ADiM BLOG
Settembre 2024
ANALISI & OPINIONI

Digitalizzazione delle procedure di ingresso: il trattamento dei dati e il difficile equilibrio tra la sicurezza pubblica e il rispetto dei diritti fondamentali degli immigrati

Cristiana Napolitano

Dottoranda di ricerca
Presso l'Università degli Studi di Cassino e del Lazio Meridionale

Parole Chiave

Dati biometrici – Sicurezza pubblica – Digitalizzazione –Diritti fondamentali –Proporzionalità

Abstract

In questo contributo viene affrontato il delicato tema dell'equilibrio tra la sicurezza pubblica e i diritti fondamentali dei migranti nell'era digitale, con particolare attenzione alla digitalizzazione delle procedure di ingresso. L'analisi si concentra, soprattutto, sulla questione della proporzionalità e della parità di trattamento nella raccolta e conservazione dei dati biometrici. Più nello specifico ci si interroga se il livello di tutela garantito ai cittadini dell'Unione europea e agli immigrati regolari sia effettivamente equiparabile al sistema di prelievo e trattamento dei dati riservato ai richiedenti asilo e agli altri migranti privi, all'arrivo, di regolare visto o permesso di soggiorno, anche alla luce della nuova normativa contenuta nell'AI Act. Quest'ultimo prevede alcune deroghe che rispondono a motivi di sicurezza pubblica che possono portare a potenziali abusi e discriminazioni, in particolare nell'uso dello strumento del riconoscimento facciale.

Abstract in inglese

This contribution addresses the delicate issue of balancing public security with the fundamental rights of migrants in the digital age, with particular attention to the digitalization of entry procedures. The analysis focuses on the issue of proportionality and equal treatment in the collection and storage of biometric data. More specifically, it examines whether the level of protection guaranteed to EU citizens and legal immigrants is comparable to the system of data collection and processing reserved for asylum seekers and other migrants without a regular visa or residence permit upon arrival. This is particularly relevant in light of the new legislation contained in the AI Act, which provides certain exemptions in response to public safety concerns that may lead to potential abuse and discrimination.

1. Premesse

Nell'ambito del tema delle politiche di integrazione degli stranieri, una questione centrale è rappresentata dall'equilibrio tra la sicurezza pubblica e i diritti fondamentali dei migranti nell'era digitale, nella prospettiva di garantire una reale ed effettiva integrazione dell'immigrato sul territorio nazionale. L'incremento dell'impiego delle tecnologie digitali, unitamente alla raccolta di dati personali, ha reso infatti impellente l'esigenza di trovare un bilanciamento tra due necessità che in apparenza possono risultare contrapposte: da un lato, la sicurezza interna dello Stato ospitante; dall'altro, il diritto ad una accoglienza che non solo rispetti la dignità dell'immigrato e, quindi sia espressione del principio di uguaglianza, inteso quale corollario del diritto dell'immigrato ad essere realmente integrato all'interno dello Stato ospitante, ma che in nessun modo vada a comprimere i suoi diritti fondamentali, quali il diritto alla privacy, alla protezione dei dati e all'accesso alle informazioni che lo riguardano.

La questione è rilevante in sé e per sé e nella misura in cui bisogna prendere atto che la digitalizzazione delle procedure di ingresso, oltre a trovare un fondamento nel nuovo Regolamento sull'Intelligenza Artificiale, c.d. AI Act, si inscrive in un contesto normativo nel quale gli strumenti digitali relativi al trattamento dei dati personali incidono prevalentemente sui cittadini di Paesi terzi. Si pensi, ad esempio, al Regolamento UE 2019/86 che ha istituito un sistema centralizzato per coloro che hanno la cittadinanza di uno Stato terzo e che a sua volta ha integrato il Sistema europeo di informazione sui casellari giudiziari; al Regolamento UE 2017/2226 che ha istituito il sistema di ingresso e di uscite o, ancora, al Sistema di informazione Schengen di seconda generazione, dove una segnalazione può essere inserita con riferimento ad un soggetto di uno Stato terzo che sia stato destinatario di una misura di allontanamento o di un rifiuto di ingresso o di espulsione.

Il processo di integrazione inizia, pertanto, già all'ingresso dell'immigrato nel Paese ospitante, rappresentando il primo momento di contatto tra quest'ultimo e lo straniero, che a sua volta deve avere, quantomeno, la percezione di godere degli stessi diritti fondamentali garantiti ai cittadini.

D'altronde, la stessa Corte costituzionale ha più volte sottolineato, in riferimento al disposto di cui all'art. 3 della Costituzione italiana, come l'uguaglianza, almeno nel suo contenuto

minimale di uguaglianza in senso formale, sia garantita a tutti, indistintamente cittadini e stranieri[1]. Nella legislazione nazionale vi è anche il dettato di cui all'art. 43 del D.lgs. n. 286/98 che, per primo, ha inserito il principio di non discriminazione all'interno di una normativa che disciplina il fenomeno migratorio. Lo stesso principio è stato poi sancito a livello europeo, in un primo momento tramite alcune direttive che hanno affrontato il tema in modo più ristretto rispetto alla lettera del citato art. 43 del D.lgs. n. 286/98. Un esempio significativo è rappresentato dalla direttiva 2000/43/CE, che, pur estendendo il principio di non discriminazione a tutti gli individui, lo limita specificamente alle discriminazioni basate sulla razza e sull'origine etnica, nonché dalla direttiva 2003/109/CE, che prevede il principio di non discriminazione solo per i cittadini di Paesi terzi che hanno ottenuto lo *status* di soggiornante di lungo periodo. Successivamente, con l'entrata in vigore della Carta dei diritti fondamentali dell'Unione Europea, il cui articolo 21 vieta espressamente qualsiasi forma di discriminazione, il principio è stato ulteriormente consolidato e ampliato, trovando applicazione nei confronti di qualunque individuo, a prescindere dalla nazionalità, purché soggetto al diritto dell'Unione.

Tuttavia, nonostante la disciplina di carattere generale esistente a livello tanto nazionale, quanto europeo, si registra di fatto una disparità nelle normative e nelle prassi relative al prelievo e trattamento dei dati sensibili con la conseguenza che le politiche di gestione dei flussi migratori finiscono per rendere più ostica l'integrazione degli immigrati nel contesto sociale. Infatti, sebbene si tratti di procedure formulate per rafforzare la sicurezza delle frontiere, esse spesso appaiono sotto certi aspetti, non pienamente conformi ai principi di non discriminazione e uguaglianza.

Come avremo modo di osservare, ragioni di sicurezza prevalgono sulle esigenze di uguaglianza: le procedure adottate ai confini, finalizzate al prelievo dei dati biometrici degli immigrati in ingresso, non garantiscono affatto un'effettiva parità, né tra immigrati e cittadini, né all'interno della stessa categoria degli immigrati, evidenziando differenze sostanziali tra immigrati regolari e irregolari.

2. La raccolta e trattamento dei dati biometrici degli immigrati alla prova del principio di proporzionalità.

Il prelievo e il trattamento dei dati personali degli immigrati, al momento del loro ingresso alle frontiere, rappresentano, si è detto, un terreno d'indagine privilegiato sul quale misurare la prevalenza dell'interesse pubblico alla sicurezza sulle ragioni di non discriminazione degli immigrati.

Sul presupposto che tali dati abbiano natura sensibile, si presume che la disciplina regolatoria

[1] *Cfr. ex multis*, Corte Cost., sentenza del 23 novembre 1967, n. 120; Corte Cost. sentenza del 20 gennaio 1977, n. 46; Corte Cost., sentenza del 21 giugno del 1979, n. 54.

debba necessariamente aderire ai principi di *data protection*, includendo misure specifiche per salvaguardare i diritti fondamentali delle persone coinvolte. Tale disciplina deve, in altri termini, risultare proporzionata alle finalità di sicurezza pubblica per cui è stata prevista, garantendo al contempo il rispetto della dignità, della privacy, dei diritti individuali degli immigrati e, soprattutto, del principio di uguaglianza.

A questa conclusione si giunge muovendo dalla considerazione che la tutela accordata al diritto alla privacy e alla protezione dei dati personali dal Regolamento UE 2016/679 (GDPR), così come previsti dalla Carta dei diritti fondamentali, non possa ritenersi limitata ai cittadini dell'Unione europea (v. Garante Europeo della protezione dei dati).

La questione assume ancora più rilevanza ove ad essere coinvolti siano, oltre ai richiedenti protezione internazionale, i minori d'età.

Le disposizioni della Carta vengono, infatti, in rilievo ogni qual volta si applichi a delle persone fisiche il diritto dell'UE, come quello contenuto nel Sistema europeo comune di asilo. Ne deriva che il soggetto che presenti una richiesta di protezione internazionale secondo la disciplina europea vigente, per il solo fatto di aver presentato la domanda, accede al Sistema europeo comune di asilo (c.d. CEAS), venendo quindi assoggettato a norme di diritto dell'UE e, di conseguenza, anche alle garanzie contenute nella Carta.

Appare dunque evidente che il GDPR debba necessariamente applicarsi anche ai richiedenti asilo all'interno dell'Unione. Tuttavia, va rilevato come la protezione dei dati personali loro garantita possa risultare, sotto alcuni profili, meno rigorosa rispetto a quella accordata ai cittadini dell'Unione Europea.

Questa disparità emerge in modo particolarmente evidente quando si adotta come parametro di riferimento il principio di proporzionalità sancito dall'art. 52, par. 1, della Carta, secondo il quale qualsiasi limitazione ai diritti garantiti deve essere strettamente necessaria e proporzionata al raggiungimento di un obiettivo legittimo. In tal senso basti pensare alla rigorosa interpretazione che di tale principio ha dato la Corte di Giustizia dell'Unione Europea con specifico riferimento al trattamento dei dati dei cittadini eurounitari. Essa ha infatti più volte sottolineato la necessità di evitare un'eccessiva compromissione del diritto alla privacy e all'autonomia informativa dei soggetti interessati, anche quando le misure in questione siano giustificate da esigenze di sicurezza interna dello Stato o da motivi di interesse pubblico. Pur riconoscendo la legittimità di tali finalità, la Corte ha ribadito che esse non devono giustificare interventi che vadano oltre quanto strettamente necessario, imponendo quindi un'attenta valutazione della proporzionalità tra l'obiettivo perseguito e l'impatto sui diritti fondamentali. Un significativo esempio è rappresentato dalla sentenza Schwarz, dove la Corte si è interrogata, in materia di prelievo di dati biometrici, circa l'esistenza di una effettiva proporzionalità tra la misura relativa al prelievo e alla conservazione delle impronte digitali dei cittadini dell'UE nei passaporti e l'esigenza di prevenire la falsificazione di questi ultimi al fine di impedirne l'uso fraudolento e di evitare, quindi, l'ingresso nel territorio europeo di persone non autorizzate.

Nell'esaminare, dunque, la reale necessità delle misure che prevedono il rilevamento delle

impronte digitali, la Corte ha sottolineato non solo come la normativa specifica contemplasse la raccolta delle impronte di sole due dita, ma anche come la conservazione centralizzata delle stesse all'interno del passaporto non comportasse, di fatto, alcun rischio, dal momento che quest'ultimo era destinato a rimane in possesso esclusivo del titolare. Non vi erano, quindi, alternative che comportassero un minore sacrificio dei diritti fondamentali, considerando altresì che le impronte digitali erano utilizzate esclusivamente per verificare l'autenticità del passaporto e l'identità del suo titolare.
Eppure, come si è detto e come si avrà modo di osservare meglio nei paragrafi successivi, questo approccio rigoroso alla proporzionalità, che è stato applicato in modo efficace per tutelare i diritti dei cittadini dell'Unione, non sempre trova un'applicazione altrettanto stringente nei confronti dei cittadini extracomunitari.
Infatti, la raccolta di dati sensibili di questi ultimi, come i dati biometrici, e il loro inserimento in database, spesso difficilmente accessibile ai migranti stessi, solleva legittime preoccupazioni riguardo alla proporzionalità di tali misure rispetto agli obiettivi di sicurezza pubblica. Si consideri, ad esempio, l'articolo 9 del GDPR il quale, pur vietando specificamente il trattamento di dati che possano rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, l'orientamento sessuale, nonché dati genetici, biometrici e sanitari (paragrafo 1), prevede al contempo delle eccezioni che invece lo consentono in circostanze particolari (paragrafo 2). Tra queste rientrano i motivi di interesse pubblico stabiliti dal diritto dell'Unione Europea e degli Stati membri. Tale ambivalenza normativa solleva importanti interrogativi riguardo alla reale tutela dei diritti individuali e alla legittimità delle deroghe adottate, soprattutto in relazione al principio di proporzionalità.
In un contesto delicato come quello dell'immigrazione, dove la necessità di garantire la sicurezza dei confini nazionali è in tensione con l'obbligo di rispettare i diritti fondamentali delle persone immigrate, il principio di proporzionalità dovrebbe infatti assumere un ruolo cruciale, vista la reale esigenza di garanzia di un effettivo bilanciamento tra situazioni giuridiche ugualmente meritevoli di tutela, ancorché tra loro potenzialmente contrastanti.

3. Eurodac: da strumento di asilo a meccanismo di sorveglianza

A questo punto, è necessario comparare il livello di tutela appena descritto, improntato al principio di proporzionalità e garantito ai cittadini dell'Unione o in generale agli immigrati regolari, con il sistema di prelievo e trattamento dei dati riservato a coloro che richiedono asilo nell'UE, nonché agli altri migranti privi, all'arrivo, di regolare visto o permesso di soggiorno.
A tale scopo, si rivela utile ricostruire le vicende che hanno interessato l'ampliamento significativo dello scopo dell'Eurodac: sistema nel quale, come noto, confluiscono i dati biometrici degli immigrati irregolari.
Si tratta delle vicende da cui emerge non solo il mancato rispetto dell'art. 52 della Carta, ma

anche dell'art. 5 del GDPR, in base al quale il trattamento dei dati personali delle persone fisiche non può avvenire per finalità indefinite, illimitate o che si estendano in base a una contingente utilità sopravvenuta.

Se originariamente lo scopo dell'Eurodac era solo quello di consentire il confronto delle impronte digitali, con la modifica introdotta nel 2013 (Regolamento UE 2013/603) il suo impiego è diventato funzionale al contrasto della criminalità grave. Non solo, con il nuovo Regolamento UE 2024/1358, che in base all'art. 63 trova applicazione a partire dal 12 giugno del 2026, si è data attuazione ad un ulteriore obiettivo perseguito tramite il database, ovverosia quello di facilitare il controllo dell'immigrazione irregolare verso l'Unione (obiettivo che a sua volta era stato introdotto con la proposta di regolamento da parte della Commissione europea del 4 maggio 2016 (la COM 2016/0272 final).

L'Eurodac è stato, in altri termini, progressivamente trasformato in uno strumento per il controllo dei migranti che richiedono protezione internazionale, così come di coloro che soggiornano illegalmente all'interno del territorio dell'Unione senza presentare tale domanda o attraversano irregolarmente una frontiera esterna dell'Unione. Esso, prevedendo la raccolta di un numero significativamente maggiore di dati relativi agli immigrati, se comparato a quello previsto per i cittadini dell'Unione Europea, introduce un trattamento differenziato rispetto a quello riservato a questi ultimi.

Sia sufficiente guardare alla tipologia di dati raccolti nel database il cui numero è stato notevolmente ampliato, a seguito prima della proposta COM 2016/0272 final e poi dell'art. 17 del nuovo Regolamento UE 2024/1358, che pure verrà applicato a decorrere, si è detto, dal 12 giugno 2026. A partire da questa data, i dati che verranno registrati nell'Eurodac per i richiedenti asilo non comprenderanno più le sole impronte digitali, ma anche una serie di informazioni personali dettagliate quali: lo Stato membro d'origine, il luogo e la data di presentazione della domanda di protezione internazionale, il sesso, il volto, i cognomi e nomi, la cittadinanza, il luogo e la data di nascita, le informazioni relative ai documenti di identità o di viaggio, nonché ulteriori dettagli.

Si consideri, inoltre, il funzionamento del database. In questa prospettiva, la raccolta di dati, apparentemente necessaria per la gestione e l'identificazione efficace dei richiedenti asilo, pone serie questioni etiche e giuridiche, soprattutto in relazione al principio di proporzionalità. Sebbene la raccolta di dati possa apparire necessaria per la gestione e l'identificazione efficace di questi ultimi, tale pratica solleva interrogativi riguardo al bilanciamento tra la sicurezza e il rispetto dei diritti fondamentali in quanto sembrerebbe essere privilegiata la sicurezza nazionale a scapito del principio di uguaglianza. Pertanto, il trattamento dei dati biometrici di tali individui, per definizione, in posizione di vulnerabilità, non rispetta lo standard di protezione e non risulta allineato con le garanzie che sono previste per i cittadini UE. L'art. 9, par. 1, del medesimo Regolamento, ad esempio, stabilisce che i dati relativi alle impronte digitali devono essere conservati per un periodo prolungato di dieci anni. È evidente come quest'ultimo rappresenti un periodo di conservazione manifestamente eccessivo. In ogni caso si tratta di una conservazione significativamente diversa da quella

valutata dalla Corte di Giustizia nella citata sentenza Schwarz, in riferimento alle impronte digitali contenute nei passaporti personali dei cittadini comunitari, che sono destinate a rimanere esclusivamente in possesso del titolare.
A ciò va aggiunta tanto la previsione dell'art. 10, par. 1, che riduce l'età minima per la raccolta dei dati biometrici a sei anni, aumentando così la quantità di dati sensibili raccolti; quanto quella del considerando 30, che ha espressamente previsto la possibilità di ricorrere alla coercizione per raccogliere le impronte digitali, anche su minori, quando necessario, sollevando una serie di dubbi di legittimità, soprattutto con riferimento al divieto di trattamenti degradanti sancito all'art. 3 CEDU. Nonostante la coercizione non sia prevista come obbligatoria, la sua eventuale applicazione per la raccolta dei dati biometrici di minori richiedenti asilo potrebbe configurarsi come un trattamento degradante, considerando il forte stress ed il senso di frustrazione che questa pratica può indurre nei minori, aggravando ulteriormente la loro già fragile condizione.
È evidente, dunque, come le disposizioni fin qui analizzate sollevino criticità significative in termini di proporzionalità, con riferimento al disposto di cui al citato art. 52, par. 1, della Carta, il quale, come detto, prevede che ogni ingerenza nei diritti fondamentali sia strettamente necessaria per il conseguimento di obiettivi legittimi: la raccolta e la conservazione per dieci anni di dati biometrici di bambini a partire dai sei anni e di adulti richiedenti asilo, nonché la possibilità di ricorrere alla coercizione fisica per il loro prelievo, non può non dar adito a legittimi interrogativi circa l'indispensabilità di tali misure e la possibilità di adottare soluzioni meno invasive.
Infine, da tutto questo emerge come anche il principio di limitazione delle finalità del trattamento dei dati, previsto dall'art. 5 del GDPR, non possa dirsi pienamente rispettato. L'Eurodac, infatti, è stato ampliato per includere una serie di dati biometrici e personali che vanno oltre lo scopo originale di gestione delle richieste di asilo, finendo per diventare uno strumento per la sorveglianza generalizzata dei migranti. Questo ampliamento delle finalità, senza adeguate garanzie di protezione, può concretamente portare a un utilizzo eccessivo e non giustificato dei dati raccolti.

4. L'impatto delle tecnologie avanzate sui diritti dei migranti

Le vicende dell'Eurodac si intrecciano con le questioni giuridiche che emergono dall'introduzione delle nuove tecnologie nella gestione delle frontiere. In proposito, può infatti sollevarsi un'ultima considerazione con riferimento all'adozione della misura del riconoscimento facciale, la quale, è noto, rappresenta un'innovazione significativa nel controllo e nella gestione dei flussi migratori. Si tratta di tecnologie che, pur offrendo vantaggi per la sicurezza pubblica, introducono rischi considerevoli in termini di violazione della privacy, come pure possono perpetuare *bias* e discriminazioni sistemiche.
In questo contesto, il nuovo Regolamento Europeo sull'Intelligenza Artificiale (AI Act), nel

disciplinare l'uso da parte degli Stati membri di sistemi di IA classificati come "ad alto rischio", introduce deroghe significative ai principi fondamentali sanciti dal GDPR, secondo i quali il trattamento dei dati personali deve avvenire in modo proporzionato, necessario e trasparente. L'articolo 46 del Regolamento, infatti, permette l'utilizzo di tali sistemi senza una valutazione di conformità adeguata, giustificandola con generiche e non ben definite situazioni di necessità. A questo va aggiunto che la precisione e l'affidabilità di tali sistemi sono spesso compromesse da *bias* algoritmici, che tendono a discriminare in modo sproporzionato donne, anziani e membri di minoranze etniche. In un contesto così delicato, dove le decisioni hanno un impatto profondo sulla vita delle persone, un errore di identificazione ascrivibile a *bias* algoritmici può portare a conseguenze ingiuste come detenzioni prolungate, negazione dell'ingresso legittimo o, in casi estremi, espulsioni ingiustificate.
Sorge, dunque, spontaneo chiedersi se la possibile disparità di trattamento nei confronti dei migranti senza documenti regolari e dei richiedenti asilo, alla luce dei principi di uguaglianza e trattamento dei dati, possa essere ritenuta proporzionata o comunque giustificata in ragione dell'esigenza di garantire la sicurezza dei confini nazionali, quale eventuale finalità di interesse generale.
La suddetta normativa apre in altri termini la strada a potenziali abusi, in quanto, in contesti di emergenza, come quelli spesso legati alla gestione dei flussi migratori irregolari, la deroga ai principi di proporzionalità, necessità e trasparenza potrebbe essere invocata per motivare misure sproporzionate, prive delle necessarie garanzie di controllo e pubblicità e potenzialmente discriminatorie a causa di "distorsioni" insite nel sistema algoritmico.
In definitiva, il riconoscimento facciale, rientrando nella categoria di sistemi di IA "ad alto rischio", richiederebbe una rigorosa valutazione di conformità che non dovrebbe essere soggetta a deroghe, in modo da garantire che il suo uso non violi i diritti fondamentali e avvenga nel rispetto del più volte menzionato principio di proporzionalità.
L'obiettivo primario dovrebbe essere quello di assicurare un equilibrio tra sicurezza e diritti fondamentali: un equilibrio che rappresenta non solo un obbligo legale, ma anche un imperativo morale, assolutamente essenziale per l'integrità delle società moderne.

RIFERIMENTI BIBLIOGRAFICI

Dottrina:

- R. BENDINELLI, *Le norme sul trattamento dei dati personali dei richiedenti asilo nell'Unione Europea: talune criticità rispetto al caso del dell'interessato minorenne,* in *Diritto, Immigrazione e Cittadinanza*, n.1/2024.
- R. BENDINELLI, *How coercive fingerprinting could violate migrants' dignity,* in *Riv. coop. giur. internaz.*, 2021.

- H. CAROLI CASAVOLA, L. CORAZZA, M. SAVINO (a cura di), *Migranti, territorio e lavoro. Le strategie d'integrazione*, Rubbettino Editore, Soveria Mannelli, 2022.
- CERRI, *L'uguaglianza nella giurisprudenza della Corte costituzionale. Esame analitico ed ipotesi ricostruttive*, Giuffré, Milano, 1976.
- L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee,* in *Federalismi.it*, 14 febbraio 2018.
- M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fonda-mentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* in *Sistema penale*, 2022.
- E. CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto penale uomo,* 2022.
- D. DUSHI, *The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications*, in *Policy Brief,* 2020.
- FRANCIS, S. WALBY, B. PATTINSON, A. ELLIOT, V. HOTI, J. PHOENIX, R. VERRAL, M. PEELO, *Data collection on trafficking in human beings in the EU: Final report*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018.
- G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative,* Napoli, 2021.
- NARDOCCI, *Artificial intelligence at the crossroads between the European Union & the Council of Europe: who safeguards what & how?*, in *Italian Journal of Public Law*, Vol. 16, Issue 1/2024, pp. 165-196.
- NARDOCCI, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia*, in *BioLaw Journal,* n.1/2024.
- PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Vol. 1, Torino, Giappichelli, 2016, p. 161.
- RESTA, *Sub art. 5 reg. 2016/679,* in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *Comm. GDPR e Normativa Privacy,* Milano, Ipsoa, 2018.

Per citare questo contributo: C. NAPOLITANO, *Digitalizzazione delle procedure di ingresso: il difficile equilibrio tra la sicurezza pubblica e il rispetto dei diritti fondamentali degli immigrati,* ADiM Blog, Analisi & Opinioni, Settembre 2024.