasferiti oltre i confini nazionali.

[58] APEC (2004), *APEC Privacy Framework*, Santiago.

[59] F. SERINI (2022), *op. cit.*, p. 74.

Capitolo 2

Il traffico di dati nella normativa giapponese

2.1. Contesto storico

Fino alla fine degli anni '90, i cittadini giapponesi dovevano registrarsi presso le autorità locali tramite un sistema cartaceo di registrazione familiare (*Koseki* 戸籍), che indicava le principali informazioni dei membri della famiglia. Insieme ad esso, ai cittadini era richiesta anche l'iscrizione a un registro individuale (*Jūminhyō* 住民票), in cui era riportato l'indirizzo di residenza[60].

Consapevole del fatto che entrambi i sistemi erano ormai antiquati, il Partito Liberal Democratico (LDP) propose di creare una rete di registrazione nazionale, ovvero il *Basic Residents' Registration Network* (*Jūmin kihon daichō network* 住民基本台帳ネットワーク), conosciuto anche come *Juki-net*. Questo sistema integrava i dati sulle generalità dei residenti di 3.200 amministrazioni comunali e assegnava ad ognuno di essi un numero identificativo di undici cifre. L'iniziativa mirava, da un lato, a creare un sistema centralizzato per la gestione dei dati da parte del governo e, dall'altro, a facilitare l'accesso dei cittadini ai servizi governativi, bancari, e commerciali grazie a una tessera apposita. Possedere il numero identificativo era obbligatorio, mentre l'acquisizione della tessera era facoltativa[61].

La questione attirò fin da subito le critiche dei media, i quali iniziarono a far circolare articoli circa i potenziali rischi di frode e abuso dei dati acquisiti, alimentando un clima di insicurezza tra la popolazione. Secondo un sondaggio condotto dall'*Asahi Shinbun*, tre quarti dei cittadini si dichiararono seriamente preoccupati e il 76% degli intervistati

---

[60] Il *koseki* viene tuttora utilizzato per tenere traccia di matrimoni, successioni e altro, mentre il *jūminhyō* è utilizzato per comprovare l'identità e l'indirizzo dei cittadini. A. ADAMS, K. MURATA, Y. ORITO (2010), *op. cit.*, pp. 108-109.

[61] G. GREENLEAF (2010), *Country Studies - B5 Japan*, in *Comparative Study on Different Approaches to New Privacy Challenges,* in *Particular in the Light of Technological Developments,* a cura di KORFF D., Commissione Europea, Directorate-General Justice, Freedom and Security, p. 4.

espresse il desiderio di "posticipare" l'emissione di *Juki-net* fino all'emanazione di una legge che tutelasse interamente il settore privato[62].

Di fronte alla pressione mediatica, il governo annunciò l'intenzione di avviare delle trattative con il *Keidanren* (*Nihon Keizai Dantai Rengōkai* 日本経済団体連合会), l'associazione economica che dava voce agli interessi delle grandi imprese giapponesi, al fine di trovare una soluzione che conciliasse le esigenze del popolo con quelle economiche e industriali del Paese. All'inizio il *Keidanren* era scettico, ma presto cambiò posizione e sostenne con decisione la causa. Si rese conto che l'adozione di un regime legislativo nazionale non avrebbe danneggiato il commercio nippo-americano, ma avrebbe anche messo le aziende giapponesi in una posizione di vantaggio competitivo nel commercio con l'UE[63].

Finalmente, dopo un'intensa fase di negoziati, il 30 maggio 2003 fu approvato un pacchetto di misure legislative che costituirono la prima legge giapponese sulla protezione dei dati personali.

2.2. La prima legge giapponese sulla protezione dei dati (APPI)

Il primo passo per la realizzazione della nuova legge sulla protezione dei dati personali si ebbe il 27 marzo 2001, quando il Consiglio dei ministri approvò il *Personal Information Protection Bill*. La proposta però incontrò una forte opposizione dei media che causò uno stallo in Parlamento per oltre un anno[64]. Di conseguenza, il governo intraprese una revisione approfondita, che fu approvata sia dalla Camera dei Rappresentanti che dalla Camera dei Consiglieri, portando alla promulgazione della prima legge giapponese sulla protezione dei dati personali il 23 maggio 2003.

La normativa consisteva in un pacchetto di cinque leggi, di cui faceva parte l'*Act on the Protection of Personal Information* (*Kojin jōhō no hogo ni kansuru hōritsu* 個人情報の保護

[62] A. ADAMS, K. MURATA, Y. ORITO (2009), *op. cit.*, p. 337.
[63] A. ADAMS, K. MURATA, Y. ORITO (2010), *op. cit.*, pp. 118.
[64] J. HARLAND (2004), *Japan's New Privacy Legislation: Are You Ready?*, Computer Law & Security Report, Vol. 20, No. 3, p. 200.

に関する法律, Legge No. 57/2003, APPI)[65], che definiva i principi fondamentali applicabili al settore privato[66]. Gli altri due provvedimenti imponevano degli obblighi di protezione dei dati esclusivamente adibiti al settore pubblico, e includevano: l'*Act on the Protection of Personal Information Held by Administrative Organs* (*Gyōsei kikan no hoyū suru kojin jōhō no hogo ni kansuru hōritsu* 行政機関の保有する個人情報の保護に関する法律, Legge No. 58/2003, PPIHAOA), che rispetto alla precedente versione incorporava anche la regolazione dei dati cartacei e stabiliva nuove sanzioni penali per i funzionari governativi che divulgavano informazioni personali senza una giustificazione adeguata; e una legge analoga per le istituzioni amministrative indipendenti, nota come *Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc.* (*Dokuritsu gyōsei hōjintō no hoyū suru kojin jōhō no hogo ni kansuru hōritsu* 独立行政法人等の保有する個人情報の保護に関する法律, Legge No. 59/2003, PPIHIAAA)[67].

Infine, vi erano due leggi relativi al settore locale, ovvero l'*Act for establishment of the Information Disclosure and Personal Information Protection Review Board* (*Jōhō kōkai-kojin jōhō hogo shinsakai secchihō* 情報公開・個人情報保護審査会設置法, Legge No. 60/2003) e l'*Act concerning the Preparation of Related Laws for the Enforcement of the Act concerning the Protection of Personal Information Held by Administrative Organs* (*Gyōsei kikan no hoyū suru kojin jōhō no hogo ni kansuru hōritsutō no shikō ni tomonau kankei hōritsu no seibitō ni kansuru hōritsu* 行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律, Legge No. 61/2003). La prima autorizzava la formazione di un comitato indipendente che poteva essere consultato dal responsabile dell'organo amministrativo coinvolto, nel caso in cui ci fossero stati reclami riguardo la decisione di rendere pubblici i documenti amministrativi o le informazioni personali. A quel punto, in qualità di ente terzo, il comitato effettuava una revisione del caso e forniva un rapporto[68]. Per quanto riguarda la seconda, essa era l'ultimo atto emanato in ordine di tempo e

[65] GOVERNO DEL GIAPPONE (2003), *Act on the Protection of Personal Information (Act No. 57 of May 30, 2003)*, Japanese Law Translation. Promulgato il 30 maggio 2003, entrato in vigore il 1° aprile 2005.
[66] J. HARLAND (2004), *op., cit.*, p. 200.
[67] G. GREENLEAF (2010), *op., cit.*, p. 7.
[68] *Ivi*, p. 9.

facilitava l'attuazione, da parte delle amministrazioni pubbliche giapponesi, delle leggi sopra citate[69].

2.2.1. *Struttura normativa*

La APPI del 2003 si componeva di sei capitoli:

I. Le *General Provisions* (*Sōsoku* 総則, artt. 1-3) specificavano gli obiettivi, i principi generali e le definizioni alla base dell'intera legge;
II. Le *Responsibilities of the State and Local governments* (*Koku oyobi chihō kōkyō dantai no sekimutō* 国及び地方公共団体の責務等, artt. 4-6) delineavano un quadro di responsabilità e compiti che le autorità pubbliche e locali dovevano rispettare;
III. Le *Measures for the Protection of Personal Information* (*Kojin jōhō no hogo ni kansuru shisakutō* 個人情報の保護に関する施策等, artt. 7-14) stabilivano le politiche e le misure pratiche per garantire una protezione efficace dei dati personali. In particolare, attraverso la collaborazione diretta tra lo Stato e le autorità locali;
IV. I *Duties of Entities Handling Personal Information* (*Kojin jōhō toriatsukai jigyōsha no gimutō* 個人情報取扱事業者の義務等, artt. 15-49) regolavano i principi che i titolari dovevano rispettare per assicurare un trattamento sicuro e trasparente dei dati personali;
V. Le *Miscellaneous Provisions* (*Zassoku* 雑則, artt. 50-55) includevano disposizioni diverse che non rientravano nelle sezioni principali della legge, ma che erano rilevanti per la sua attuazione e interpretazione;
VI. Le *Penal Provisions* (*Bassoku* 罰則, artt. 56-59) delineavano le sanzioni e le penalità per le violazioni delle disposizioni della legge.

[69] Si fa riferimento alle leggi PPIHAOA, PPIHIAAA e del Comitato di revisione. GOVERNO DEL GIAPPONE (2003), *Act concerning the Preparation of Related Laws for the Enforcement of the Act concerning the Protection of Personal Information Held by Administrative Organs (Act No. 61 of 2003)*, The House of Representatives.
https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/15620030530061.htm

Focalizzandoci sul Capitolo IV, i principi citati si ispiravano alle direttive OCSE seguenti[70]:

a. specificazione dello scopo di utilizzo: imponevano al titolare del trattamento di indicare le finalità per cui i dati venivano utilizzati e di non modificarle senza il consenso dell'interessato, rispettando i limiti necessari al raggiungimento di tale scopo (artt. 15-16);
b. corretta acquisizione e notifica dello scopo di utilizzo: prevedevano che lo scopo dovesse essere comunicato al momento dell'acquisizione, senza ricorrere a mezzi ingannevoli. Qualora lo scopo venisse modificato, l'interessato doveva essere tempestivamente informato (artt. 17-18);
c. accuratezza dei dati: il titolare garantiva la correttezza e l'aggiornamento dei dati nella misura necessaria per ottenere lo scopo specificato (art. 19);
d. sicurezza dei dati: il titolare doveva assicurarsi che i propri dipendenti e i fiduciari (*trustees*) non compromettessero la sicurezza del trattamento (artt. 20-22);
e. restrizione del trasferimento a terze parti: vietava i trasferimenti di dati verso un soggetto terzo senza il permesso dell'interessato (art. 23)[71]. Nonostante la disposizione del paragrafo però, il titolare del trattamento poteva procedere al trasferimento senza il consenso, qualora avesse notificato in anticipo le modalità, le finalità, e avesse preventivamente comunicato all'interessato la possibilità di interrompere la fornitura in ogni momento (art. 23.2). Questa politica è definita "*opt-out*"[72];
f. accesso e trasparenza: il titolare era tenuto a rivelare all'interessato informazioni sullo scopo del trattamento, sul responsabile, sulle procedure di accesso e sulla divulgazione dei dati. Inoltre, gli interessati avevano il diritto di accedere, correggere o sospendere il trasferimento dei propri dati in caso di errori o usi impropri (art. 24-27).

---

[70] J. HARLAND (2004), *op., cit.*, pp. 201-202.
[71] A questo disposto si escludevano i seguenti casi di trasferimento: (i) quando avveniva per leggi e regolamenti; (ii) quando era coinvolta la vita, la salute fisica o la proprietà di una persona ed era difficile ottenere il consenso; (iii) quando era necessario per promuovere l'igiene pubblica o il benessere dei bambini ed era difficile ottenere il consenso; (iv) quando era necessario per la cooperazione con enti governativi o locali, o con soggetti da essi incaricati, nello svolgimento di compiti previsti dalla legge, e il consenso avrebbe potuto ostacolare tale cooperazione.
[72] F. SERINI (2022), *op. cit.*, p. 110.

2.2.2. *Definizioni e applicazioni*

L'art. 2 della APPI 2003 definiva separatamente "informazione personale" (*Kojin jōhō* 個人情報) e "dato personale" (*Kojin dēta* 個人データ). Il primo termine si riferiva a qualsiasi informazione che, tramite il nome, la data di nascita o altri elementi contenuti in essa (inclusi quelli che, se combinati tra loro, permettevano una facile identificazione di un individuo specifico), potesse identificare una persona fisica (*Honnin* 本人, "interessato"). Il secondo termine corrispondeva a un'informazione personale che costituiva un "*personal information database*" (*Kojin jōhō dētabēsutō* 個人情報データベース等, "database di dati personali"), ossia un insieme di informazioni organizzate in modo tale da poter essere recuperate tramite un computer, oppure una raccolta di informazioni stabilita da un'ordinanza governativa (*Seirei* 政令) che consentiva il facile accesso a specifici dati. Coloro che utilizzavano questi database per le proprie attività erano definiti "*business operator handling personal information*" (*Kojin jōhō toriatsukai jigyōsha* 個人情報取扱事業者, "titolari del trattamento"), tra i quali non figuravano gli organi statali, i governi locali, le agenzie amministrative incorporate e tutti gli enti specificamente indicati da un'ordinanza governativa, in quanto regolati da altra legislazione[73].
Infine, l'APPI introduceva un'altra nozione di informazione, il "dato personale conservato" (*Hoyu kojin dēta* 保有個人データ) [74], rispetto al quale il titolare aveva il compito di seguire specifici obblighi nei confronti dell'interessato. In particolare, il titolare era tenuto a: fornire l'accesso a questi dati su richiesta, tranne quando la divulgazione avrebbe potuto danneggiare i diritti o gli interessi del richiedente o di terzi; ostacolare l'esecuzione delle attività del titolare; o violare altri regolamenti (art. 25). Inoltre, qualora l'interessato avesse richiesto la correzione, l'aggiunta o la cancellazione dei dati, il titolare avrebbe dovuto valutare la richiesta e decidere tempestivamente se accoglierla o respingerla (art.

[73] G. GREENLEAF (2010), *op., cit.*, p. 11.
[74] Sono esclusi da questa definizione i dati che sono stati valutati da un'ordinanza governativa come dannosi per gli interessi pubblici o privati se la loro presenza o assenza è conosciuta; e i dati che devono essere cancellati entro massimo un anno. Si veda Act No. 57/2003, art. 2.5 (APPI).

26). L'interruzione del trattamento invece si verificava in presenza della violazione degli artt. 16, 17 e 23, salvo nei casi in cui l'operazione risultava particolarmente onerosa o complessa; in quest'ultima circostanza, dovevano essere adottate misure alternative (art. 27).

Tutte le regole sopra citate erano applicate solo a coloro che si trovavano sul territorio nazionale. Infatti, la normativa, nella sua prima versione, non presentava alcuna regolamentazione specifica per i soggetti stabiliti fuori dal Paese. Per regolamentare questo ambito, il Giappone faceva affidamento sulle restrizioni a terzi che imponevano il consenso dell'interessato, nonostante potessero essere facilmente aggirate da una notifica di "*readily accessible condition*", che non obbligava neppure a specificare la destinazione estera dei dati (art. 23.2). In più, non esisteva alcuna norma che imponesse ai destinatari il rispetto della legge giapponese[75].
Da questa disamina appare quindi evidente che, se i dati fossero stati correttamente divulgati secondo l'art. 23 a una terza parte straniera non presente in Giappone nessuno sarebbe stato ritenuto responsabile[76].

2.2.3. *Autorità regolatorie e sanzioni*

Le lacune normative dell'APPI del 2003 si riflettevano in un sistema regolatorio frammentato. All'epoca non era ancora stata disposta un'autorità garante nazionale dedicata esclusivamente alla protezione dei dati personali. La responsabilità della supervisione e della gestione dei reclami era affidata alla struttura ministeriale esistente. Alcuni ministri governativi, detti ministri competenti (*Shumu daijin* 主務大臣), erano autorizzati a indagare e a fornire consulenza ai titolari del trattamento che avevano violato i doveri prescritti dalla legge[77]. A tale scopo, il ministro competente poteva anche designare, ai sensi dell'art. 37, un'organizzazione autorizzata (*Nintei kojin jōhō hogo dantai* 認定個人情報保護団体, APIPO) che si occupava dei reclami di altre imprese

[75] G. GREENLEAF (2010), *op., cit.*, p. 21
[76] *Ibidem*. Eccetto nel caso in cui l'entità straniera agiva come fiduciario per conto dell'esportatore giapponese (secondo gli artt. 20-22), allora la legge giapponese si applicava comunque, anche se questa entità non aveva una presenza in Giappone.
[77] Chi non avesse rispettato le direttive dei ministri, avrebbe ricevuto una multa di massimo 300.000 yen o una pena detentiva di massimo 6 mesi (artt. 56-59). Si veda J. HARLAND (2004), *op., cit.*, p. 203.

(*Taishō jigyōsha* 対象事業者, "*target entities*"). Ogni impresa "*target*" doveva entrare a far parte di un APIPO, la quale successivamente rendeva pubblica l'adesione (art. 41). Inoltre, l'impresa era tenuta a collaborare nelle indagini e a non rifiutare le richieste delle APIPO senza una giustificazione valida (art. 42). Dal canto loro, le APIPO dovevano pubblicare le proprie linee guida (art. 43) e, su richiesta del ministro competente, seguire ordini di revisione procedurale (art. 47), altrimenti rischiavano la revoca dell'autorizzazione (art. 48).

Sebbene il *Quality of Life Policy Council*[78] riconoscesse l'importanza di tali organismi nella risoluzione delle controversie, ne criticava la scarsa attività, soprattutto per quanto concerne la fuga di dati personali[79]. D'altronde, nella cultura giapponese, un evento simile rappresenta un danno gravissimo, poiché può compromettere i rapporti di fiducia con i clienti e con la comunità, portando a un crollo vertiginoso della reputazione aziendale[80].

2.3. La riforma del 2015

La riforma dell'APPI si rese necessaria a seguito degli sviluppi tecnologici che caratterizzarono la cosiddetta "era dei *big data*", quel periodo tra la seconda metà degli anni 2000 e i primi anni del 2010 in cui le aziende e le organizzazioni cominciarono a servirsi di enormi volumi di dati per scopi commerciali. Questo scenario divenne possibile grazie allo sviluppo dell'*Internet of Things* (*IoT*) e dei *social networks*, che rivoluzionarono la raccolta e la diffusione dei dati su larga scala, favorendo la profilazione degli utenti attraverso l'analisi approfondita delle loro attività online[81].

Con lo scopo di promuovere un piano di crescita basato sull'utilizzo di questi dati, l'*IT Strategic Headquarters* (*IT Sōgō Senryaku Honbu* IT 総合戦略本部) istituì un gruppo di studio per esaminare la revisione della legge[82]. In un contesto globale che sollecitava un

---

[78] Organo consultivo istituito dal governo giapponese dedicato alla formulazione di politiche atte a migliorare il benessere e la qualità della vita dei cittadini.
[79] G. GREENLEAF (2010), *op., cit.*, p. 29.
[80] H. MIYASHITA (2011), *op., cit.*, p. 233.
[81] La profilazione è una tecnica che prevede la raccolta di dati su uno o più individui per analizzarne le caratteristiche e i modelli comportamentali, spesso con finalità commerciali. Si veda A. ALONGI, F. POMPEI (2021), *op., cit.*, p. 160.
[82] R. MORI (2014), *Nihon no kojin jōhō hogo-hō kaisei no jōkyō* (Stato delle revisioni della legge giapponese sulla protezione dei dati personali), in *Pāsonaru dēta no rikatsuyō ni okeru gijutsu oyobi kakkokuhō seido no dōkō*, Eichi hōritsu jimusho, Vol. 55, No. 12, p. 1353.

coordinamento delle normative per garantire l'uso sicuro dei dati a livello internazionale, la proposta fissò come obiettivo l'abbattimento della "*barrier to the utilization of personal data*", che rischiava di compromettere la gestione responsabile dei dati da parte delle aziende e l'adeguata tutela della *privacy* degli individui[83].

A tal proposito, uno degli episodi più controversi fu senza dubbio lo scandalo che coinvolse la più grande compagnia ferroviaria del Paese. Nel giugno 2013, la *East Japan Railway Company* (JR) annunciò una collaborazione con la società Hitachi Ltd.[84], con la quale condivise informazioni sui percorsi di viaggio senza il consenso dei clienti. L'azienda si giustificò spiegando che la vendita era avvenuta in forma del tutto anonima, ma questo non bastò a placare il crescente senso di turbamento tra la popolazione in merito alla sicurezza e all'affidabilità dei trasferimenti di dati[85].

Alla luce di questi fatti, nel settembre 2015 il governo approvò la riforma dell'*Act on the Protection of Personal Information*, che entrò in vigore il 30 maggio 2017[86]. Il nuovo ordinamento aveva l'obiettivo di risolvere tre criticità principali, ovvero: le "zone grigie" relative all'uso dei dati, per le quali era complesso determinare la categoria a cui certi dati appartenevano; l'insufficiente sicurezza nella gestione dei *big data* contenenti informazioni personali; e l'inadeguatezza normativa riguardo al flusso transfrontaliero di dati[87].

Per attuare il piano, l'intervento legislativo si concentrò su una serie di azioni mirate a[88]:

- Chiarire la definizione di dato personale e dato sensibile
- Regolare l'utilizzo dei dati anonimizzati
- Garantire la correttezza della circolazione dei dati attraverso norme e registri per le forniture a terzi

---

[83] STRATEGIC HEADQUARTERS (2014), *Policy Outline of the Institutional Revision for Utilization of Personal Data*, Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, pp. 6-7.

[84] Multinazionale giapponese fondata nel 1910, con interessi che spaziano dalla tecnologia dell'informazione all'energia, dai trasporti all'industria manifatturiera.

[85] Per approfondimenti si veda il link: https://www.jreast.co.jp/information/aas/20151126_torimatome.pdf

[86] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2016), *Amended Act on the Protection of Personal Information (Tentative Translation)*.

[87] T. ASAI (2018), *Japan Data Protection Law. A Practical Guide in Comparison With GDPR*, CreateSpace Independent Publishing Platform, p. 16.

[88] Si veda il seguente link: https://www.soumu.go.jp/main_content/000441469.pdf

- Istituire un'autorità indipendente per la protezione dei dati personali e definire le sue competenze
- Rispondere alla globalizzazione attraverso disposizioni per l'applicazione extraterritoriale e sui terzi stranieri
- Promuovere il sistema *Cross Border Privacy Rules* (CBPR)

2.3.1. *Le nuove definizioni*

Attraverso l'analisi dei *big data* era diventato possibile identificare un soggetto specifico combinando i suoi dati con quelle di altri individui, anche se al momento dell'acquisizione non era stato identificato[89]. Tenendo conto di questo fattore, la nuova legge modificò alcune definizioni ormai obsolete e ne introdusse di nuove.

Il termine "informazione personale" è stato esteso a tutte le informazioni relative a un individuo che rientrano in una delle seguenti voci: nome, data di nascita e altre descrizioni; informazioni espresse tramite voce, movimenti e altri metodi; registrazioni in formato elettronico o altro tipo; e, per l'appunto, informazioni che, se combinate con altre, permettono di identificare una persona specifica. In questa categoria, rientrano anche quelle informazioni che contengono un "codice identificativo personale" (*Kojin shikibetsu fugō* 個人識別符号) specificato da un'ordinanza governativa, vale a dire ogni carattere, lettera, simbolo o altro codice che può identificare un individuo specifico (art. 2.2). Inoltre, per la prima volta è stato incluso il "dato sensibile" (*Yōhairyo kojin jōhō* 要配慮個人情報)[90], di cui fanno parte le informazioni sulla razza, la religione, lo stato sociale, l'anamnesi, gli eventuali precedenti penali o le altre descrizioni che possono generare pregiudizi e discriminazioni ingiuste (art. 2.4). In linea di principio, è permesso ottenere questo genere di dato solo con il consenso dell'individuo (art. 17.2)[91].

---

[89] F. SHINPO (2016), *Kaisei kojin jōhō hogohō no ronten* (Punti di discussione riguardo la revisione della legge giapponese sulla protezione delle informazioni personali del 2015), Kenpō Gakkai, Kenpō Kenkyū, No. 48, p. 30.

[90] Letteralmente "informazione che richiede speciale attenzione".

[91] Tranne nei casi in cui: (i) sia previsto dalla legge; (ii) sia necessario per proteggere la vita, l'integrità fisica o la proprietà di un individuo; (iii) sia una necessità speciale per migliorare la salute pubblica o promuovere la crescita sana dei bambini; (iv) sia indispensabile per collaborare con un organo del governo nazionale o locale; (v) siano state rese pubbliche dalla persona stessa, da un organo governativo nazionale o locale, o da un operatore economico definito ai sensi dell'art. 76.1 o specificato del PPC; (vi) vi siano altri casi previsti da un'ordinanza governativa. Art. 17.2, APPI.

L'ultimo significativo contributo in questa sezione ha riguardato il "dato anonimizzato" (*Tokumei kakō jōhō* 匿名加工情報)[92]. Esso si riferisce ai dati relativi a un individuo che, attraverso specifici trattamenti, vengono modificati per prevenire l'identificazione diretta del soggetto. Il sistema di anonimizzazione dei dati è stato ideato, innanzitutto, per promuovere le transazioni tra gli operatori economici, consentendo, sotto determinate condizioni, l'utilizzo di tali dati per scopi diversi da quelli originariamente previsti, e in secondo luogo, grazie alla loro natura anonima, per permettere la fornitura dei dati a terzi senza l'obbligo di ottenere il consenso dell'interessato[93]. Nel paragrafo 9 dell'art. 2 sono illustrate le azioni necessarie per impedire la ricostruzione o il recupero di tali dati:

- cancellare una parte delle descrizioni contenute nelle informazioni personali che rientrano nell'art. 2.1 (comma 1) (compresa la sostituzione di dette descrizioni con altre, mediante tecniche che ne impediscono il recupero);
- cancellare tutti i codici identificativi personali contenuti nelle informazioni personali che rientrano nell'art. 2.1 (comma 2) (inclusa la sostituzione dei detti codici con altre descrizioni, mediante tecniche che ne impediscono il recupero)[94].

In riferimento agli obblighi del titolare del trattamento dei dati anonimizzati (*Tokumei kakō jōhō toriatsukai jigyōsha* 匿名加工情報取扱事業者), egli ha il dovere di seguire delle regole specifiche durante la procedura di creazione, fornitura, gestione e sicurezza[95].

---

[92] Lett. "informazioni trattate in forma anonima".
[93] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2017), *op., cit.*, p. 19.
[94] Per ulteriori approfondimenti si veda COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2017), *Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information*, Towards Balanced Promotion of Personal Data Utilization and Consumer Trust.
[95] L'art. 36 disciplina le regole di creazione per il titolare: i) deve trattare il dato creato secondo gli standard stabiliti dal PPC, garantendo l'impossibilità di identificare una persona specifica o ripristinare i dati originali; ii) deve adottare tutte le misure per prevenire la divulgazione di descrizioni eliminate, codici identificativi personali o dettagli sui metodi di anonimizzazione; iii) deve divulgare al pubblico gli elementi riguardanti l'individuo inclusi nei dati anonimizzati; iv) prima di fornire i dati anonimizzati a terze parti, deve dichiarare quali dati sono stati inclusi, in che modo, e specificare che si tratta di dati anonimizzati; v) non deve incrociare i dati anonimizzati con altre informazioni per identificare gli individui; vi) deve impegnarsi a gestire i reclami e assicurare una gestione corretta dei dati, rendendo pubbliche le misure effettuate. L'art. 37 disciplina le regole di fornitura: quando il titolare condivide il dato anonimizzato a terze parti (esclusi i dati creati dall'operatore stesso) gli elementi relativi agli individui inclusi in quei dati e il metodo con cui tali informazioni sono state rese pubbliche devono essere diffusi in anticipo. Inoltre, deve informare esplicitamente ai terzi che i dati sono anonimi. L'art. 38 disciplina le regole di divieto di

Tuttavia, anche con questi accorgimenti, è un compito estremamente complesso progettare sistemi di anonimizzazione realmente sicuri e non reversibili, poiché l'incrocio dei dati provenienti da diverse fonti incrementa il rischio di re-identificazione[96].

2.3.2. *La Commissione per la Protezione dei Dati Personali*

Quando nel 2013 fu emanato l'*Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure*, denominato "*My Number Act*" (*Gyōsei tetsuzuki ni okeru tokutei no kojin wo shikibetsu suru tame no bangō no riyoutō ni kansuru hōritsu* 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, Legge No. 27/2013)[97], venne anche formato un organo per supervisionarlo. La responsabilità fu affidata alla *Specific Personal Information Protection Commission* (*Tokutei Kojin Jouhou Hogo Iinkai* 特定個人情報保護委員会, SPIPC), che però mancava dei mezzi necessari per garantire il rispetto delle normative, sebbene potesse richiedere rapporti e condurre ispezioni in loco presso le aziende[98].

Dopo la riforma del 2015, quest'organo svolse un ruolo cruciale per la creazione di una nuova autorità regolatoria: la Commissione per la Protezione dei Dati Personali (*Kojin Jōhō Hogo Iinkai* 個人情報保護委員会, PPC)[99]. Un organo indipendente dal governo

---

identificazione: il titolare non deve acquisire descrizioni cancellate dalle informazioni personali, codici di identificazione personale o informazioni relative al metodo di trattamento effettuato ai sensi delle disposizioni dell'art. 36.1, né deve incrociare i dati anonimizzati con altre informazioni per identificare individui specifici. L'art. 39 disciplina le regole di sicurezza: il titolare deve adoperarsi per eseguire le misure necessarie e appropriate per gestire in sicurezza i dati anonimizzati e trattare i reclami, anche rendendo pubbliche le misure effettuate. COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2017), *op., cit.*, pp. 16-17.

[96] F. SHINPO (2016), *op., cit.,* p. 38. In sostanza, nonostante un dato venga trattato in modo tale da impedirne l'identificazione diretta, l'incrocio con altri dati disponibili potrebbe far risalire all'individuo specifico a cui quei dati appartengono.

[97] La legge prevedeva l'assegnazione di un numero identificativo di 12 cifre (*ID number*) per ogni cittadino che stanziava in Giappone per più di tre mesi. Allo scopo di rendere più efficienti le procedure amministrative, era utilizzato nei settori legati alla tassazione, alla sicurezza sociale e alle misure di controllo delle emergenze. L'utilizzo di tali codici da parte di aziende private e banche fu oggetto di forti critiche popolari. GOVERNO DEL GIAPPONE (2013). *Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of May 31, 2013)*, Japanese Law Translation.

[98] A. G. MARCÉN (2021), *The New Personal Data Protection in Japan: Is It Enough?*, in *Media Technologies for Work and Play in East Asia: Critical Perspectives on Japan and the Two Koreas*, a cura di LEE. M., CHUNG P., Bristol University Press, Bristol, p. 109.

[99] La sua giurisdizione copriva solo il settore privato; del settore pubblico si occupava il *Ministry of Internal Affairs and Communications* (*Sōmushō* 総務省, MIC). G. GREENLEAF (2015), *Japan: Toward international standards - except for "big data",* Privacy Laws & Business International Report, p. 2.

composto da un presidente e otto membri di commissione, tra cui esperti nei settori della protezione dei dati, della tutela dei consumatori, delle tecnologie dell'informazione, della gestione dei numeri di identificazione e delle attività commerciali (art. 63). I partecipanti vengono eletti con un mandato quinquennale dal Primo Ministro mediante il consenso delle due Camere ed esercitano un'autorità indipendente (art. 62).

La mansione principale del PPC consiste nell'elaborare delle politiche di base per l'attuazione del corretto trattamento di ogni tipo di dato personale. Infatti, può richiedere rapporti o documentazioni ed effettuare verifiche, così come fornire consulenza e orientamento (artt. 40, 41), senza però interferire con la libertà religiosa, accademica, politica e di parola del titolare (art. 43).

In situazioni di violazioni per cui la Commissione ritenga necessario proteggere i diritti e gli interessi di un individuo, può anche raccomandare al titolare delle misure correttive (art. 42). Un'inosservanza di tali avvertimenti e la falsificazione delle documentazioni sono punite con la reclusione per un periodo non superiore a sei mesi o con una multa non superiore a 300.000 yen (artt. 84, 85)[100].

Affidando gran parte dei poteri di vigilanza al PPC, i ministri ricoprono un ruolo più marginale nella giurisprudenza giapponese. Tuttavia, mantengono ancora diversi compiti, tra cui l'incarico di segnalare eventuali violazioni che avvengono sotto la loro giurisdizione (art. 45). Inoltre, in casi urgenti o in circostanze specificate da un'ordinanza governativa, possono richiedere rapporti ai titolari del trattamento (art. 44). Persino le APIPO devono rispondere direttamente al PPC quando redigono delle linee guida[101]. In tal caso, devono notificare immediatamente la Commissione, che a sua volta si occuperà di pubblicarle (art. 50).

Passando a un contesto internazionale, il PPC svolge un ruolo chiave nella cooperazione con le organizzazioni estere, poiché è in grado di fornire informazioni utili per l'applicazione della presente legge anche alle autorità estere che operano in sistemi

[100] Ove ricorra una fuga di dati o una divulgazione di segreti professionali, il soggetto, anche se fuori dal territorio nazionale, può essere condannato ai lavori forzati per un massimo di due anni o ad una multa non superiore a 1 milione di yen (art. 82). Mentre, se il titolare che gestisce i dati personali, insieme ai suoi dirigenti, dipendenti o ex dipendenti, ruba tali dati per ottenere guadagni illeciti per sé o altri, è punito con una pena detentiva fino a un anno o con una multa fino a ¥500.000 (art. 83).

[101] Esse si riferiscono a come specificare: lo scopo dell'uso delle informazioni personali; le misure per garantire una gestione sicura delle informazioni personali; le procedure per trattare le richieste di divulgazione da parte delle persone interessate e altri aspetti; le modalità per creare e gestire le informazioni anonimizzate e gesti (art. 53.1)

giuridici equivalenti a quello giapponese (art. 78.1). In generale però ciò non può avvenire per richieste riguardanti indagini penali, salvo ottenimento di un consenso specifico della Commissione. Tale consenso viene emesso tranne per i crimini politici, per i reati avvenuti in Giappone ma non punibili dalla legge, e qualora il paese estero non garantisse un trattamento analogo (artt. 78.2, 78.3).

Da quanto traspare, l'efficacia complessiva della normativa dipende dalla capacità della Commissione di esercitare la propria indipendenza, applicare regole mai pienamente attuate in precedenza e ottenere le risorse necessarie per un'applicazione uniforme ed efficace. Questo aspetto è determinante, non solo per avvicinare il Giappone agli standard internazionali, ma anche per consolidare il ruolo del PPC come modello di riferimento nella protezione dei dati personali.

2.3.3. *Le conseguenze del "caso Benesse"*

Benesse Corporation è uno dei principali operatori di istruzione a distanza del Giappone, in quanto fornisce programmi di educazione per bambini. Nel luglio 2014 fu protagonista di una violazione a opera di un dipendente di un subappaltatore esterno, che rubò i dati di oltre 30 milioni di clienti, costituendo il più grande caso di fuga di dati personali verificatosi nel Paese (*Benesse jiken* ベネッセ事件). Le informazioni trapelate riguardavano le generalità di genitori e figli, indirizzi e numeri di contatto, poi ceduti a operatori di marketing diretto[102].

I primi sospetti sorsero a seguito delle insistenti lamentele dai clienti, che segnalavano la ricezione di comunicazioni pubblicitarie da altre aziende del settore dell'istruzione, nonostante si fossero registrati solo a Benesse. L'azienda formò un'unità interna d'indagine per comprendere le cause e scoprì che l'elenco di informazioni ottenuto dalle comunicazioni conteneva dati di cui solo Benesse era in possesso, accertando così l'avvenuto furto.

Dopo giorni di ricerca, la polizia arrestò Matsuzaki Masaomi, un ingegnere di sistema di una compagnia di sviluppo software incaricata da Symphon (una sussidiaria di Benesse), non con l'accusa di violazione dell'APPI, bensì per violazione dell'*Unfair Competition*

[102] A. PARDIEK (2023), *Privacy Matters: Data Breach Litigation in Japan*, Washington International Law Journal, p. 26.

Prevention Act (*Fusei kyōsō bōshihō* 不正競争防止法, Legge No. 47/1993, UCPA), che prevede responsabilità civile e penale per il furto di segreti commerciali[103]. Infatti, l'APPI del 2003 non contemplava sanzioni di grande entità, ma solo delle pene lievi in caso di inosservanza delle raccomandazioni emesse dal ministro competente (art. 56). Matsuzaki fu quindi condannato a 2 anni e 6 mesi di reclusione e a una multa di 3 milioni di yen[104].
Dal canto suo, Benesse cercò di risarcire tutte le vittime con un voucher di 500 yen, ma tale somma non fu ritenuta appropriata. Al contrario, le persone offese intentarono un'azione legale collettiva con l'accusa di negligenza e danno morale. Il numero di cause raggiunse circa le 12.000 e, sebbene fossero collegate allo stesso incidente, ci furono sanzioni diverse tra i vari tribunali[105].
In una di queste, il Tribunale distrettuale di Kobe confermò che vi era stata una fuga di dati, ma stabilì che la responsabilità non ricadeva su Benesse perché non vi erano prove sufficienti a sostenere la loro negligenza[106]. Anche la Corte d'Appello di Osaka espresse lo stesso concetto, affermando che il disagio e l'ansia provati dalla vittima non giustificavano una richiesta di risarcimento danni[107]. Tuttavia, la Corte Suprema annullò la sentenza originale perché l'entità del danno psicologico del ricorrente era stata valutata unicamente sulla mancanza di prove relative alla comparsa di danni peggiori, falsando l'intera decisione[108]. Il caso fu dunque rinviato all'Alta Corte di Osaka per un ulteriore esame, nel quale fu accertata la responsabilità dell'azienda in violazione dell'art. 22, che richiede l'attenta supervisione sul fiduciario per garantire la sicurezza dei dati. Inoltre, l'impossibilità dell'appellante di controllare chi utilizzasse i suoi dati, insieme alla condivisione senza consenso preventivo, furono ritenuti un danno tale da legittimare un

---

[103] I. IZUMI (2021), *Benesse kojin jōhō rōei mondai: An analysis of the Benesse Corporation Customer Data Leak* (Problema di fuga di informazioni personali di Benesse: Un'analisi della fuga di dati dei clienti della società Benesse), p. 101. I segreti commerciali sono i dati tecnici o aziendali utili per le attività commerciali, che non sono di dominio pubblico. Il furto di tali dati consiste in una pena detentiva di massimo 10 anni o una multa fino a 3 milioni di yen per le persone fisiche e una multa che può arrivare a 300 milioni di yen per le persone giuridiche. GOVERNO DEL GIAPPONE (1993), *Unfair Competition Prevention Act (Act No. 47 of May 19, 1993)*, Japanese Law Translation, pp. 26, 28.
[104] ALTA CORTE DI TOKYO, *Heisei nijūkyūnen sangatsu nijūichinichi hanketsu* (Sentenza del 21 marzo 2017), Hanreijiho, No. 974, p. 1.
[105] A. PARDIEK (2023), *op., cit.*, p. 27.
[106] M. SHIZAWA (2020), *Puraibashī to jiko jōhō ni kansuru kōsatsu: `Benesse kojin jōhō rōei jiken' (sai han hira 29-10-23 banji 2351-7) wo chūshin ni* (Riflessioni sulla privacy e sulle informazioni personali: studio dettagliato sul "caso Benesse" (Corte Suprema, 23 ottobre 2016, 2351-7), Tōyō Daigaku Gendai Shakai Sōgō Kenkyūsho, Vol. 17, p. 125.
[107] *Ibidem*.
[108] CORTE SUPREMA DEL GIAPPONE, *Heisei nijūkyūnen jūgatsu nijūsannichi hanketsu* (Decisione del 23 ottobre 2017), Hanreijiho, No. 1892, p. 2.

risarcimento[109]. Il risultato fu che Benesse venne condannata a risarcire la parte lesa con un importo di 1.000 yen[110].

Il caso Benesse ha contribuito in maniera determinante alla riforma del 2015, in particolare alla formulazione delle norme di sicurezza e delle sanzioni. Le indagini avevano evidenziato l'assenza di registri utili al tracciamento dei dati nelle operazioni di trasferimento a terzi. A tale scopo fu aggiunto l'art. 25 che obbligava il titolare del trattamento a conservare tali registri. All'articolo seguente invece si stabiliva che i destinatari dovevano verificare l'identità dell'operatore che aveva effettuato la comunicazione e le modalità con cui avevano acquisito i dati (art. 26)[111].
Sul fronte delle sanzioni penali, vennero aumentate le pene. Fu previsto che, qualora un dipendente o un ex dipendente del titolare del trattamento, renda noti o rubi indebitamente dati personali contenuti in un database per ottenere un guadagno illecito per sé o per terzi, debba essere soggetto a una pena detentiva con lavori socialmente utili fino a un anno oppure a una multa fino a 500.000 yen (art. 83)[112].

2.3.4. *Trasmissione dei dati personali a Paesi esteri*

Nella previgente APPI, l'ambito di applicazione della legge era confinato al territorio nazionale, generando diverse incertezze per i soggetti coinvolti nelle operazioni internazionali. Tuttavia, con l'implementazione del nuovo art. 24 (*Gaikoku ni aru daisansha he no teikyō no seigen* 外国にある第三者への提供の制限)[113], la normativa ha esteso la sua giurisdizione, coinvolgendo anche i trasferimenti transnazionali.
In particolare, il disposto stabilisce che il trasferimento di dati a una "terza parte situata all'estero" è permesso previo consenso esplicito dell'interessato, eccetto per tre categorie specifiche[114]:

---

[109] A. PARDIEK (2023), *op., cit.*, p. 33.
[110] I. IZUMI (2021), *op., cit.*, p. 109.
[111] K. ISHII, T. KOMUKAI (2016), *A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K.*, 12th IFIP International Conference on Human Choice and Computers, United Kingdom, p. 189.
[112] *Ibidem*.
[113] Lett. "Restrizioni sulla fornitura a terze parti situate all'estero".
[114] G. GREENLEAF (2018), *Questioning 'Adequacy' (Pt I) – Japan*, Privacy Laws & Business International Report, p. 6.

- nazioni estere che il PPC reputa equivalenti al Giappone, in termini di tutela dei diritti e degli interessi individuali;
- eccezioni previste dall'art. 23.1 sul trasferimento a terze parti[115];
- nazioni estere che si impegnano a garantire una protezione equivalente a quella giapponese, adottando un sistema conforme alle regole del PPC.

Riguardo a quest'ultimo aspetto, il PPC ha deciso, ai sensi dell'art. 24, che le imprese certificate non devono essere vincolate alle restrizioni sull'esportazione di dati personali dal Giappone (artt. 24-26), a condizione che rispettino gli altri obblighi imposti dalla normativa giapponese. Tale meccanismo è volto a ottimizzare il processo di trasferimento di dati tra le imprese giapponesi e le aziende estere certificate al CBPR[116].

L'applicazione extraterritoriale della legge è prevista nell'art. 75, il quale stabilisce che, quando un titolare del trattamento ha ottenuto informazioni personali nel corso della fornitura di beni o servizi a individui all'interno del paese, e gestisce tali informazioni e i risultanti dati anonimizzati all'estero, allora devono essere applicate le disposizioni della legge[117]. Al contrario, se una filiale in Giappone condivide informazioni con la sede centrale situata all'estero, le disposizioni precedenti non si applicano, poiché il passaggio avviene all'interno dello stesso gruppo societario.
Nel caso in cui il titolare del trattamento riceva dati personali da un ente esterno, ha l'obbligo di verificarne la completezza. Allo stesso modo, la terza parte ha la responsabilità di garantire che tali informazioni siano accurate, complete e formattate correttamente, evitando qualsiasi rischio di errore a danno del titolare del trattamento[118].
Inoltre, si sottolinea che la versione emendata dell'APPI ha introdotto nuovi obblighi di conservazione dei registri per le aziende, con lo scopo di documentare tutti i trasferimenti, compresi quelli transfrontalieri. Mentre, i trasferimenti che rientrano nelle eccezioni o

---

[115] L'articolo disciplina che il titolare del trattamento non può fornire dati personali a terze parti senza il consenso preventivo del soggetto interessato, salvo nei casi già indicati alla nota 70. COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2016), *Amended Act on the Protection of Personal Information (Tentative Translation)*, p. 12.
[116] G. GREENLEAF (2016), *op., cit.,* p. 19.
[117] Si riferisce ai seguenti articoli: art. 15 (*Specifying a Utilization Purpose*); art. 16 (*Restriction due to a Utilization Purpose*); art. 18, escluso il secondo paragrafo (*Notification etc. of a Utilization Purpose when Acquiring*); dagli artt. 19 a 25; dagli artt. 27 a 36; art. 41 (*Guidance and Advice*); art. 42.1 (*Recommendation and Order*); l'art. 43 (*Restriction on the Personal Information Protection Commission's Exercising the Authority*); e art. 76 (*Exclusion from Application*).
[118] R. WALTERS, L. TRAKMAN, B. ZELLER (2019), *op., cit.,* p. 251.

esenzioni sopra menzionate sono generalmente dispensati dall'obbligo di conservazione[119].

2.3.5. *Promozione del sistema CBPR*

Il CBPR, introdotto nel 2011 come sistema a partecipazione volontaria, ha l'obiettivo di disciplinare il flusso elettronico di dati privati tra le economie APEC. Esso è amministrato dallo ECSG, per mano del *Joint Oversight Panel* (JOP), un gruppo di supervisione composto da rappresentanti dei paesi membri dell'APEC. Il suo obiettivo è innalzare il livello di protezione nella regione, creando un ambiente di fiducia per la crescita economica e l'integrazione regionale[120]. Per questo fine, si basa su un "*approccio responsabile*", in cui le organizzazioni sono chiamate a seguire i principi del programma, piuttosto che adeguarsi a normative che potrebbero non essere adatte alle specifiche esigenze di ciascuna organizzazione[121].

Gli *Accountability Agents* (AA) sono gli enti pubblici o privati, approvati dall'ECSG tramite un processo specifico, che si occupano di certificare la conformità delle aziende agli standard del sistema CBPR. Una volta convalidato il processo di approvazione, l'AA può considerarsi "riconosciuto" e può iniziare a svolgere il suo ruolo. Oltre a certificare le aziende, deve anche monitorarle continuamente. Pertanto, alle imprese è richiesto di presentare attestati annuali di conformità. In caso di violazione di qualsiasi impegno, gli AA sono tenuti a informare gli organi preposti e a comunicare prontamente eventuali sospensioni alle autorità di controllo della *privacy* e al CBPR *Secretariat*[122].

Le organizzazioni e le imprese che desiderano aderire al CBPR devono seguire delle specifiche direttive[123]:

---

[119] Y. SAKO, N. KAWANAKA (2017), *Data Security in Japan: New Cross-Border Data Transfer Rule*, K&L Gates, p. 8.
[120] APEC (2019), Benefits of the APEC Cross-Border Privacy Rules – Protecting Information, Driving Growth, Enabling Innovation, p. 3.
[121] A. C. RAUL (2022), *The Privacy, Data Protection and Cybersecurity Law Review*, Law Business Research Ltd, Sidley, p. 55.
[122] APEC (2010), *Accountability Agent Apec Recognition Application*.
[123] APEC (2019), *op., cit.,* p. 11-12.

a. avere almeno un'autorità garante della *privacy* all'interno del *Cross-Border Privacy Enforcement Arrangement* (CPEA)[124];
b. presentare una lettera di intenti al JOP che assicuri, tra le altre cose, l'intenzione di nominare almeno un *Accountability Agent*;
c. le economie, che hanno inviato tutta la documentazione necessaria, possono partecipare a una consultazione con il Presidente del JOP, durante la quale vengono esaminati i materiali o richieste informazioni aggiuntive;
d. alla conclusione della consultazione, il JOP emette un rapporto finale, che determina se l'economia ha soddisfatto o meno i requisiti. ln caso di esito positivo, viene rilasciata una attestazione, che consente l'ingresso nel sistema CBPR.

Dopo un lungo processo iniziato nel 2013, il Giappone ha formalizzato la sua partecipazione al sistema APEC-CBPR nel febbraio 2016, designando come AA il *Japan Institute for Promotion of Digital Economy and Community* (JIPDEC) [125].
Lo Stato giapponese ha scelto di aderire per due ragioni: in primo luogo, per agevolare il trasferimento dei dati tra il Giappone e i paesi della regione APEC, favorendo così una maggiore cooperazione regionale ed economica; in secondo luogo, per rendere il marchio delle imprese giapponesi più attraente ai consumatori, aumentando il potere di vendita e la competitività come partner commerciali all'interno del sistema[126].
Nonostante questo nuovo provvedimento sembri vantaggioso, Greenleaf, in un suo articolo, esprime dubbi sull'effettiva utilità per le imprese giapponesi. Egli evidenzia il fatto che il JIPDEC accredita solo imprese secondo gli standard del sistema APEC, senza prendere in considerazione la normativa nazionale, che offre dei requisiti più rigorosi e dei meccanismi di applicazione più solidi. Di conseguenza, un consumatore che affida le proprie informazioni a un'impresa preferirebbe sapere che essa è conforme alla legge giapponese (specialmente ora che il Giappone ha l'Autorità Garante), piuttosto che al CBPR,

[124] Accordo di cooperazione multilaterale che facilita l'interazione tra le varie autorità garanti dell'APEC *Privacy Framework*.
[125] Il JIPDEC è una fondazione senza scopo di lucro nota per svolgere, oltre al ruolo di AA nel CBPR, anche la funzione di controllo del *PrivacyMark*, il sistema giapponese di accreditamento che valuta la conformità delle imprese alle normative e il loro livello di sicurezza nella gestione dei dati personali. Si veda G. GREENLEAF (2010), *op., cit.*, p. 29.
[126] https://www.ppc.go.jp/files/pdf/CBPR_lets_think_about_it.pdf consultato il 22/12/2024

dato che non ha una comprovata esperienza di applicazione. L'accreditamento potrebbe risultare utile solo se il paese estero non riconoscesse l'APPI e aderisse al sistema CBPR. Tuttavia, solo otto delle ventuno economie APEC partecipano al sistema (Giappone, Stati Uniti, Canada, Messico, Singapore, Taiwan, Corea del Sud e Australia), rendendo la sua efficacia molto limitata[127].

2.4. Il diritto all'oblio

L' origine del diritto all'oblio risale alla legislazione francese e svizzera e si riferisce a un concetto giuridico secondo cui le informazioni personali, in particolare quelle legate a reati passati, non devono rimanere accessibili indefinitamente, poiché non sono più di interesse pubblico. In sostanza, questo diritto consente agli individui, dopo un certo periodo, di richiedere la cancellazione delle proprie informazioni dai motori di ricerca e da altre piattaforme online, per evitare che continuino a essere visibili e accessibili a chiunque in modo permanente.

Sebbene questo diritto sia stato formalmente riconosciuto dalla Corte di Giustizia dell'Unione Europea nel 2014, in Giappone non è ancora pienamente accettato né implementato[128]. Ciononostante, ci furono dei processi dove il diritto all'oblio è stato riconosciuto. Un esempio significativo fu quello trattato dal Tribunale distrettuale di Saitama nel 2015, in cui l'attore chiese la cancellazione delle informazioni relative alla sua condanna per prostituzione minorile risalente a tre anni prima, lamentando che i dettagli della sua storia di arresto erano ancora disponibili nel motore di ricerca di Google. Avendo già scontato la pena e completato il percorso di riabilitazione, ritenne che la presenza di quelle informazioni ostacolasse la sua possibilità di ricostruirsi una vita.

Durante il processo, gli avvocati di Google difesero la piattaforma, spiegando che i risultati delle ricerche erano prodotti automaticamente da algoritmi, senza intervento umano diretto[129]. Nonostante ciò, il giudice Kobayashi Hisaki concluse che, anche per i criminali, esisteva il diritto di essere "dimenticati" dalla società, poiché sarebbe stato estremamente difficile vivere una vita tranquilla una volta che certe informazioni restavano online e si

[127] G. GREENLEAF (2016), *Japan joins APEC-CBPRs: Does it matter?*, Privacy Laws & Business International Report, p. 18.
[128] R. WALTERS, L. TRAKMAN, B. ZELLER (2019), *op., cit.,* p. 253.
[129] F. SERINI (2022), *op. cit.*, p. 173.

diffondevano senza controllo[130]. In base a queste considerazioni, il Tribunale di primo grado ordinò la rimozione dei *link* dai risultati di ricerca, giudicando che la tutela dei diritti personali dell'individuo superasse l'interesse pubblico[131]. Tuttavia, l'anno successivo l'Alta Corte di Tokyo riformò la sentenza, sulla base del fatto che il diritto all'oblio non era legittimato dalla legislazione giapponese e che i suoi requisiti e gli effetti non erano chiari[132].

Nel caso in esame, la Corte respinse la richiesta di cancellazione in quanto, i titoli e gli "*snippet*"[133] utilizzati, erano elementi indipendenti e che Google, in qualità di motore di ricerca, non poteva essere ritenuto responsabile di una violazione dei diritti alla reputazione. La Corte, inoltre, osservò che il crimine, essendo ancora di interesse pubblico, non aveva perso la sua rilevanza. Rimuovere quei risultati, secondo i giudici, avrebbe potuto compromettere in modo significativo sia la libertà di espressione che il diritto all'informazione di molti utenti[134].

Tale verdetto fu confermato anche dalla Corte Suprema quando furono delineati i criteri generali da seguire per valutare se la diffusione di articoli online, che violano la *privacy*, potesse configurare un illecito[135]. In particolare, vennero considerati: la natura e i fatti resi pubblici; l'entità del danno alla *privacy* causato dalla loro diffusione; la posizione sociale e l'influenza della persona coinvolta; lo scopo e il significato delle informazioni pubblicate; il contesto sociale al momento della pubblicazione e i risvolti successivi; infine, la necessità di includere tali informazioni nell'articolo[136]. Se il diritto alla *privacy* si fosse dimostrato chiaramente superiore rispetto alle ragioni per fornire quei risultati di ricerca, l'operatore avrebbe potuto essere chiamato a eliminare gli URL. Tuttavia, tenendo conto della rilevanza pubblica, dell'entità del reato commesso e del ristretto ambito di diffusione,

---

[130] H. MIYASHITA (2016), *The "right to be forgotten" and search engine liability*, Brussels Privacy Hub Working Paper, Vol. 2, No. 8, p. 8.

[131] TRIBUNALE DISTRETTUALE DI SAITAMA, *Heisei nijūnananen jūnigatsu nijūnichi hanketsu* (Sentenza del 22 dicembre 2015), Hanreijiho, Vol. 2282, p. 82.

[132] ALTA CORTE DI TOKYO, *Heisei nijūhachinen shichigatsu jūninichi kettei* (Decisione del 12 luglio 2016), Hanreijiho, No. 2318, p. 24.

[133] Gli "*snippet*" sono brevi estratti di contenuto generati automaticamente dai motori di ricerca, che offrono un'anteprima delle informazioni contenute in una pagina web. Vengono personalizzati in base alla query dell'utente.

[134] G. SHISHIDO (2017), *Kensaku kekka no sakujo o meguru saibanrei to kongo no kadai* (Giurisprudenza sulla rimozione dei risultati di ricerca e le sfide future), Jōhō Hōsei Kenkyū, Vol. 1, 49.

[135] R. WALTERS, L. TRAKMAN, B. ZELLER (2019), *op., cit.,* p. 253.

[136] CORTE SUPREMA DEL GIAPPONE, *Heisei nijūkyūnen ichigatsu sanjūichinichi kettei* (Decisione del 31 gennaio 2017), Hanreijiho, No. 45, p. 3.

la Corte ribadì che la violazione in questione non fosse sufficiente a giustificare la rimozione dei risultati da Google[137].

Considerato quanto sopra, il diritto all'oblio non risulta applicato all'interno della legge giapponese, eppure anche il Giappone sembra avvicinarsi alla sua accettazione, anche se rimane una notevole apprensione nell'applicare tale diritto nello stesso modo dell'UE, perché pone tali decisioni nelle mani di intermediari di Internet anziché di giudici, creando conflitti con il diritto alla libertà di espressione e il diritto all'informazione[138]. L'approccio giapponese appare quindi più cauto e meno formalizzato rispetto a quello europeo, lasciando ancora spazio a un'evoluzione giuridica futura.

[137] *Ibidem*.
[138] A. G. MARCÉN (2021), *op., cit.,* p. 118.

Capitolo 3

Giappone ed Europa sul trasferimento di dati: accordi e divergenze

3.1. Il Regolamento europeo (GDPR): tra passato e presente

Il trasferimento internazionale di dati è una questione complessa, specialmente tra paesi con tradizioni normative e culturali distanti, come il Giappone e l'Europa. Perciò, per comprendere al meglio i punti in comune e le differenze che hanno influenzato il dialogo nel processo di armonizzazione delle due giurisdizioni, si ritiene essenziale approfondire l'evoluzione normativa europea sui trasferimenti transfrontalieri.

Oltre alle già citate Linee guida OCSE e Convenzione 108, la prima vera direttiva europea che inquadrava l'ambito della circolazione transfrontaliera era la Direttiva 95/46 (c.d. "Direttiva madre"). Essa stabiliva che gli Stati membri potevano trasferire dati verso un paese terzo solo se quest'ultimo garantiva "*un livello di protezione adeguato*" (art. 25) e onorava tutte le condizioni sottintese dal trasferimento, vale a dire "*la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate*" (art. 25. 2). Qualora tali condizioni non fossero state rispettate, gli Stati membri avrebbero dovuto impedire ogni forma di trasferimento verso il paese inosservante (art. 25. 4), eccetto per i casi contemplati nell'art. 26[139].

[139] PARLAMENTO EUROPEO (1995), *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, European Union Law, Bruxelles, pp. 145-146. In deroga all'art. 25, il trasferimento può avvenire se: a) la persona interessata ha dato inequivocabilmente il proprio consenso; b) è essenziale per eseguire un contratto tra la persona interessata e il responsabile del trattamento, o per attuare misure precontrattuali; c) serve per stipulare o concludere un contratto, nell'interesse della persona interessata, tra il responsabile del trattamento e un soggetto terzo; d) è richiesto dalla legge per tutelare un interesse pubblico rilevante, o per verificare, esercitare o difendere un diritto in sede legale; e) è indispensabile per proteggere l'interesse vitale della persona interessata; f) riguarda dati presenti in un registro pubblico accessibile per legge, a condizione che la consultazione rispetti le regole previste per quel registro.

Nonostante gli articoli non prevedessero una chiara definizione, si può dedurre che il trasferimento di dati verso un paese terzo era considerato tale quando avveniva come parte di un processo di trattamento che richiedeva un'azione attiva del titolare[140]. Ciò includeva il caricamento di dati nelle piattaforme online, che da quel periodo in avanti, sarebbero diventate cruciali per il consolidamento delle attività economiche digitali. Per questo motivo, all'alba del nuovo millennio, per l'Europa era indispensabile raggiungere un accordo di adeguatezza con il paese con cui intratteneva i maggiori rapporti commerciali, ovvero gli Stati Uniti. Così, la Commissione Europea e il Dipartimento del Commercio degli Stati Uniti d'America si accordarono sui principi del Safe Harbor tramite la Decisione 2000/520, per cui le organizzazioni private statunitensi, che volevano trattare i dati provenienti dall'Europa, dovevano dare il loro impegno a rispettare i cosiddetti "principi dell'approdo sicuro"[141].

Nei primi 15 anni di validità, le oltre quattromila aziende, che avevano aderito al Safe Harbor, sembravano trarre ampio vantaggio dalla collaborazione transatlantica nei settori digitali, anche grazie alla rapida espansione commerciale dell'epoca[142]. Tuttavia, dopo un'attenta revisione da parte della Commissione europea, emersero molte irregolarità nel trattamento dei dati personali tra i due continenti[143]. In particolare, la confessione dell'ex dipendente della CIA Edward Snowden nello scandalo *Datagate* rivelò l'esistenza di un sistema di sorveglianza di massa implementato dal governo statunitense, denominato PRISM, che "spiava" i dati trasferiti con il Safe Harbor[144]. Queste dichiarazioni spinsero l'avvocato austriaco Maximilian Schrems a denunciare Facebook al Garante per la *privacy*

---

[140] P. GUARDA, G. BINCOLETTO (2023), *op., cit.,* p. 133.

[141] A. ALONGI, F. POMPEI (2021), *op., cit.*, p. 241. Tali principi erano: 1) Notifica: comunicare chiaramente all'interessato le finalità del trattamento dei dati, i contatti per quesiti o reclami, i terzi destinatari dei dati e i mezzi per limitarne l'uso o la divulgazione; 2) Scelta: concedere agli individui la facoltà di rifiutare che le loro informazioni siano condivise a terzi o usate per scopi diversi da quelli inizialmente previsti (per i dati sensibili è necessario un consenso esplicito); 3) Trasferimento successivo: trasferire dati a terzi solo se il destinatario rispetta i principi di notifica e scelta, e assicura un livello di protezione equivalente; 4) Sicurezza: i dati devono essere protetti da accessi non autorizzati, perdite o abusi; 5) Integrità dei dati: i dati devono essere pertinenti, accurati e aggiornati rispetto ai fini dichiarati; 6) Accesso: possibilità agli individui di accedere, correggere o cancellare i propri dati, salvo costi sproporzionati o rischi per altri; 7) Garanzie d'applicazione: implementare meccanismi che garantiscano il rispetto dei principi, offrano agli individui ricorsi in caso di violazioni e assicurino sanzioni adeguate per le organizzazioni inadempienti. Si veda COMMISSIONE EUROPEA (2000), *Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti*, European Union Law, Bruxelles, pp. 11-12.

[142] P. M. SCHWARTZ (2019), *Global Data Privacy: The EU Way*, New York University Law Review, Vol. 94, p. 799.

[143] A. ALONGI, F. POMPEI (2021), *op., cit.*, p. 242.

[144] *Ivi*, p. 243

irlandese (dove ha sede la filiale europea di Facebook Inc.), per la violazione dei propri dati durante il loro trasferimento verso gli Stati Uniti. Egli sosteneva che la normativa americana non garantiva una protezione adeguata contro le agenzie di sorveglianza governative del paese[145].
Inizialmente, la Commissione irlandese respinse la denuncia, ribadendo che mancavano prove sufficienti e che la Commissione europea aveva già riconosciuto l'adeguatezza del sistema americano con la Decisione 2000/520. Quando però la questione arrivò all'Alta Corte irlandese, fu deciso di rivolgersi in via pregiudiziale alla Corte di Giustizia europea (CGUE) per chiarire se le autorità garanti nazionali potessero invalidare un trasferimento extra-UE, nonostante la decisione di adeguatezza della Direttiva 95/46. La CGUE affermò che le autorità garanti non potevano trasgredire la decisione, ma avevano la facoltà di rivolgersi ai tribunali per sottoporre la questione alla stessa Corte di Giustizia. A conclusione degli accertamenti della Corte, fu pronunciata la storica sentenza Schrems I, la quale stabilì che il Safe Harbor non rispettava gli standard di protezione richiesti dall'Europa[146].

La Commissione europea non rimase impassibile davanti alla sentenza e si mise prontamente a lavoro avviando i negoziati per un nuovo accordo. Nel luglio 2016, venne definita la Decisione 2016/1250, conosciuta come il c.d. UE-USA Privacy Shield.
Dal punto di vista dei principi fondamentali, il nuovo regime non si discostava troppo dal precedente, anche la modalità di certificazione era rimasta pressoché invariata, con le aziende statunitensi che autocertificavano la loro adesione presso il Dipartimento del Commercio, impegnandosi a rispettare i principi dello scudo[147].
Le vere novità invece riguardavano tre misure chiave[148]:

1) l'imposizione di obblighi più stringenti verso le aziende statunitensi che trattavano i dati dei cittadini europei;

[145] R. WALTERS, L. TRAKMAN, B. ZELLER (2019), *op., cit.,* p. 75.
[146] C. SPINIELLO (2018), *(Sche)Dati. Il diritto alla protezione dei dati personali nella legislazione europea*, Democrazia e Sicurezza, pp. 168-169.
[147] COMMISSIONE EUROPEA (2016), *Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la* privacy, European Union Law, Bruxelles, p. 4.
[148] A. ALONGI, F. POMPEI (2021), *op., cit.*, p. 246.

2) l'introduzione di una verifica annuale congiunta per monitorare l'attuazione del regime;
3) la disposizione di meccanismi funzionali al rispetto dei principi e fornire all'interessato, stabilito in UE, tutti i mezzi necessari per attuare ricorsi in maniera efficace.

Su quest'ultimo punto, lo scudo prevedeva una figura specializzata nell'ambito dei ricorsi per la sicurezza nazionale: il "Mediatore dello scudo". Egli era un funzionario indipendente che collaborava con gli organi di controllo e con le agenzie di intelligence americane, affinché i reclami fossero gestiti correttamente[149].
Dati questi presupposti, il Privacy Shield sembrava dunque essere in grado di risolvere le criticità che erano state imputate al Safe Harbor. Tuttavia, le aspettative riposte in questo accordo furono disattese, come emergerà chiaramente nella successiva sentenza Schrems II.

Per comprendere le ragioni del suo fallimento, bisogna prima esaminare le disposizioni del Regolamento generale sulla protezione dei dati 2016/679 (*General Data Protection Regulation*, GDPR), che aveva appena sostituito l'ormai superata "Direttiva madre"[150].
Il nuovo Regolamento era chiamato a uniformare le incongruenze legislative tra i paesi membri e assicurare una disciplina comune, avente diritti equi per tutti i cittadini europei. Al contempo, riconosceva i benefici derivanti dal libero scambio di dati con i paesi terzi per il commercio e la cooperazione internazionale.
Secondo l'attuale GDPR, il trasferimento al di fuori dell'Unione è ammesso esclusivamente nel rispetto delle rigorose condizioni previste dal Regolamento, che impongono al titolare del trattamento il pieno rispetto delle normative, indicate al Capo II sui "diritti dell'interessato"[151]. Esse stabiliscono l'obbligo di informarlo sull'intenzione di destinare i suoi dati a terzi o a organizzazioni internazionali, fornendogli in modo chiaro e trasparente specifici elementi, sia che i dati vengano raccolti direttamente da lui sia che

[149] P. GUARDA, G. BINCOLETTO (2023), *op., cit.,* p. 138.
[150] C. SPINIELLO (2018), *op., cit.,* pp. 163-164.
[151] A. ALONGI, F. POMPEI (2021), *op., cit.*, pp. 235-238.

provengano da altri (artt. 12, 13, 14). L'interessato ha, inoltre, il diritto di conoscere le garanzie adeguate previste dall'art. 46 (art. 15.2)[152].

Il Capo V è invece demandato alle condizioni affinché i trasferimenti verso paesi terzi o organizzazioni internazionali (inclusi i trasferimenti successivi) siano effettuati, in conformità con il GDPR, dal titolare del trattamento e dal responsabile "*al fine di garantire che il livello di protezione delle persone fisiche non sia pregiudicato*"[153]. Il trasferimento si configura su tre condizioni giuridiche: la decisione di adeguatezza (art. 45); le garanzie adeguate (artt. 46-48); e le deroghe in specifiche situazioni (art. 49)[154].

La decisione di adeguatezza della Commissione europea, come abbiamo visto, determina se il paese terzo, situato fuori dall'UE, offre una protezione adeguata al libero scambio di dati, ovvero senza necessità di particolari autorizzazioni (art. 45.1), proprio come se avvenisse tra due membri dell'Unione[155]. Per valutare l'adeguatezza, il GDPR prende in considerazione svariati elementi come lo stato di diritto, l'esistenza di un'autorità di controllo, gli impegni internazionali assunti e molto altro (art. 45.2). Inoltre, tramite atti di esecuzione, la Commissione può predisporre per i paesi e le organizzazioni internazionali "adeguate" una verifica periodica, con cadenza almeno quadriennale, che prende in considerazione gli sviluppi più recenti (art. 45.3); al termine della quale può essere imposta la modifica, la sospensione o persino la revoca della decisione (art. 45.5).

Quando l'accordo di adeguatezza non è previsto, il titolare del trattamento ha la possibilità di trasferire i dati all'estero a condizione che abbia dato garanzie adeguate e che l'interessato possa avere accesso a meccanismi di ricorso efficienti e diritti azionabili (art. 46.1). Tali garanzie sono diverse a seconda che l'autorità di controllo conceda l'approvazione o meno[156].

Infine, anche in assenza di tali garanzie, esistono una serie di deroghe, attuate in specifiche situazioni, che consentono il trasferimento. Per esempio, qualora l'interessato abbia

---

[152] PARLAMENTO EUROPEO (2016), *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, European Union Law, Bruxelles, pp. 40-43.

[153] *Ivi*, p. 60.

[154] P. GUARDA, G. BINCOLETTO (2023), *op., cit.,* p. 140.

[155] A. ALONGI, F. POMPEI (2021), *op., cit.*, p. 247.

[156] Costituiscono garanzie adeguate senza necessitare di approvazione (art. 46.2): a) gli strumenti giuridicamente vincolanti con efficacia esecutiva; b) le norme vincolanti d'impresa; c) le clausole tipo di protezione dei dati; d) i codici di condotta; e) i meccanismi di certificazione. Costituiscono garanzie adeguate con necessità di approvazione (art. 46.3): a) le clausole contrattuali; b) gli accordi amministrativi tra autorità pubbliche e organismi pubblici. PARLAMENTO EUROPEO (2016), *op., cit.*, p. 62.

approvato il trasferimento in maniera esplicita oppure sussistano motivi di rilevante interesse personale, pubblico o giudiziario; o ancora, risulti indispensabile per l'esecuzione di un contratto tra l'interessato e il titolare (art. 49.1).

Tra le condizioni di trasferimento citate, uno degli aspetti più dibattuti nella sentenza Schrems II riguardava proprio l'applicabilità del GDPR ai trasferimenti basati sui principi delle garanzie adeguate, in particolare l'attenzione era rivolta alla validità e all'interpretazione della decisione 2010/87, relativa alle clausole contrattuali tipo di protezione dei dati che utilizzava Facebook Ireland per il passaggio di dati verso gli Stati Uniti[157].
Il verdetto finale della CGUE stabilì che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso previsti dal GDPR dovevano essere interpretati in modo tale da assicurare che i diritti delle persone, i cui dati erano trasferiti verso un paese terzo sulla base di clausole tipo, fossero tutelati con un livello di protezione sostanzialmente equivalente a quello garantito dall'Unione. Secondo la Corte, la normativa interna degli Stati Uniti non soddisfaceva tali requisiti, poiché i programmi di sorveglianza non offrivano garanzie appropriate per i dati degli stranieri. Al termine della pronuncia pregiudiziale, la Corte dichiarò invalida la decisione 2016/1250, mentre non emersero sufficienti elementi per invalidare le clausole contrattuali tipo contenute nella decisione 2010/87[158].

I casi del Safe Harbor e del Privacy Shield dimostrano la complessità delle relazioni transfrontaliere e l'importanza di adottare misure solide che bilanciano la tutela dei diritti fondamentali degli individui con le esigenze del commercio e della cooperazione internazionale. In questo, il GDPR rappresenta "*un modello di protezione che si sta dimostrando una sorta di benchmark globale, con un 'effetto domino' (effetto Bruxelles) su altri ordinamenti giuridici, anche oltreoceano*"[159], un fenomeno che sarà evidente nel caso giapponese.

[157] C. PERARO (2021), *Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione europea verso Paesi terzi*, Ordine Internazionale e Diritti Umani, p. 677.
[158] A. ALONGI, F. POMPEI (2021), *op., cit.*, pp. 252-253.
[159] P. GUARDA, G. BINCOLETTO (2023), *op., cit.,* p. 60.

3.2. Gli accordi di libero scambio

Le relazioni tra Giappone ed Europa affondano le loro radici nei primi accordi bilaterali stipulati agli inizi degli anni '90. Da allora, vennero fatti diversi tentativi per consolidare il partenariato economico e commerciale, ma non ci furono risultati concreti a livello globale per un lungo periodo[160].

La grande svolta si verificò nel 2013, quando le due parti avviarono formalmente i negoziati per l'"Accordo di Libero Scambio UE-Giappone" (JEFTA), che comprendeva l'Accordo di Partenariato Strategico (APS) e l'Accordo di Partenariato Economico (APE). Il primo era un accordo di natura politica che prevedeva una stretta collaborazione politica e piani d'azione congiunti su questioni di reciproco interesse[161]. Il secondo, che sarà analizzato in maggiore dettaglio, si proponeva di liberalizzare le attività di commercio e investimento, promuovendo un vincolo economico più stretto tra le parti[162].

I dialoghi per raggiungere un'intesa totale proseguirono molto a rilento e sembravano non giungere a nessuna conclusione, poiché entrambi i paesi erano impegnati in altre importanti trattative[163]. Tuttavia, nel 2016, l'adozione di una politica protezionistica da parte del nuovo presidente americano Donald Trump fece sospendere tali trattative, dando priorità ai negoziati tra il Giappone e l'Unione Europea. Tale determinazione può essere spiegata con l'interesse politico di entrambi i paesi nel voler inviare un forte messaggio alla comunità internazionale e agli Stati Uniti, rispondendo all'amministrazione Trump con l'apertura dei mercati, la cooperazione e l'adozione di standard comuni[164].

Al termine di numerosi incontri, il 17 luglio 2018, il Presidente della Commissione Europea Jean-Claude Juncker, il Presidente del Consiglio Europeo Donald Tusk e il Primo Ministro giapponese Shinzō Abe firmarono l'APE. L'accordo, entrato in vigore dal 1°

---

[160] P. CRISTÓBAL CISNEROS (2021), *The Economic Partnership Agreement between Japan and the European Union: analysis of the first years of life and prospects for the future*, Australian and New Zealand Journal of European Studies, Vol. 13, No. 2., p. 56. L'autore si riferisce, in particolare, al Piano d'Azione lanciato a seguito del decimo summit della Dichiarazione Congiunta del 2001.

[161] COMMISSIONE EUROPEA (2018), *Accordo di partenariato strategico tra l'Unione europea e i suoi Stati membri, da una parte, e il Giappone, dall'altra*, European Union Law, Bruxelles, p. 5.

[162] COMMISSIONE EUROPEA (2018), *Accordo tra l'Unione europea e il Giappone per un partenariato* economico, European Union Law, Bruxelles, p. 7.

[163] P. CRISTÓBAL CISNEROS (2021), *op., cit.*, p. 57. Si tratta del "*Comprehensive and Progressive Agreement for Trans-Pacific Partnership*" (CPTPP) per il Giappone e del "*Transatlantic Trade and Investment Partnership*" (TTIP) tra UE e Stati Uniti.

[164] *Ibidem.*

febbraio 2019, rappresenta una delle più grandi aree di libero scambio al mondo, coinvolgendo circa un terzo del PIL mondiale e 635 milioni di consumatori[165].
Il Giappone aveva registrato un calo significativo nella sua quota nelle esportazioni di beni dell'UE (dal 6,9% nel 1990 al 3,2% nel 2017) e nella quota di merci giapponesi nel paniere delle importazioni dell'UE (dal 12% nel 1990 al 3,7% nel 2017), tale da considerare l'APE una componente essenziale della cosiddetta "terza freccia" del piano "*Abenomics*", al fine di rivitalizzare il commercio e gli investimenti con l'UE e ampliare le opportunità per i produttori giapponesi nel continente asiatico[166]. Per ottenere questi risultati, le due nazioni concordavano sul fatto che l'aumento degli scambi di beni e servizi dovesse essere accompagnato da una circolazione sicura e libera dei dati. La norma UE però non consentiva che questo argomento fosse oggetto di trattative in un accordo di libero scambio; di conseguenza, la Commissione europea decise di lavorare alle due questioni parallelamente[167].
La Commissione europea e il PPC si mostrarono dunque favorevoli a considerarsi reciprocamente equivalenti dal punto di vista del regolamento sulla protezione dei dati. Nel luglio 2017, infatti, in una dichiarazione congiunta, entrambi i commissari espressero la loro soddisfazione nel constatare che, sulla base dei lavori svolti, le riforme recenti avevano avvicinato ancor di più le rispettive legislazioni, offrendo l'opportunità di facilitare ulteriormente lo scambio reciproco di dati, attraverso una simultanea constatazione di un livello di protezione adeguato da entrambe le parti. La speranza era di concludere i negoziati entro l'inizio del 2018, prima dell'entrata in vigore del GDPR prevista per il 25 maggio 2018[168].

3.3. La decisione di adeguatezza

Prima di esaminare i dialoghi che hanno portato alla decisione di adeguatezza, si ritiene opportuno condurre una breve analisi comparata nell'ambito dei trasferimenti

---

[165] *Ivi*, p. 58.
[166] A. SAPIR, A. TERZI, S. CHOWDHRY (2018), *The EU - Japan Economic Partnership Agreement*, Commissione Europea, Directorate-General for External Policies of the Union, Bruxelles, p. 7.
[167] M. HORIBE (2020), *Nichi EU kan no jūbunsei sōgo nintei to chikyū kibo no jiyūna kojin dēta ryūtsūron* (La decisione di adeguatezza tra Giappone e UE e il desiderio di realizzare il libero flusso di dati personali su scala globale), Journal of Information and Communications Policy, Vol. 4, No. 2, p. 14.
[168] Y. SUDA (2020), *op., cit.*, p. 519.

internazionali tra il GDPR e l'APPI nella versione del 2015, offrendo una prospettiva più chiara del contesto giuridico in cui è avvenuta.

Come già osservato, il Giappone ha introdotto l'istituto sul trasferimento internazionale soltanto con la riforma dell'APPI nel 2015. In essa, l'art. 24 afferma che il titolare del trattamento deve ottenere il consenso preventivo dell'interessato prima di trasferire i suoi dati verso un paese situato fuori dai confini nazionali, salvo per tre casi[169]. Pertanto, sia l'APPI che il GDPR sembrano prevedere delle basi di legittimità; tuttavia, il primo si concentra principalmente sul consenso, mentre il secondo comprende anche altre condizioni di legittimità[170]. Inoltre, contrariamente al GDPR, la legge giapponese non fa riferimento alle organizzazioni internazionali, lasciando presumere che trasferimenti verso tali entità vengano trattati come previsto dall'art. 23 sulle restrizioni per i soggetti terzi[171].

In termini di applicazione, l'extraterritorialità del GDPR include le organizzazioni che non si trovano in Europa, ma che offrono beni e servizi ai cittadini europei o monitorano il comportamento di persone situate all'estero (art. 3.2). Un trattamento simile avviene in Giappone: l'art. 75 infatti stabilisce che certe disposizioni si applicano anche nei casi in cui il titolare del trattamento, in relazione alla fornitura di un bene o servizio a una persona in Giappone, abbia gestito i suoi dati in un paese straniero.

Alla luce di ciò, sembrano dunque esserci sufficienti elementi per affermare che le due legislazioni condividano una sostanziale armonia, che agevolerà significativamente le trattative per la realizzazione dell'accordo di adeguatezza [172].

Affinché un paese sia riconosciuto come "adeguato", è necessario che soddisfi una serie di criteri. Nel GDPR, tali criteri possono essere ricondotti al rispetto dello Stato di diritto, dei diritti umani e delle libertà fondamentali, all'esistenza di leggi che garantiscono i diritti degli interessati e a meccanismi di ricorso efficaci. Inoltre, è indispensabile la presenza di un'autorità di controllo indipendente e la collaborazione negli impegni internazionali. Dopo il caso Schrems, sono state anche introdotte garanzie sul livello di sicurezza verso l'accesso dei dati da parte delle autorità pubbliche[173].

---

[169] Cfr. capitolo 2.3.3 per i casi in questione.
[170] F. SERINI (2022), *op. cit.*, pp. 170-171. Le condizioni a cui si fa riferimento sono: la decisione di adeguatezza, le garanzie adeguate e le deroghe.
[171] *Ibidem*.
[172] *Ibidem*.
[173] H. MIYASHITA (2020), *EU-Japan Mutual Adequacy Decision*, Blogdroiteuropéen, pp. 2-3.

Il percorso per ottenere una decisione di adeguatezza è quindi complesso e spesso richiede molto tempo. Infatti, il Giappone ha impiegato ben due anni e dieci mesi prima di concludere l'accordo. Prima di tutto, lo Stato giapponese ha presentato una proposta ufficiale alla Commissione Europea, dando avvio alla fase di valutazione preliminare. Successivamente, il Comitato europeo per la protezione dei dati (EDPB) e gli Stati membri dell'Unione Europea hanno esaminato la candidatura, esprimendo le proprie opinioni e fornendo un parere complessivo. La valutazione ha richiesto un'analisi approfondita, coinvolgendo persino esperti locali per superare la scarsa disponibilità di fonti in lingua inglese[174]. La fitta rete di negoziati e scambi di contributi è stata portata avanti grazie ai dialoghi intrapresi tra la Commissione Europea, la PPC, la EDPB, la Commissione per le libertà civili, la giustizia e gli affari interni (LIBE), nonché tra i rispettivi governi e parlamenti coinvolti[175]. A conclusione di questo lungo processo, la Commissione Europea ha infine adottato la decisione di adeguatezza, riconoscendo al Giappone un livello adeguato di protezione[176].

Durante le trattative, tuttavia, non sono mancate complicazioni. L'urgenza politica di approvare la decisione in concomitanza con l'entrata in vigore dell'Accordo di Partenariato Economico UE-Giappone ha sollevato interrogativi sul grado di approfondimento con cui sono state affrontate le questioni più spinose[177]. Una delle maggiori preoccupazioni riguardava la mancanza di riferimenti nella bozza della decisione verso le garanzie in caso di accesso ai dati delle autorità pubbliche e la debolezza del regime sanzionatorio giapponese in merito alle violazioni. Infatti, confrontando le pesanti multe stabilite dal GDPR, le punizioni giapponesi apparivano molto più leggere[178].

Un altro argomento di apprensione era il fatto che, per il diritto di accesso ai "dati personali conservati", l'APPI imponeva ai titolari di fornire all'interessato i propri dati, ma escludeva quelli che dovevano essere cancellati entro sei mesi[179]. Questa disposizione destava perplessità, poiché si discostava dai principi sanciti dal GDPR, che attribuiva agli

---

[174] *Ibidem*.

[175] E. FAHEY, I. MANCINI (2023), *Cross-border data flows between the EU, Japan and the UK. A triangular relationship*, Keio Law Journal, No. 49, p. 64.

[176] *Ivi,* p. 3.

[177] A. G. MARCÉN (2021), *op., cit.*, p. 113.

[178] *Ivi*, p. 112. Il GDPR stabilisce che, per le violazioni più gravi, le multe possono arrivare fino a 200 milioni di euro o, nel caso di un'impresa, fino al 4% del fatturato globale annuo totale dell'anno finanziario precedente.

[179] Y. SUDA (2020), *op., cit.*, p. 520. Questa esclusione è stabilita all'art. 3 dell'ordinanza governativa nr. 507. GOVERNO DEL GIAPPONE (2003), *Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order No. 507 of December 10, 2003)*, Japanese Law Translation.

interessati un controllo più ampio sui propri dati personali, indipendentemente dalla durata del loro trattamento.

Nonostante tutte queste preoccupazioni, la decisione di adeguatezza tra Giappone e UE rimane, in ogni caso, un grande esempio di cooperazione internazionale tra due paesi apparentemente lontani. Per la prima volta nella storia, l'Europa ha riconosciuto il quadro normativo di un paese extraeuropeo come "essenzialmente equivalente" (*Kihonteki ni hitoshiku* 基本的に等しく)[180], dando vita alla più grande area di trasferimento sicuro e libero di dati al mondo, fondata su un elevato livello di protezione[181]. Come afferma Miyashita, l'adeguatezza non deve però essere intesa come una semplice copia delle normative o un mero strumento pratico, ma come un'opportunità per riflettere la convergenza tra le rispettive filosofie sulla protezione dei dati[182].

3.4. Le Norme Supplementari

Dal procedimento svolto per il conseguimento dell'accordo di adeguatezza pare chiaro che sia stato il sistema giapponese a doversi adattare a quello europeo e non viceversa. Perciò, al fine di ridurre le discrepanze normative, il governo giapponese ha pensato di affidare alla PPC l'arduo compito di adottare misure a tale scopo. In quest'ottica, la Commissione ha emanato delle "norme supplementari" che erano, in realtà, già previste nell'art. 12.3 dall'APPI del 2015 e che imponevano una revisione triennale della legge in considerazione dei progressi nelle tecnologie dell'informazione e della comunicazione che si sarebbero presentati da lì in avanti.

Gli aspetti principali che sarebbero stati oggetto della revisione erano[183]:

- La definizione e il rispetto dei diritti individuali relativi ai dati personali;
- Il meccanismo per la segnalazione di violazioni dei dati;

[180] Lett. "fondamentalmente uguale". M. HORIBE (2020), *op., cit.*, p. 15.
[181] F. WANG (2020), *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, Harvard Journal of Law & Technology, Vol. 33, No. 2, p. 671.
[182] H. MIYASHITA (2019), *The impact of GDPR in Japan*, in *National Adaptations of the GDPR*, a cura di MC CULLAGH K., TAMBOU O., BOURTON S., Blogdroiteuropéen, p. 127.
[183] M. AKIYAMA (2020), *Kojin jōhō hogohō minaoshi no gaiyō* (Panoramica della revisione della legge sulla protezione dei dati personali), National Diet Library, No. 1089, p. 2.

- Le misure per incentivare le imprese a implementare pratiche efficaci per la protezione dei dati;
- Le politiche di utilizzo dei dati;
- Le modalità di sanzione;
- L'applicazione extraterritoriale della legge;
- L'armonizzazione internazionale dei sistemi e i trasferimenti transfrontalieri di dati.

Sulla base di questi punti, la PPC ha analizzato e organizzato le politiche nazionali e internazionali, le tecnologie, le situazioni industriali e ha condotto revisioni approfondite, coinvolgendo esperti, rappresentanti industriali e consumatori[184]. A seguito di queste consultazioni, è stato presentato un riepilogo intermedio per raccogliere anche le opinioni pubbliche, dal quale sono stati raccolti 525 commenti su un totale di 137 organizzazioni, operatori economici e privati cittadini[185]. Il piano generale è stato invece elaborato il 13 dicembre 2019, mediante l'*Act on the Protection of Personal Information "The Every-Three-Year Review"* (*Kojin jōhō hogohō iwayuru san'nen goto minaoshi ni kakaru kentō* 個人情報保護法・いわゆる３年ごと見直しに係る検討), con l'obiettivo di presentare un nuovo disegno di legge durante la sessione ordinaria della Dieta del 2020. Dopo un periodo di preparazione, che serviva a dare tempo agli operatori economici di adeguarsi alle nuove disposizioni, la Riforma vera e propria è entrata in vigore il 1° aprile 2022[186]. Tali disposizioni coprivano molteplici ambiti, ma in relazione all'argomento della tesi prenderemo in considerazione unicamente quelli più attinenti.

3.4.1. *I diritti dell'interessato*

Il primo oggetto di revisione faceva riferimento al rafforzamento dei diritti dell'interessato relativamente alla gestione dei propri dati personali. Il problema maggiore che era emerso

---

[184] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019). *Act on the Protection of Personal Information "The Every-Three-Year Review" Outline of the System Reform,* pp. 6-7.
[185] *Ibidem*. Il riepilogo è consultabile in lingua originale al seguente link: https://www.ppc.go.jp/files/pdf/press_betten1.pdf consultato il 23/05/2025.
[186] *Ibidem*. L'*Amended Act on the Protection of Personal Information (Tentative Translation)* del 2020 è disponibile al seguente link: https://www.ppc.go.jp/files/pdf/APPI_english.pdf.

dalle consultazioni riguardava l'insoddisfazione da parte dei consumatori sul metodo di sospensione o cancellazione dei "dati personali conservati" dalle aziende. L'obiettivo era quindi quello di "*semplificare i requisiti per la cessazione dell'utilizzo, la cancellazione e la cessazione della fornitura a terzi, e ampliare l'ambito dei diritti individuali per rispondere a potenziali violazioni*"[187]. A tal fine, è stato implementato l'art. 30.5-6 che richiedeva al titolare di accettare o rifiutare la richiesta solo dopo un'appropriata valutazione, e in caso negativo di comunicarlo immediatamente all'interessato[188].
Infine, per quanto concerne gli interventi per migliorare l'accessibilità dei "dati conservati", il lavoro si era concentrato sulla digitalizzazione delle richieste di accesso, consentendo agli interessati di scegliere la modalità di divulgazione preferita tra formati elettronici o magnetici; e sul prolungamento del termine per l'esercizio dei diritti dell'interessato oltre i sei mesi previsti[189].

3.4.2. *Gli obblighi per il titolare del trattamento*

La seconda revisione apportava cambiamenti significativi alle responsabilità imposte ai titolari del trattamento che si trovavano in Giappone, mirati a prevenire utilizzi scorretti e rafforzare così l'orientamento etico nell'impiego dei dati personali[190].
La segnalazione alla PPC di incidenti di sicurezza, inclusa la perdita o la divulgazione non autorizzata di dati personali non era legalmente obbligatoria, infatti molti titolari erano restii a rivelarli pubblicamente. Perciò, è stato deciso di promuovere buone pratiche tra i titolari del trattamento grazie alla diffusione di linee guida e consigli utili, derivanti dai casi segnalati[191].
Con la riforma, l'avvenuto incidente di violazione ("*data breach*") doveva essere segnalato alla PPC e notificato al soggetto interessato tempestivamente, qualora l'incidente rientrasse in determinate categorie, come una perdita massiccia di dati o la divulgazione di dati sensibili. Doveva inoltre essere messa a disposizione una relazione completa, comprensiva delle cause e delle misure correttive effettuate, per permettere alla PPC di

---

[187] *Ivi*, p. 10.
[188] F. SERINI (2022), *op. cit*., pp. 180-181. Ciò non è necessario quando la richiesta comporta ingenti spese, risulta di difficile realizzazione o sia necessaria un'azione alternativa.
[189] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019), *op., cit.,* pp. 11-12.
[190] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019), *Act on the Protection of Personal Information "The Every-Three-Year Review" Outline of the System Reform (Main Points)*, p. 2.
[191] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019), *op., cit.,* pp. 17-18.

venire a conoscenza dell'evento in una fase precoce e di dare tempo al soggetto interessato di adottare le misure necessarie[192].
Quando non era possibile rintracciare gli interessati per informarli della violazione, era previsto che il titolare del trattamento adottasse misure alternative, come la pubblicazione di un avviso pubblico e la predisposizione di un canale di contatto per eventuali richieste (art. 22-2).

3.4.3. *Il "dato pseudonimizzato"*

Nel GDPR, la "pseudonimizzazione" è definita come:

> il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Il "dato pseudonimizzato" (*Kana kakō jōhō* 仮名加工情報)[193] è quindi un dato "reversibile" che, pur essendo stato sottoposto a un processo di trasformazione per ridurre il rischio di identificazione diretta dell'interessato, consente, sotto certe condizioni, di risalire a quest'ultimo.
Il fatto che l'APPI del 2015 descriveva i dati anonimizzati con caratteristiche proprie di quelli pseudonimizzati, lasciando aperta la possibilità di risalire all'interessato, era stato oggetto di chiarimenti durante le trattative per l'adeguatezza. E, nonostante fosse stata appurata la natura irreversibile di tali dati, la PPC aveva ritenuto necessario introdurre all'art. 2 la nozione di "processo di pseudonimizzazione" e di "titolare del trattamento di dati personali pseudonimizzati"[194].
Al paragrafo 9 dell'articolo, il contenuto era pressoché identico a quello del GDPR, entrambi affermavano che l'identificazione diretta dell'interessato non era possibile senza l'uso di informazioni aggiuntive. Il paragrafo 10 invece definiva il titolare del trattamento di dati pseudonimizzati come colui che gestisce e mette a disposizione, per scopi

[192] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019), *op., cit.*, *(Main Points),* p. 2.
[193] Letteralmente "Dati elaborati con pseudonimi".
[194] F. SERINI (2022), *op. cit.*, pp. 178-179.

commerciali, una mole organizzata di questa tipologia di dati, strutturati in modo tale da permettere ricerche rapide e specifiche tramite dispositivi elettronici.
Gli obblighi legati a questa figura erano dettagliati nella Sezione 2 della riforma. L'art. 35-2 disciplinava le modalità e le restrizioni per l'utilizzo. Innanzitutto, si specificava che i titolari erano tenuti a rispettare le regole prescritte dalla PPC, affinché fosse impossibile identificare direttamente un individuo senza l'ausilio di informazioni aggiuntive e si prevenisse qualunque violazione (par. 1, 2). Inoltre, erano tenuti a limitare il trattamento dei dati esclusivamente agli scopi specificati, senza eccedere quanto necessario per il raggiungimento degli obiettivi previsti (par. 3). Altri adempimenti consistevano nel cancellare i dati quando non erano più utili (par. 5); non condividerli con terzi (par. 6); non combinare certi dati con altri per identificarne il proprietario (par. 7); e non utilizzarli per instaurare contatti diretti (par. 8).
L'obbligo previsto al par. 6 veniva approfondito all'art. successivo, dove si ribadiva che un titolare non poteva fornire questi dati a terzi, salvo nei casi previsti dalla legge; le regole e gli obblighi previsti per chi riceveva questi dati si applicavano anche ai terzi che li ricevevano (art. 35-3).

3.4.4. *Estensione dell'ambito di applicazione extraterritoriale e novità sul trasferimento transfrontaliero*

Dopo l'implementazione dell'art. 75 nell'APPI del 2015 era stato formulato per la prima volta un regime per chi trattava, su consenso, i dati personali o i dati anonimizzati di una persona situata in Giappone in un paese straniero. Eppure, secondo la legge previgente, le eventuali segnalazioni, le ispezioni sul posto e gli ordini non si applicavano al titolare straniero. L'Autorità Garante era limitata ad azioni prive di potere esecutivo, come la fornitura di linee guida, consigli o raccomandazioni[195].
Con la revisione del 2020 invece, tutti i titolari stranieri si dovevano adoperare per mettere in atto le azioni appropriate per il controllo della sicurezza e della gestione del trattamento dei dati, indipendentemente dal fatto che essi fossero pseudonimizzati o anonimizzati. Inoltre, poiché l'autorità pubblica non poteva essere esercitata nei territori di altri paesi senza il loro consenso, era possibile cooperare con le autorità estere coinvolte

[195] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019), *op., cit.,* pp. 34-35.

(art. 78). Se il titolare non avesse ottemperato a tali ordini, la PPC sarebbe stata autorizzata a renderlo noto pubblicamente e a sanzionarlo (art. 79).

Sebbene l'art. 24 sui trasferimenti transfrontalieri ponesse già delle restrizioni al trasferimento estero in determinate circostanze, restavano dei timori legati ai rischi di trattamento improprio che potevano sorgere a seconda del paese in cui erano trasferiti i dati. Per mitigare tali rischi era importante considerare attentamente sia il titolare che il paese destinatario[196]. In questo senso, è stato stabilito che, in presenza del consenso, il titolare era tenuto ad informare l'interessato del nome del paese ricevente, del sistema giuridico in materia di protezione dei dati di quel paese e di ogni diritto che poteva esercitare. Mentre, in assenza di consenso, l'interessato aveva facoltà di richiedere qualunque informazione, a patto che il sistema di chi riceveva i dati garantisse una gestione continua e appropriata in caso di sviluppi normativi o di segnalazioni per irregolarità[197].

3.4.5. *Il "caso Rikunabi" e il potenziamento delle sanzioni*

L'APPI ha un sistema sanzionatorio che include le cosiddette "doppie sanzioni per le persone giuridiche" (art. 87)[198], dove l'efficacia delle sanzioni pecuniarie dipende principalmente dalla solvibilità dei soggetti accusati. Nella versione del 2015, l'ammontare massimo previsto risultava spesso insufficiente a garantire un reale effetto deterrente per le aziende con significative risorse economiche[199]. Infatti, il numero di segnalazioni presentati alla PPC e che richiedevano ispezioni in loco era in allarmante aumento. Un caso in particolare attirò le attenzioni della Commissione e dell'opinione pubblica: nell'agosto del 2019, la Recruit Career Company, fu al centro di uno scandalo di grande impatto sociale che prese il nome di "*caso Rikunabi*" (*Rikunabi jiken* リクナビ事件).

---

[196] *Ivi*, pp. 36-37.
[197] A. C. RAUL (2022), *op., cit.*, p. 248.
[198] L'art. stabilisce che, se il rappresentante, l'agente, il dipendente o un altro lavoratore di una società o di un individuo commette una violazione prevista dagli art. 83-85 nell'ambito dell'attività della società o dell'individuo, oltre a punire direttamente chi ha commesso la violazione, anche la società o l'individuo sarà soggetto alla multa prevista dall'articolo corrispondente.
[199] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019), *op., cit.,* p. 32

Nel Paese esiste un'usanza detta *Shinsotsu Ikkatsu Saiyō* 新卒一括採用[200], in cui gli studenti neolaureati si dedicano alla ricerca di lavoro in un periodo specifico dell'anno. L'azienda metteva a disposizione un sito, chiamato Rikunabi, che permetteva di accedere a una serie di servizi, tra cui la ricerca e candidatura per offerte di lavoro, informazioni sulle aziende e possibilità di partecipare a eventi di orientamento e selezione, registrandosi tramite il numero identificativo e l'università. Solo nel 2020 il numero di aziende registrate era di 31.564, mentre quello degli studenti iscritti era circa 800.000, rendendolo il più grande sito di inserimento lavorativo del Giappone[201].

La violazione si perpetrava perché la Recruit Career impiegava un algoritmo di profilazione avanzato, che incrociava i cookies con i dati degli utenti e calcolava il cosiddetto "*Naitei jitairitsu*" 内定辞退率[202], ossia la probabilità che un candidato declinasse un'offerta di lavoro. Questo dato veniva ceduto alle aziende partner, che lo usavano per decidere se e quando investire nel reclutamento di un candidato, cercando di minimizzare il rischio di ricevere un rifiuto. Naturalmente questa notizia scatenò l'indignazione e la rabbia degli studenti, poiché tali dati erano stati prelevati senza il loro consenso, influenzando la selezione da parte delle società coinvolte e, di conseguenza, la loro carriera professionale[203].

Data la gravità del fatto, la PPC emise delle istruzioni (art. 41) e una raccomandazione ufficiale (art. 42.1) contro la compagnia[204]. Questi provvedimenti sollecitavano a rivedere la struttura organizzativa dell'azienda e a cambiare la mentalità lavorativa attraverso un approccio manageriale più responsabile verso il corretto trattamento dei dati. Nel dettaglio, si contestava il mancato rispetto delle misure di sicurezza richieste all'art. 20 e la fornitura di 7.983 dati personali a terzi senza il consenso degli interessati, in contrasto a quanto stabilito dall'art. 23[205]. Per quanto riguarda le sanzioni, lo scandalo ha determinato anche un inasprimento delle pene: la violazione delle raccomandazioni della

---

[200] Letteralmente "reclutamento simultaneo dei neolaureati".
[201] F. KUDO, H. ARAI, A. EMA (2020), *Ethical Issues Regarding the Use of AI Profiling Services for Recruiting: The Japanese Rikunabi Data Scandal*, arXiv, p. 1.
[202] Letterlamente "tasso di rifiuto delle offerte informali di lavoro".
[203] T. KIYOSHI (2023), *Rikunabi jiken no sono go: Seifu ni yoru hōteki taiō wa ikani?* (Dopo il caso Rikunabi: Qual è la risposta legale del governo?), Toyama Daigaku Keizai Gakubu, Vol. 69, p. 69.
[204] H. MIYASHITA (2021), *Human-centric data protection laws and policies: A lesson from Japan*, Computer Law & Security Review, Elsevier, Vol. 40, p. 2.
[205] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019), *Kojin jōhō no hogo ni kansuru hōritsu dai yonjūnijō dai ichikō no kitei ni motozuku kankokutō ni tsuite* (Raccomandazioni, ecc., ai sensi dell'articolo 42, comma 1, della Legge sulla protezione dei dati personali), p. 2.

PPC è punita con la reclusione fino a un anno oppure una multa di non oltre 1 milione di yen (art. 83 dell'APPI 2020); mentre, per la cessione illegale o l'uso occulto di un database di dati personali da parte di una persona giuridica, la sanzione pecuniaria può arrivare fino a 100 milioni di yen (art. 87.1 dell'APPI 2020). Per i titolari del trattamento la multa raggiunge massimo 500.000 yen e la detenzione non può superare un anno (art. 84 dell'APPI 2020).

3.5. Questioni in sospeso

Nonostante tutti gli interventi che nel tempo hanno allineato l'APPI agli standard internazionali, il confronto con il GDPR evidenzia tutt'ora delle divergenze. Oltre al già citato "diritto all'oblio", che non trova ancora disciplina nella legislazione giapponese, esistono altre importanti difformità nell'ambito dei diritti degli interessati. Ad esempio, nella legge giapponese non è presente il "diritto alla portabilità dei dati" per cui l'interessato ha la facoltà di ricevere i dati che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivi automatici, e di trasferirli liberamente a un altro titolare senza impedimenti (art. 20 del GDPR). Manca inoltre l'esplicita previsione del "diritto di opposizione" (art. 21 del GDPR), che permette di fermare in qualsiasi momento il trattamento, compreso quello per la profilazione degli identificativi online quali gli indirizzi IP, cookie o dati di localizzazione.

Nel GDPR essi sono considerati veri e propri dati personali perché "*possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*"[206], ad esempio con il tracciamento per fini pubblicitari. In Giappone invece non esiste una regolamentazione verso questi identificativi, in quanto le informazioni dei cookie, combinate con gli ID unici di utenti di cui non si conosce l'identità, non sono considerate dei dati personali (come dimostrato dal caso *Rikunabi*)[207].

Un'altra presa di posizione tra il GDPR e l'APPI si registra nel meccanismo del consenso, in quanto il GDPR impone un consenso preventivo ed esplicito come requisito fondamentale per il trattamento, privilegiando un modello di tipo "*opt-in*" (art. 7 del GDPR); mentre

[206] PARLAMENTO EUROPEO (2016), *op., cit.*, p. 6.
[207] H. MIYASHITA (2021), *op., cit.*, p. 2.

l'APPI 2020, all'art. 23.2, autorizza la cessione di dati personali senza il consenso dell'interessato attraverso il modello "*opt-out*", se vengono rispettati alcuni requisiti. Con le ultime riforme, sono stati inclusi dei requisiti di trasparenza più dettagliati, che devono essere notificati all'interessato e alla PPC come le informazioni di chi effettua il trasferimento, le categorie di dati trasferiti, il metodo di raccolta e di trasferimento, e le modalità con cui l'interessato può opporsi al trattamento. Inoltre, viene specificato che questo meccanismo non può essere applicato ai dati sensibili, ai dati raccolti con modalità ingannevoli o illecite (in violazione dell'ex art.17), o a dati già trattati da altri titolari[208].
Per ultimo, si cita anche l'assenza di disposizioni sulla protezione dei dati personali dei bambini. Infatti, la normativa giapponese del 2020 non dava nessuna direttiva sul trattamento di dati dei minori.

Nell'ottica del trasferimento internazionale, la riforma successiva alla decisione di adeguatezza ha quasi completamente colmato la distanza tra le due normative, tuttavia rimangano alcune differenze. In assenza di standard equivalenti riconosciuti, l'APPI non delinea altre misure specifiche di protezione appropriate per il trasferimento estero dei dati, ma richiede ai soggetti terzi di istituire un sistema conforme ai principi dettati dalla PPC (ex art. 24.3). Al contrario, l'UE fornisce ulteriori salvaguardie nel dettaglio (art. 46 del GDPR)[209].
Diversamente dal GDPR, si osserva inoltre che nell'APPI non ci sono riferimenti agli accordi internazionali per la cooperazione giudiziaria sui trasferimenti transfrontalieri. Si ricorda tuttavia che il Giappone è un membro del *Cross Border Privacy Rules System* che consente ai titolari di trasferire dati personali a paesi stranieri certificati, purché rispettino le regole del sistema.

3.6. Ultimi sviluppi

Il 19 maggio 2021, il governo giapponese ha emanato l'*Act on the Arrangement of Related Acts for the Formation of a Digital Society* (*Dejitaru shakai no keisei o hakaru tame no kankei hōritsu no seibi ni kansuru hōritsu* デジタル社会の形成を図るための関係法律の

[208] F. SERINI (2022), *op. cit.*, p. 186.
[209] Si rimanda alla nota 155.

整備に関する法律, Legge No. 37/2021)[210], come parte di un pacchetto di leggi utili a promuovere la formazione di una "società digitale"[211]. Tra i sei disegni di legge, la presente apporta significative modifiche all'APPI 2020[212].

Come sappiamo, la Legge sulla protezione dei dati personali tracciava una linea di separazione tra il settore pubblico e privato, dove l'APPI si occupava del privato, mentre gli organi amministrativi nazionali (secondo la legge "PPIHAOA") e le istituzioni amministrative indipendenti (secondo la legge "PPIHIAAA") trattavano quello pubblico. Tuttavia, si è ritenuto che questa differenziazione potesse ostacolare la circolazione dei dati; perciò, è stato deciso di unificare entrambi i settori, in modo da stabilire regole comuni e facilitare il controllo della PPC[213].

Gli enti che più hanno beneficiato di questo aggiornamento sono stati gli ospedali e le università. I primi, essendo nella maggior parte gestiti dalle istituzioni indipendenti, in precedenza avevano difficoltà nel condividere informazioni con le altre strutture sanitarie private, a causa delle diverse norme. I secondi invece erano esclusi dall'applicazione dell'APPI quando i dati personali venivano utilizzati per studi accademici (ex art. 76, comma 3). Il trasferimento di tali dati non era quindi soggetto alla decisione di adeguatezza, impedendo la conduzione di ricerche congiunte[214]. Oggi invece esistono delle esenzioni che prevedono l'utilizzo (art. 18.3, comma 5), l'accesso ai dati sensibili (art. 20.2, comma 6) e la fornitura a terzi (art. 27.1, comma 6) per scopi di ricerca.

Tra le altre novità si segnalano anche: l'integrazione delle definizioni di "dato personale" a livello nazionale, locale e privato, inclusi codici ID e dati sensibili; e il chiarimento degli obblighi relativi al trattamento di dati anonimizzati da parte degli organi amministrativi[215].

La cosiddetta "*Six Digital Reform – Related Laws*" (*Dejitaru kaikaku kanren roku hōan* デジタル改革関連 6 法案) era dunque un progetto di legge autonomo, separato dal ciclo di

---

[210] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2021), *Dejitaru shakai no keisei o hakaru tame no kankei hōritsu no seibi ni kansuru hōritsu* (Legge per il consolidamento delle leggi correlate alla formazione di una società digitale).

[211] https://www.sangiin.go.jp/japanese/ugoki/r3/210512.html consultato il 07/06/2025

[212] L'APPI 2021 con le ultime modifiche è visibile al seguente link: https://www.japaneselawtranslation.go.jp/en/laws/view/4241

[213] https://www.ppc.go.jp/files/pdf/seibihouan_gaiyou.pdf consultato il 07/06/2025

[214] https://inplp.com/latest-news/article/hird-amendment-of-the-japanese-privacy-law-amendment-based-on-the-digital-arrangement-act/ consultato il 07/06/2025

[215] https://www.ppc.go.jp/files/pdf/seibihou_gaiyou.pdf consultato il 07/06/2025

riforme legislative contenuto nella revisione triennale, che invece è attesa per il 2025. Nel frattempo, però, è già stata pubblicata dalla PPC una relazione intermedia, che ci dà modo di dare un primo sguardo ai propositi del nuovo aggiornamento.

Con il nome di "*Interim Summary*" (*Kojin jōhō hogohō - 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), il rapporto consiste in un riepilogo preliminare che riassume le valutazioni della PPC, basato sulle discussioni e gli approfondimenti emersi fino ad oggi[216].
L'interesse si focalizza su tre macro-argomenti:

1) la protezione dei diritti e degli interessi individuali;
2) le modalità di monitoraggio e supervisione;
3) e le modalità di supporto per le iniziative relative all'utilizzo dei dati.

Per quanto riguarda la voce 1), si fa preciso riferimento ai dati biometrici, ovvero quei dati derivanti da caratteristiche fisiche e comportamentali che identificano univocamente una persona. Attualmente, essi sono regolamentati come semplici codici di identificazione, ma è necessario che vengano immediatamente adottati provvedimenti, prendendo spunto dal sistemo giuridico europeo, che li considera dati particolarmente sensibili[217].
Secondariamente, si menzionano le norme relative al "divieto di utilizzo improprio" (art. 19 (ex art. 12-2)) e alla "corretta acquisizione" dei dati personali (art. 20.1 (ex art. 17.1)). Tali articoli, pur vietando complessivamente comportamenti illeciti, lascerebbero ampi margini di discrezionalità ai titolari del trattamento. Per questo motivo, occorrerebbe specificare e classificare gli ambiti di applicazione, al fine di proteggere i diritti e gli interessi individuali[218].
Inoltre, ci sono state riflessioni sul dibattuto sistema "*opt-out*", poiché si sono verificati casi in cui l'assenza di un obbligo per le aziende di accertare la validità delle finalità dichiarate e l'identità dei destinatari hanno causato la fornitura involontaria di dati a

[216] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2024), *Kojin jōhō hogohō - iwayuru san'nen goto minaoshi ni kakaru kentō no chūkan seiri* (Legge sulla protezione dei dati personali - Riepilogo intermedio delle considerazioni relative alla revisione triennale), p. 2.
[217] *Ivi*, pp. 3-4.
[218] *Ivi*, pp. 4-5.

gruppi criminali. Quindi, la PPC ritiene fondamentale imporre alle aziende di confermare l'identità e la legittimità dell'acquisizione dei terzi a cui vengono inviati i dati[219].
Un altro tema riguarda i bambini, i quali, come precedentemente accennato, non hanno un regime dettagliato, se non fosse per due circostanze incorporate nell'APPI attuale:

1) quando c'è una richiesta di divulgazione da parte di un minore, il nominato rappresentante legale può fare una richiesta di divulgazione per conto suo (art. 76.2);
2) in situazioni in cui si ritiene che un minorenne non abbia la capacità di giudicare le conseguenze derivanti dal consenso relativo al trattamento dei propri dati personali, è necessario ottenere il consenso da un tutore legale o da un rappresentante legale. Secondo le linee guida della PPC, l'età del consenso è presumibilmente dai 15 anni in poi[220].

Da questi punti si evince una certa vaghezza rispetto al Regolamento europeo, che invece considera i bambini come dei soggetti che "*meritano una specifica protezione*"[221], con maggiore accortezza per l'utilizzo dei loro dati a fini di marketing e di profilazione. Pertanto, i titolari del trattamento devono mettere in atto misure ragionevoli per verificare che il consenso sia stato autorizzato dal rappresentante legale, tenendo conto della tecnologia disponibile (art. 8.2 del GDPR). Nel farlo, devono anche fornire le informazioni del trattamento in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice, di facile comprensione per il minore. In questo caso, l'età minima del consenso è fissata a 16 anni con possibilità di abbassamento fino a 13 anni nei singoli Stati membri (art. 8.1 del GDPR).
Pertanto, si chiede di rivedere le procedure, implementando il consenso obbligatorio del rappresentante legale, l'estensione del diritto di sospensione dell'uso dei dati, l'adozione di misure di sicurezza più stringenti e la definizione dell'età minima del consenso a 16 anni[222].

---

[219] https://www.ppc.go.jp/files/pdf/chukanseiri_gaiyo_r6.pdf consultato il 08/11/2025
[220] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2020), *Kojin jōhō no hogo ni kansuru hōritsu ni tsuite no gaidorain ni kansuru Q&A* (Domande e risposte relative alle linee guida della Legge sulla protezione dei dati personali), p. 16.
[221] PARLAMENTO EUROPEO (2016), *op., cit.*, p. 7.
[222] https://www.hoganlovells.com/en/publications/interim-report-on-the-revision-of-the-act-on-the-protection-of-personal-information consultato il 08/11/2025

Infine, l'argomento esplora la materia dei diritti dei consumatori, considerando l'eventuale introduzione di un sistema di *class action* contro le violazioni. In Giappone esiste già un meccanismo legale che consente a organizzazioni autorizzate di agire contro aziende inadempienti, ma tale sistema non è attualmente applicabile ai rimedi previsti dall'APPI. La volontà sarebbe quella di estendere questo strumento ai diritti specifici degli interessati, come la possibilità di richiedere la cessazione del trattamento dei dati personali in situazioni particolari. Ciononostante, a fronte delle obiezioni emerse, la PPC valuta indispensabile un ulteriore esame sulla sua utilità e fattibilità nella tutela dei diritti dei consumatori[223].

Procedendo alla voce 2), la relazione si occupa della dibattuta normativa sanzionatoria. Per le pene amministrative, la legge attuale si limita a strumenti come ammonimenti, raccomandazioni e ordini, ma questi non impediscono che i profitti derivanti dalle violazioni restino nelle mani dei titolari. Pertanto, la PPC si occuperà di analizzare i seguenti punti[224]:

- le tipologie di illeciti soggetti a tali sanzioni, ad esempio la fornitura illegale di dati personali a terzi o la negligenza nelle misure di sicurezza, nonostante la consapevolezza del rischio di fuga di dati;
- il metodo di calcolo delle sanzioni, che potrebbe basarsi sia sui profitti illeciti derivanti dalla vendita di dati personali sia sull'aumento dei guadagni dovuto all'elusione degli obblighi di pagamento;
- la fissazione di un importo minimo per le sanzioni e la possibilità di aumenti o diminuzioni in base a precise casistiche.

Ai sensi del Capitolo "*Penal Provisions*" (ex Cap. 7) invece, l'APPI stabilisce una punizione diretta per il trattamento improprio di dati personali, con un incremento della pena per le persone giuridiche. Tuttavia, il costante aumento dei casi potrebbe comportare un'estensione dell'ambito di applicazione delle sanzioni.

---

[223] https://www.globalcompliancenews.com/2024/08/05/japan-personal-data-protection-commission-announces-interim-report-of-triennial-review/ consultato il 08/11/2025
[224] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2024), *op., cit.,* p. 12.

Restando sulla questione delle violazioni, alla luce degli oltre 10.000 incidenti di fuga di dati l'anno, la PPC sta riconsiderando l'obbligo di segnalazione (art. 26.1 (ex art. 22.2, comma 1)) e notifica dell'avvenuta fuga dei titolari (art. 26.2 (ex 22.2, comma 2))[225]. Secondo le organizzazioni interessate, tutti questi obblighi rappresentano un onere eccessivo per le aziende; pertanto, è stato richiesto di modificare le modalità di applicazione, rimuovendo certe condizioni, in base al rischio di violazione[226].

Nella voce 3), si riflette sulle strategie da attuare in cooperazione con le entità competenti, in risposta all'aumento della domanda di utilizzo di dati sensibili nei settori della sanità, dell'istruzione, della prevenzione dei disastri e della protezione dei bambini. L'*Interim Summary* fa coincidere questo obiettivo con il bisogno di lasciare più libertà alle imprese di usufruire dei dati personali senza il consenso dell'interessato[227].
Nella nuova APPI, il principio del consenso è regolato principalmente dagli art. 18 (ex art. 16), 20 (ex art. 17) e 27 (ex art. 23), che presuppongono delle eccezioni in ogni settore. Tuttavia, nel parere della PPC non sarebbe opportuno riconoscere le eccezioni solo dal punto di vista della promozione dell'utilizzo, ma bisognerebbe riconoscerle anche da quello della protezione dei diritti dell'interessato[228]. Quindi, si suggerisce di stabilire nuove eccezioni, tenendo conto del grado di necessità sociale e dell'interesse pubblico, in quanto si ritiene che le eccezioni attuali siano difficili da applicare a tecnologie innovative come l'IA generativa[229].
Infine, l'ultimo commento si concentra sulla promozione di iniziative autonome nel settore privato: si prende in considerazione la possibilità di implementare la Valutazione dell'impatto sulla *privacy* (PIA), e il Responsabile della protezione dei dati (RDP).
Il PIA è una tecnica di gestione del rischio, che valuta in anticipo l'impatto che il trattamento dei dati ha sui diritti di *privacy* individuali, specialmente quando si tratta di attività che comportano la raccolta di dati personali. Sebbene in Giappone non sia un obbligo legale, ma venga solo menzionato nelle politiche di base, in Europa è obbligatoria nel caso in cui il trattamento, "*considerati la natura, l'oggetto, il contesto e le finalità del*

---

225 https://www.nishimura.com/sites/default/files/newsletters/file/data_protection_240802_en.pdf consultato il 08/11/2025. L'obbligo di segnalazione non è previsto nel caso di fornitura illecita di dati personali sensibili a terzi (art. 27.2).
226 COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2024), *op., cit.,* pp. 20-21.
227 *Ivi*, p. 22.
228 *Ivi*, p. 23.
229 https://www.nishimura.com/sites/default/files/newsletters/file/data_protection_240802_en.pdf consultato il 08/11/2025

trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35.1 del GDPR).

In merito al responsabile, l'APPI obbliga l'assegnazione di un soggetto autorizzato alla supervisione dei dipendenti e dei fiduciari delle imprese, ma con responsabilità e poteri decisamente inferiori rispetto al RDP (art. 24-25, ex artt. 21-22). Infatti, nel Regolamento europeo, egli supervisiona tutto il processo di trattamento, fungendo da consulente, intermediario con le autorità di controllo e garante dell'osservanza del GDPR, compreso lo svolgimento corretto della PIA (art. 39). Inoltre, deve possedere le conoscenze specialistiche in materia di protezione dei dati e il suo esercizio non deve comportare conflitti di interesse (art. 38.6).

Concludendo, il riepilogo sottolinea che è auspicabile incoraggiare sia l'adozione delle PIA che la nomina dei RDP, tenendo conto della fattibilità e delle conseguenze verso le organizzazioni coinvolte[230].

La Revisione Intermedia è stata divulgata dal 27 giugno al 29 luglio 2024. A seguito dei riscontri ricevuti dal pubblico, la PPC intende finalizzare le modifiche proposte. Sebbene non sia stato ancora annunciato un calendario ufficiale, si prevede che una bozza venga pubblicata nel 2025 ed entri in vigore nel 2027[231].

[230] COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2024), *op., cit.,* pp. 24-25.

[231] https://www.morihamada.com/sites/default/files/newsletters/newsletters/pdf/DATA%20SECURITY%20NEWSLETTER%20July%202024%20%28en%29.pdf consultato il 09/06/2025

Conclusioni

La ricostruzione storico-sociale e legislativa del Giappone in materia di *privacy* prima, e di protezione dei dati personali dopo, discussa nel corso della ricerca, si reputa che evidenzi un unico filo conduttore: il desiderio di stare al passo con le sfide della società digitale attraverso un processo di continuo rinnovamento che ha permesso al paese di confrontarsi con gli ordinamenti più avanzati a livello globale, senza mai rinunciare alle proprie radici culturali e giuridiche. Lo dimostra il fatto che l'ordinamento giapponese è passato da un modello condiviso di riferimento proprio della regione dell'Asia-Pacifico, a un sistema giuridico geograficamente lontano e apparentemente irraggiungibile, come quello europeo[232].

Il cammino verso ottenimento dell'adeguatezza non è stato privo di difficoltà e ha comportato anni di studio e revisioni. Basti pensare che la prima legge del 2003 non prevedeva né un'autorità regolatoria indipendente, né tantomeno una disciplina per il trasferimento transfrontaliero dei dati. Piuttosto, presentava dei fragili principi, aggravati dalla poca trasparenza e dalla limitata applicazione, in un sistema che chiedeva alle persone di fidarsi senza offrire prove concrete[233].

In questo senso, la Riforma del 2015 ha rappresentato un passaggio fondamentale per costituire un ordinamento più solido e maggiormente allineato al modello europeo, grazie alla creazione della Commissione per la protezione dei dati personali, all'estensione dell'applicabilità ai soggetti esteri, così come alle misure per il trattamento dei dati anonimizzati e sensibili e al rafforzamento delle sanzioni. Questa base legislativa e le successive Norme Supplementari hanno così consentito di raggiungere i criteri sufficienti per stipulare l'accordo di adeguatezza con l'Unione Europea[234], il cui obiettivo non era integrare le normative, bensì creare un sistema comune che permettesse di convivere e collaborare, lasciando spazio alle proprie specificità. In questo modo, il quadro di

[232] F. SERINI (2022), *op., cit.*, p. 191.
[233] G. GREENLEAF (2014), *op. cit.*, p. 263.
[234] In una dichiarazione del Comitato europeo per la protezione dei dati (EDPB) sul funzionamento della decisione di adeguatezza è stato stabilito di posticipare le revisioni ogni quattro anni, anziché due. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI (2023). *Statement 1/2023 on the first reviewof the functioning of the adequacy decision for Japan*, European Data Protection Board, p. 4.

adeguatezza europeo ha esercitato un'influenza positiva, che per il Giappone ha funzionato da incentivo al miglioramento della propria legislazione (*effetto Bruxelles*)[235].
A tal proposito, l'impegno verso il perfezionamento normativo è proseguito, non solo con il "*The Every-Three-Year Review*", previsto ogni tre anni, ma anche attraverso iniziative separate. La "*Digital Reform*", in particolare, ha unificato il settore pubblico e privato in un'unica legge, rinforzando i poteri di supervisione della PPC; ha operato per superare le imperfezioni della condivisione dei dati sensibili, come quelli medici e accademici; e ha ampliato gli obblighi di trasparenza e responsabilità per i titolari del trattamento.
Malgrado ciò, questi ambiziosi sforzi si scontrano tuttora con altre difformità con il Regolamento europeo. Le più significative riguardano il campo dei diritti dell'interessato: nell'APPI attuale non troviamo il "diritto alla portabilità dei dati", il "diritto esplicito di opposizione" e il "diritto all'oblio". Persiste anche la questione della profilazione automatizzata che, nonostante le raccomandazioni della PPC e l'aumento delle sanzioni a seguito del caso *Rikunabi*, rimane un nodo irrisolto. In più, vi sono le lacunosità nelle norme sul trattamento nei bambini, nelle figure responsabili della supervisione come l'RDP o di accertamenti come le PIA. Sul piano delle sanzioni invece, nonostante il recente invigorimento delle pene, il Giappone continua ad assumere un criterio meno severo rispetto al GDPR, preferendo raccomandazioni e misure correttive.
In riferimento al trasferimento di dati, infine, si può affermare che i grandi passi in avanti del Giappone fino ad oggi abbiano reso il quadro giuridico giapponese ormai equivalente a quello europeo. Le rimanenti diversità riguardano il meccanismo di "*opt-out*", che lascia eccessivi margini di discrezionalità, compromettendo la fiducia degli interessati, e la mancanza di appropriate precauzioni in assenza di una decisione di adeguatezza. In tali casi, il trasferimento transfrontaliero si basa sui requisiti stabiliti dalla PPC, che però non contemplano i trasferimenti effettuati nell'ambito di accordi internazionali per la cooperazione giudiziaria o relativi ai registri pubblici.
Su alcune di queste problematiche e su altre questioni emergenti, l'*Interim Summary*, in seno alla revisione triennale prevista per il 2025, ha mantenuto comunque aperto il dibattito con il pubblico, fornendo un'idea delle prossime proposte e analizzandone l'impatto nel lungo periodo.

[235] H. MIYASHITA (2020), *op., cit.*, pp. 1.

A detta di alcuni studiosi, la persistenza di tali discrepanze ha radici nella natura collettivistica giapponese, secondo cui la *privacy* in Giappone si fonda tradizionalmente sull'assunto che un individuo venga protetto come parte di un gruppo. Pertanto, è improbabile che la sensibilità giapponese sulla questione possa mai raggiungere i livelli occidentali[236].

Tuttavia, pur confermando la veridicità di questo pensiero, si ritiene che il percorso intrapreso dal Paese condurrà a un ulteriore riduzione del divario tra il modello giapponese ed europeo, consolidando il ruolo del Giappone come partner strategico nel panorama internazionale[237]. Sarà dunque essenziale che i futuri interventi normativi non si limitino esclusivamente a colmare le carenze attuali, ma mirino ad anticipare le sfide emergenti nella protezione dei dati, mantenendo un delicato equilibrio tra innovazione tecnologica e conservazione culturale.

[236] Y. ORITO, K. MURATA, (2005), *op., cit.*, p. 8. Sul punto si cita anche: "*But because privacy in Japan traditionally has been based heavily on the assumption that an individual will be protected as part of a group, the Japanese government sometimes may be less aggressive than other governments in extending privacy protection in new situations*". M. MIZUTANI, J. DORSEY, J. MOORE (2004), *op. cit.*, p. 127.

[237] Si rende noto che nel 2020 il Giappone ha formalizzato una decisione di adeguatezza con la Gran Bretagna, che ha recentemente rinnovato nel 2025. https://www.gov.uk/government/publications/uk-japan-data-adequacy-joint-statement/uk-japan-data-adequacy-joint-statement consultato il 12/06/2025

Bibliografia

ADAMS A., MURATA K., ORITO Y. (2009). *The Japanese Sense of Information Privacy*, AI & Soc, Vol. 24, 327-341.
https://doi.org/10.1007/s00146-009-0228-z

ADAMS A., MURATA K., ORITO Y. (2010). *The Development of Japanese Data Protection*, Policy & Internet, Vol. 2, No. 2, 95-126.
https://doi.org/10.2202/1944-2866.1038

AKIYAMA Mizuki, *Kojin jōhō hogohō minaoshi no gaiyō* (Panoramica della revisione della legge sulla protezione dei dati personali), National Diet Library, No. 1089, 2020.
秋山瑞季、個人情報保護法見直しの概要、国立国会図書館、号 1089、2020 年.
https://www.ndl.go.jp/jp/diet/publication/issue/2020/index.html

ALONGI A., POMPEI F. (2021). *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*, Cyber-Security-Defense.

ASAI T. (2018). *Japan Data Protection Law. A Practical Guide in Comparison With GDPR*, CreateSpace Independent Publishing Platform.

BARTL M., IRION K. (2017). *The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun*, Amsterdam.
https://ssrn.com/abstract=3099390

BENEDICT R. (1946). *The Chrysanthemum and the Sword: Patterns of Japanese Culture*, Houghton Mifflin, Boston.

BURRI M. (2022). *Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions: Implications for the Future EU-ASEAN Agreement*, Legal Issues of Economic Integration, No. 49, 149-168.
https://ssrn.com/abstract=3804975

CALDIROLA D. (2006). *Il diritto alla riservatezza*, Padova, Cedam.

CALIFANO L. (2018). *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, in *I profili del diritto Regole, rischi e opportunità nell'era digitale*, a cura di SCAFFARDI L., Giappichelli, Torino.
https://www.giappichelli.it/media/catalog/product/excerpt/9788892103405.pdf

CASALINI F., GONZÀLEZ J. L. (2019). *Trade and Cross Border Data Flows*, OECD Trade Policy Papers, No. 220, Parigi.
https://doi.org/10.1787/b2023a47-en

COLOMBO G. F. (2008). *Giappone*, in *Diritto dell'Asia Orientale,* a cura di CAVALIERI R., Venezia, Editrice Cafoscarina.

COLOMBO G. F. (2013). *Japan as a Victim of Comparative Law*, Michigan State International Law Review.
https://ssrn.com/abstract=2916156

CRISTÓBAL CISNEROS P. (2021). *The Economic Partnership Agreement between Japan and the European Union: analysis of the first years of life and prospects for the future*, Australian and New Zealand Journal of European Studies, Vol. 13, No. 2., 54-65.
https://doi.org/10.30722/anzjes.vol13.iss2.15605

DOI T. (1973). *The anatomy of dependence,* trad. di BESTER J., Kodansha International.

DRYSDALE P. (1988). *International Economic Pluralism: Economic Policy in East Asia and the Pacific*, Allen and Unwin, Sydney.

FABRIS F. (2009). *Il diritto alla privacy tra passato, presente e futuro*, Trieste, Tigor.
http://hdl.handle.net/10077/3394

FAHEY E., MANCINI I. (2023). *Cross-border data flows between the EU, Japan and the UK. A triangular relationship*, Keio Law Journal, No. 49, 61-69.
https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=AA1203413X-20230330-0061

GAMBINI M. (2013). *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*.

GLANCY D. (1979). *The Invention of the Right to Privacy*, Arizona Law Review, Vol. 21.

GREENLEAF G. (2003). *The APEC privacy initiative: "OECD Lite" for the Asia-Pacific?,* Privacy Law and Business, Vol. 71, pp. 16-18.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=510683

GREENLEAF G. (2009). *Five years of the APEC Privacy Framework: Failure or Promise?*, Computer Law & Security Report, Vol. 25, 28-43.
https://ssrn.com/abstract=2022907

GREENLEAF G. (2010). *Country Studies - B5 Japan*, in *Comparative Study on Different Approaches to New Privacy Challenges,* in *Particular in the Light of Technological Developments,* a cura di KORFF D., Commissione Europea, Directorate-General Justice, Freedom and Security.
https://ssrn.com/abstract=2025557

GREENLEAF G. (2014). *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford University Press.
https://doi.org/10.1093/acprof:oso/9780199679669.001.0001

GREENLEAF G. (2015). *Japan: Toward international standards - except for "big data",* Privacy Laws & Business International Report.
https://ssrn.com/abstract=2649556

GREENLEAF G. (2016). *Japan joins APEC-CBPRs: Does it matter?*, Privacy Laws & Business International Report, 18-21.
https://ssrn.com/abstract=2964499

GREENLEAF G. (2017). *2014-2017 Upgrade to Graham Greenleaf's Asian Data Privacy Laws. Trade and Human Rights Perspectives*, UNSW Law Research Series, Sydney. https://dx.doi.org/10.2139/ssrn.3000766

GREENLEAF G. (2018). *2017-2018 Further Update to Graham Greenleaf's Asian Data Privacy Law. Trade and Human Rights Perspectives*, UNSW Law Research Series, Sydney. https://ssrn.com/abstract=3285086

GREENLEAF G. (2018). *Japan: EU Adequacy Discounted*, Privacy Laws & Business International Report.
https://ssrn.com/abstract=3276016

GREENLEAF G. (2018). *Japan's Proposed EU Adequacy Assessment: Substantive Issues and Procedural Hurdles*, Privacy Laws & Business International Report, UNSW Law Research Series, Sydney.
https://ssrn.com/abstract=3219728

GREENLEAF G. (2018). *Questioning 'Adequacy' (Pt I) – Japan*, Privacy Laws & Business International Report.
https://ssrn.com/abstract=3096370

GUARDA P., BINCOLETTO G. (2023). *Diritto comparato della privacy e della protezione dei dati personali*, Milano, Ledizioni.

HARLAND J. (2004). *Japan's New Privacy Legislation: Are You Ready?*, Computer Law & Security Report, Vol. 20, No. 3, 200-203.
https://doi.org/10.1016/S0267-3649(04)00037-8

HENDRY J. (2019). *Understanding Japanese Society*, Routledge.

HIGASHIZAWA N., AIHARA Y. (2017). *Data Privacy Protection of Personal Information versus Usage of Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan),* Defense Counsel Journal, Vol. 84, No. 4.
https://www.iadclaw.org/assets/1/19/Data_Privacy_Protection_of_Personal_Information_Versus_Usage_of_Big_Data.pdf?228

HORIBE M. (1980). *Contemporary Privacy*, Tōkyō, 1980.

HORIBE Masao, *Nichi EU kan no jūbunsei sōgo nintei to chikyū kibo no jiyūna kojin dēta ryūtsūron* (La decisione di adeguatezza tra Giappone e UE e il desiderio di realizzare il libero flusso di dati personali su scala globale), Journal of Information and Communications Policy, 2020, Vol. 4, No. 2, 1-23.
堀部政男、日 EU 間の十分性相互認定と地球規模の自由な個人データ流通論、情報通信政策研究、巻 4、号 2、2020 年、pp. 1-23.
https://doi.org/10.24798/jicp.4.2_1

IASELLI M., GORLA S. (2015). *Storia della Privacy*, Lex et Ars, Roma.

ISHII K., KOMUKAI T. (2016). *A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K.*, 12th IFIP International Conference on Human Choice and Computers, United Kingdom. 86-105.
https://doi.org/10.1007/978-3-319-44805-3_8

ITO M. (1964). *Issues in the "After the Banquet" Decision*, trad. di BRADSHAW C. J., Jurist, No. 309, 1964, 47-51.

IZUMI Inoue, *Benesse kojin jōhō rōei mondai: An analysis of the Benesse Corporation Customer Data Leak* (Problema di fuga di informazioni personali di Benesse: Un'analisi della fuga di dati dei clienti della società Benesse), 2021, 110-118.

井上泉、ベネッセ個人情報漏えい問題： An analysis of the Benesse Corporation Customer Data Leak、2021 年、pp. 100-118.

https://doi.org/10.20664/jabesssb.1.0_100

JITSUHARA Takashi, *Kojin jōhō hogo hōsei to kenpō* (La legge e la Costituzione sulla protezione dei dati personali), Jōhō hōsei kenkyū, Vol. 12, 2022, 38-48.

實原隆志、個人情報保護法制と憲法、情報法制研究、巻 12、2022 年、pp. 38-48.

https://doi.org/10.32235/alis.12.0_038

KANEKO Keiko, *Ōbei ni okeru shingai tsūchi no jōkyō to Nihon he no shisa* (Notifica di violazione dei dati negli Stati Uniti e nell'UE e la sua lezione per l'operazione in Giappone), IPSJ SIG Technical Report, 2021.

金子啓子、欧米における侵害通知の状況と日本への示唆、情報処理学会研究報告、2021 年.

http://id.nii.ac.jp/1001/00209295/

KAZUMA Kobayashi, *GDPR ni miru Nihon ni okeru kojin jōhō toriatsukai to sono seisaku kadai* (Gestione delle informazioni personali in Giappone e relative questioni politiche secondo il GDPR), Chūō Gakuin Daigaku Shōgakubu, Vol. 37, No. 1, 2022, 17-22.

小林和馬、2022、GDPR に見る日本における個人情報取り扱いとその政策課題、中央学院大学商学部、巻 37、号 1、2022 年、pp. 17-22.

https://cgu.repo.nii.ac.jp/records/1911

KENT P. (1999). *Japanese perceptions of the "Chrysantemum and the Sword"*, Dialectical Anthropology, Vol. 24, No. 2, pp. 181-192.

https://www.jstor.org/stable/29790600

KIYOSHI Takechi, *Rikunabi jiken no sono go: Seifu ni yoru hōteki taiō wa ikani?* (Dopo il caso Rikunabi: Qual è la risposta legale del governo?), Toyama Daigaku Keizai Gakubu, Vol. 69, 2023, 69-94.

竹地潔、リクナビ事件のその後：政府による法的対応はいかに？、富山大学経済学部、巻 69、2023 年、pp. 69-94.
https://doi.org/10.15099/0002000005

KOBAYASHI Shintarō, *Kojin Jōhō Hogo Iinkai ni yoru ichigentekina seido un'yō e no kitai to kadai* (Aspettative e sfide per un funzionamento centralizzato del sistema da parte della Commissione per la Protezione delle Informazioni Personali), Chiteki Shisan Sōzō, Vol. 24, No. 16, 2016, 38-49.
小林慎太郎、個人情報保護委員会による一元的な制度運用への期待と課題、知的資産創造、巻 24、号 16、2016 年、pp. 38-49.
http://id.ndl.go.jp/bib/027764633

KOMUKAI T. (2020). *A Comparative Study of the Extraterritorial Enforcement of Data Protection Rules in the EU, US and Japan*, in *Global Privacy Law Review*, a cura di PEHLIVAN C. N., Wolters Kluwer, Vol. 1, No. 3, 180-185.

KUDO F., ARAI H., EMA A. (2020). *Ethical Issues Regarding the Use of AI Profiling Services for Recruiting: The Japanese Rikunabi Data Scandal*, arXiv.
https://doi.org/10.48550/arXiv.2005.08663

KUNER C. (2011). *Regulation of Transborder Data Flows under Data Protection and Privacy Law. Past, present and future*, OCSE Digital Economy Papers.
https://dx.doi.org/10.2139/ssrn.1689483

LAWSON C. (2006). Japan's New Privacy Act in Context, UNSW Law Journal, Vol. 29(2), 88-113.
https://www.researchgate.net/publication/297686355

MARCÉN A.G. (2021). *The New Personal Data Protection in Japan: Is It Enough?*, in *Media Technologies for Work and Play in East Asia: Critical Perspectives on Japan and the Two Koreas*, a cura di LEE. M., CHUNG P., Bristol University Press, Bristol.

MIYASHITA H. (2011). *The evolving concept of data privacy in Japanese law*, International Data Privacy Law, Vol. 1, No. 4, 229-238.
https://doi.org/10.1093/idpl/ipr019

MIYASHITA H. (2016). *The "right to be forgotten" and search engine liability*, Brussels Privacy Hub Working Paper, Vol. 2, No. 8.
https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N8.pdf

MIYASHITA H. (2019). *The impact of GDPR in Japan*, in *National Adaptations of the GDPR*, a cura di MC CULLAGH K., TAMBOU O., BOURTON S., Blogdroiteuropéen, 122-127.
https://hal.science/hal-03521416

MIYASHITA H. (2020). *EU-Japan Mutual Adequacy Decision*, Blogdroiteuropéen.
https://blogdroiteuropeen.com/wp-content/uploads/2020/06/miyashita-redo.pdf

MIYASHITA H. (2021). *Human-centric data protection laws and policies: A lesson from Japan*, Computer Law & Security Review, Elsevier, Vol. 40.
https://doi.org/10.1016/j.clsr.2020.105487

MIZUTANI M., DORSEY J., MOORE J. (2004). *The internet and Japanese conception of privacy*, Ethics and Information Technology, Vol. 6, 121-128.
https://doi.org/10.1023/B:ETIN.0000047479.12986.42

MONTI A. (2019*). Tutela della vita privata, protezione dei dati personali e privacy. Ambiguità semantiche e problemi definitori*, Diritto di Internet, Pacini Giuridica, 11-15.
https://www.researchgate.net/publication/333634491_Tutela_della_vita_privata_protezione_dei_dati_personali_e_privacy_Ambiguita_semantiche_e_problemi_definitori

MORI R., *Nihon no kojin jōhō hogo-hō kaisei no jōkyō* (Stato delle revisioni della legge giapponese sulla protezione dei dati personali), in *Pāsonaru dēta no rikatsuyō ni okeru gijutsu oyobi kakkokuhō seido no dōkō*, Eichi hōritsu jimusho, Vol. 55, No. 12, 2014, 1353-1360.

森亮二、日本の個人情報保護法改正の状況、パーソナルデータの利活用における技術および各国法制度の動向、英知法律事務所、巻 55、号 12、2014 年、pp. 1353-1360.
http://id.nii.ac.jp/1001/00106682/

NAKADA M., TAMURA T. (2005). *Japanese Conception of Privacy: An Intercultural Perspective*, Ethics and Information Technology, Vol. 7, 27-36.
https://doi.org/10.1007/s10676-005-0453-1

NIGER S. (2006). *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Le Monografie di Contratto e Impresa, Padova.

OKUBO T., et al. (2018). *Quantifying the EU-Japan Economic Partnership Agreement,* Institute for Economics Studies, Keio University.
https://www.econstor.eu/handle/10419/185439

ONODERA Y., TANAKA H., SHIMAMURA N. (2024). *Data Protection & Privacy 2024 - Japan*, Chambers and Partners, 367-387.
https://www.mhmjapan.com/en/publications/year/2024/90.html

ORITO Y., MURATA K., (2005). *Privacy Protection in Japan: Cultural Influence on the Universal Value*, Electronic proceedings of Ethicomp.
https://www.isc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf

ORITO Y., MURATA K. (2008). *Socio-cultural analysis of personal information leakage in Japan*, Journal of Information, Communication and Ethics in Society, Vol. 6, No. 2, 161-171.

ORITO Y., MURATA K. (2008). *Rethinking the concept of the right to information privacy: a Japanese perspective, Journal of Information, Communication and Ethics in Society, Vol. 6, No. 3, 233-245.*
https://doi.org/10.1108/14779960810916237

OROFINO M. (2018). *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, a cura di PANELLA L., Editoriale Scientifica, 245-268.
https://hdl.handle.net/2434/954514

ORTOLANI A. (2011), *Giappone (diritto moderno)*, Digesto delle discipline privatistiche, Torino, 435-450.
https://www.academia.edu/1169476/Giappone_diritto_moderno_

PAGANO R. (1986). *La tutela dei dati personali. Evoluzione delle legislazioni europee e stato del dibattito,* Informatica e diritto, 67-94.

PARDIEK A. (2023). *Privacy Matters: Data Breach Litigation in Japan*, Washington International Law Journal.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4514628

PEHLIVAN C. N. (2020). After the Banquet and Beyond: Privacy and Data Protection in Japan, in *Global Privacy Law Review*, Wolters Kluwer, Vol. 1, No. 3, 126-130.
https://ssrn.com/abstract=4364953

PERARO C. (2021). *Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'Unione europea verso Paesi terzi*, Ordine Internazionale e Diritti Umani.
http://hdl.handle.net/10446/187922

RAUL A. C. (2022). *The Privacy, Data Protection and Cybersecurity Law Review*, Law Business Research Ltd, Sidley.
https://www.sidley.com/en/insights/publications/2022/11/the-privacy-data-protection-and-cybersecurity-law-review

REPETA L. (2015). *Personal Information, Media Control, and Government Power - Legislative Battles in Japan, 1999-2003*, Meiji Law Journal.
http://hdl.handle.net/10291/17286

RODOTÀ S. (1974). *La "privacy" tra individuo e collettività*, in *Politica del diritto, 545-563.*

RODOTÀ S. (2014). *Il mondo della rete, quali diritti, quali vincoli,* Laterza.

SAKO Y., KAWANAKA N. (2017). *Data Security in Japan: New Cross-Border Data Transfer Rule*, K&L Gates.
https://files.klgates.com/files/publication/12246b9b-1f8d-4404-aacb-3bf1dd855095/presentation/publicationattachment/a86adc7a-7e0c-4046-bbb8-49095395eae8/privacy_data_protection_and_information_management_alert_062017.pdf

SATO K. (1970), *The Constitutional Position on Privacy. A Comparative Study of Japan and the United States* (Privacy no Kenri (Sono Kohotekisokumen) no Kenpotekikousatsu), Hogaku Ronso, Vol. 86.

SAPIR A., TERZI A., CHOWDHRY S. (2018). *The EU - Japan Economic Partnership Agreement*, Commissione Europea, Directorate-General for External Policies of the Union, Bruxelles.
https://data.europa.eu/doi/10.2861/658535

SCHWARTZ P. M. (2019). *Global Data Privacy: The EU Way*, New York University Law Review, Vol. 94, 772-817.
https://ssrn.com/abstract=3468554

SEKI Keiichirō, *Kojin jōhō hogohō to sono 10-nenburi no kaisei ni tsuite* (Riguardo la legge sulla protezione dei dati personali e il suo primo emendamento in 10 anni), Chiteki shisan sōzō, 2015.
関啓一郎、個人情報保護法とその 10 年ぶりの改正について、知的資産創造、2015 年.

SERINI F. (2022). *La protezione dei dati personali tra Giappone e Unione europea*, Roma, Aracne.

SHINPO Fumio, *Kaisei kojin jōhō hogohō no ronten* (Punti di discussione riguardo la revisione della legge giapponese sulla protezione delle informazioni personali del 2015), Kenpō Gakkai, Kenpō Kenkyū, No. 48, 2016, 29-55.
新保史生、改正個人情報保護法の論点、憲法学会、憲法研究、号 48、2016 年、pp. 29-55.
http://id.ndl.go.jp/bib/027568999

SHISHIDO George, *Kensaku kekka no sakujo o meguru saibanrei to kongo no kadai* (Giurisprudenza sulla rimozione dei risultati di ricerca e le sfide future), Jōhō Hōsei Kenkyū, Vol. 1, 2017, 45-54.
宍戸常寿、検索結果の削除をめぐる裁判例と今後の課題、情報法制研究、巻 1、2017 年、pp. 45-54.
https://doi.org/10.32235/alis.1.0_45

SHIZAWA Masumi, *Puraibashī to jiko jōhō ni kansuru kōsatsu: `Benesse kojin jōhō rōei jiken' (sai han hira 29-10-23 banji 2351-7) wo chūshin ni* (Riflessioni sulla privacy e sulle informazioni personali: studio dettagliato sul "caso Benesse" (Corte Suprema, 23 ottobre 2016, 2351-7), Tōyō Daigaku Gendai Shakai Sōgō Kenkyūsho, Vol. 17, 2020, 123-130.
始澤真純、プライバシーと自己情報に関する考察：「ベネッセ個人情報漏えい事件」（最判平 29・10・23 判時 2351・7）を中心に、東洋大学現代社会総合研究所、巻 17、2020 年、pp. 123-130.
https://doi.org/10.34375/gensoken.2019.17_123

SOLOVE D. J. (2006). *A Brief History of Information Privacy Law*, Proskauer On Privacy, PLI.
https://ssrn.com/abstract=914271

SPINIELLO C. (2018). *(Sche)Dati. Il diritto alla protezione dei dati personali nella legislazione europea*, Democrazia e Sicurezza.

SUDA Y. (2020). *Japan's Personal Information Protection Policy Under Pressure, Asian Survey: The Japan-EU Data Transfer Dialogue and Beyond*, Vol. 60, No. 3, 510-533.

SUGANO T. (1970). *Privacy in Japan,* The Comparative and International Law Journal of Southern Africa, Vol. 3, No. 2, 225–227.
http://www.jstor.org/stable/23240786

TAN J.G. (2008). *A Comparative Study of the APEC Privacy Framework*: *A new voice in the data protection dialogue*?, Asian Journal of Comparative Law, Vol. 3, 1-44.

TOMOYASU Hiroshi, *Shōsetsu 'Utage no ato' to puraibashī* (Il romanzo "After the banquet" e la privacy), Bunkyōdaigaku, Jōhō kenkyū, Vol. 18, 1997, pp. 105-123.
小説 『宴のあと』とプライバシー、文教大学、情報研究、巻 18、 1997 年、 pp. 105-123.
https://bunkyo.repo.nii.ac.jp/records/3454

URATA S. (2007). *Japan's FTA Strategy and Free Trade Area of Asia Pacific (FTAAP)*, PECC/ABAC Joint Study on Free Trade Area of the Asia Pacific.
https://www.pecc.org/resources/trade-and-investment-1/2038-japans-fta-strategy-and-free-trade-area-of-asia-pacific-ftaap

WALTERS R., TRAKMAN L., ZELLER B. (2019). *Data Protection Law. A Comparative Analysis of Asia-Pacific and European Approaches*, Springer.

WANG F. (2020). *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, Harvard Journal of Law & Technology, Vol. 33, No. 2, 661-690.
https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf

WARREN S., BRANDEIS L. (1890). *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, 193-220.
https://doi.org/10.2307/1321160

WESTIN A. (1967). *Privacy and freedom*, New York, Atheneum.

YAMAMOTO Tatsuhiko, *Nihon no kojin jōhō hogo hōsei no genzai-mirai* (Presente e futuro della legge giapponese sulla protezione dei dati personali), Jōhō shisutemu gakkaishi, Vol. 17, No. 1, 2020, 45-60.

山本龍彦、日本の個人情報保護法制の現在・未来、情報システム学会誌、 巻 17、 号 1、2021 年、pp. 45-60.

https://doi.org/10.19014/jissj.17.1_45

ZELLER B. et al. (2018). *The Right to be Forgotten: The EU and Asia Pacific Experience (Australia, Indonesia, Japan and Singapore),* European Human Rights Law Review, Vol. 23. https://ssrn.com/abstract=3320860

Fonti giurisprudenziali

ALTA CORTE DI TOKYO, *Heisei nijūhachinen shichigatsu jūninichi kettei* (Decisione del 12 luglio 2016), Hanreijiho, No. 2318, p. 24.

東京高等裁判所、平成 28 年 7 月 12 日決定、判例時報、号 2318、2016 年、p. 24

https://www.cc.kyoto-su.ac.jp/~suga/hanrei/183-2.html

ALTA CORTE DI TOKYO, *Heisei nijūkyūnen sangatsu nijūichinichi hanketsu* (Sentenza del 21 marzo 2017), Hanreijiho, No. 974.

東京高等裁判所、平成 29 年 3 月 21 日判決、号 974、2017 年.

https://www.courts.go.jp/app/files/hanrei_jp/028/087028_hanrei.pdf

CORTE DI GIUSTIZIA EUROPEA, *Sentenza della Corte (Grande Sezione) del 6 ottobre 2015. Maximillian Schrems contro Data Protection Commissioner*, European Union Law, Bruxelles.
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:62014CJ0362

CORTE DI GIUSTIZIA EUROPEA, *Sentenza della Corte (Grande Sezione) del 16 luglio 2020. Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, European Union Law, Bruxelles.
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62018CJ0311

TRIBUNALE DISTRETTUALE DI SAITAMA, *Heisei nijūnananen jūnigatsu nijūnichi hanketsu* (Sentenza del 22 dicembre 2015), Hanreijiho, Vol. 2282, p. 82.

埼玉地方裁判所、平成 27 年 12 月 22 日判決、判例時報、巻 2282、2015 年、p. 82.

TRIBUNALE DISTRETTUALE DI TOKYO, *Shōwa sanjūkyūnen kyūgatsu nijūhachinichi hanketsu* (Sentenza del 28 settembre 1964), Hanreishū, Vol. 15, No. 9, p. 2317.

東京地方裁判所、昭和 39 年 9 月 28 日判決、判例集、巻 15、号 9、1964 年、p. 2317.

https://www.cc.kyoto-su.ac.jp/~suga/hanrei/10-1.html

CORTE SUPREMA DEL GIAPPONE, *Shōwa yonjūyon'nen jūnigatsu nijūyon'nichi hanketsu* (Sentenza del 24 dicembre 1969), Keishū, Vol. 23, No. 12, p. 1625.

最高裁判所大法廷、昭和 44 年 12 月 24 日判決、刑集、巻 12、号 12、1969 年、p. 1625.

https://www.courts.go.jp/app/hanrei_jp/detail2?id=51765

CORTE SUPREMA DEL GIAPPONE, *Heisei nijūkyūnen ichigatsu sanjūichinichi kettei* (Decisione del 31 gennaio 2017), Hanreijiho, No. 45.

最高裁判所大法廷、平成 29 年 1 月 31 日決定、号 45、2017 年.

https://www.courts.go.jp/app/hanrei_jp/detail4?id=86482

CORTE SUPREMA DEL GIAPPONE, *Heisei nijūkyūnen jūgatsu nijūsannichi hanketsu* (Decisione del 23 ottobre 2017), Hanreijiho, No. 1892.

最高裁判所大法廷、平成 29 年 10 月 23 日判決、号 1892、2017 年.

https://www.retio.or.jp/wp-content/uploads/2024/12/1184.pdf

Sitografia

APEC (2004). *APEC Privacy Framework*, Santiago. https://www.apec.org/docs/default-source/press/newsrelease/2004/04_amm_014rev1.pdf consultato il 01/10/2024

APEC (2010). *Accountability Agent Apec Recognition Application.* https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-AccountabilityAgentApplication.pdf consultato il 01/10/2024

APEC (2011). *APEC-CBPR – Policy, Rules and Guidelines*, San Francisco. https://mddb.apec.org/documents/2011/ecsg/ecsg2/11_ecsg2_012.pdf consultato il 01/10/2024

APEC (2015). *APEC Privacy Framework*, Digital Economy Steering Group. https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015) consultato il 01/10/2024

APEC (2019). *APEC at 30: A Region in Constant Change*, APEC Regional Trends Analysis, Singapore. https://www.apec.org/publications/2019/05/apec-regional-trends-analysis---apec-at-30 consultato il 03/10/2024

APEC (2019). Benefits of the APEC Cross-Border Privacy Rules – Protecting Information, Driving Growth, Enabling Innovation. http://cbprs.org/wp-content/uploads/2019/05/Benefits-of-CBPR-System-Guide_Jan-2019_FINAL.pdf consultato il 11/10/2024

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI (2023). *Statement 1/2023 on the first reviewof the functioning of the adequacy decision for Japan*, European Data Protection Board.

https://www.edpb.europa.eu/system/files/2023-07/edpb_statement_202301_statement_on_japan_adequacy_review_en.pdf consultato il 11/06/2025

COMMISSIONE EUROPEA (2000). *Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti*, European Union Law, Bruxelles.
http://data.europa.eu/eli/dec/2000/520/oj consultato il 28/03/2025

COMMISSIONE EUROPEA (2016). *Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy*, European Union Law, Bruxelles.
http://data.europa.eu/eli/dec_impl/2016/1250/oj consultata il 01/04/2025

COMMISSIONE EUROPEA (2019). *Decisione di esecuzione (UE) 2019/419 della Commissione, del 23 gennaio 2019, a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio per quanto riguarda la protezione adeguata dei dati personali da parte del Giappone a norma della legge sulla protezione delle informazioni personali*, European Union Law, Bruxelles.
http://data.europa.eu/eli/dec_impl/2019/419/oj consultato il 19/03/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2016). *Amended Act on the Protection of Personal Information (Tentative Translation)*.
https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf consultato il 05/09/2024

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2016). *Enforcement Rules for the Act on the Protection of Personal Information (Tentative translation)*.
https://www.ppc.go.jp/files/pdf/PPC_rules.pdf consultato il 25/02/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2016). *APEC-CBPR Certification – Let's Think About It!.*
https://www.ppc.go.jp/files/pdf/CBPR_lets_think_about_it.pdf consultato il 22/12/2024

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2017). *Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information*, Towards Balanced Promotion of Personal Data Utilization and Consumer Trust.
https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf consultato il 02/10/2024

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2018). *Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision*.
https://www.ppc.go.jp/files/pdf/supplementary_rules.pdf consultato il 21/05/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019). *Act on the Protection of Personal Information "The Every-Three-Year Review" Outline of the System Reform.*
https://www.ppc.go.jp/files/pdf/APPI_The_Every_Three_Year_Review_Outline_of_the_System_Reform.pdf consultato il 23/05/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2019). *Act on the Protection of Personal Information "The Every-Three-Year Review" Outline of the System Reform (Main Points).*
https://www.ppc.go.jp/files/pdf/The_Every_Three_Year_Review_of_the_APPI_Outline_of_the_System_Reform_main_points.pdf consultato il 23/05/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI, *Kojin jōhō no hogo ni kansuru hōritsu dai yonjūnijō dai ichikō no kitei ni motozuku kankokutō ni tsuite* (Raccomandazioni, ecc., ai sensi dell'articolo 42, comma 1, della Legge sulla protezione dei dati personali), 2019.
個人情報保護委員会、個人情報の保護に関する法律第 42 条第 1 項の規定に基づく勧告等について、2019 年.

https://www.ppc.go.jp/files/pdf/190826_houdou.pdf consultato il 30/05/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI (2020). *Amended Act on the Protection of Personal Information (Tentative Translation)*.
https://www.ppc.go.jp/files/pdf/APPI_english.pdf consultato il 23/05/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI, *Kojin jōhō no hogo ni kansuru hōritsu ni tsuite no gaidorain ni kansuru Q&A* (Domande e risposte relative alle linee guida della Legge sulla protezione dei dati personali), 2020.
個人情報保護委員会、「個人情報の保護に関する法律についてのガイドライン」 に関するＱ＆Ａ、2020 年.
https://www.ppc.go.jp/files/pdf/2506_APPI_QA.pdf consultato il 01/06/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI, *Dejitaru shakai no keisei o hakaru tame no kankei hōritsu no seibi ni kansuru hōritsu* (Legge per il consolidamento delle leggi correlate alla formazione di una società digitale), 2021.
個人情報保護委員会、デジタル社会の形成を図るための関係法律の整備に関する法律、2021 年.
https://www.ppc.go.jp/files/pdf/seibihou.pdf consultato il 01/06/2025

COMMISSIONE PER LA PROTEZIONE DEI DATI PERSONALI, *Kojin jōhō hogohō - iwayuru san'nen goto minaoshi ni kakaru kentō no chūkan seiri* (Legge sulla protezione dei dati personali - Riepilogo intermedio delle considerazioni relative alla revisione triennale), 2024.
個人情報保護委員会、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、2024 年.
https://www.ppc.go.jp/files/pdf/chukanseiri_honbun_r6.pdf consultato il 02/12/2024

GOVERNO DEL GIAPPONE (1993). *Unfair Competition Prevention Act (Act No. 47 of May 19, 1993)*, Japanese Law Translation.

https://www.japaneselawtranslation.go.jp/en/laws/view/83 consultato il 06/06/2024

GOVERNO DEL GIAPPONE (2003). *Act on the Protection of Personal Information (Act No. 57 of May 30, 2003)*, Japanese Law Translation.
https://www.japaneselawtranslation.go.jp/en/laws/view/130 consultato il 20/07/2024

GOVERNO DEL GIAPPONE (2003). *Act for Establishment of the Information Disclosure and Personal Information Protection Review Board (Act No. 60 of 2003)*, e-Gov.
https://laws.e-gov.go.jp/law/415AC0000000060 consultato il 20/07/2024

GOVERNO DEL GIAPPONE (2003). *Act concerning the Preparation of Related Laws for the Enforcement of the Act concerning the Protection of Personal Information Held by Administrative Organs (Act No. 61 of 2003)*, The House of Representatives.
https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/15620030530061.htm consultato il 20/07/2024

GOVERNO DEL GIAPPONE (2003). *Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order No. 507 of December 10, 2003)*, Japanese Law Translation.
https://www.japaneselawtranslation.go.jp/en/laws/view/2617 consultato il 20/07/2024

GOVERNO DEL GIAPPONE (2013). *Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of May 31, 2013)*, Japanese Law Translation.
https://www.japaneselawtranslation.go.jp/en/laws/view/2755

GOVERNO DEL GIAPPONE (2021). *Act on the Protection of Personal Information (Partly unenforced) (Act No. 57 of 2003)*, Japanese Law Translation.
https://www.japaneselawtranslation.go.jp/en/laws/view/4241 consultato il 02/06/2025

FEDERAZIONE GIAPPONESE DEGLI ORDINI DEGLI AVVOCATI (2022). *Special Report on Important Matters after the Release of the List of Issues (CCPR/C/JPN/QPR/7) - Six Digital Reform-Related Laws*, Federation Japan Bar Association (JFBA).
https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCCPR%2FCSS%2FJPN%2F50080&Lang=en consultato il 07/06/2025

PARLAMENTO EUROPEO (1995). *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, European Union Law, Bruxelles.
http://data.europa.eu/eli/dir/1995/46/oj consultato il 22/03/2025

PARLAMENTO EUROPEO (2016). *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, European Union Law, Bruxelles.
http://data.europa.eu/eli/reg/2016/679/oj consultato il 08/04/2025

STRATEGIC HEADQUARTERS (2014). *Policy Outline of the Institutional Revision for Utilization of Personal Data,* Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society.
https://japan.kantei.go.jp/policy/it/20140715_2.pdf consultato il 20/02/2025

TESSORE L. C. (2024), *Diritto alla privacy: dalle origini ai giorni nostri*, Studio Cataldi, https://www.studiocataldi.it/articoli/47042-diritto-alla-privacy-dalle-origini-ai-giorni-nostri.asp consultato il 08/09/2024

UFFICIO DEL GABINETTO DEL GIAPPONE (2018). *Comprehensive and Progressive Agreement for Trans-Pacific Partnership – Chapter 14: Electronic Commerce*.
https://www.cas.go.jp/jp/tpp/tppinfo/kyotei/tpp_text_en/pdf/14.Electronic_Commerce.pdf consultato il 17/04/2025

UNIONE EUROPEA (2001). *An Action Plan for EU-Japan Cooperation*, European Union–Japan Summit, Bruxelles.
https://japan.kantei.go.jp/koizumispeech/2001/1208eu_kodo_e.pdf consultato il 15/11/2025

UNIONE EUROPEA (2018). *Accordo tra l'Unione europea e il Giappone per un partenariato economico*, European Union Law, Bruxelles.
http://data.europa.eu/eli/agree_internation/2018/1907/2022-02-01 consultato il 15/03/2015

UNIONE EUROPEA (2018). *Accordo di partenariato strategico tra l'Unione europea e i suoi Stati membri, da una parte, e il Giappone, dall'altra*, European Union Law, Bruxelles.
http://data.europa.eu/eli/agree_internation/2018/1197/oj consultato il 15/03/2015

https://www.jreast.co.jp/information/aas/20151126_torimatome.pdf consultato il 07/01/2025

https://www.soumu.go.jp/main_content/000441469.pdf consultato il 09/01/2025

https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_17_1880 consultato il 03/05/2025

https://ec.europa.eu/commission/presscorner/detail/it/ip_18_5433 consultato il 14/05/2025

https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf consultato il 19/05/2025

https://www.ppc.go.jp/files/pdf/press_betten1.pdf consultato il 23/05/2025

https://www.tmi.gr.jp/eyes/blog/2024/16304.html?utm_source consultato il 28/05/2025

https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan consultato il 01/06/2025

https://www.amt-law.com/en/insights/others/publication_0029311_en_001/ consultato il 01/06/2025

https://www.ppc.go.jp/files/pdf/seibihouan_gaiyou.pdf consultato il 07/06/2025

https://www.ppc.go.jp/files/pdf/seibihou_gaiyou.pdf consultato il 07/06/2025

https://inplp.com/latest-news/article/hird-amendment-of-the-japanese-privacy-law-amendment-based-on-the-digital-arrangement-act/ consultato il 07/06/2025

https://www.sangiin.go.jp/japanese/ugoki/r3/210512.html consultato il 07/06/2025

https://www.ppc.go.jp/files/pdf/chukanseiri_gaiyo_r6.pdf consultato il 05/06/2025

https://www.globalcompliancenews.com/2024/08/05/japan-personal-data-protection-commission-announces-interim-report-of-triennial-review/ consultato il 05/06/2025

https://www.hoganlovells.com/en/publications/interim-report-on-the-revision-of-the-act-on-the-protection-of-personal-information consultato il 08/06/2025

https://www.nishimura.com/sites/default/files/newsletters/file/data_protection_240802_en.pdf consultato il 08/11/2025

https://www.morihamada.com/sites/default/files/newsletters/newsletters/pdf/DATA%20SECURITY%20NEWSLETTER%20July%202024%20%28en%29.pdf consultato il 09/06/2025

https://www.gov.uk/government/publications/uk-japan-data-adequacy-joint-statement/uk-japan-data-adequacy-joint-statement consultato il 12/06/2025