# Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti

*di Giulia Formici*

**Abstract: "Identification" systems and biometric data: a new challenge for Legislators and Courts** – The article examines different 'identification' systems and the legal problems arising from the use of sensitive data, such as biometric data. The need to strike a balance between, on the one hand, good governance and correct identification (for security reasons as well as for the efficient allocation of public services and resources) and, on the other hand, the right to privacy and data protection, is at the centre of the present contribution, which aims to analyse the Indian Supreme Court so-called Aadhaar Judgement, the French jurisprudence about the fichier TES and the Belgian legislation about Electronic Identity Cards.

**Keywords:** Biometric data; Identification systems; Privacy; Aadhaar project; Fichier TES.



## 1. Premessa: le potenzialità dei sistemi di riconoscimento fondati sui dati biometrici e i rischi per riservatezza e protezione dei dati

"Identity is inseparable from the human personality. An identity is a statement of who an individual is. Our identities define who we are. They express what we would wish the world to know us as"[1]: con queste parole del Giudice D. Chandrachud, viene messa in evidenza l'unicità e la complessità del concetto di 'identità'; questa, proprio per il suo intrinseco legame con la persona, assume rilievo sotto il profilo antropologico, filosofico, sociologico ma anche giuridico e delle attività svolte dalle pubbliche autorità. Con riferimento a questi due ultimi ambiti, tale termine è poi spesso associato a quello di 'riconoscimento'[2], ovvero l'insieme di procedure (di varia natura, come si avrà modo di vedere) con le quali viene associata ad un soggetto una determinata identità. Questi meccanismi, che possono sembrare scontati o dal semplice funzionamento, soprattutto alle nostre latitudini, rivelano invece, di fronte ad uno studio più attento, tutta la loro complessità e la difficoltà di radicarsi in diverse realtà giuridiche[3].

[1] Dissenting Opinion, Giudice D. Chandrachud, *Justice Puttaswamy v. Union of India*, sentenza del 26 settembre 2018 (D.N. 35071/2012), Corte Suprema indiana, par. 179.

[2] Merita sin da ora precisare che il termine 'riconoscimento' è stato appositamente utilizzato per indicare, in senso generico, le operazioni di associazione identità-soggetto. Tale scelta è volta ad evitare possibili confusioni con i termini di 'identificazione' e 'verifica', qui intesi in senso tecnico, che delineano invece specifiche modalità di riconoscimento.

[3] Come si vedrà, la problematica dell'attribuzione ad un soggetto di una determinata identità è realmente sentita in determinati ordinamenti e crea disagi e malfunzionamenti sotto il

ISSN: 2037-6677

In questo specifico contesto, il progresso tecnologico rappresenta una risorsa di impareggiabile valore, consentendo di creare mezzi di riconoscimento innovativi e sofisticati, fondati, in misura ancora più ampia rispetto al passato, sull'utilizzo di dati 'personalissimi' e dal carattere unico: i dati biometrici. Questi ultimi, infatti, seguendo la definizione più recente del legislatore europeo, sono descritti come i "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici"[4]. Rientrano dunque in questa categoria, a titolo di mero esempio, le impronte digitali, la scansione dell'iride, la struttura vascolare della mano o quella della retina, le caratteristiche della voce, la struttura del volto.

Benché alcune forme di riconoscimento mediante dati biometrici abbiano origini storiche risalenti[5], è proprio nello scorso secolo e ancor più in quello attuale, che, grazie all'evoluzione tecnico-scientifica, l'utilizzo di questa particolare forma di determinazione dell'identità ha vissuto – e sta vivendo – la sua massima espansione, coprendo una grande vastità di scopi e di ambiti di applicazione. A determinarne il successo e l'impiego su larga scala sono le caratteristiche proprie di questi dati: l'unicità, l'universalità, la facile "catturabilità" e utilizzo, nonché la permanenza (sebbene, è bene precisarlo sin da ora, con qualche eccezione)[6]. Il nostro corpo dunque è divenuto una vera e propria chiave di accesso, una password di riconoscimento.



profilo della corretta ed efficiente gestione dei servizi pubblici o del mantenimento della pubblica sicurezza. In Africa ad esempio l'identificazione dei cittadini rappresenta una sfida estremamente attuale, considerata la vasta estensione territoriale e la presenza di ampie zone rurali in cui le autorità statali difficilmente riescono ad arrivare. Il progetto ID4Africa è un chiaro segnale dell'importanza, per i Governi di questo continente, dell'attribuzione di una identità giuridica ai propri cittadini: "ID4Africa was motivated by the need to promote legal identity for all in Africa (consistent with Sustainable Development Goal 16.9) and to empower individuals to claim their rights and to benefit from the fruits of development", www.id4africa.com/.

[4] Art. 4, co. 1, n. 14), General Data Protection Regualtion (GDPR), Reg. UE 679/2016.

[5] Nel 1882, ad esempio, nelle carceri parigini venne elaborato da Alphonse Bertillon un sistema di riconoscimento scientifico biometrico, fondato sulla rilevazione e annotazione delle misure corporee e delle caratteristiche fisiche dei carcerati. Per una analisi approfondita sul tema della biometria, come scienza che determina l'identità di un individuo mediante l'analisi di specifici elementi fisici o comportamentali, si rimanda a: S. Amato, S. Cristofari, S. Raciti, *Biometria: i codici a barre del corpo*, Torino, 2013.

[6] Non si può infatti parlare di una assoluta infallibilità dei sistemi di riconoscimento biometrici: si sono rilevati casi in cui la procedura identificativa presenta margini di errore a causa di mutamenti delle parti del corpo interessate, legate talvolta a determinate malattie (secchezza dell'epidermide, assottigliamento delle creste papillari, deterioramento dei polpastrelli, mutamento della struttura retinale dovuta a forme gravi di diabete, glaucoma, pressione alta). Per approfondimenti sul punto: J. Wayman, A. Jain, D. Maltoni, D. Maio (eds), *Biometric Systems*, London, 2005. Si vuole già da ora evidenziare comunque come la mancata identificazione o riconoscimento di un soggetto mediante l'uso dei propri dati biometrici possa causare gravi problemi e avere conseguenze estremamente impattanti sulla vita dell'individuo: qui basti pensare al caso in cui ad un soggetto venga negato l'accesso ad un luogo o la concessione di un sussidio statale perché le proprie impronte non corrispondono a quelle contenute nel documento d'identità.

Le enormi potenzialità dell'uso dei dati biometrici e la loro duttilità[7] non sono certamente sfuggite alle grandi aziende e agli attori privati che hanno usato questi dati personalissimi per consentire agli utenti l'accesso a determinati servizi o l'attivazione di dispositivi elettronici, o ancora per lo sviluppo di programmi di assistenza virtuali attivabili mediante riconoscimento vocale, sfruttando sistemi di Intelligenza Artificiale e Machine-Learning. Molti datori di lavoro si propongono di utilizzare i dati biometrici per stabilire univocamente l'identità dei dipendenti presenti sul luogo di lavoro, mentre gli istituti bancari fanno sempre più uso di questi sistemi per individuare con certezza il soggetto avente accesso ad uno specifico luogo.

Accanto a questi attori privati, tuttavia, anche le autorità pubbliche hanno preso consapevolezza dell'importanza del riconoscimento biometrico, sul versante della sicurezza pubblica o nazionale, delle indagini penali, della lotta al crimine, anche con finalità antiterroristiche[8] o di controllo delle frontiere, oltre che per incrementare l'efficiente allocazione delle risorse e una corretta gestione dei servizi pubblici.

Ma i possibili campi di sviluppo e di applicazione di sistemi di riconoscimento fondati sui dati biometrici sono estremamente ampi e adattabili alle più disparate realtà: non è un caso che molti progetti umanitari statali o internazionali, coinvolgenti sia soggetti pubblici che privati e ONG, abbiano alla base proprio l'implementazione di meccanismi di determinazione biometrica dell'identità di individui a rischio, richiedenti asilo o da utilizzare in situazioni di emergenza umanitaria[9].



[7] "With the pronounced need for robust human recognition techniques in critical applications such as secure access control, international border crossing and law enforcement, biometrics has positioned itself as a viable technology that can be integrated into large-scale identity management systems. Biometric systems operate under the premise that many of the physical or behavioral characteristics of humans are distinctive to an individual, and that they can be reliably acquired via appropriately designed sensors and represented in a numerical format that lends itself to automatic decision-making in the context of identity management. Thus, these systems may be viewed as pattern recognition engines that can be incorporated in diverse markets", in A. Jain, P. Flynn, A. Ross, *Handbook of biometrics*, New York, 2008, 7.

[8] Si pensi alle più recenti e innovative tecniche di *face recognition*, che permettono di riconoscere i soggetti mediante lo studio dei tratti somatici del viso. Merita rilevare sin da ora come questi sistemi identificativi basati sui dati biometrici spesso necessitino di software o sistemi di Intelligenza Artificiale in grado di gestire, comparare e collegare una mole di informazioni e dati vastissima. Per una analisi tecnica approfondita del tema, si legga tra gli altri: P. Campisi (ed), *Security and Privacy in Biomtrics*, London, 2013.

[9] L'enorme diffusione di sistemi identificativi basati sui dati biometrici nel settore umanitario è testimoniata da svariati progetti: nel 2015, l'UNCHR (Ufficio dell'Alto Commissario delle Nazioni Unite per i Rifugiati) ha avviato il *Biometric Identity Management System* (BIMS), finalizzato alla raccolta e utilizzo di dati biometrici per individuare univocamente i soggetti beneficiari di contributi cd. *cash-based* rivolti a rifugiati o persone bisognose nonché per poter iniziare procedure formali di richiesta di asilo per soggetti privi di documenti identificativi. Ciò allo scopo di meglio coordinare una corretta ed efficiente distribuzione degli aiuti, riducendo i rischi di erronea allocazione delle risorse. Si legga al proposito: UNHCR Innovation Service, *Using biometrics to bring assistence to refugees in Jordan*, 30 agosto 2016, www.unhcr.org/innovation/using-biometrics-bring-assistance-refugees-jordan/. È importante rimarcare come UNCHR e varie altre organizzazione umanitarie, come Oxfam, siano consapevoli dei rischi a cui l'utilizzo di queste tecniche espone i soggetti sottoposti e della

Di fronte a tutte queste applicazioni e positive potenzialità, lo sguardo del giurista deve però essere estremamente attento, cogliendo anche la delicatezza e i rischi connessi allo sfruttamento di tali sistemi; i pericoli risiedono proprio nei richiamati punti di forza di cui i dati biometrici sono caratterizzati: l'unicità, l'univocità, l'insostituibilità e irripetibilità. Sono queste qualità, infatti, che impediscono di mutare o sostituire con altre tale categoria di informazioni, qualora ad esempio siano oggetto di furto: se le impronte digitali di un soggetto ignaro venissero sottratte e clonate, l'identità della vittima non potrebbe più essere determinata mediante riconoscimento dattiloscopico[10]. Il pericolo poi di un indebito uso, non autorizzato, di dati sensibili[11] quali appunto quelli biometrici raccolti a fini di verifica o identificazione, o ancora l'impiego degli stessi al di fuori degli scopi specifici per i quali sono stati acquisiti, mettono in rilievo la necessità di predisporre opportune protezioni e idonee tutele non solo tecniche ma anche giuridiche[12]. Queste devono coprire il rischio di diffusione dei dati (a causa di *data breach* di un sistema centralizzato di conservazione di impronte digitali, ad esempio) o quello ben più insidioso dell'incrocio di dati biometrici con altre informazioni personali (cd. *function creep*), in grado di portare, mediante aggregazione dei dati, a vere e proprie operazioni di profilazione di soggetti[13]. A ciò devono aggiungersi anche i pericoli connessi alle informazioni delicatissime, "indirettamente" ricavabili da questa particolare categoria di dati: le rilevazioni biometriche della struttura vascolare della mano possono rivelare malattie



necessità di predisporre tutele forti per garantire idonea protezione ai diritti alla riservatezza e alla protezione dei dati; sul punto: Oxfam, *Biometrics in the humanitarian sector*, marzo 2018, policy-practice.oxfam.org.uk/publications/biometrics-in-the-humanitarian-sector-620454.

[10] Estrema chiarezza assumono le parole del già citato Giudice D. Chandrachud: "Once a biometric system is compromised, it is compromised forever. In the event of biometric identity theft, there would appear to be no alternative but to withdraw the user from the system. Passwords and numbers can be changed, but how does one change the basic biological features that compromise biometrics in the event that there is a theft?", par. 132, *Dissenting Opinion* del Giudice D. Chandrachud, *Justice Puttaswamy v. Union of India*.

[11] Si sottolinea sin da subito come i dati biometrici, nella disciplina normativa europea, siano considerati appartenenti ad una "categoria particolare di dati personali" (art. 9, GDPR) e siano pertanto sottoposti ad una specifica disciplina, maggiormente tutelante, "dal momento che il contesto del trattamento (di tali dati) potrebbe creare rischi significativi per i diritti e le libertà fondamentali", Considerando 51, GDPR.

[12] Anche il Gruppo per la tutela dei dati personali (Gruppo Art. 29), nel suo documento più recente in materia di tecnologie biometriche (*Opinion 3/2012 on developments in biometric technologies*), adottato il 27 aprile 2012 (00720/12/EN WP193), ha sottolineato: "The second risk is the purpose diversion either by the data controller itself or by a third-party including law enforcement authorities. This common threat regarding personal data becomes a crucial one when biometric data are used. Manufacturers should take all security measures to avoid any improper use of the data and make sure that any data that are not needed anymore for the purpose of the processing are deleted immediately".

[13] Come chiaramente delineato nella normativa europea, per profilazione si intende "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica", art. 4, par. 4), GDPR. Il quoziente elevato di rischio rappresentato dalla profilazione basata sull'utilizzo di dati biometrici viene sottolineata dal legislatore europeo (Considerando 91).

cromosomiche, così come la *signature recognition* (la rilevazione della firma e dello stile di scrittura) può permettere di determinare la presenza di malattie neurologiche[14].

Questa analisi delle minacce e insidie derivanti da sistemi di riconoscimento biometrici non può però astrarre da alcune considerazioni tecniche, da individuarsi nella distinzione tra le due maggiori tipologie di sistemi di riconoscimento biometrico: quelli che effettuano una mera 'verifica' e quelli che invece pongono in essere una 'identificazione' del soggetto. Tale categorizzazione, lungi dal voler essere unicamente formale, risulta di grande rilievo per la completa comprensione delle successive considerazioni e analisi; in base al diverso sistema cui ci si riferisce, infatti, anche il livello di rischio per la riservatezza si presenta in gradazioni molto diverse e, con esso, anche la qualità e quantità di tutele e protezioni da porre in essere.

Nella prima delle tipologie sopra individuate, la verifica dell'identità di un soggetto consiste in un confronto di dati biometrici attraverso un approccio cd. *one-to-one*: si compara cioè il dato fornito durante le operazioni di riconoscimento con i dati raccolti precedentemente, al momento dell'emissione di un documento o di un badge e inseriti in quel solo e unico supporto[15].

Diverso invece è il sistema di identificazione che prevede un approccio cd. *one-to-many* e che quindi presuppone l'esistenza di un database contenente molteplici dati biometrici appartenenti ad un numero di soggetti generalmente elevato; il match in questo caso viene effettuato controllando la corrispondenza del dato biometrico prelevato al momento dell'identificazione con tutti quelli contenuti nella banca dati[16]. Ciò presuppone pertanto una fase di *enrollment* (di acquisizione del dato dell'utente), con relativa conservazione nel *repository* unico, e una successiva fase di *authentication*, basata sull'esito del processo di confronto (*matching*) tra il modello corrente e quello memorizzato a livello centralizzato, effettuato mediante l'uso di appositi algoritmi.



[14] Si legga sul punto l'analisi ricostruttiva svolta dal Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010, bioetica.governo.it/it/documenti/pareri-e-risposte/l-identificazione-del-corpo-umano-profili-bioetici-della-biometria/.

[15] Rientra in questa categoria la verifica dell'identità di un soggetto in possesso di uno smartphone mediante l'uso del lettore di impronta digitale, inserito nel dispositivo elettronico. Un software dedicato stabilisce infatti la corrispondenza tra l'impronta raccolta al momento della verifica (quando cioè l'utilizzatore vuole accedere al proprio device) e quella memorizzata e conservata nel dispositivo stesso sin dalla sua configurazione. Ancora è il caso delle Carte d'Identità Elettroniche, munite di chip, all'interno del quale è contenuta una copia delle impronte digitali raccolte al momento della erogazione del documento; nel caso in cui si volesse verificare l'identità del possessore del documento, verrà effettuato un match tra il dato biometrico fornito al momento del controllo e quello immagazzinato nel chip del documento. Ben si comprende come il confronto sia uno-a-uno: il dato 'sorgente', da confrontare con quello di volta in volta fornito, è infatti solo uno.

[16] Si legga sul punto il Garante per la Protezione dei Dati Personali, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica; Allegato A al Provvedimento del garante del 12 novembre 2014*, 2014, reperibile online www.garanteprivacy.it/documents/10160/0/All+A+al+Provv.+513+del+12+novembre+2014+-+Linee-guida+biometria.pdf. Riassuntivamente il sistema *one-to-one* può essere ritenuto rispondente alla domanda: "Sei chi dici di essere?", mentre il sistema *one-to-many* è volto a rispondere al quesito: "Chi sei?".

Come è facilmente comprensibile, l'ultimo sistema descritto comporta un livello di pericolosità per i diritti fondamentali, quali quelli alla riservatezza e alla protezione dei dati, più elevato rispetto al modello *one-to-one*: i dati biometrici infatti vengo lasciati a disposizione in un unico *repository* ed è proprio tale conservazione, solitamente su ampia scala, a renderli più vulnerabili e maggiormente esposti al rischio di attacchi, *data breach*, furti e riutilizzo non controllato; aumentano inoltre le possibilità di cd. falsi match, falsi negativi o errori nelle procedure di identificazione. Altrettanto chiaro però, dall'altro lato, è il superiore grado di controllo che questa tipologia di sistema permette di garantire, rendendo più difficili frodi, sostituzioni di persona e duplicazioni di identità rispetto al modello *one-to-one*; quest'ultimo certamente pone minori problemi, per quanto non inesistenti, rispetto alla tutela della privacy e della protezione dei dati, ma offre una minore efficacia delle operazioni di riconoscimento.

In questo contesto così tecnicamente complesso e variegato, un ruolo essenziale viene assunto dal legislatore – e, come vedremo, anche dal giudice – chiamato a delineare paletti e forme di mitigazione nella raccolta e conservazione dei dati, nelle modalità di utilizzo degli stessi, nella individuazione dei soggetti autorizzati ad accedervi, nei diversi usi che possono essere fatti dei dati sensibili trattenuti in un unico supporto o in banche dati e che paiono dover essere ispirati a principi di necessità e proporzionalità della compressione dei diritti fondamentali rispetto alla finalità da perseguire[17]. Una attenta riflessione giuridica sulle implicazioni derivanti dall'uso di questi sistemi, fondati sulla raccolta di dati così personali, risulta dunque ormai inevitabile.



L'attualità della tematica e del suo necessario studio è testimoniata con forza ed evidenza da alcuni casi emblematici che stanno interessando, in diversi Paesi, giudici, legislatori e autorità nazionali per la protezione dei dati, ma anche società civile e organizzazioni a tutela dei diritti fondamentali dei cittadini: il cd. caso *Aadhaar*, di cui si è occupata la Corte Suprema dell'Unione Indiana; la normativa in materia di *ficher Titre électroniques sécurisés (TES)* francese, su cui è stato chiamato a pronunciarsi recentemente il Conseil d'État e prima ancora il Conseil Constitutionnel; la discussa legislazione belga in materia di Carte d'Identità Elettronica. I casi richiamati sono rappresentazione plastica dei modelli sopra delineati: *one-to-many* per gli esempi indiano e francese (pur con alcune differenze) e *one-to-one* per quello belga. Benché questi Paesi siano ovviamente distanti da un punto di vista ordinamentale, l'analisi di questi casi permette un esame delle criticità e delle problematiche derivanti dalle diverse tipologie di sistemi di riconoscimento adottati.

[17] "The power and efficiency proffered by such tools, both pose and mount a great urgency to identify and to mitigate modern risks associated with system breach and the compromise of vital information in those identity systems and to ensure that digital identity systems do not become tools of suppression, oppression, exclusion and discrimination", P. Dixon, *A failure to "Do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health and Technologies*, n. 6 (2017), 2.

L'ampiezza del progetto *Aadhaar*, la sua complessa e inedita struttura nonché l'ampio dibattito e interesse che la sua implementazione ha portato nella società civile, fino ad arrivare nelle aule della Corte Suprema, hanno reso il caso indiano imprescindibile punto di partenza per individuare le insidie e le necessarie tutele connesse alla raccolta e uso dei dati biometrici.

L'esame invece del sistema identificativo francese e dell'intervento, anche in questo caso, come in India, dei giudici delle più alte Corti, risulta opportuno e quanto mai necessario per comprendere come, anche in contesti in cui il diritto alla riservatezza e protezione dei dati vanta una tradizione di forte riconoscimento e tutela, l'attenzione sull'adozione di modelli *one-to-many* sia alta e la loro compatibilità e proporzionalità rispetto ai diritti fondamentali dubbia.

Lo studio della normativa belga, infine, adottata nel contesto di un sistema di tipo *one-to-one*, completa il quadro ricostruttivo e arricchisce l'analisi di spunti di riflessione utili a meglio valutare la direzione delle scelte normative relativamente a questo modello e a determinarne i limiti.

In ultima analisi, questo studio vuole dimostrare la forte rilevanza e trasversalità delle sfide giuridiche che l'utilizzo dei dati biometrici a scopi di riconoscimento pone in sistemi giuridici anche molto differenti tra loro, in un contesto in cui si moltiplicano peraltro le autorità nazionali o sovranazionali – dai Paesi africani alla recente proposta legislativa dell'Unione Europea – che cercano di dotarsi di sistemi di riconoscimento fondati sui dati biometrici, elaborando differenti soluzioni alla necessità di bilanciare interessi e diritti talvolta contrapposti.



## 2. L'*Aadhaar project* indiano al vaglio della Corte Suprema: un difficile bilanciamento

L'India è un paese tecnologicamente avanzato nel cui panorama normativo e giurisprudenziale stanno emergendo con forza quelle grandi sfide che le nuove tecnologie pongono al mondo del diritto anche alle nostre latitudini.

In tale contesto, con particolare riferimento alla creazione e adozione di modelli di riconoscimento *one-to-many* (identificazione) e delle problematiche giuridiche ad essi connesse, grande importanza assume un recente caso di estremo interesse, che consente di sviluppare rilevanti considerazioni di sistema: la Corte Suprema è stata infatti chiamata a pronunciarsi sulla legittimità costituzionale del controverso *Aadhaar project*, un sistema nazionale finalizzato ad individuare in maniera univoca l'identità dei cittadini indiani[18] mediante l'attribuzione di un cd. *Aadhaar number*, un codice unico, non riassegnabile, composto da 12 cifre, stabilite in maniera randomica ed emesso da una apposita Autorità nazionale centrale, la *Unique Identification Authority of India* (UIDAI). Ai fini dell'ottenimento di questo codice, che, come vedremo, è divenuto essenziale

[18] Il sistema identificativo *Aadhaar* non prevede l'assegnazione di un *Aadhaar number* anche ai soggetti residenti illegalmente sul suolo indiano; si legga sul punto l'art. 2, lett. V) del Chapter 1 dell'*Aadhaar Act* , n. 18/2016.

per la vita della quasi totalità della popolazione indiana, ogni cittadino è tenuto a fornire ad apposite autorità, pubbliche o private (*Enrolment Centres*), sia "informazioni demografiche" (nome, cognome, data e luogo di nascita, età, sesso, indirizzo) che dati biometrici (in quantità peraltro rilevante, essendo richieste dieci impronte digitali, la scansione di entrambe le iridi e una foto del viso).

Lo scopo del Governo indiano, che ha iniziato a concettualizzare questo ambizioso progetto nel 2006 per poi renderlo operativo nel 2009, è quello di fornire una prova di identità che possa essere universale, valida e funzionante in maniera eguale in tutto il Paese, in grado di consentire una corretta e univoca identificazione dei cittadini. Ciò che rileva comprendere però, ai fini anche di una migliore analisi della sentenza della Corte Suprema, è la motivazione, estremamente concreta e pratica, che ha mosso alla creazione di tale sistema identificativo, dall'architettura assai complessa: il problema che il Governo si trovava ad affrontare infatti era quello di allocare efficacemente sussidi, benefici, sovvenzioni e servizi pubblici ai soggetti più bisognosi e alle fasce più povere della società. Con una delle popolazioni più numerose al mondo e un territorio estremamente vasto, le autorità pubbliche hanno da sempre dovuto fronteggiare difficoltà legate a furti o duplicazioni di identità, volte ad accedere illegittimamente a fonti di approvvigionamento e sostegno statali; la mancanza di una identità giuridica formalmente riconosciuta e dei relativi documenti, comportava inoltre l'impossibilità di accedere a servizi quali l'iscrizione scolastica ma spesso anche l'apertura di conti correnti bancari, favorendo la mancata trasparenza nella gestione dei flussi di danaro[19]. Ecco allora che l'ideazione di un sistema di identificazione quanto più insostituibile e univoco, è divenuta una priorità per il Governo indiano. Il sistema identificativo *Aadhaar* è stato pertanto sviluppato proprio allo scopo di incentivare l'inclusione sociale e la regolarità sul piano finanziario, permettendo a larghe fasce di popolazione, prima escluse e prive di "identità" in senso giuridico, di emergere da tale "limbo", accedendo a servizi bancari e facilitando una efficiente distribuzione del danaro e delle risorse pubbliche mediante, ad esempio, il trasferimento diretto dei sussidi sul conto bancario del beneficiario individuato tramite il codice *Aadhaar*, rilasciato in maniera facile e veloce. Ciò permette di evitare il ricorso ad altre tipologie di documenti identificati non altrettanto univoci e sicuri, per il rilascio dei quali erano e sono spesso richieste complesse procedure[20].



[19] Per una ricostruzione ottimistica degli effetti dello stesso: N. S. Ramnath, C. Assisi, *The Aadhaar effect: why the world's largest identity project matters*, Oxford, 2018.

[20] Si stima che dal funzionamento del sistema *Aadhaar*, 309 milioni di nuovi conti bancari siano stati aperti, supportati proprio dall'identificazione mediante eKYC (*electronic Know Your Customer*), basati sul numero *Aadhaar*. Ciò ha avuto impatto positivo non solo sulle fasce di popolazione più povere ma anche sulle donne, la cui inclusione sociale ha sempre rappresentato una forte sfida nel contesto indiano. Sul punto si legga: M. Mathew, *Empowering rural indian women through financial inclusion: challenges and opportunities*, in *International Journal of Exclusive Management Research*, 4 (2014); S. Garg, P. Agarwal, *Financial Inclusion in India: a review of initiatives and achievements*, in *Journal of Business and Management*, 6 (2014), 52-61.

Se da questa prima analisi il progetto *Aadhaar* pare estremamente promettente, efficace e dai bassi costi di gestione[21], risulta tuttavia necessario spingersi ad un esame più approfondito delle modalità di funzionamento e soprattutto del trattamento che viene riservato ai dati biometrici raccolti al fine dell'ottenimento dell'*Aadhaar number*. Innanzitutto i dati raccolti al momento della prima registrazione (*enrolment*) vengono conservati all'interno di un database centrale (*Central Identities Repository*), sotto il controllo e la gestione della UIDAI. Ogni volta poi che un cittadino desideri accedere a sussidi e benefici statali (individuati in quelli forniti dal *Consolidated Fund of India*), si renderà necessario recarsi presso una apposita autorità (*Requesting Entities*, RE) e procedere alle attività di *authentication*, ovvero una procedura di accertamento dell'identità: i dati, compresi quelli biometrici, forniti all'atto dell'autenticazione, vengono inviati alla UIDAI che ha il compito di svolgere una comparazione tra i dati inviati dalle RE e quelli presenti nel database centralizzato. Solo in caso di confronto positivo viene stabilita e confermata l'identità del soggetto in maniera univoca: un sistema dunque di raffronto *one-to-many*, vista la presenza di un *repository* vastissimo di dati sensibili, che oggi copre quasi 1.2 miliardi di cittadini indiani[22].

Come ben si può comprendere, emergono però con forza due ordini di questioni problematiche: innanzitutto la mancanza, per svariati anni, di una base normativa regolante il sistema; l'*Aadhaar Act*[23] è stato approvato infatti solo nel 2016, a 7 anni dalla instaurazione del modello di riconoscimento. A ciò deve sommarsi la persistente carenza di una specifica legislazione in materia di privacy e di protezione dei dati (anche di quelli così personali e sensibili quali quelli biometrici)[24], che ha fatto sorgere nella società civile e in numerose organizzazioni a protezione dei diritti dei cittadini, dubbi circa l'adeguatezza e la proporzionalità del trattamento dei dati raccolti e conservati per l'erogazione dell'*Aadhaar number*, nonché, più ampiamente, della legittimità costituzionale del



[21] Per una analisi approfondita: A. Gelb, A. D. Metz, *Identification revolution: can digital ID be harnessed for development?*, Washington, 2018.

[22] Per una analisi dettagliata del funzionamento tecnico di questo complesso sistema, si rimanda a R. Khera, T*he UID Project and Welfare schemes*, in *Economic and Political Weekly*, Vol. 46 (2011), 38-43; ma anche, più schematicamente, R. Kalra, R. Verma, C. Nasa, *Aadhaar Thumb: one platform to all services*, in *International Journal of Recent Research Aspects*, 1 (2018), 12-14;

[23] *Aadhaar (Targeted delivery of financial and other subsidies, benefits and services) Act*, 25 marzo 2016.

[24] Nel corso degli anni si sono succeduti diversi progetti di legge in materia di privacy e data protection, l'ultimo dei quali, il *Personal Data Protection Bill*, è stato proposto dal Governo nell'ottobre 2018 (meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf). Questi tentativi dimostrano, anche a seguito degli interventi giurisprudenziali degli ultimi anni, una crescente sensibilità verso il tema della tutela della riservatezza e protezione dei dati ed evidenziano l'esigenza, sempre più sentita, di una apposita disciplina normativa in una materia così delicata e di grande impatto sui diritti fondamentali dei cittadini. Interessante è anche il complesso report elaborato da una Commissione guidata dal Giudice Srikrishna, contenente raccomandazioni in materia di *data management* e *data privacy* (Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, 2018, meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf).

sistema identificativo *Aadhaar*. Questa crescente sensibilità al tema della tutela della privacy, oltre al timore per le incertezze nell'utilizzo dei dati, è stata peraltro accresciuta nel momento dell'introduzione dell'*Aadhaar Act*: quest'ultimo non solo aveva reso obbligatorio il possesso del codice *Aadhaar* (e quindi l'obbligo per il cittadino di fornire dati demografici e biometrici) per l'accesso ad un novero sempre più ampio di benefici e servizi[25], ma aveva anche esteso il suo utilizzo come strumento identificativo in ambiti legati al mondo privato, quali quello bancario o dei servizi di telefonia, che potevano imporre il possesso dell'*Aadhaar number* per l'apertura di conti correnti bancari o l'acquisto di SIM.

La sempre più percepita invasività nella sfera privata del cittadino, è così sfociata, sin da pochi anni dopo l'introduzione del sistema *Aadhaar*, in un susseguirsi di *writ petitions* da parte di individui e organizzazioni per la tutela dei diritti fondamentali. Questi interventi erano volti a dimostrare come le tutele apprestate dalla normativa del 2016 non fossero sufficienti ad evitare rischi per i dati personali dei cittadini, sotto molteplici profili: dal punto di vista della sicurezza del sistema, della predisposizione di idonee misure volte ad evitare *data breach* e accessi non autorizzati o sottrazione illegittime di dati; ma anche dal punto di vista dei limiti stabiliti all'utilizzo dei dati da parte dello Stato: può dirsi veramente scongiurato il pericolo di una vera e propria *mass surveillance society* in un sistema in cui un database centralizzato, controllato dalle autorità pubbliche, contiene i dati biometrici di tutti i cittadini? Le tutele apprestate per evitare l'utilizzo dei cd. *authentication records*, cioè delle informazioni relative ad ogni singola operazione di autenticazione di un soggetto presso REs volte ad ottenere l'accesso ad un determinato servizio, sono adeguate ad evitare il rischio di operazioni di profilazione dei cittadini[26]? La costruzione di un tale sistema è parsa ai numerosi ricorrenti sproporzionata ed eccessivamente lesiva dei diritti



[25] Ad esempio, per l'accesso a sussidi e benefit statali forniti dal *Consolidated Fund of India*, servizi legati al sistema pensionistico, iscrizione a scuola.

[26] Secondo gli oppositori del sistema *Aadhaar* infatti non sarebbe garantita una idonea tutela contro la disseminazione di informazioni che mina alla base il diritto dell'individuo di *informational privacy*, cioè di mantenere il controllo sui dati che lo riguardano (per approfondimento su questa interessante dimensione connessa al diritto alla privacy, si veda C. P. Moniodis, *Moving from Nixon to NASA: privacy's second strand. A right to informational privacy*, in *Yale Journal of Law and Technology*, 1/2012, 139-168). Questi timori sono ben riassunti al par. 45 della già richiamata sentenza *Justice Puttaswamy v. Union of India*, del 26 settembre 2018 (D.N. 35071/2012), Corte Suprema indiana, di cui si parlerà ampiamente a breve: "the most delicate and fragile part, susceptible to misuse, is the authentication process which is to be carried out each time the holder of *Aadhaar* number wants to establish her identity. At that stage, not only the individual parts with the biometric information again with the RE (which may again be a private agency as well), the purpose for which such a person approaches the RE would also be known i.e. the nature of transaction which is supposed to be undertaken by the said person at that time. Such information relating to different transactions of a person across the life of the citizen is connected to a central database. This record may enable the State to profile citizens, track their movements, assess their habits and silently influence their behavior. Over a period of time, the profiling would enable the State to stifle dissent and influence political decision making. It may also enable the State to act as a surveillant state and there is a propensity for it to become a totalitarian state". Sul punto, più approfonditamente si legga anche: D. Chaudhary, *On Aadhaar: surveillance and profiling*, in *RMLNLU Law Review Blog*, 26 settembre 2018, rmlnlulawreview.wordpress.com/2018/09/26/on-aadhar-part-i-surveillance-and-profiling/

fondamentali degli utenti, cui peraltro non è data, nella concretezza dei fatti, la possibilità di un reale *opt-out* dal sistema e neppure di accesso e controllo sui dati forniti al sistema centralizzato. Anche la disciplina che regola le varie autorità, pubbliche e private, operanti sia nella fase di *enrolment* che di *authentication*, deputate pertanto alla raccolta e trasferimento dei dati demografici e biometrici, pare non disporre una protezione adeguata ai rischi e alla natura delle informazioni trattate[27].

Il quadro risulta ulteriormente complicato se si analizzano disposizioni articolate e delicate quali quelle della *Section 33* dell'*Aadhaar Act*, in cui viene stabilita la possibilità di *disclosure* non solo dei dati identificativi (quindi sia demografici che biometrici) ma anche degli *authentication records*, contenuti nel database centrale, in particolari casi[28], per scopi di indagine, di *law enforcement* e garanzia della sicurezza nazionale.

In questo particolare contesto, caratterizzato dal moltiplicarsi di ricorsi, prima avverso *orders* o decisioni delle Corti statali o federali e della UIDAI stessa (mancando una base legislativa della quale contestare la legittimità) e, successivamente, avverso l'*Aadhaar Act* direttamente, la Corte Suprema si è pronunciata il 26 settembre 2018. Dopo anni di travagliato percorso[29], costellato da numerosi *interim orders* della medesima Corte, aventi ad oggetto singoli aspetti specifici della disciplina[30], quest'ultima sentenza vaglia la legittimità costituzionale dell'intero atto normativo regolante il sistema identificativo[31].

[27] Si consideri inoltre che, sino al 2017 (come si vedrà in seguito), il diritto alla privacy e alla protezione dei dati non era mai stato riconosciuto come diritto fondamentale e non era (e non è tutt'ora) tutelato da un apposita normativa; in questo contesto, una proposta di legge promuoveva l'istituzione di una specifica autorità pubblica ma indipendente, la *National Identification Autohority*, deputata proprio al vaglio delle questioni problematiche connesse alla privacy e derivanti dall'attuazione del sistema *Aadhaar*. La proposta relativa all'istituzione di questa autorità, che poteva, quanto meno in un primo momento, sopperire alla carenza di tutele legislative, non è stata mai approvata. Sulle ragioni di tale mancata approvazione, si veda: P. Reddy, A. Sengupta, S. Ambast, et al., *A briefing document on the national identification authority of india bill, 2010: questions of constitutionality & legislative options open to parliament*, in *SSRN online*, 2016, ssrn.com/abstract=1759719.

[28] Nel primo paragrafo della *Section 33* viene data la possibilità di *disclosure* in presenza di una decisione di un Giudice non inferiore al *District Judge*, per finalità di indagine; nel secondo paragrafo, invece, tale possibilità viene concessa, esclusivamente per ragioni di sicurezza nazionale, in presenza di una decisione di un ufficiale "not below the rank of Joint Secretary to the Governement of India specially authorized in this behalf by an order of the Central Government" e successivamente vagliata da un "Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology, before it takes effect". Tale provvedimento assume una validità di tre mesi dalla data di emissione, ulteriormente estendibile per un periodo di tre mesi (Section 33, *Aadhaar Act*).

[29] Non bisogna dimenticare che apparivano nel frattempo reportage, su svariate testate giornalistiche e siti internet, denuncianti la facilità di accesso e di frode al sistema identificativo *Aadhaar*; sul punto più approfonditamente P. Dixon, *A failure to "Do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, op. cit.,7; ma anche R. Shah, *Is your sensitive data like Aadhaar, PAN card details safe with the government?*, in *DNA daily news and analysis*, 23 marzo 2017, www.dnaindia.com/money/report-is-your-sensitivedata-like-aadhaar-pan-card-safe-with-the-government-2364851.

[30] Tra le tante, merita essere ricordata l'ordinanza del 23 settembre 2013, nella quale viene precisato come "No person should suffer for not getting the Aadhaar card in spite of the fact

La mole di dubbi e questioni di legittimità, che sono stati sottolineati sopra, è così sfociata in una decisione estremamente complessa, composta da 1448 pagine (comprensive di una *partly concurring opinion* del Giudice A. Bhushan e una *dissenting opinion* del Giudice D. Chandrachud) e che giunge peraltro dopo un'altra importantissima pronuncia dalla storica portata della Corte stessa[32], originata proprio dal caso *Aadhaar*, nella quale è stata per la prima volta affermata la natura fondamentale del diritto alla riservatezza.

L'articolata sentenza della *majority*, perfettamente in linea con la struttura caratteristica e peculiare delle pronunce della Suprema Corte indiana, si presenta come un vero trattato dottrinario, che ricostruisce con estrema precisione in primis origini e natura del diritto alla privacy per poi dedicarsi al complesso bilanciamento tra diritto alla riservatezza e alla protezione dei dati da un lato e diritto al cibo e all'abitazione dall'altro, questi ultimi ricompresi nel più ampio diritto alla dignità umana. Proprio tale specifico diritto, posto – in maniera piuttosto inedita – su uno dei due piatti della bilancia, assume grande interesse e rappresenta una divergenza rispetto ai casi di cui le Corti si occupano e si sono occupate nel contesto europeo: quello indiano infatti non è un sistema identificativo volto alla tutela della sicurezza pubblica bensì un sistema finalizzato a garantire servizi essenziali ai cittadini indiani e a permettere loro di condurre una vita dignitosa. Ciò si contrappone però con la necessità di



that some authority had issued a circular making it mandatory and when any person applies to get the Aadhaar card voluntarily, it may be checked whether that person is entitled for it under the law and it should not be given to any illegal immigrant". Per una ricostruzione puntuale degli *interim orders* più rilevanti in materia, si rimanda al par. 19 della sentenza *Justice Puttaswamy v. Union of India*. Anche con riferimento alla Section 33 si sono registrati vari interventi di numerose Corti che avevano cercato di limitare con le proprie decisioni il ricorso alla *disclosure* di dati biometrici: "We have already noticed that against the order of the High Court of Bombay in some criminal proceedings, order was passed directing the Authority to give biometric information of a person, the Authority had filed Special Leave Petition (Criminal) No. 2524 of 2014 challenging the said order on the ground that giving of such biometric information was contrary to the provisions of the Aadhaar Act as the information was confidential", par. 343, *Justice Puttaswamy v. Union of India*, ma anche par. 20 della stessa pronuncia.

[31] Diary number 35071/2012, Case Number No. 000494-000494/2012, *Justice Puttaswamy v. Union of India*. L'illegittimità costituzionale dell'*Aadhaar Act* infatti era stata sollevata, con una *public interest litigation*, da parte di K. S. Puttaswamy, ex Giudice della High Court del Karnataka, cui poi sono state unite le numerose altre *writ petitions* promosse da soggetti privati o organizzazioni a tutela dei diritti fondamentali, succedutesi nel tempo.

[32] "Il 18 luglio 2015 un collegio presieduto dal Chief Justice, preso atto dell'importanza della questione sottoposta al vaglio della Corte Suprema (nel caso vertente sulla legittimità del sistema identificativo Aadhaar, ndr.) e del fatto che le decisioni M P Sharma e Kharak Singh erano state emesse rispettivamente da un collegio di otto e di sei giudici, ordinava che la questione venisse esaminata da un organo giudicante composto da nove giudici", M. Senor, *Il riconoscimento della tutela costituzionale del diritto alla privacy in India*, in *MediaLaws*, 6 dicembre 2017, 3. Su questa *landmark decision*, si legga anche: L. Pelucchini, *Diritto alla privacy, data protection e costituzioni mute: la Corte Suprema indiana riconosce finalmente il diritto alla vita privata come inalienabile*, in *Nomos*, 2 (2017); R. Singh, *Human dignity and right to privacy: the Puttaswamy Judgement*, in *India Constitutional Law Review Blog*, 6 maggio 2018, iclrq.in/blog-posts/human-dignity-and-right-to-privacy-the-puttaswamy-judgment/; V. Bhandari, A. Kak, S. Parsheera, F. Rahman, *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*, in *IndraStra Global*, 11 (2017), 1-5, nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2.

predisporre idonee garanzie a tutela della privacy tali da impedire un utilizzo sproporzionato dei dati raccolti e conservati rispetto al fine perseguito[33]. Ed è proprio sul test di proporzionalità che si concentra con minuziosa precisione la Corte Suprema, vagliando una ad una le singole disposizioni dell'*Aadhaar Act* impugnate dai ricorrenti, con una ricostruzione che peraltro volge lo sguardo oltre i confini nazionali. Grande attenzione infatti è riservata ad una analisi lucida e attuale delle nuove tecnologie, dell'impatto dei *big data* e della loro natura composita fatta di potenzialità e minacce[34], nonché della giurisprudenza straniera più rilevante sul tema, attraverso il richiamo a note pronunce della Corte Suprema americana ma anche della Corte di Giustizia dell'Unione Europea e della Corte Europea dei Diritti dell'Uomo[35].

Per quanto interessante, non risulta possibile in questa sede rilevare tutti i molteplici aspetti trattati dalla sentenza[36], che presenta numerosissime sfaccettature, partendo dalla corretta individuazione dell'*Aadhaar Act* come *Money Bill*[37]. Ciò che però interessa e maggiormente rileva è una lettura della decisione della Corte Suprema nella parte in cui ha dichiarato costituzionalmente legittimo il sistema *Aadhaar*, salvo poi espungere talune singole disposizioni che non hanno superato il vaglio di proporzionalità.

Alla domanda circa la violazione o meno da parte dell'*Aadhaar project*, così come strutturato, del diritto alla privacy, la Corte risponde che l'invasione rispetto a tale diritto fondamentale è da considerarsi minima e che il sistema

[33] La Corte infatti, dopo una attenta ricostruzione del diritto alla privacy nella giurisprudenza e nella disciplina normativa nazionale (ma anche straniera), afferma la natura non assoluta di tale diritto fondamentale, che può dunque essere limitato in presenza di *just, fair and reasonable law*, per la cui determinazione si rende necessario un giudizio di proporzionalità (par. 88 e ss., *Justice Puttaswamy v. Union of India*).

[34] Par. 159-162, *Justice Puttaswamy v. Union of India.*

[35] Interessante è l'affermazione circa il ruolo importante della comparazione, che rappresenta un fondamentale tassello sia in questo giudizio sia nella precedente storica pronuncia sul diritto alla riservatezza: "In this hue, it can also be remarked that comparative law has played a very significant role in shaping the aforesaid judgment on privacy in Indian context, notwithstanding the fact that such comparative law has only a persuasive value", par. 84, *Justice Puttaswamy v. Union of India.* Si legga anche sul tema: V. R. Scotti, *La Corte Suprema dell'Unione Indiana e l'utilizzo del precedente straniero*, in P. Martino (a cura di), *I giudici di Common Law e la (cross) fertilization: i casi di Stati Uniti d'America, Canada, Unione Indiana e Regno Unito*, Rimini, 2014, 61-82. Nella sentenza in esame vengono richiamati casi noti della più recente giurisprudenza della Corte di Giustizia dell'Unione Europea, come *Digital Rights Ireland Ltd & others*, C-293/12; *Tele2 Sverige and Watson*, C-203/15 e C-698/15; *Schrems*, C-362/14; mentre vengono studiate anche alcune pronunce della Corte Europea dei Diritti dell'Uomo, quali *S. and Marper v. UK*, n. 1581/2008; *Szabo & Vissy v. Hungary*, n. 37138/14, oltre ad altri *leading cases* di alcune Corti nazionali (Corte Costituzionale tedesca, Corte Suprema USA). Si rimanda più approfonditamente ai par. 172 ss, *Justice Puttaswamy v. Union of India.*

[36] Per una analisi puntuale si rimanda a: G. Bathia, *The Aadhaar Judgement: a round-up*, in *Indian Constitutional Law and Philosophy*, 5 ottobre 2018, indconlawphil.wordpress.com/2018/10/05/the-aadhaar-judgment-a-round-up/

[37] Questa qualificazione non è priva di conseguenze: l'individuazione della natura dell'atto come *Money Bill* ha comportato l'esclusione dal procedimento legislativo della Camera Alta del Parlamento, il *Rajya Sabha*, e ha dunque permesso un processo approvativo più snello e rapido. Diversamente da quanto ritenuto dal Giudice Chandrachud nella sua *dissenting opinion*, la sentenza *majority* considera legittima la qualifica dell'*Aadhaar Act* come *Money Bill* (si legga più ampiamente sui motivi di questa decisione, par. 388-413).

identificativo è un "vital tool for ensuring good governance in a social welfare state. We therefore are of the opinion that the Aadhaar Act meets the test of balancing as weel(..). We find that the Aadhaar Act has struck a fair balance between the right to privacy of individual with the right to life of the same individual as beneficiary"[38]. Pur ammonendo infatti il Parlamento e il Governo della necessità di un'apposita disciplina normativa in materia di tutela della privacy e protezione dei dati[39], la Corte ha ritenuto che neppure il margine di errore e di falsi negativi, causati proprio dall'utilizzo dei dati biometrici alla base del procedimento identificativo *one-to-many*[40], sia argomentazione sufficiente per ritenere incostituzionale, nel complesso, l'intero progetto: "what we are emphasising is that the remedy is to plug the loopholes rather than axe a project, aimed at the welfare of a large section of the society"[41].

Passaggio successivo necessario è stato poi quello di valutare ogni specifica misura dell'atto normativo al vaglio, al fine di garantire, in ogni aspetto del funzionamento e disciplina del sistema *Aadhaar*, il corretto bilanciamento tra lo scopo del sistema stesso e la tutela del diritto alla privacy. Ecco che allora viene vietato il carattere obbligatorio dell'uso del sistema identificativo *Aadhaar* da parte di soggetti privati, con la conseguenza che banche e operatori telefonici non potranno più richiedere il possesso del codice *Aadhaar* come condizione esclusiva per l'apertura di conti correnti o l'acquisto di una scheda telefonica. Il sistema dunque è considerato eccessivamente lesivo della privacy nella parte in cui stabilisce che dati biometrici siano forniti per scopi che non hanno come obiettivo la garanzia della dignità umana, sotto forma di accesso a sussidi e servizi essenziali. Solo in questo ultimo caso pertanto l'obbligatorietà del possesso del codice (e dunque l'invasione nella sfera privata del cittadino) risulta legittima e proporzionata. La Corte ammonisce anche a ridurre, sulla scorta dello stesso ragionamento, il tempo di conservazione delle *authentication information* da 7 anni a 6 mesi, e a considerare illegittima l'obbligatorietà del possesso dell'*Aadhaar number* per i soggetti minorenni al fine dell'iscrizione al servizio scolastico nazionale, ritenuto non rientrante nella categoria di benefit e sussidi che legittimano il vincolo di adesione al sistema identificativo. Particolare attenzione viene poi prestata agli *authentication records* contenuti del database centrale, che registrano le trasmissioni, condivisioni e accessi ai dati biometrici o



[38] Par. 309-313, *Justice Puttaswamy v. Union of India.*
[39] Par. 223-230, *Justice Puttaswamy v. Union of India.* Sul punto si richiama quanto già riportato in nota n. 24 a proposito del *Personal Data Protection Bill.*
[40] S. Singh, *Understanding Aahaar: the Unique Identification Authority of India and its challenges*, in *Human Rights Defender*, 3 (2018), 21-24 per un'analisi storica e critica delle problematiche legate a questo sistema (falsi negativi, che portano a problemi di autenticazione; difficoltà di connessione Internet in zone rurali; malfunzionamento della strumentazione deputata all'*enrolment* o alla *authentication*; vulnerabilità del sistema sotto il profilo della sicurezza informatica; timore e diffidenza da parte della popolazione; difficoltà – quando non impossibilità – di *opt-out* dal sistema; possibilità della sola UIDAI di denunciare episodi di *data breach*). Per una ricostruzione critica si legga anche: A. Saraph, L. Kathpalia, A. Kidwai, A. Joshi, *Is India's unique identification number a legally valid identification?*, New York, 12 giugno 2018, arxiv.org/abs/1806.04410
[41] Par. 219, *Justice Puttaswamy v. Union of India.*

ai *process meta-data*, cioè a tutte quelle informazioni che descrivono i risultati delle operazioni di autenticazione richieste dal cittadino: il totale divieto, stabilito dalla Corte, di trasmissione e utilizzo di questi dati rende necessaria una modifica del testo normativo. Allo stesso modo i giudici impongono al legislatore una modifica della *Section 33*, nella direzione di una maggiore tutela del singolo e di una riduzione dei casi di *disclosure* dei dati raccolti e conservati nella banca dati, diluendo dunque la forza delle disposizioni inizialmente previste[42].

Dalla ricostruzione dei punti salienti di questa rilevante pronuncia emerge quanto l'utilizzo di metodi tecnologicamente raffinati ma sempre più invasivi della privacy degli individui, ponga sfide inedite a legislatori e giudici, a qualsiasi latitudine, come dimostrato dalla ampia giurisprudenza straniera citata dalla Corte Suprema: l'impiego di mezzi identificativi basati su dati così sensibili e insostituibili quali quelli biometrici è da considerare con grande attenzione e cautela[43]. Pur non escludendo la necessità di sfruttare queste innovazioni per

[42] L'utilizzo di termini quali "*interest of national security*" sono considerati dai ricorrenti come caratterizzati da eccessiva "*vagueness and arbitrariness*", con la conseguenza di prestarsi potenzialmente ad un utilizzo e accesso ai dati illimitato da parte di autorità di *law enforcement*. Ciò renderebbe la *Section 33* illegittima in quanto non rispettosa dei criteri di proporzionalità. Questo orientamento non è stato accolto dalla Corte Suprema che nella sua pronuncia ha considerato in gran parte la *Section 33* conforme al dettato costituzionale, precisando però la necessità di garantire al soggetto colpito dalla richiesta di accesso ai dati, di essere ascoltato e di poter impugnare la decisione di fronte alle autorità giudiziarie (proponendo dunque una lettura costituzionalmente orientata del dettato normativo). Ciò che la Corte Suprema ha ritenuto incostituzionale è invece il soggetto abilitato ad emanare un *order* di accesso ai dati per motivi di sicurezza nazionale: la carica maggiormente idonea ad una decisione di tale importanza e impatto per la vita privata del soggetto cui i dati appartengono, viene individuata infatti non nel *Joint Secretary*, come vuole la disposizione dell'*Aadhaar Act*, bensì in un funzionario di grado più elevato, la cui identificazione è lasciata al legislatore, chiamato a modificare la normativa sul punto. Viene ribadita poi la possibilità, se non il dovere, della UIDAI di promuovere opposizione avverso gli *order* di accesso avanzati, laddove ritenuti illegittimi o sproporzionati, come già peraltro affermato in alcuni precedenti *Interim Order* della Corte Suprema stessa (*Interim Order* 24 marzo 2014; *Interim Order* 16 marzo 2015).

[43] Ciò è stato rilevato con chiarezza dal giudice Chandrachud nella più volte richiamata *dissenting opinion*. Questa, per gli interessanti spunti di riflessione, è stata accolta dai ricorrenti e da alcuni commentatori come pronuncia dalla storica portata (G. Bahtia, *The Aadhaar Judgement; a dissent for the age*, in *Indian Constitutional Law and Philosophy*, 27 settembre 2018, indconlawphil.wordpress.com/2018/09/27/the-aadhaar-judgment-a-dissent-for-the-ages/). Nella sua lunga analisi, il Giudice prende in considerazione tutti gli aspetti problematici del sistema *Aadhaar*, evidenziando non solo diverse conclusioni giuridiche ma, prima ancora, una differente ricostruzione tecnica del sistema e del suo funzionamento, ricostruzione portatrice di una opposta decisione finale. Particolare attenzione viene prestata alle percentuali di errore (falsi negativi) che possono registrarsi e agli effetti disastrosi che ciò comporta per la vita e il godimento di taluni diritti fondamentali dei cittadini indiani ("Denial of subsidies and benefits to them due to the infirmities of biometric technology is a threat to good governance and social parity", par. 262), aggravata dalla mancata previsione di metodi alternativi di riconoscimento. Il Giudice, di conseguenza, assume una posizione molto diversa circa il rischio di profilazione e sorveglianza di massa, che è concreto nella lettura di Chandrachud e non escluso come ritenuto invece dai giudici nella sentenza di maggioranza. Sotto il profilo del principio di proporzionalità e di *data minimization* poi, il legislatore, nel regolare il sistema *Aadhaar*, non ha dimostrato l'inesistenza di una misura meno intrusiva dell'autenticazione biometrica e parimenti idonea a soddisfare gli obiettivi posti. Concludendo dunque il Giudice afferma: "Creating strong privacy protection laws and instilling safeguards may address or at the very least assuage

aumentare l'efficienza dell'intervento dello Stato, sempre più attivo nella tutela di diritti sociali e fondamentali, è indispensabile un apparato normativo in grado di garantire adeguata protezione del diritto alla riservatezza e alla protezione dei dati. Quello che il Giudice Chandrachud nella sua *dissenting opinion* infatti afferma, richiamando le parole del Professor Upendra Baxi[44], è la necessità di un corretto bilanciamento tra *bread* e *freedom*, tra *human rights* e *rights to be human*, la cui presunta antitesi deve essere composta da un legislatore e un giudice sapienti. Particolare attenzione quindi deve essere prestata da un lato all'evoluzione tecnologica e ai suoi potenziali utilizzi, dall'altro ai pericoli che essa comporta per quel *right to be alone* da leggere, sempre di più, con la lente del principio di proporzionalità[45]. Per raggiungere questo obiettivo, fondamentale peso assume il principio "*policy before technology*"[46], che non è tuttavia stato rispettato nel caso indiano: prima è stato attuato il sistema *Aadhaar* e solo successivamente, anche a fronte di problematiche legali, continui ricorsi ed emergenti debolezze, si è provveduto all'adozione di una disciplina normativa *ad hoc*, al momento ancora claudicante, peraltro priva di una sempre più fondamentale legislazione in materia di privacy e *data protection*. Ora, a seguito dell'intervento dei giudici, viene richiesto un intervento a "ritroso", apportando emendamenti all'*Aadhaar Act* del 2016, inseguendo un sistema già esistente ed operativo e correggendolo nella direzione di una maggiore garanzia della tutela della privacy[47].



some of the concerns associated with the Aadhaar scheme which severely impairs informational self-determination, individual privacy, dignity and autonomy. In order to uphold the democratic values of the Constitution, the government needs to address the concerns highlighted in this judgment which would provide a strong foundation for digital initiatives, which are imminent in today's digital age. However, in its current form, the Aadhaar framework does not sufficiently assuage the concerns that have arisen from the operation of the project which have been discussed in this judgment" (par. 339). Sulla ricostruzione delle divergenze emergenti sotto il profilo prettamente scientifico si legga: G. Bathia, *The Aadhaar Judgement and reality: on uniqueness*, in *Indian Constitutional Law and Philosophy*, 27 settembre 2018, indconlawphil.wordpress.com/2018/09/27/guest-post-the-aadhaar-judgment-and-reality-i-on-uniqueness/, che, al termine di una lettura molto critica della pronuncia della *majority*, parla addirittura di "*constitutionalism of convenience*", di facciata, nell'applicazione del principio di proporzionalità e di quello di *reasonable expectation of privacy*.

[44] Par. 103, Dissenting Opinion, Giudice Chandrachud, *Justice Puttaswamy v. Union of India*.

[45] Par. 197, Dissenting Opinion, Giudice Chandrachud, che richiama A. B. Serwin, *Privacy 3.0 – The Principle of Proportionality*, in *University of Michigan Journal of Law Reform*, Vol. 42 (2009).

[46] Espressione usata da P. Dixon in *A failure to "Do no harm"" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, op. cit., 9.

[47] Il testo dell'*Aadhaar and other laws (Amendment) bill 2019* (n. 261-C/2018), proposto dal Governo e approvato dalla *Lok Sabha* il 4 gennaio 2019, prevedeva numerose modifiche al testo del 2016, nel tentativo di recepire quanto indicato dalla Corte Suprema; tale testo è tuttavia successivamente decaduto a seguito del periodo di stallo dei lavori parlamentari, dovuto alla conclusione della legislatura e alla indizione di nuove elezioni. Durante la fase di revisione di questo contributo, il Presidente della Repubblica indiana ha deciso di intervenire in materia riprendendo quanto già proposto nel *Bill* sopra citato, promulgando l'*Aahdaar and other laws (Amendment) Ordinance*, n. 9/2019, del 2 marzo. Tale decisione si fondava sulla asserita quanto discussa "necessity to take immediate action", che ha portato ad azionare i poteri attribuiti al Presidente sulla base dell'art. 123 della Costituzione. A seguito dell'insediamento del nuovo Parlamento, è stato recentemente proposto dalla Camera Bassa un nuovo *Aadhaar and other laws (Amendment) bill 2019* (n. 86/2019 del 24 giugno 2019), che

### 3. La giurisprudenza francese alla prova: il *fichier* TES (Titres électroniques sécurisés)

La Corte Suprema indiana non è stata la prima e la sola ad occuparsi della legittimità costituzionale di sistemi di identificazione *one-to-many* che prevedono la raccolta e conservazione dei dati biometrici in un unico database. L'idea di creare una banca dati centralizzata non è infatti sconosciuta alle nostre latitudini: in Francia infatti il Governo aveva proposto, nel 2012, una modifica alla *Loi relative à la protection de l'identité* – concernente la disciplina del documento d'identità – finalizzata non solo all'inserimento delle impronte digitali nel documento stesso bensì anche alla raccolta e conservazione di tali dati biometrici all'interno di un database nazionale, riguardante, potenzialmente, tutta la popolazione francese. Questa proposta, tuttavia, aveva fatto sorgere timori e dubbi in merito alla possibilità di accessi incontrollati o illegittimi, di *data breach* oltre che di utilizzo dei dati per scopi differenti da quelli di mera identificazione. Ulteriore dubbio di legittimità costituzionale della misura era legato alla concessa facoltà di accesso ai dati da parte di forze dell'ordine e autorità di *law enforcement*, per scopi piuttosto ampi e indicati in maniera del tutto sommaria e poco delimitata a casi o soggetti specifici. Tutte queste perplessità sulla proporzionalità della disciplina proposta rispetto al fine di identificazione, erano sfociate nella richiesta, da parte della cd. *saisine parlementaire*, di un intervento preventivo del Conseil Constitutionnel. Con decisione n. 2012-652 del 22 marzo



andrebbe a sostituire l'Ordinanza del Presidente prima richiamata, pur ricalcandone sostanzialmente il contenuto. I principali cambiamenti rispetto al testo del 2016 sono quelli relativi alla obbligatorietà del possesso dell'*Aadhaar number*, non più estesa ai servizi di telefonia e bancari, per i quali dunque il codice diventa meramente volontario (per quanto non senza problemi per gli operatori di settore, che si trovano a dover valutare opzioni differenti di riconoscimento e di eKYC dei propri utenti). Viene modificata la discussa *Section 33*: sul punto rimangono comunque alcuni dubbi sulla conformità di questa modifica rispetto alle conclusioni dei giudici (non viene previsto infatti l'intervento di revisione e controllo di un'autorità giudiziaria rispetto all'ordine di accesso). Viene specificato inoltre che la mancata autenticazione non deve tradursi, come più volte ribadito dalla Corte Suprema, in un diniego di accesso a servizi e benefici, pur non essendo espressamente previsti metodi alternativi. Il *Telecom Disputes Settlement and Appellate Tribunal* viene indicato come *appellate authority* nei casi di violazioni denunciate dal possessore del numero *Aadhaar* s perpetrate da autorità pubbliche o private; l'introduzione di *civil penalties* per il mancato rispetto delle norme in materia di raccolta, conservazione e utilizzo dei dati, è accompagnata dalla eliminazione della *Section 57* (che prevedeva la possibilità di utilizzo del metodo identificativo mediante *Aadhaar* da parte di soggetti privati), ritenuta eccessivamente invasiva dei diritti alla riservatezza e protezione dei dati da parte della Corte. Per quanto qui solo schematicamente e riassuntivamente richiamate (altre misure sono la *Digital ID* e la possibilità di una *offline identification*), le modifiche intervenute paiono lasciare alcuni aspetti problematici irrisolti: permane la mancanza di una specifica normativa in materia di privacy e *data protection*, cui certamente gli emendamenti apportati all'*Aadhaar Act* non possono sopperire. Inoltre è da chiedersi se anche la volontarietà dell'uso del metodo identificativo *Aadhaar* per compagnie telefoniche e banche sia conforme a quanto indicato dalla Corte, che sembrava invece per certi versi vietare *in toto* l'uso del codice da parte di entità private. Più ampiamente sulle nuove soluzioni, anche da un punto di vista tecnico: A. Rajput A, K. Gopinath, *Analysis of Newer Aadhaar Privacy Models*, in V. Ganapathy, T. Jaeger, R. Shyamasundar (eds), *Information Systems Security*, Berlin, 2018, 386-404.

2012, i giudici costituzionali hanno ritenuto che le misure degli art. 5[48] e 10[49] del progetto (oltre ad altre ad esse legate) non potessero considerarsi proporzionate rispetto allo scopo della normativa, che travalicava, nelle disposizioni indicate, il mero fine identificativo. Il Conseil non mancava di sottolineare infatti come l'ampiezza del *repository*, la delicatezza della natura dei dati biometrici raccolti[50] e l'estensione delle finalità per le quali era reso possibile accedere ai dati, portassero alla mancata proporzionalità della normativa sottoposta al suo esame[51]. Profili critici erano da individuare dunque nell'assenza di limitazioni di ordine temporale alla conservazione e trattenimento del dato nel database così come nella mancanza di idonee e adeguate salvaguardie e restrizioni circa l'uso della banca dati, soprattutto con riferimento alla possibilità di accesso alla stessa a scopo di indagine per determinati reati (tra i quali terrorismo), su autorizzazione del Procuratore della Repubblica e previa informazione al soggetto interessato. A seguito della pronuncia richiamata, la proposta di legge, depurata dagli elementi patologici rilevati dal Conseil, si limitava a prevedere l'inserimento delle impronte digitali nel chip della carta d'identità, senza provvedere alla creazione di un database ed escludendo la possibilità di accesso ai

[48] L'art. 5 della legge proposta prevedeva quali scopi della raccolta e conservazione dei dati biometrici "en premier lieu, lors de l'établissement des titres d'identité et de voyage, en deuxième lieu, pour les besoins de l'enquête relative à certaines infractions, sur autorisation du procureur de la République ou du juge d'instruction, et, en troisième lieu, sur réquisition du procureur de la République aux fins d'établir, lorsqu'elle est inconnue, l'identité d'une personne décédée, victime d'une catastrophe naturelle ou d'un accident collectif".



[49] Questa disposizione amplia il novero dei soggetti legittimati all'accesso al database, individuati "aux agents individuellement dèsignès et dument habilités des services de police et de gendarmerie nationales d'avoir accès au traitement de données à caractère personnel créé en application de l'article 5, pour les besoins de la prévention et de la répression des atteintes à l'indépendance de la Nation, à l'intégrité de son territoire, à sa sécurité, à la forme républicaine de ses institutions, aux moyens de sa défense et de sa diplomatie, à la sauvegarde de sa population eg France et à l'étranger et aux éléments essentiels de son potentiel scientifique et économique et des actes de terrorisme".

[50] Il Conseil sul punto riprende quanto affermato dal CNIL (Commission nationale de l'informatique et des libertés) nella sua nota del 25 ottobre 2011: "La Commission rappelle que les données biométriques ne sont pas des données à caractère personnel "comme les autres". Elles présentent en effet la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir. À la différence de toute autre donnée à caractère personnel, la donnée biométrique n'est donc pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable. Elle appartient donc à la personne qui l'a générée et tout détournement ou mauvais usage de cette donnée fait alors peser un risque majeur sur l'identité de celle-ci".

[51] "Considérant, en second lieu, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en oeuvre de manière adéquate et proportionnée à cet objectif. (..). Considérant qu'il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi", decisione n. 2012-652, del 22 marzo 2012.

dati biometrici se non per scopi di validazione e controllo del documento stesso (Loi n. 410/2012, 27 marzo 2012).

La problematica e i timori sollevati in occasione dell'introduzione di un database centralizzato di raccolta di impronte digitali non è però stata trattata dai giudici francese solamente in quella occasione: se ci allontaniamo per un attimo dalla disciplina attinente la carta d'identità per analizzare invece quella riguardante il passaporto, è possibile notare come il Conseil d'État si fosse già pronunciato in materia di raccolta e conservazione di dati biometrici nel 2008[52], con riferimento al Décret n° 2008-426, del 30 aprile 2008[53], che prevedeva non solo la raccolta di ben otto impronte digitali (rispetto alle due richieste dalla normativa europea in materia), ma anche la costruzione di un database centralizzato. In quella occasione il Consiglio di Stato aveva ritenuto illegittima, in quanto sproporzionata, eccessiva e non pertinente allo scopo, la richiesta di un numero così elevato di impronte, confermando però la legittimità della conservazione in un *repository* nazionale delle impronte raccolte. Per giungere a tale conclusioni, i giudici amministrativi infatti avevano tenuto in considerazione sia gli effetti positivi della presenza di un *fichier national*, che facilita il sistema identificativo e lo rende più efficace avverso la lotta alle frodi d'identità, sia la sua incidenza non sproporzionata sulla riservatezza e vita privata dei cittadini, ritenendo idonee e sufficientemente tutelanti le precauzioni previste nel decreto di istituzione del database (finalità espressamente previste e durata di conservazione limitata ed esplicitamente fissata)[54]. Riducendo infatti la possibilità



[52] Conseil d'État, Ass, 26 octobre 2011, *Association pour la promotion de l'image et autres*, n° 317827.

[53] Questo decreto interveniva modificando il previo *Décret* n. 2005-1726 del 30 dicembre 2005, *relatif aux passeports électroniques*. Tale disposizione normativa era stata adottata in attuazione del Reg. UE 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri. Tale Regolamento europeo stabilisce la necessità di inserire due impronte digitali nel passaporto, oltre ad una immagine fotografica del viso. Questo obbligo non implica però anche la necessità di predisporre un database centralizzato per la conservazione dei dati stessi. Sul punto ha avuto modo di pronunciarsi anche la Corte di Giustizia dell'Unione Europea nel caso *Michael Schwarz v. Stadt Bochum* (C-291/12 del 17 ottobre 2013), nel quale i giudici di Lussemburgo, hanno affermato: "Poiché tale regolamento non prevede nessun'altra forma né alcun altro mezzo di conservazione di dette impronte, esso non può essere interpretato, come sottolineato dal considerando 5 del regolamento n. 444/2009, come idoneo a fornire, in quanto tale, un fondamento giuridico ad una eventuale centralizzazione dei dati raccolti in base ad esso oppure all'impiego di questi ultimi a fini diversi da quello di impedire l'ingresso illegale di persone nel territorio dell'Unione" (par. 62). La Corte dunque non si è pronunciata in merito alla legittimità della creazione di un database nazionale e non lo ha fatto neppure in occasione della sentenza *Willems et al. v. Burgemeester van Nuth et al.*, C- 446/12 a C-449-12,16 aprile 2015, in cui ha statuito che la normativa europea in materia di passaporto non richiede agli Stati Membri di garantire che i dati raccolti non vengano conservati, trattati o usati per altri scopi diversi da quello identificativo.

[54] "Le Conseil d'État n'a ainsi pas suivi la CNIL qui, dans un avis du 11 décembre 2007, s'était déclarée défavorable à l'enregistrement des données biométriques dans le fichier TES, qu'elle estimait disproportionné aux objectifs poursuivis. Le Conseil d'État a relevé que le fichier n'était consulté qu'en cas de demande ou de renouvellement d'un passeport ou en cas de falsification probable de celui-ci. En outre, et surtout, toute recherche dans le fichier TES à partir d'éléments biométriques est impossible, notamment du fait du stockage dans des

di accesso alla banca dati alle sole finalità di rilascio o rinnovo del passaporto o per verificare, in caso di dubbi, la veridicità del documento, viene resa impossibile "toute recherche dans le fichier TES (Titres électroniques sécurisés) à partir d'éléments biométriques, notamment du fait du stockage dans des bases différentes des données biométriques et des données d'identité"[55]. In questo caso si può dunque notare come non venga messa in discussione né la legittimità della raccolta a scopo identificativo di dati biometrici né, in sé e per sé, la creazione di un database degli stessi. Ciò che dunque porta il Conseil d'État a pronunciarsi diversamente rispetto al Conseil Constitutionnel, è la differente valutazione circa la sussistenza, nella disciplina regolativa della banca dati, di apposite tutele e limitazioni in grado di arginare le derive lesive dei diritti fondamentali dei cittadini francesi.

Proprio su questo aspetto e sull'analisi della presenza di tali elementi di garanzia, si fonda anche una più recente decisione del Conseil d'État (sentenza n. 404966 del 3 ottobre 2018), chiamato questa volta a pronunciarsi su un'istanza di annullamento del Décret n. 2016-1480, 20 ottobre 2016, *Autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*. Tale disposizione normativa prevede infatti l'istituzione di un database (*Fichier TES - Titres électroniques sécurisés*), posto sotto il controllo del Ministero dell'Interno, deputato alla conservazione dei dati personali e biometrici raccolti in occasione della erogazione di carte d'identità. Anche in questo caso la decisione finale del Conseil di respingere la richiesta dei ricorrenti è stata dettata dalla presenza di restrizioni e precauzioni ritenute adeguate a scongiurare possibili abusi nelle fasi di utilizzo e di accesso, diversamente da quanto previsto nella richiamata proposta del 2012, che non aveva superato il vaglio del Conseil Constitutionnel. Viene infatti sottolineato come il trattamento dei dati, anche biometrici, raccolti non abbia altra finalità se non quella di permettere il rilascio del documento e di migliorare l'efficacia dei controlli: gli artt. 1 e 2 del decreto esaminato escludono infatti qualsiasi possibilità di ricerca e identificazione effettuata a partire dai dati biometrici[56] e, ai sensi dell'art. 3, ciò è vietato anche nei casi in cui, per ragioni di tutela degli interessi fondamentali della Nazione, l'accesso al database sia concesso ad autorità di *law enforcement*[57].



bases différentes des données biométriques et des données d'identité", come riassunto dal Conseil Constitutionnel, in *Commentaire à la décision n. 2012-652 DC* del 22 marzo 2012, reperibile sul sito del Conseil all'indirizzo www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2012652dc/ccc_652dc.pdf.

[55] Un'analisi approfondita di questa pronuncia può essere letta in M. Cappelletti, *Il principio di proporzionalità tra tutela della privacy e sicurezza: il caso della carta d'identità biometrica francese*, in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato*, Santarcangelo di Romagna, 2013, 649-666.

[56] L'accesso viene dunque effettuato solo a partire dal soggetto in possesso del documento di riconoscimento.

[57] Le preoccupazioni dei ricorrenti, che hanno peraltro ampiamente richiamato la giurisprudenza del Conseil Constitutionnel del 2012, erano rivolte in particolare a disposizioni dubbie quali l'art. 4, laddove stabilisce "les agents des services de la police nationale, les militaires des unités de la gendarmerie nationale et les agents des services spécialisés du reinsegnement" possono, a scopi di prevenzione e repressione di attentati agli interessi fondamentali della Nazione e di atti di terrorismo, accedere ai dati contenuti nel

Restano comunque i timori, espressi peraltro da CNIL (*Commission nationale de l'informatique et des libertes*), *Secrétariat d'Etat au Numerique*) e dall'ANSSI (*Agence Nationale de la sécurité des systémes d'information*)[58], che un simile sistema possa essere deviato e allontanato dalle finalità strettamente legate alle operazioni di identificazione, aprendo ad un possibile uso arbitrario dei dati stessi[59].

La recente giurisprudenza francese e il continuo ripresentarsi all'attenzione dei giudici nazionali di questioni relative alla creazione di sistemi identificativi basati sulla conservazione di dati biometrici in database centralizzati, aiutano a comprendere come i dubbi giuridici e di legittimità costituzionale di tali misure, così potenzialmente lesive della riservatezza dei cittadini, siano persistenti e impegnino sempre di più Corti e legislatori nel tentativo di trovare un corretto bilanciamento tra interessi e diritti e di predisporre idonee garanzie e protezioni.

## 4. Dai sistemi identificativi *one-to-many* alla inclusione dei dati biometrici nelle Carte d'Identità Elettroniche: rilievi conclusivi e aspetti problematici

Il dibattito sull'utilizzo di dati biometrici a scopo di riconoscimento è fortemente sentito e attuale non solo rispetto alle modalità di identificazione *one-to-many* e alla previsione di database centralizzati, bensì anche con riferimento ai sistemi *one-to-one*. Esemplificative di questa tendenza sono le vicende e le discussioni che hanno segnato il Belgio negli ultimi mesi del 2018: il Parlamento nazionale ha infatti approvato una legge[60] integrante l'obbligo di inserire due impronte digitali, oltre alla fotografia del soggetto richiedente, all'interno del documento di identità nazionale in formato elettronico, a partire dal mese di aprile 2019. Tale misura non prevede la creazione di un database centralizzato, sull'esempio francese o indiano, bensì solamente l'inserimento dei dati biometrici all'interno di un chip posto nel documento[61], imponendo la distruzione dei dati stessi dopo un



database. È facilmente comprensibile quanto la nozione di "interesse fondamentale della Nazione" sia molto ampia e non abbia nulla a che vedere (o poco) con la *ratio* della normativa, volta ad individuare falsificazioni della documentazione. Il Conseil d'État, considerando che la stessa disposizione afferma l'impossibilità di accedere "*aux images numérisées*" delle impronte, ritiene che la disciplina predisposta sia tale da far sì che la consultazione dei dati biometrici possa avvenire solo per confermare che la persona che presenta una domanda di rinnovo della carta d'identità sia quella cui il documento era stato attribuito e assicurare così l'assenza di frodi.

[58] Questo, nella deliberazione in materia di TES, ha espresso riserve e dubbi sul sistema ritenendo come, di fronte all'evoluzione tecnologica e alle minacce di *cybercrimes* e di *data breach*, la struttura del TES sia tecnicamente perfettibile.

[59] Per una analisi critica di questa pronuncia, si legga: J.P. Foegle, *Fichier TES: le Conseil d'Etat donne son feu vert au fichage biométrique de 67 millions de francais*, in *La revue des droits de l'homme*, 2 novembre 2018, journals.openedition.org/revdh/4879. Restano poi aperti interrogativi circa la possibilità, da parte delle forze dell'ordine, di accedere al database per utilizzare non tanto le impronte digitali, che sono espressamente escluse da qualsiasi uso differente rispetto a quello identificativo, quanto più delle immagini del volto, magari per implementare sistemi di riconoscimento facciale.

[60] *Loi portant des dispositions diverses concernant le Registre national et les registres de population*, del 14 novembre 2018, che modifica la Legge del 19 Luglio 1991.

[61] Ciò è simile a quanto avviene in Italia. Per un approfondimento sulla normativa italiana, si richiama il D. l. 19 giugno 2015, n. 78 e il Decreto del Ministero dell'Interno, 23 dicembre 2015, recante disposizioni sulle "Modalità tecniche di emissione della Carta d'identità

periodo massimo di 3 mesi dalla raccolta[62]. Questa decisione tuttavia non ha mancato di sollevare dubbi e critiche: il Garante nazionale della privacy belga (*Autorité de Protection des donnés*, APD) ha infatti espresso parere sfavorevole[63] alla richiamata normativa, ritenendo non rispettato il principio di proporzionalità; non sono infatti presenti adeguate misure di sicurezza e protezione dei dati, nonché un elenco specifico delle finalità per le quali le autorità pubbliche (con particolare riferimento a quelle di *law enforcement*) possano effettuare operazioni di controllo tra le impronte contenute nella carta d'identità e quelle del soggetto sottoposto a riconoscimento. Per l'APD inoltre mancano adeguate giustificazioni all'adozione di una simile misura normativa: il Governo infatti avrebbe dovuto presentare prove attestanti l'inefficacia o l'insufficienza delle misure di garanzia di sicurezza e autenticità relative alle carte d'identità già esistenti (che contengono ad esempio un ologramma e l'immagine del titolare). Ciò che rileva particolarmente poi nel parere espresso dall'Autorità garante belga è la connessione e l'esplicito riferimento alla disciplina in materia di dati biometrici contenuta nel GDPR[64]: tali dati, infatti, come richiamato sopra,

elettronica", in materia di CIE (Carta d'Identità Elettronica). Le impronte digitali del richiedente il documento sono raccolte e inserite nel chip posto all'interno della Carta e non vengono conservate in nessun altro luogo, bensì cancellate al termine del periodo di tempo strettamente necessario per il rilascio del documento stesso. Non viene quindi prevista alcuna banca dati (l'unica sussistente è quella del Casellario centrale d'identità, che rappresenta un consistente archivio della Polizia italiana, contenente le impronte digitali dei soggetti fermati per accertamenti o crimini). L'art. 3 del Decreto del Ministero dell'Interno sopra richiamato assume grande rilevanza in quanto limita l'uso dei dati biometrici solamente alla verifica dell'autenticità del documento d'identità mediante la comparazione dei dati in quest'ultimo contenuti con quelli rilevati dal soggetto la cui identità vuole essere accertata, escludendo dunque sistemi identificativi del tipo *one-to-many*, specificando espressamente come gli elementi biometrici debbano essere usati esclusivamente per verificare l'autenticità della CIE e l'identità del titolare attraverso elementi comparativi direttamente disponibili.



[62] Per una lettura critica della normativa, considerata sproporzionata rispetto al fine, si veda: W. Vandeelde, *If you've got nothing to hide, you've got nothing to fear: fingerprints on Belgian eID cards*, in *Centre for IT & IP Law Blog*, 15 gennaio 2019, www.law.kuleuven.be/citip/blog/if-youve-got-nothing-to-hide-youve-got-nothing-to-fear-fingerprints-on-belgian-eid-cards/

[63] APD, *Avis d'initiative* n. 106/2018, 17 ottobre 2018 – *Audition de l'Autorité de Protection des données sur le project de la loi portant des dispositions diverses concernant le Registre National et les Registres de Population* (DOC 543256); l'Autorità si era peraltro già precedentemente pronunciata sul punto con l'*Avis* n. 18/2018 del 28 febbraio 2018.

[64] Non potendo in questa sede ricostruire l'intera disciplina europea dei dati biometrici, si vuole solo sottolineare come dubbi e criticità permangano circa l'applicazione del GDPR al trattamento di tali categorie di dati per scopi identificativi. Tra i molti profili problematici, sicuramente rilevante è la disciplina particolare nel caso di trattamento di tali dati da parte di *law enforcement authorities*: questa facoltà è rimessa al rispetto delle condizioni indicate dalla Dir. 2016/680 UE, fuoriuscendo dunque dalla disciplina del GDPR (si dovranno attendere in materia le normative nazionali di recepimento per comprendere come i criteri di stretta necessità e proporzionalità saranno considerati dai legislatori degli Stati Membri). Il legislatore europeo inoltre parla genericamente di dati biometrici come quelli utilizzati per scopi identificativi, senza distinguere in alcun modo tra sistemi identificativi in senso tecnico (quelli *one-to-many*, che prevedono l'uso di un database) e di verifica (*one-to-one*), il che porta a chiedersi se il medesimo regime normativo sia da applicarsi all'una e all'altra categoria di metodi di utilizzo. A ciò si somma il fatto che specifiche normative nazionali possano prevedere ulteriori condizioni e tutele (come concesso dall'art. 9, co. 4, GDPR), che rischiano di complicare ulteriormente un quadro già molto articolato. Da notare infine è il fatto che il GDPR vieta il 'trattamento' dei dati biometrici ma non parla della mera raccolta o

rientrano nella "categoria particolare di dati personali" e seguono pertanto la peculiare disciplina dell'art. 9. Questa permette di superare il divieto generale di trattamento solo in alcuni casi eccezionali (art. 9, co. 2, GDPR), tra i quali si annoverano le esigenze di interesse pubblico. Anche in questo caso viene comunque richiesto il rispetto del principio di proporzionalità con riferimento al fine perseguito, nonché il rispetto dell'essenza del diritto alla protezione dei dati e la predisposizione di misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi del soggetto cui i dati appartengono (art. 9, co. 2, lett. g). Secondo l'Autorità belga proprio questi elementi sarebbero insussistenti nella normativa nazionale, che non presenta idonee salvaguardie volte ad evitare un'intrusione eccessiva nei diritti alla privacy e *data protection* dei cittadini (garanzie sia tecniche che normative, quali una specifica indicazione e limitazione delle finalità di accesso, garanzie specifiche per i dati temporaneamente conservati e individuazione dei soggetti responsabili per gli stessi, nonché una limitazione a quanto strettamente necessario della conservazione dei dati biometrici all'interno del documento). Egualmente mancante sarebbe anche la predisposizione di un adeguato *Data Protection Impact Assessment* (DPIA)[65], richiesto ai sensi dell'art. 35, co. 3, lett. b) del GDPR, prima del trattamento su larga scala di categorie speciali di dati, quali quelli biometrici.

A parere del Garante belga poi risulta particolarmente curioso – e non del tutto appropriato - il richiamo alla proposta di un nuovo Regolamento a livello sovranazionale dei documenti d'identità, che il Governo nazionale utilizza per giustificare la propria decisione normativa[66]. Questa normativa, che vorrebbe estendere l'obbligo di inclusione dei dati biometrici alle carte d'identità degli Stati Membri, ha ricevuto infatti un giudizio fortemente critico da parte del Garante Europeo della Protezione dei Dati (2018/C 338/12)[67]. Le motivazioni di questo parere negativo paiono molto interessanti e utili per giungere alle conclusioni di questa disamina dei sistemi di riconoscimento: ciò che il Garante Europeo rileva infatti è la mancata previsione, nella proposta della Commissione, di espresse "salvaguardie contro l'istituzione, da parte degli Stati membri, di banche dati dattiloscopiche nazionali nel contesto dell'attuazione della proposta stessa. Alla proposta dovrebbe essere aggiunta una disposizione che stabilisca



conservazione degli stessi. Per una puntuale e critica analisi della disciplina dei dati biometrici ai sensi del GDPR, si legga: E. J. Kindt, *Having yes, using no? About the new legal regime for biometric data*, in *Computer Law and Security Review*, 34 (2018), 523-538. Per una panoramica più generale si rimanda ai tanti commentari del GDPR, tra cui G. M. Riccio, G. Scorza, E. Belisario, *GDPR e normativa privacy commentario. Regolamento (UE) 2016/679 del 27 aprile 2016. Decreto di adeguamento D. Lgs. n. 101/2018. Codice privacy D. Lgs n. 196/2003*, Milano, 2018; M. Soffientini (a cura di), *Privacy. Protezione e trattamento dei dati*, Milano, 2018.

[65] Si veda sul punto anche il Considerando 91 del GDPR.

[66] COM (2018) 212, Proposta di Regolamento del Parlamento Europeo e del Consiglio sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione.

[67] Garante Europeo della Protezione dei Dati, *Parere sulla proposta di Regolamento sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e di altri documenti*, 2018/C 338/12, 10 agosto 2018.

ISSN: 2037-6677

esplicitamente che i dati biometrici trattati nel suo contesto debbano essere cancellati immediatamente dopo il loro inserimento nel microprocessore e non possano essere ulteriormente trattati per finalità diverse da quelle esplicitamente indicate nella proposta"[68].

Ecco dunque che queste considerazioni richiamano tutte le vicende giudiziarie esaminate sino ad ora e forniscono lo spunto per chiudere il cerchio iniziato con l'analisi del caso indiano: le critiche mosse al sistema *Aadhaar* così come quelle rivolte al modello francese, che hanno portato, in entrambi i casi, a discuterne la legittimità costituzionale, si fondano proprio sulla ingerenza sproporzionata nella privacy dei cittadini, rappresentata dalla previsione di database centralizzati di dati biometrici. Sotto questo profilo, le posizioni espresse dal Garante Europeo della Protezione dei Dati sembrano indicare un livello di tutela e di applicazione del principio di proporzionalità fortemente restrittivo rispetto alla possibilità di conservazione di dati sensibili in database nazionali, rilevando la lesività non solo del momento del trattamento bensì anche di quello preventivo di raccolta e successivo di conservazione. Da ciò emerge con chiarezza come la molteplicità di soluzioni tecniche ma anche giuridiche nonché i diversi standard di tutela della riservatezza e di protezione dei dati, rendano certamente il dibattito sull'utilizzo di dati biometrici a scopi di riconoscimento ancora aperto.

Spingendoci oltre la singola scelta dei sistemi di riconoscimento e riflettendo sulle conseguenze e sulle domande cui l'analisi della tematica trattata deve indurci, si nota come il *fil rouge* che lega tutti i casi e le normative analizzate possa essere individuato nel forte bisogno di ripensare il ruolo del diritto, che, di fronte all'avanzamento tecnologico, ha il compito non di frenarne lo sviluppo e le potenzialità, bensì di trovare il corretto bilanciamento tra diritti e interessi che



[68] Durante la fase di revisione di questo contributo, la procedura legislativa relativa alla proposta di Regolamento esaminata è stata completata e il testo del Regolamento, sottoscritto dal Presidente del PE e del Consiglio il 20 giugno 2019, è ora in attesa di pubblicazione sulla Gazzetta Ufficiale dell'UE. Merita essere sottolineato come il testo finale includa talune delle indicazioni del Garante Europeo, prevedendo nei Considerando 21 e 22 specifiche tutele e chiarimenti rispetto alla raccolta, conservazione e distruzione dei dati biometrici trattati a scopi di riconoscimento. Viene pertanto stabilito, richiamando anche la giurisprudenza della CGUE sopra richiamata con riferimento ai passaporti, che: "Il presente regolamento non fornisce una base giuridica per la costituzione o il mantenimento di banche dati a livello nazionale per la conservazione di dati biometrici negli Stati membri, che è una questione di diritto nazionale da trattare nel rispetto del diritto dell'Unione in materia di protezione dei dati. Il presente regolamento, inoltre, non fornisce una base giuridica per la costituzione o il mantenimento di una banca dati centralizzata a livello dell'Unione. (22) Gli identificatori biometrici dovrebbero essere raccolti e conservati nel supporto di memorizzazione delle carte d'identità e dei titoli di soggiorno ai fini della verifica dell'autenticità del documento e dell'identità del titolare. Tale verifica dovrebbe essere effettuata soltanto da personale debitamente autorizzato e soltanto quando la legge prevede che sia necessario il documento. Inoltre, i dati biometrici memorizzati ai fini della personalizzazione delle carte d'identità o dei titoli di soggiorno dovrebbero essere conservati in modo altamente sicuro e soltanto fino alla data di acquisizione del documento e, in ogni caso, per non oltre 90 giorni dalla data di rilascio di tale documento. Trascorso tale periodo, tali dati biometrici dovrebbero essere immediatamente cancellati o distrutti. Ciò dovrebbe far salvo qualsiasi altro trattamento di tali dati in conformità del diritto dell'Unione e nazionale in materia di protezione dei dati".

paiono inconciliabili. L'esempio fornito dalle innovative modalità di identificazione/verifica dell'identità induce a porci due cruciali quesiti, riassunti magistralmente dal Giudice Chandrachud nella sua più volte richiamata *dissenting opinion*: "First, are there competing interests between human rights and 'welfare furthering technology' in democratic societies? Can technologies which are held out to bring opportunities for growth, also violate fundamental human freedoms? Second, if the answer to the first is in the affirmative, how should the balance be struck between these competing interests?"[69]. Le tentazioni, cui le autorità pubbliche sono sottoposte, di creare meccanismi di maggiore controllo sui cittadini per aumentare l'efficienza nell'allocazione delle risorse (come nel caso del progetto di identificazione universale indiano) o per garantire verifiche dell'identità più efficaci, rappresentano un nuovo *stress-test* per il legislatore così come per le Corti, spesso chiamate a svolgere la funzione di veri e propri "scudi" di fronte a queste possibili derive[70].

L'esempio indiano poi, proprio sotto il profilo del bilanciamento, induce ad una ulteriore riflessione e aggiunge un elemento di complessità agli aspetti già rilevati: mentre nel contesto europeo siamo abituati, di fronte all'utilizzo dei dati personali, a vedere la garanzia della sicurezza come contrapposta alla tutela della privacy e alla protezione dei dati[71], nel caso sottoposto all'attenzione della Corte Suprema indiana i due piatti della bilancia sono occupati da riservatezza da un lato e dal diritto alla dignità umana dall'altro. Ciò a significare quanto le nuove tecnologie, mediante l'uso di dati, quali quelli biometrici ad esempio, vengano impiegate oggi per risolvere problematiche non più relegate al solo ambito delle indagini o prevenzione dei crimini ma anche per rispondere ad altri bisogni fondamentali quali il diritto al cibo e ad una esistenza dignitosa. Tali utilizzi, mutando anche i diritti in gioco, non possono che aprire a tutta una nuova serie di considerazioni e valutazioni sulla proporzionalità delle misure adottate. Se infatti si registrano sempre maggiori potenzialità e utilizzi a garanzia di diritti quali la dignità e la vita, non può essere ignorato quanto queste nuove forme di tecnologie rendano possibile, anche mediante l'uso di dati sensibili e personalissimi, la creazione di sistemi in grado di tramutarsi in "forme discrete ma non meno insidiose di biosorveglianza"[72], capaci di trasformare il corpo e l'identità umana in un vero e proprio strumento di controllo.



Compito del legislatore, del giudice e del giurista in generale, è far sì che, di fronte a queste prospettive, "the constitutional guarantees cannot be subject to

[69] Giudice D. Chandrachud, Dissenting Opinion, par. 12, *Justice Puttaswamy v. Union of India.*
[70] Si legga più ampiamente sul punto: L. Scaffardi, *Dati genetici e biometrici: nuove frontiere per le attività investigative*, in L. Scaffardi (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, 37-64.
[71] Si pensi alle già richiamate sentenze della CGUE *Digital Rights Ireland Ltd & others, Tele2 Sverige and Watson* in materia di conservazione e accesso ai dati relativi alle comunicazioni per finalità di sicurezza, o alla recentissima *Big Brother Watch & Others v. UK*, (58170/13, 62322/14 e 24960/15) decisa dalla Corte EDU sui dati conservati e utilizzati dai servizi di intelligence per la tutela della sicurezza nazionale.
[72] Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: i profili bioetici della biometria*, cit.

the vicissitudes of technology"[73]. Ciò deve valere ancora di più quando in gioco è la cessione, più o meno imposta, di una parte dell'individuo stesso, come quella che avviene mediante l'utilizzo dei dati biometrici[74]. In questo caso assume grande valore quel principio di "*policy before technology*" sopra richiamato, che impone regole in grado di prevedere e arginare rischi e compressioni sproporzionate dei diritti fondamentali alla riservatezza e alla protezione dei dati, anche e soprattutto in un'era "*of ubiquitous dataveillance*"[75].



[73] Giudice D. Chandrachud, Dissenting Opinion, par. 269, *Justice Puttaswamy v. Union of India*.

[74] "Biometrics have the ability to create trusted identities and where that exists in digital, transactional ecosystems, a high degree of risk to fundamental civil liberties and privacy also exists. It is simply not possible to have a digital ID with biometrics that does not create fundamental risks of surveillance, risks of social and or political control using the system, and the risk of pervasive privacy violations. No matter what the level of economic or legislative development exists for a region, *Do not harm* must be the bedrock guiding principle of all digital biometric identity systems", P. Dixon, *A failure to "Do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, op. cit., 7.

[75] Y. McDermott, *Conceptualizing the right to data protection in an era of Big Data*, in *Big Data and Society*, 1 (2017), 1 ss. Per ulteriori spunti di riflessione sul rapporto tra tecnologia e diritti fondamentali, con particolare riferimento al diritto alla privacy e alla protezione dei dati, si rimanda a: D. Brin, *The transparent society. Will technology force us to choose between privacy and freedom?*, Cambridge, 1998; D. Solove, *"I've got nothing to hide" and other misunderstandings of privacy*, in *San Diego Law Review*, 44 (2007), 745-772.