Diritto, Immigrazione e Cittadinanza
Fascicolo n. 1/2025

L'ISPEZIONE PER FINALITÀ IDENTIFICATIVE DELLO *SMARTPHONE* IN USO ALLO STRANIERO, TRA "PERSUASIONE" E COAZIONE SENZA GARANZIE

di Elena Valentini

Abstract: *Il contributo analizza una recente novità apportata dal "decreto flussi" (d.l. 11 ottobre 2024, n. 145), istitutiva dell'accesso ai dispositivi elettronici in uso a stranieri soggetti a trattenimento, richiedenti asilo e minori non accompagnati, e preposta allo scopo di acquisire informazioni utili alla loro identificazione e alla ricostruzione del loro percorso migratorio. Dopo aver mostrato come la pratica di ispezionare i telefoni cellulari dei migranti non sia affatto inedita nel panorama europeo, l'A. sottolinea la natura altamente intrusiva dell'istituto, mette in dubbio la compatibilità della soluzione normativa italiana con la Costituzione e con il diritto dell'Unione europea (in particolare alla luce di una recente pronuncia della Corte di giustizia), evidenziandone altresì le numerose criticità procedurali.*

Abstract: *The paper analyzes a recent measure introduced by the "decreto flussi" (d.l. No. 145 of October 11, 2024), which establishes access to electronic devices used by foreigners subject to detention, asylum seekers, and unaccompanied minors, with the aim of collecting information useful for their identification and for reconstructing their migration routes. After illustrating how the practice of inspecting migrants' mobile phones is by no means unprecedented in the European context, the author highlights the intrusive nature of the measure, questions the compatibility of the Italian legislative solution with the Constitution and EU law (particularly in light of a recent judgment by the Court of Justice), and also points out its numerous procedural shortcomings.*

ISSN 1972-4799

L'ISPEZIONE PER FINALITÀ IDENTIFICATIVE DELLO *SMARTPHONE* IN USO ALLO STRANIERO, TRA "PERSUASIONE" E COAZIONE SENZA GARANZIE

di Elena Valentini*

SOMMARIO. 1. "Migranti con il cellulare". – 2. Di cosa parliamo quando parliamo di *smartphone*. – 3. L'accesso ai dispositivi elettronici degli stranieri nel diritto UE. – 4. Uno sguardo oltre confine: la soluzione tedesca. – 5. La via italiana: premessa. – 6. L'oggetto dell'accesso e l'idoneità dell'istituto allo scopo perseguito. – 7. L'accesso "acconsentito" al *device*. – 8. Il ricorso alle maniere forti: i destinatari dell'accesso immediato al *device*. – 9. L'accesso immediato: profili procedurali. – 9.1. *Segue*: l'inevitabile contrasto con l'art. 15 Cost. – 9.2. *Segue*: ulteriori aspetti critici. – 10. Una novità dirompente: la sentenza della Corte di giustizia del 4 ottobre 2024. – 11. Conclusione.

1. "Migranti con il cellulare"

Questo scritto intende concentrarsi su un'importante novità del "decreto flussi" (d.l. 11.10.2024, n. 145, conv. con mod. dalla l. 9.12.2024, n. 187): quella, racchiusa nell'art. 12, che apre alla pubblica autorità le porte di accesso ai dispositivi elettronici in uso a diverse categorie di stranieri (richiedenti asilo, persone a vario titolo sottoposte a trattenimento e minori stranieri non accompagnati), nella prospettiva di renderne possibile una compiuta identificazione.

Avremo modo di constatare come una simile disciplina non sia affatto inedita nel panorama europeo. Al netto di ciò, certamente essa risulta in linea con la politica del governo in carica, così attenta agli *smartphone* in uso ai migranti da voler introdurre anche il divieto di vendere una Sim card a coloro che siano sguarniti di titolo di soggiorno (divieto racchiuso nel "d.d.l. Sicurezza" all'esame del Parlamento[1]).

Per quanto sorrette da motivazioni non omologabili, le due novità del momento – quella appena varata (sulla quale ci concentreremo) e l'altra, ancora allo stadio *de iure condendo* (ma verosimilmente destinata a tramontare benché già forte di una prima approvazione alla Camera) – riflettono un assillo, quello per i telefoni in uso agli stranieri, veicolato dalla retorica sui "migranti con il cellulare" e già sfociato nella prassi che vede le persone sottoposte a trattenimento private del proprio telefono quando fanno ingresso nei Centri di detenzione amministrativa[2].

Sintetizzando all'osso, il combinato disposto degli artt. 12 d.l. n. 145/2024 e (se mai dovesse essere approvato) dell'art. 32 del controverso "d.d.l. Sicurezza" intenderebbe

* Professoressa associata di Procedura penale, Università di Bologna.

1. V. art. 32 d.d.l. n. S. 1236 «disposizioni in materia di sicurezza pubblica, di tutela del personale in servizio, nonché di vittime dell'usura e di ordinamento penitenziario», nel testo approvato alla Camera il 18.9.2024. Il disegno di legge si propone (fra l'altro) di intervenire sugli artt. 30 e 98-*undetricies* del codice delle comunicazioni elettroniche (d.lgs. 1.8.2003, n. 259), onde subordinare all'acquisizione di copia del «titolo di soggiorno» l'acquisto di una SIM, e altresì andando a colpire per la trasgressione del divieto le imprese autorizzate alla vendita con la sanzione amministrativa accessoria della chiusura dell'esercizio o dell'attività per un periodo da cinque a trenta giorni». Non solo: la proposta di riforma si prefigge anche di introdurre l'incapacità di contrattare con gli operatori (per un periodo da sei mesi a due anni) per coloro che siano stati condannati per il delitto di sostituzione di persona, quando il fatto è commesso al fine della sottoscrizione del contratto di acquisto della SIM.

2. Su tale prassi si tornerà infra, § 8.

prefiggersi questo risultato: se lo straniero possiede uno *smartphone*, la polizia potrà ispezionarne il contenuto; se lo straniero è invece sguarnito di utenza telefonica e versa in condizioni di irregolarità, la tentazione governativa è quella di negargli l'acquisto della scheda SIM.

Tale ipotetico scenario dimostra come lo *smartphone* possa subire una doppia strumentalizzazione, prestandosi a divenire: innanzitutto una formidabile miniera di informazioni per l'autorità di pubblica sicurezza, dichiaratamente alle prese con l'esigenza di accertare identità, nazionalità, età dello straniero (come pure il percorso geografico da lui intrapreso per raggiungere l'Italia), ma che ben potrebbe sfruttare la disponibilità del *device* anche per acquisire in modo abusivo ulteriori conoscenze; al contempo, un congegno di cui impedire l'accesso ai "clandestini", con un divieto – stando ai proponenti volto a rendere «identificabili eventuali responsabili di reati intercettati», ma lapalissianamente destinato all'eterogenesi dei fini[3] – foriero di pura vessazione, poiché inteso solo a punire e a isolare lo straniero privo di titolo di soggiorno.

2. Di cosa parliamo quando parliamo di *smartphone*

Per inquadrare la sostenibilità costituzionale di qualsiasi intervento normativo concernente il rapporto tra lo straniero e il suo dispositivo elettronico bisogna considerare cosa rappresenta, oggi, lo *smartphone*[4].

In conseguenza della sua natura multiuso, la disponibilità di un'utenza telefonica e telematica (e del dispositivo in grado di supportarla) incide infatti sul concreto esercizio di svariati diritti. Oltre a costituire un mezzo di comunicazione (telefonica, videotelefonica, per iscritto) non più surrogabile dalla telefonia fissa (così come riconosciuto anche dalla sentenza costituzionale n. 2 del 2023[5]), esso permette la connessione al *web*, condizionando

3. Asseritamente, tale disposizione aiuterebbe a proteggere la sicurezza dei cittadini e a ridurre il mercato di "SIM fantasma", rendendo «identificabili eventuali responsabili di reati intercettati». Secondo le dichiarazioni del deputato Giovanni Donzelli, l'idea nasce «da un confronto con alcuni investigatori delle squadre mobili, che hanno segnalato una difficoltà nel condurre indagini, attraverso intercettazioni, su SIM con intestatari di fatto irrintracciabili o fasulli. Esiste un vero e proprio mercato di SIM fantasma utilizzate da gruppi criminali. L'obiettivo del testo è quello rendere così identificabili eventuali responsabili di reati intercettati» (il virgolettato è tratto dal post *Basta sim fantasma, aiutano i criminali*, tratto dal sito www.giovannidonzelli.it, 14.9.2024). A parte i numerosi problemi che un simile istituto potrebbe determinare (finendo per penalizzare una platea di persone molto più vasta di quella che l'iniziativa vorrebbe colpire: v. A. Buzzi, *DDL Sicurezza, ha davvero senso la "stretta" sulle carte SIM?*, in www.lacostituzione.info, 2.10.2024), esso inevitabilmente produrrebbe esiti opposti a quelli dichiarati, incentivando (e non certo contrastando) l'acquisto di schede telefoniche da parte di persone con permesso di soggiorno, che poi le rivenderebbero a persone sguarnite di tale titolo. La conseguenza (non voluta o perseguita?) sarebbe dunque solo un'ulteriore marginalizzazione degli stranieri irregolari.

4. Nelle prossime pagine ci si riferirà quasi sempre a questo specifico tipo di *device*, perché, anche se la legge menziona più asetticamente «dispositivi o supporti elettronici», l'attenzione politica e tecnica si è concentrata in particolare sugli *smartphone* (I. Josipovic, *Digitalising Asylum Procedures: The Ligitimisation of Smartphone Data Extraction for Restrospective Border Control*, in *Geopolitics*, 2024, vol. 29, n. 5, p. 1836).

5. Come noto, la pronuncia ha dichiarato l'illegittimità dell'art. 3, comma 4, del d.lgs. 6.9.2011, n. 159 (il cosiddetto "codice antimafia"), nella parte in cui include i telefoni cellulari tra gli *apparati di comunicazione radiotrasmittente* di cui il questore può vietare, in tutto o in parte, il possesso o l'utilizzo, quale prescrizione accessoria all'avviso orale. Dopo aver ammesso che le limitazioni relative all'uso di un determinato mezzo o strumento di comunicazione non necessariamente si convertono in restrizioni al diritto fondamentale soddisfatto tramite l'impiego dello strumento medesimo, la Corte ha affermato che «esiste tuttavia un limite, superato il quale la disciplina che incide sul mezzo – in ragione del particolare rilievo che questo riveste a livello relazionale e sociale – finisce per penetrare all'interno del nucleo essenziale del diritto, determinando evidenti ricadute restrittive sulla libertà tutelata dalla Costituzione». Sulla scorta di ciò (e alla luce della

dunque l'accesso al mondo dell'informazione (inteso in senso lato, e dunque anche per reperire notizie necessarie alla vita quotidiana).

Per lo straniero, la connessione risulta ancor più indispensabile: per affrontare il percorso migratorio [6] (tanto da costituire un'importante voce di spesa per poterlo intraprendere [7]); ma anche dopo l'arrivo in Italia, per rendersi reperibile (*in primis* ai familiari) anche quando le condizioni di precarietà abitativa rendono arduo essere rintracciati.

Da altro punto di vista, lo *smartphone* individua uno scrigno di informazioni e di dati personali, meritevoli di tutela indipendentemente dalla loro riconducibilità al concetto di corrispondenza; dati che agli occhi delle agenzie di controllo risultano tanto più preziosi proprio alla luce del ruolo cruciale che il *device* riveste durante il viaggio verso l'Europa.

Alla luce di tali constatazioni, i due tasselli della strategia normativa cui s'è fatto cenno in esordio vanno a coinvolgere le differenti dimensioni del telefono cellulare. In particolare, mentre la disposizione racchiusa nel "d.d.l. sicurezza" incide (negandola) sulla *libertà* di comunicazione, di corrispondenza e di "connessione", quella appena entrata in vigore – l'art. 12 del "decreto flussi", sul quale d'ora in poi concentreremo le nostre riflessioni – è suscettibile di violare la *segretezza* della corrispondenza, nonché, più in generale, di porsi in contrasto con il diritto alla vita privata (tutelato dall'art. 8 CEDU oltre che dall'art. 7 della Carta di Nizza).

3. L'accesso ai dispositivi elettronici degli stranieri nel diritto UE

Da sempre, uno dei più significativi ostacoli nella "gestione" degli stranieri (anche richiedenti asilo) presenti sul territorio europeo è costituito dalla difficoltà di procedere alla loro compiuta identificazione, come pure di stabilirne la nazionalità. Non a caso, l'esigenza di raggiungere tale risultato ispira numerose norme di diritto dell'Unione europea[8].

---

lettura della Cassazione, che, riconducendo il telefono cellulare alla nozione di apparato di comunicazione radiotrasmittente, riteneva che il questore potesse vietarne il possesso o l'utilizzo ai sensi della norma sottoposta a censura), il Giudice delle leggi ha appunto dichiarato l'illegittimità costituzionale della disposizione, nella parte in cui non prevede l'intervento dell'autorità giudiziaria prescritto dall'art. 15 Cost.

6. Gli *smartphone* sono utilizzati dai migranti durante il loro pericoloso viaggio per mantenere la comunicazione con i *social network*, navigare attraverso territori sconosciuti e raccogliere informazioni attraverso *affordance* multimediali (così M. Gillespie-S. Osseiran-M. Cheesman, *Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances*, in *Social Media + Society*, V. 4, Issue 1, gennaio 2018, p. 1 ss.).

7. V. in proposito quanto segnalato già quasi dieci anni fa nel rapporto UNHCR, *Connecting refugees. How Internet and Mobile Connectivity can Improve Refugee Well-Being and Transform, Humanitarian Action*, Ginevra, settembre 2016, in www.unhcr.org, o da I. Kaplan, *How smartphones and social media have revolutionized refugee migration*, in UNHCR Blogs, 26.10.2018. Oltre a consentire l'uso della geolocalizzazione per scegliere quali vie intraprendere, il *device* è essenziale per procacciarsi le conoscenze necessarie a superare eventuali controlli di frontiera, come pure per superare difficoltà di comprensione linguistica.

8. Si pensi, fra le altre, alle disposizioni racchiuse nel regolamento Eurodac (reg. (UE) 2013/603), che dal 12 giugno 2026 verrà soppiantato dal reg. (UE) 2024/1358, varato nell'ambito del Patto sulla migrazione e l'asilo. Il nuovo regolamento determinerà un deciso rafforzamento degli strumenti messi in campo, prefiggendosi la memorizzazione anche delle immagini facciali e la raccolta sistematica dei dati biometrici dei migranti (con un abbassamento da quattordici a sei anni dell'età minima per la relativa raccolta), destinati ad essere conservati fino a dieci anni e a risultare accessibili alle forze di polizia di tutta l'Unione europea. Al nuovo regolamento Eurodac si affianca (fra l'altro) il regolamento *Screening* (reg. (UE) 2024/1356), che, ponendosi in un'ideale linea di continuità con l'*hotspot approach* già risalente all'Agenda europea delle migrazioni del 2015, renderà molto più invasivi i controlli, fra l'altro stabilendo che i dati personali e biometrici di ogni persona entrata nel territorio UE vengano fra l'altro sottoposti a confronti incrociati con quelli conservati nei sistemi digitali gestiti da Europol e Interpol (v. in particolare art. 14 reg. *Screening*).

L'identificazione pone sfide ardue, in particolare nei confronti delle persone che chiedono asilo ma non sono in possesso del passaporto. Tanto che per saggiare la loro credibilità vengono sfruttati nuovi strumenti digitali, quali la biometria linguistica [9], la traslitterazione del nome e ricerche sui *social media* [10]. Mezzi che possono rendersi indirettamente utili anche ad altri scopi, e in particolare per monitorare eventuali minacce terroristiche[11].

In tale scenario, fino al 2024 l'accesso ai dati racchiusi negli *smartphone* dei migranti non ha costituito oggetto di una *esplicita* considerazione nella disciplina comunitaria.

Stando al codice delle frontiere Schengen (v. gli artt. 2, § 1, punto 11, e art. 8, § 1 del Reg. (UE) 2016/399, che per il caso di perquisizione rinvia alla legislazione dello Stato membro), le operazioni di controllo possono «riguardare anche i mezzi di trasporto e *gli oggetti di cui sono in possesso le persone che attraversano la frontiera*». Tuttavia, né tale disciplina né altre disposizioni comunitarie riguardanti poteri di ispezione e perquisizione degli stranieri a scopo identificativo menzionano *espressamente* l'accesso ai *device*, limitandosi più genericamente a indicare la possibilità di perquisire gli effetti personali del migrante.

È il caso della direttiva 2013/32/UE, il cui art. 13 prevede che lo Stato membro imponga ai richiedenti protezione internazionale di «cooperare con le autorità competenti ai fini dell'accertamento dell'identità e degli altri elementi di cui all'articolo 4, § 2, della direttiva 2011/95/UE» (art. 13, § 1). Premesso che, in forza di tale rinvio, gli «elementi» rispetto ai quali si estrinseca l'obbligo di cooperazione sono quelli «relativi all'età, all'identità e alla cittadinanza, nonché ai Paesi in cui ha soggiornato o è transitato», fra i numerosi suoi precetti il paragrafo 2 del medesimo art. 13 ammette la possibilità che «le autorità competenti possano perquisire il richiedente *e i suoi effetti personali*» (lett. *d*). Tale lett. *d*) si limita tuttavia a chiarire che, «fatta salva qualsiasi perquisizione effettuata per motivi di sicurezza», alla perquisizione debba provvedere «una persona dello stesso sesso nel pieno rispetto dei principi di dignità umana e di integrità fisica e psicologica», senza nulla stabilire, di più specifico, in ordine alla possibilità di procedere all'ispezione di dispositivi elettronici.

Il ricorso alla perquisizione ai fini dell'esame della domanda di protezione internazionale è stato riproposto pressoché identico all'art. 9, § 5, del nuovo "regolamento Procedure" (UE/2024/1348), varato nell'ambito del Patto sulla migrazione e l'asilo e destinato a sostituire la direttiva 2013/32 a decorrere dal 12 giugno del 2026[12]. Sennonché, malgrado anche tale norma continui a riferirsi alla (sola) possibile perquisizione «*del richiedente o dei suoi effetti personali*», il *considerando* n. 22 del medesimo regolamento menziona gli apparecchi elettronici in uso, nominando espressamente *laptops*, *tablet computers* o *mobile phones*.

Sulla scorta di ciò, oltre che emulare l'esperienza maturata in altri ordinamenti (di cui diremo subito), è probabile che con l'art. 12 del "decreto flussi 2024" il legislatore italiano

9. A. Siccardo, *L'algoritmo che discrimina i richiedenti asilo in Europa*, in www.altreconomia.it, 16.9.2022.

10. D. Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, in www.rsc.ox.ac.uk, 23.1.2023.

11. M. Forti, *Migrants and refugees in the cyberspace environment: privacy concerns in the European approach*, in *European Journal of Privacy Law & Technologies*, 2020, f. 2, p. 244.

12. Eccone il testo: «fatta salva qualsiasi perquisizione effettuata per motivi di sicurezza, là dove necessario e debitamente giustificato per l'esame della domanda, le autorità competenti possono disporre la perquisizione del richiedente o dei suoi effetti personali in conformità del diritto nazionale. L'autorità competente fornisce al richiedente i motivi della perquisizione e li inserisce nel fascicolo del richiedente. A qualsiasi perquisizione del richiedente prevista dal presente regolamento provvede una persona dello stesso sesso nel pieno rispetto dei principi di dignità umana e di integrità fisica e psicologica».

abbia inteso assecondare le indicazioni sovranazionali desumibili dal *considerando* appena citato (peraltro privo di diretta forza precettiva). Ora, una perquisizione analogica e una perquisizione digitale presentano livelli di intrusività marcatamente distanti tra loro; proprio per questo, pur "aprendo" alla perquisizione dei dispositivi elettronici, il *considerando* n. 22 precisa che «qualsiasi perquisizione di questo tipo dovrebbe essere effettuata nel rispetto dei diritti fondamentali e del principio di proporzionalità».

4. Uno sguardo oltre confine: la soluzione tedesca

Dinanzi alla recente novità normativa italiana, è utile volgere lo sguardo oltre confine: infatti, l'accesso ai telefoni cellulari degli stranieri – anche richiedenti asilo – opera, da anni, in numerosi Paesi europei.

Schematizzando all'estremo, lo scenario è più o meno questo: in alcuni Stati (specie in quelli in cui l'autorità di polizia è coinvolta nella identificazione e registrazione dei richiedenti asilo[13]), la pratica è stata inaugurata sulla scorta di un'esegesi estensiva di norme legittimanti le perquisizioni degli effetti personali dello straniero, norme che spesso sono poi state modificate in seconda battuta, onde chiarirne espressamente la riferibilità anche ai dispositivi elettronici[14]; all'opposto, altri Paesi si sono prima dotati dello strumento giuridico (introducendo riforme atte a consentire l'accesso ai *device* dei migranti), ma hanno però evitato di renderlo immediatamente operativo in concreto, nella consapevolezza del suo

13. M. P. Bolhuis-J. van Wijk, *Seeking asylum in the digital era: Social-media and mobile-device vetting in asylum procedures in five European countries*, in *Journal of Refugee Studies*, 2021, 34 (2), p. 1603.

14. Tra i primi Paesi in cui da almeno una decina d'anni ha preso piede questa pratica ci sono la Danimarca, l'Olanda e la Gran Bretagna. In Danimarca tale prassi risale almeno al 2015, fondandosi su una lettura estensiva dell'art. 40, par. 10 della *Udlændingeloven* (la legge sugli stranieri), che autorizza la polizia a prendere in custodia «documenti e oggetti» che possano servire ad accertare identità o nazionalità dello straniero (norma che nel 2017 ha visto un ampliamento dei presupposti applicativi): v. A. Biselli-L. Beckmann, *Invading Refugees' Phones: Digital Forms of Migration Control in Germany and Europe*, Gesellschaft fr Freiheitsrechte e. V., Berlino, 2020, p. 44. Anche in Olanda la pratica di ispezionare gli *smartphone* in uso agli stranieri si fonda su un'esegesi estensiva dell'art. 55 (§ 2) della legge sugli stranieri del 2000, che permette all'autorità di pubblica sicurezza di procedere a perquisizione della persona e dei suoi effetti personali per cercare documenti utili all'identificazione. Il fatto che tale pratica abbia preso avvio a legislazione invariata ha fatto sì che essa non sia stata portata all'attenzione del Parlamento; per tale ragione, essa è passata pressoché inosservata presso l'opinione pubblica, diversamente da quanto accaduto in altri Paesi (M. P. Bolhuis-J. van Wijk, *Seeking asylum in the digital era*, cit., p. 1602). In Gran Bretagna, va detto innanzitutto che la legge sulla protezione dei dati del 2018 contempla ampie eccezioni alle garanzie generali di trattamento dei dati là dove esso sia finalizzato allo scopo di controllare i flussi migratori (c.d. *immigration exemption*, di cui all' allegato 2, § 4 del *Data protection Act 2018*). La prassi di requisire e trattenere (anche per mesi) i telefoni cellulari dei migranti giunti nel Regno unito era già invalsa da alcuni anni quando la *High Court* è stata chiamata confrontarsi con essa: lo ha fatto con una decisione del 25.3.2022 (cui poi ne sono seguite altre), espressasi sulla vicenda paradigmatica in cui tre richiedenti asilo appena sbarcati nel Regno unito erano stati sottoposti al sequestro del telefono, avevano subito pressioni per rivelare le relative *password* di accesso e si erano poi visti realizzare un'estrazione completa dei dati racchiusi nei dispositivi. La pronuncia ha stigmatizzato il *modus procedendi* del Ministero degli interni, posto in essere in difetto di base legale, violando il principio di stretta necessità e di proporzionalità (visto che, oltretutto, i dispositivi non erano stati prontamente restituiti ai proprietari ma trattenuti per alcuni mesi); più in generale, l'Alta corte ha censurato la politica generalizzata di sequestro e detenzione dei telefoni cellulari poiché in contrasto con l'art. 8 CEDU. Sempre in Gran Bretagna, una modifica legislativa operata nel 2013 all'art. 93 § 5 del *Police Act* del 1997 ha accordato anche ai funzionari dell'immigrazione poteri fino a quel momento riconosciuti alle sole forze di polizia, ossia quello di intercettare e sorvegliare in modo occulto i telefoni, con l'obiettivo di affidare a tali funzionari «una gamma completa di tecniche investigative per affrontare efficacemente tutti i reati di immigrazione» (M. Townsend, *Revealed: Immigration officers allowed to hack phones*, *The Guardian*, 10.4.2016).

forte impatto sui diritti fondamentali dei migranti (oltre che per le difficoltà applicative ad esso associate)[15].

Benché il panorama offra anche molte altre esperienze rilevanti, nel contesto comunitario è importante dar conto, in particolare, della soluzione tedesca e della risposta giurisprudenziale che l'ha contraddistinta, non a caso menzionate sia dal *Dossier* del Servizio Studi del Senato sul disegno di legge di conversione del d.l. n. 145/2024[16] sia dal Garante della *privacy*, chiamato ad esprimersi su questo specifico contenuto del decreto quando era in corso di conversione in legge[17]. Essa può infatti costituire un importante precedente per esaminare con maggior consapevolezza la soluzione italiana, che descriveremo in seguito.

Proprio per offrire una patente di legittimità a prassi già operanti in concreto (per risalire all'identità e nazionalità dei migranti, ma anche consentire di individuare il Paese di primo ingresso nell'Unione europea ai fini del regolamento di Dublino), nel luglio 2015 il

15. Il 2017 è stato un anno di svolta, perché, sull'onda dell'introduzione dell'istituto in Germania, anche altri Paesi hanno deciso di approntare una disciplina che consente l'accesso ai dispositivi (M. P. Bolhuis-J. van Wijk, *Seeking asylum in the digital era: Social-media and mobile-device vetting in asylum procedures in five European countries*, in *Journal of Refugee Studies*, 2021, 34 (2), p. 1595 ss.). Tra questi, il Belgio, l'Austria, la Svizzera. In Belgio, grazie a un'innovazione normativa del 21.11.2017, le autorità preposte a raccogliere le domande di asilo possono procedere all'accesso dei dispositivi elettronici in uso al richiedente ove ci siano ragioni per ritenere nasconda informazioni rilevanti. La disciplina, che non ha trovato immediata applicazione, è molto poco garantistica, consentendo anche l'accesso alla corrispondenza, e qualifica il rifiuto del migrante a consegnare il proprio *device* come una violazione dell'obbligo di cooperazione (suscettibile di determinare il rigetto della richiesta di asilo). La novella ha ricevuto le critiche del Commissario per la protezione dei dati personali, fra l'altro perché, oltre a condizionare l'accesso allo *smartphone* a una valutazione eccessivamente soggettiva, non tutela i diritti dell'interessato, e non regolamenta esattamente le modalità di raccolta dei dati. Nel 2018, il Coordinamento e le Iniziative per i Rifugiati e gli Stranieri (CIRé) ha interpellato la Corte costituzionale belga, che, con una decisione del 25.2.2021, pur avallando la pratica, ha consigliato di modificare la formulazione normativa onde limitare la discrezionalità delle autorità competenti in materia di asilo. Secondo la decisione della Corte, il *Commissariat Général aux Réfugiés et aux Apatrides* (CGRA) deve avere buone ragioni per ritenere che i supporti di dati, come i telefoni cellulari, contengano informazioni essenziali. L'Austria e la Svizzera (che, pur non facendo parte dell'UE, fa comunque parte del SECA) hanno visto innovazioni normative mosse dalla volontà politica di determinare il Paese di primo ingresso nel territorio dell'Unione europea (I. Josipovic, *Digitalising Asylum Procedures*, cit., p. 1840). In particolare, in Austria, una novità normativa è stata introdotta nel settembre del 2018, e, similmente a quanto stabilito dalla soluzione belga, non contempla limitazioni improntate al principio di proporzionalità. Tanto che anche questa proposta ha incontrato numerose critiche (alcune delle quali si prestano ad essere riferite anche alla soluzione italiana). In particolare, per il fatto che la polizia possa effettuare copie di *backup* complete dei dati senza doverle successivamente cancellare, nonché per la violazione del principio di uguaglianza rispetto alle ben differenti garanzie applicabili a tale tipo di accertamento là dove disposto in un procedimento penale (A. Adensamer-A. Hanel-L.D. Klausner- H. R. Pecina, *Stellungnahme zum Fremdenrechtsänderungsgesetz von epicenter.works*, 15.5.2018). In Svizzera, la novità legislativa risale a una modifica alla LAsi (la legge sull'asilo del 27.10.1998), risalente al 21.10. 2021, che ha modificato l'art. 8, consentendo alla Segreteria di Stato della migrazione (Sem) l'accesso ai dispositivi secondo una disciplina piuttosto dettagliata. Nel 2024 è stata approntata una disciplina regolamentare che chiarisce a quali dati è permesso l'accesso (v. la notizia giornalistica *Richiedenti l'asilo, possibile ora esaminare cellulari e pc*, in www.laregione.ch, 1.5.2024), nella prospettiva di far entrare in funzione l'istituto nel corso del 2025. Le informazioni sommariamente riportate in questa e nella precedente nota sono in gran parte state riprese da A. Biselli-L. Beckmann, *Invading Refugees' Phones*, cit., p. 41 ss., cui si rinvia, oltre che per maggiori dettagli e per i riferimenti normativi e bibliografici, anche per la descrizione della situazione concernente altri Paesi.

16. Disposizioni urgenti in materia di lavoratori stranieri, caporalato, flussi migratori e protezione internazionale d.l. 145/2024 – A.S. 1310, 28.11.2024, reperibile sul sito istituzionale del Senato.

17. Audizione del professor Pasquale Stanzione, Presidente del Garante per la protezione dei dati personali, dinanzi alla I Commissione, affari costituzionali, sul decreto-legge 145/2024, resa in data 24.10.2024 e il cui testo scritto si può leggere sul sito www.garanteprivacy.it.

legislatore era intervenuto dapprima sulla legge sulla residenza (*Aufenthaltsgesetz*[18]), e, nel 2017, sulla legge sull'asilo (*Asylgesetz*). L'evoluzione della relativa disciplina ha visto susseguirsi svariati interventi di riforma, l'ultimo dei quali risale alla *Gesetz zur Verbesserung der Rückführung* del 26.2.2024[19].

A partire dal 2015, la possibilità di accedere al telefono dello straniero (anche a fini di rimpatrio) è dunque prevista dagli artt. 48 e 48a della *AufenthG*; essa è stata estesa anche al richiedente protezione internazionale con una novella del 27 luglio 2017, che ha inserito nell'art. 15 *Asylgesetz* (riguardante gli obblighi generali di cooperazione prescritti al richiedente) una specificazione normativa idonea a fungere da base giuridica per legittimare l'accesso al telefono dello straniero.

In forza di tali modifiche, e anche grazie all'innesto del successivo art. 15a nell'*Asylgesetz* (parimenti risalente al 2017), i richiedenti asilo privi di passaporto (o di un documento equipollente) sono tenuti a consegnare i "supporti di dati" (*datenträger*) di cui sono in possesso[20]. In caso di inottemperanza, tali supporti – definizione comprensiva anche di dispositivi mobili e dei servizi *cloud*[21] – possono essere comunque fatti oggetto di perquisizione[22], anche se la relativa valutazione è consentita solo se la perquisizione è necessaria e lo scopo della misura non può essere raggiunto con mezzi più blandi (*mildere mittel*)[23].

In forza degli artt. 48 (§ 3, periodi da 2 a 8) e 48a della legge sulla residenza, e dall'omologo art. 15a della legge sull'asilo, l'accesso ai dispositivi è precluso ove sussistano motivi per ritenere che l'analisi dei dati possa tradursi nell'acquisizione di informazioni tutelate dal diritto alla riservatezza. In tal caso, è prescritto un divieto d'uso e un obbligo di cancellazione immediata (cancellazione peraltro comunque prescritta una volta che i dati impiegati per stabilire l'identità e la nazionalità dello straniero non siano più necessari a tali scopi). Non solo: secondo quanto stabilito, alle operazioni può procedere solo «un dipendente abilitato a ricoprire funzioni giudiziarie».

Naturalmente, è possibile insorga la necessità di ottenere le chiavi di accesso per sbloccare il *device* in uso al richiedente asilo. Se la richiesta viene rifiutata, il fornitore di servizi di telecomunicazione può essere tenuto a fornire i dati utilizzati per proteggere l'accesso ai dispositivi (§48a (1) *AufenthG*). Tuttavia, prima ancora che abbia luogo la valutazione circa l'effettiva necessità di accedere al dispositivo elettronico, secondo una ricerca svolta nel 2022 il richiedente asilo è concretamente obbligato a firmare un modulo,

18. In particolare, l'intervento era stato operato dalla legge sulla ridefinizione del diritto di soggiorno e sulla cessazione del soggiorno (*BleiRÄndG*) del 27.7.2015, e aveva investito l'art. 48 e inserito l'art. 48a della *Aufenthaltsgesetz*.

19. *Rückführungsverbesserungsgesetz*, traducibile con l'espressione «legge sul miglioramento del rimpatrio».

20. E ciò per acquisire questi elementi, indicati al § 3, n. 7, dell'art. 15: 1. tutti i documenti e i documenti che, oltre al passaporto o alla sostituzione del passaporto, possono essere importanti per l'accertamento dell'identità e della nazionalità; 2. visti e permessi di soggiorno rilasciati da altri Paesi e altri documenti per l'attraversamento della frontiera; 3. biglietti aerei e altri documenti di viaggio; 4. documenti relativi al percorso dal Paese di origine al territorio federale, ai mezzi di trasporto utilizzati e al soggiorno in altri Paesi, la partenza dal Paese d'origine e prima dell'ingresso nel territorio federale; 5. tutti gli altri atti e documenti ai quali fa riferimento lo straniero o che sono necessari per l'adozione di decisioni e misure in materia di diritto dell'asilo e degli stranieri, compresa la determinazione e l'affermazione della possibilità di rimpatrio in un altro Stato.

21. V. art. 48, § 3a della legge sulla residenza (*Aufenthaltsgesetz*), richiamata dalla disciplina in esame.

22. Il § 4 del medesimo art. 15 affida infatti alle autorità responsabili dell'attuazione della legge sull'asilo e alle autorità dei *Länder* responsabili dei Centri di accoglienza la possibilità perquisire lo straniero e gli oggetti da lui trasportati se lo straniero non adempie ai suoi obblighi e non produce o consegna i supporti di dati su richiesta, e vi sono indicazioni circa il fatto che sia in possesso di tali documenti.

23. V. art. 15a *AsylG*.

che associa alla casella di rifiuto la seguente formula: «sono consapevole che questo rifiuto comporterà regolarmente l'interruzione della procedura di asilo, poiché sto violando il mio obbligo di collaborare alla procedura di asilo»[24]. Chiaro come una simile pratica finisca in concreto per esercitare una forte pressione sul richiedente.

La fisionomia di questa disciplina, invasiva ma comunque più attenta al rispetto del principio di proporzionalità di quanto (come vedremo) non sia quella italiana, ha consentito al Tribunale amministrativo federale – in una pronuncia resa il 16.2.2023 (*Urteil vom* 16.02.2023 - *BVerwG* 1 C 19.21[25]) e confermativa di una precedente decisione del Tribunale amministrativo di Berlino [26] – di stigmatizzare l'azione dell'Ufficio federale per l'immigrazione e i rifugiati (*Bundesamt für Migration und Flüchtlinge-BAMF*) rispetto a una fattispecie in cui l'accesso forzoso al *device* di una richiedente asilo afghana era stato intrapreso senza rispettare il principio dell'*extrema ratio*, viceversa esplicitamente prescritto dall'art. 15 *Asylgesetz*. Nel caso specifico, infatti, il *BAMF* poteva contare su almeno tre documenti presentati dalla richiedente asilo: la *tazkira* (cioè la carta di identità), il certificato di matrimonio e un certificato dell'Ambasciata afghana. Tanto il Tribunale amministrativo quanto quello federale di Berlino ne hanno dedotto che, al momento dell'ordinanza impugnata, il *BAMF* disponesse di elementi probatori che non rendevano necessario procedere all'accesso al *device*.

Questa importante pronuncia ha determinato le premesse per una modifica del quadro normativo. La "legge sul miglioramento del rimpatrio"[27] del 26.2.2024 ha infatti modificato l'art. 15a dell'*Asylgesetz*, in termini che sembrano far tesoro dell'approdo giurisprudenziale appena menzionato, circoscrivendone espressamente l'operatività ai casi in cui il cittadino straniero non solo non sia in possesso di un passaporto valido (o di un documento sostitutivo del passaporto), ma anche di un altro documento d'identità idoneo[28].

Tuttavia, accanto a questa novità di segno garantistico, se ne deve segnalare un'altra, che divarica sensibilmente la posizione dello straniero da identificare a fini di rimpatrio rispetto a quella del richiedente asilo: una modifica all'art. 48 della legge sulla residenza prevede infatti che la necessità di accedere allo *smartphone* possa legittimare anche una perquisizione domiciliare ove il migrante si rifiuti di consegnare il *device* (perquisizione che deve essere disposta dal giudice, e, in caso di pericolo imminente, anche dalle autorità incaricate dell'esecuzione della legge sull'asilo).

Inoltre, sullo sfondo rimane una questione, molto spinosa e destinata a proporsi anche in Italia. Una volta sbloccato il telefono per abilitare la cosiddetta "lettura" (*Auslesen*), il dispositivo viene collegato a un computer, che analizza i dati e produce un rapporto sui risultati (*Auswerten*). All'uopo viene impiegata una tecnologia informatica messa a

24. Copia del modulo si può trovare a questo indirizzo: https://fragdenstaat.de/anfrage/bamfs-use-of-mobile-phone-data-in-asylum-applications-use-of-mobile-phone-data-by-the-bamf-for-asylum-applications/716361/anhang/d1705-einverstndniserklrung-amd.pdf.

25. L'importante pronuncia si può leggere a questo indirizzo: https://www.bverwg.de/160223U1C19.21.0.

26. VG Berlin, sentenza 1.6.2021-9 K 135/20.A (*Asylmagazin* 9/2021, p. 338 ss.), in https://www.asyl.net/rsdb/m29743.

27. *Rückführungsverbesserungsgesetz* (v. *retro*, nota 19).

28. Non solo: a norma dell'art. 15a § 3, la lettura, la valutazione e la cancellazione dei dati (che vanno cancellati immediatamente, non appena non sono più necessari per determinare l'identità o la nazionalità) devono essere documentate nel fascicolo sull'asilo. Stando alla disposizione, devono altresì essere «adottate misure tecniche e organizzative adeguate ai sensi degli articoli 24, 25 e 32 del Regolamento (UE) 2016/679 per garantire che non vi sia accesso non autorizzato ai dati letti».

disposizione dalla società di sicurezza MSAB[29]. In particolare, invece di leggere manualmente i dati, gli *smartphone* sono collegati a un *hardware* che compila e memorizza automaticamente diversi tipi di metadati, fornendo un *report* sui risultati. I dati spaziano dai nomi di accesso e dalle informazioni del profilo dei social media e degli indirizzi *e-mail* alla lingua utilizzata nei messaggi, ai codici Paese salvati nei contatti e alla memoria delle chiamate e dei messaggi, alle desinenze di dominio della cronologia di navigazione, nonché ai dati di geolocalizzazione da applicazioni e fotografie[30].

Se da un lato dovrebbe limitare l'accesso ai soli metadati, l'impiego di una simile tecnologia espone il sistema al rischio di decisioni sulle domande di asilo sempre più dipendenti dai risultati di verifiche operate da programmi informatici, di cui né i diretti interessati né i responsabili delle decisioni medesime sono in grado di valutare la reale affidabilità[31].

5. La via italiana: premessa

Stando alla recente novella italiana, la possibilità di procedere all'accesso dei «dispositivi o supporti elettronici digitali» (con o senza consenso dell'interessato) è prevista «al solo fine di acquisire gli elementi relativi all'età, all'identità e alla cittadinanza, nonché ai Paesi in cui [lo straniero] ha soggiornato o è transitato».

In sé e per sé considerato, lo scopo della disciplina in esame è legittimo, non potendo essere invocato alcun diritto alla non collaborazione in capo allo straniero. Nel diritto interno, il dovere di rendere possibile la propria identificazione riguarda chiunque, così come (fra l'altro) si ricava dalla disciplina del cosiddetto fermo identificativo di polizia[32]. Nel diritto dell'Unione europea, per soddisfare l'esigenza di acquisire le informazioni concernenti i dati anagrafici e i Paesi in cui egli è transitato (descritta dall'art. 4, § 2 della "direttiva Qualifiche" (2011/95/UE) è stabilito un obbligo di cooperazione in capo al richiedente protezione internazionale (previsto all'art. 13, § 1 della "direttiva Procedure" dir. 2013/32/UE); obbligo ribadito anche dalla disciplina nazionale (art. 11 d.lgs. 28.1.2008, n. 25).

Ciò posto, la innovazione racchiusa dall'art. 12 del d.l. 11.10.2024, n. 145, determina un significativo salto di qualità. La novella sembra infatti voler superare la tradizionale refrattarietà del nostro Paese ad immettere nell'ordinamento strumenti di identificazione

29. A. Biselli-L. Beckmann, *Invading Refugees' Phones*, cit., p. 27.

30. Queste informazioni sono tratte da F. Palmiotto-D. Ozkul, *"Like Handing My Whole Life Over". The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures*, in https://verfassungsblog.de, 28.2.2023.

31. A. Biselli-L. Beckmann, *Invading Refugees' Phones*, cit., p. 49, che evidenziano come la particolare vulnerabilità dei rifugiati venga sfruttata per testare nuove tecnologie di controllo e monitoraggio che in futuro potrebbero essere estese anche ad altre porzioni della popolazione.

32. In proposito, l'art. 11 d.l. 21.3.1978, n. 59 (conv. con mod. con l. 18.5.1978, n. 191) consente agli ufficiali ed agenti di polizia di accompagnare nei propri uffici chiunque, richiestone, rifiuti di dichiarare le proprie generalità, e di trattenerlo per il tempo strettamente necessario al solo fine dell'identificazione e comunque non oltre le ventiquattro ore. L'istituto (operante anche quando ricorrono sufficienti indizi per ritenere la falsità delle dichiarazioni della persona richiesta sulla propria identità personale o dei documenti d'identità da essa esibiti: comma 2) è applicabile nei confronti tanto del cittadino quanto dello straniero, e prevede il coinvolgimento del Procuratore della Repubblica, cui va data immediata comunicazione dell'accompagnamento e che può ordinare il rilascio della persona accompagnata (comma 3).

specificamente riferiti allo straniero, e volti a superare l'eventuale resistenza del diretto interessato mediante l'uso della forza[33].

La disciplina risulta articolata, andando ad interpolare numerose disposizioni poste in contesti topografici distinti, a loro volta riferiti a diverse categorie soggettive. Lo fa secondo un disegno a intensità crescente, che solo nei confronti di persone sottoposte a trattenimento e dei minori stranieri non accompagnati vede entrare in campo modalità coattive, tali da sfociare nell'ispezione del «dispositivo o supporto elettronico» anche a prescindere dal "consenso" del diretto interessato. Consenso che è invece indispensabile ove si tratti di accedere al dispositivo del richiedente asilo "semplice" (ossia che non rientri nelle altre due categorie del trattenuto e del MSNA).

La differenza più significativa tra le due discipline – sfociate nell'interpolazione del primo comma dell'art. 11 d.lgs. 28.1.2008, n. 25 (ad opera dell'art. 12, comma 1 d.l. n. 145/2024) e nell'inserimento dei commi 2-*bis* e 2-*ter* dell'art. 10-*ter* TU (ad opera del capoverso del medesimo art. 12) – riguarda dunque la possibilità o meno di procedere a un accesso forzato al dispositivo elettronico. Tuttavia, come vedremo, non si tratta dell'unico elemento di diversità.

Infatti, le modifiche alla disciplina degli obblighi di cooperazione del richiedente asilo (collocata nel primo comma dell'art. 11 d.lgs. n. 25/2008) risultano molto più stringate rispetto a quelle stabilite in relazione all'accesso coattivo al *device* regolato dai commi 2-*bis* e 2-*ter* dell'art. 10-*ter* TU; il che – come vedremo – lascia insoluti molti dubbi in ordine alle modalità di accesso allo *smartphone* nella disponibilità del richiedente asilo "consenziente".

Ciò premesso, è bene per ora analizzare due aspetti pregiudiziali, concernenti rispettivamente i dati che possono essere fatti oggetto di osservazione mediante l'accesso al *device* e l'idoneità dell'istituto rispetto allo scopo perseguito dal legislatore. Si tratta, come intuibile, di due profili avvinti fra loro, dovendo l'idoneità dell'istituto rispetto al suo scopo essere valutata anche in considerazione del tipo di dati legittimamente acquisibili.

6. L'oggetto dell'accesso e l'idoneità dell'istituto allo scopo perseguito

Quanto all'oggetto dell'accesso, il testo del rinnovato art. 11 del "decreto Procedure" nulla dice in proposito, limitandosi a stabilirne lo scopo, che è quello di reperire «elementi relativi all'età, all'identità e alla cittadinanza, nonché ai Paesi in cui [il richiedente asilo] ha soggiornato o è transitato». Tuttavia, alcune indicazioni in più si possono ricavare dalla disciplina inserita nel nuovo comma 2-*ter* dell'art. 10-*ter* TU, che, mossa da identico obiettivo, menziona l'accesso immediato «ai dati identificativi dei dispositivi elettronici e delle eventuali schede elettroniche (S.I.M.) o digitali (eS.I.M.) in possesso dello straniero, nonché ai documenti, anche video o fotografici, contenuti nei medesimi dispositivi o supporti elettronici o digitali».

La norma disorienta non poco: infatti, se la prima parte della frase sembra circoscrivere in modo deciso l'oggetto del possibile accertamento, il successivo generico riferimento a «documenti, anche video o fotografici» descrive un potere intrusivo molto più penetrante.

È vero: il precetto vieta l'accesso alla corrispondenza o ad ogni altra forma di comunicazione. Tuttavia, per come formulato, esso si presta comunque a violare la

33. Tale refrattarietà aveva finora indotto il legislatore a privilegiare il ricorso al trattenimento per lo straniero riottoso a farsi identificare (piuttosto che istituire strumenti coattivi di identificazione): v. il comma 3 dell'art. 10-*ter*, TU (inserito con d.l. 17.2.2017, n. 13, conv. con mod. dalla l. 13.4.2017, n. 90), nonché il comma 3-*bis* dell'art. 6 d.lgs. 18.8.2015, n. 142 (aggiunto con d.l. 4.10.2018, n. 113, conv. con mod. dalla l. 1.12. 2018, n. 132).

segretezza della corrispondenza, ove si pensi all'esempio del documento – magari presente nella galleria delle immagini e quindi non collocato in seno a una *chat* o a un'applicazione di messaggistica, cui evidentemente dovrebbe ritenersi precluso l'accesso – dello *screenshot* di un messaggio (tipo *whatsapp*) o di una e-mail.

Non solo: proprio per come scritta, la definizione degli elementi che possono costituire oggetto di osservazione da parte della pubblica autorità rischia comunque di porsi in contrasto con le regole poste a tutela dei dati personali, il cui trattamento va improntato ai principi di giustizia, correttezza e trasparenza, e stando alle quali il soggetto interessato deve essere reso edotto in merito a quali dati che lo riguardano vengono processati e per quali finalità (art. 5 GDPR). Infatti, malgrado le garanzie prescritte per i dati personali non siano *ex se* estensibili anche ai cosiddetti metadati[34], la formulazione impiegata dal comma 2-*ter* dell'art. 10-*ter* TU non assicura che l'accesso sia ristretto a questi ultimi. Ciò avrebbe dovuto indurre maggiore prudenza nella definizione del perimetro della disciplina: espungendo il problematico riferimento a documenti e fotografie (come era stato suggerito dal Garante della *privacy*[35]), oppure irrobustendo le garanzie per accedere anche a elementi diversi dai cosiddetti metadati, nel rispetto della disciplina in materia.

Il rischio di un impatto sulla riservatezza dei dati personali e sull'inviolabilità della corrispondenza (la cui nozione va aggiornata a quanto affermato dalla sentenza costituzionale n. 170 del 2023[36]) induce dunque ad escludere un accesso "manuale"[37]. Interpretando la disciplina in modo rigoroso, andrebbe in sostanza privilegiato l'impiego di tecnologie informatiche simili a quelle utilizzate in Germania, che (come abbiamo visto[38]) permettono di acquisire i soli metadati e i dati esterni delle comunicazioni, così evitando anche solo il rischio di prendere cognizione della corrispondenza e di dati personali da proteggere.

Alla luce di ciò, si può avanzare più di un dubbio sull'idoneità del mezzo a perseguire il suo scopo. Infatti, e in particolare ove l'analisi dovesse effettivamente risultare circoscritta ai soli metadati (soluzione da privilegiare, anche alla luce di quanto diremo a proposito delle più recenti evoluzioni della giurisprudenza di Lussemburgo), diventa importante tener presente la comprovata tendenza all'uso del medesimo *smartphone* da parte di più persone

34. Dopo aver rammentato che il GDPR non fornisce alcuna disciplina in merito ai cosiddetti metadati (ossia alle informazioni relative ai dati), M. Forti (in *Flussi migratori e protezione dei dati personali: alla ricerca di un punto di equilibrio tra sicurezza pubblica e tutela della* privacy *dei migranti e dei rifugiati all'interno del territorio europeo*, in *Media Laws*, 2020, f. 2, p. 217) ricorda come debba farsi riferimento alla direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche), che fornisce una definizione di «dati relativi al traffico» (art. 2 lett. *b*) e di «dati relativi all'ubicazione» (art. 2 lett. *c*), prescrivendo una specifica disciplina a tutela di tali dati (v. in part. artt. 6 e 9). Sennonché, l'A. ricorda come l'art. 15 della direttiva preveda la possibilità per gli Stati membri di derogare alle regole prescritte dalla direttiva medesima per finalità quali la sicurezza interna, la prevenzione e il perseguimento di attività criminali: «la gestione dei flussi migratori potrebbe quindi rientrare nelle attività sottoponibili a deroga, pur dovendo essere comunque rispettati i diritti fondamentali di migranti e rifugiati e i principi sanciti dal GDPR, quali la necessarietà, la giustizia e correttezza».

35. Audizione del professor Pasquale Stanzione, cit., p. 3 della relazione disponibile in pdf.

36. Come noto, secondo quanto chiarito da tale fondamentale pronuncia (forte di ampi richiami alla giurisprudenza della Corte EDU), la tutela costituzionale della corrispondenza non si esaurisce con la ricezione del messaggio da parte del destinatario, ma perdura fin tanto che esso conservi carattere di attualità e interesse per gli interlocutori.

37. Accesso manuale che sicuramente ha operato in Danimarca, secondo quanto riportato da T. R. Nielsen-T. Gammeltoft-Hansen-N. Holten Møller, *Mobile Phone Data Trans- forming Casework in Asylum Decision-making: Insights from the Danish Case*. ACM J. *Responsib. Comput.* 1, 4, Article 27 (December 2024), p. 2.

38. Cfr. *retro*, § 4.

durante il viaggio migratorio[39], come pure quella all'uso di pseudonimi da parte di rifugiati che temono di essere sorvegliati: il che conduce ad escludere la possibilità di accordare una comprovata rilevanza dimostrativa ai dati contenuti nel telefono[40].

A ciò si aggiunga che, stando a statistiche svolte in Germania, nella stragrande maggioranza dei casi gli elementi conoscitivi ricavati dai telefoni hanno confermato quanto dichiarato dai richiedenti asilo alle autorità[41].

L'analisi circa oggetto e scopo dell'accesso al *device* induce dunque a diffidare dell'opportunità politica e giuridica di uno strumento che, oltre a risultare inadeguato rispetto al fine perseguito (in generale, e a maggior ragione rispetto ai meri dati del traffico telefonico e ai profili di accesso ad applicazioni *internet*), alla prova dei fatti si è comunque dimostrato superfluo, non avendo, se non in rari casi, smentito le narrazioni dei richiedenti asilo[42].

7. L'accesso "acconsentito" al *device*

Tutto ciò premesso, è ora il momento di esaminare più nel dettaglio la disciplina di nuovo conio.

Innanzitutto, viene arricchito il contenuto dell'art. 11 del d. lgs. 28.1.2008, n. 25 (il cosiddetto "decreto Procedure"), concernente la definizione degli obblighi di collaborazione del richiedente protezione internazionale, stabilendo che questi è oggi tenuto anche a «cooperare con le autorità […] ai fini dell'accertamento dell'identità e [ad] esibire o produrre gli elementi in suo possesso relativi all'età, all'identità e alla cittadinanza, nonché ai Paesi in cui ha soggiornato o è transitato, *consentendo, quando è necessario per acquisire i predetti elementi, l'accesso ai dispositivi o supporti elettronici o digitali in suo possesso*» (comma 1)[43].

Tale precetto non contempla la possibilità di accesso forzoso al *device*. Nondimeno, e com'è dimostrato dall'esperienza tedesca (di cui s'è dato conto *retro*), la sua effettività poggia sull'interesse del richiedente asilo a mostrarsi collaborativo, nella prospettiva di ottenere un esame benevolo della propria domanda (e comunque anche in quella di evitare il trattenimento eventualmente disposto secondo quanto prescritto dai commi 3 dell'art. 10-*ter* TU per lo straniero rimpatriando, e 3-*bis* dell'art. 6 d.lgs. n. 142/2015 per il richiedente protezione internazionale).

È proprio la natura non propriamente libera e incondizionata del consenso all'ispezione informatica a rendere poco rassicurante quel generico «quando è necessario per acquisire i predetti elementi» costituente il discrimine in ordine alla scelta se procedere o meno all'invito a consentire l'accesso al *device*: la disposizione sembra infatti lasciare un margine

39. Il dato è rilevato da numerosi osservatori. V per tutti M. Gillespie-S. Osseiran-M. Cheesman, *Syrian Refugees and the Digital Passage to Europe*, cit., p. 4.

40. A. Biselli-L. Beckmann, *Invading Refugees' Phones*, cit., p. 29.

41. *Ibid*.

42. Negano l'idoneità dello strumento rispetto al suo scopo (ossia il soddisfacimento del primo dei tre "sotto-criteri" del principio di proporzionalità, con quanto ne consegue in ordine al mancato rispetto dell'art. 52, § 1, CDFUE) F. Palmiotto-D. Ozkul, *"Like Handing My Whole Life Over"*, cit.

43. «Con il termine "dispositivi o supporti elettronici o digitali" si intendono tutti quegli strumenti che sono pienamente utilizzabili seguendo la mobilità dell'utente, quali, ad esempio, cellulari, palmari, *smartphone*, *tablet*, *notebook*, lettori MP3, ricevitori GPS, ecc. Possono essere dunque dispositivi dedicati – ossia dispositivi che possono essere utilizzati da un solo processo alla volta – oppure *general purpose*, ossia dispositivi versatili, adatti a molteplici impieghi»: così si legge nella relazione illustrativa del disegno di legge di conversione del d.l. n. 145/2024 (Atto Camera n. 2088, presentato l'11.10.2024).

di discrezionalità troppo ampio all'autorità di pubblica sicurezza, non esprimendo in modo abbastanza chiaro la necessità di considerare l'accesso al dispositivo elettronico quale *extrema ratio*. Sarebbe stato opportuno aggiungere un *assolutamente* accanto a quel *necessario*. Di più: sarebbe stata senz'altro preferibile una soluzione analoga a quella fatta propria dal legislatore tedesco, che – come abbiamo ricordato – nel 2024 ha messo nero su bianco la possibilità di accedere ai dispositivi elettronici solo ove il cittadino straniero non sia in possesso di un passaporto valido o di altra documentazione in grado di comprovarne l'identità.

La (consueta) scarsa attenzione per la posizione del migrante è poi testimoniata anche dalle eclatanti lacune della disciplina dinamica. In proposito, il primo comma dell'art. 12 d.l. n. 145/2008 non si premura di specificare alcun tipo di tutela per il migrante "accondiscendente". Infatti, a meno che non s'intendano implicitamente operanti le (come vedremo assai deficitarie) garanzie prescritte dal comma successivo, concernente l'ipotesi in cui l'accesso al *device* venga comunque disposto a prescindere dal consenso del diretto interessato, pare quasi che tale consenso venga considerato come una delega in bianco alla pubblica autorità, svincolata financo da qualsiasi obbligo documentativo in ordine alle attività svolte sul domicilio informatico del migrante. Una soluzione, quest'ultima, inaccettabile, che induce dunque a ritenere che tali "garanzie" – di cui diremo nei prossimi paragrafi – debbano necessariamente operare anche rispetto a tale prima ipotesi di accesso. Sennonché, come vedremo, tali tutele sono topograficamente collocate non in seno all'art. 11 d.lgs. n. 25/2008, ma in un differente contesto normativo, e segnatamente nel comma 2-*ter* dell'art. 10-*ter* TU, richiamato da tutte le ulteriori disposizioni che ammettono l'accesso immediato (i.e. coattivo) al *device* ma non anche dal rinnovato art. 11 del "decreto Procedure".

Ciò finisce giocoforza per determinare un difetto della trasparenza richiesta dall'art. 5 § 1 del UE 2016/679 (RGPD) per il trattamento dei dati personali. Anche perché la disciplina non contempla espressamente alcuna conseguenza tipizzata in ordine alle ricadute dell'eventuale dissenso all'accesso al *device*, che tuttavia potrebbe essere preso in considerazione per le valutazioni di credibilità del richiedente asilo, con implicazioni negative per l'esito della relativa domanda.

8. Il ricorso alle maniere forti: i destinatari dell'accesso immediato al *device*

La possibilità di prescindere dal *placet* del migrante è prevista dalle altre disposizioni parimenti inserite con l'art. 12 del d.l. n. 145 del 2024, le quali riguardano, rispettivamente: i migranti condotti o trattenuti negli *hotspot* (art. 12, comma 2, lett. *a*); coloro che si trovino in stato di trattenimento nei CPR in quanto attinti da un provvedimento espulsivo (art. 12, comma 2, lett. *b*); i richiedenti protezione internazionale trattenuti ai sensi degli artt. 6 (art. 12, comma 3, lett. *a*) e 6-*bis* del d.lgs. n. 142 del 2015 (precetto, quest'ultimo, che regola la detenzione amministrativa contestuale allo svolgimento della procedura accelerata di frontiera) (art. 12, comma 3, lett. *b*); i minori stranieri non accompagnati (art. 19-*bis* d.lgs. n. 286 del 1998, interpolato dall'art. 12, comma 3, lett. *c*).

Sulla scorta di tale quadro, nei confronti di queste categorie di persone, accanto a quella di cui al comma 2-*bis* dell'art. 10-*ter* TU vige anche l'inedita disciplina racchiusa nel successivo comma 2-*ter*. Ne consegue che, mentre per il "semplice" richiedente asilo la disciplina sembra limitarsi a una forma (assai persuasiva e incalzante) di *nudging*, nei confronti di minori stranieri non accompagnati, stranieri tradotti in un *hotspot* e stranieri a

vario titolo sottoposti a trattenimento[44] l'accesso ai dispositivi elettronici possa scattare anche in mancanza di consegna "spontanea" del *device*.

Per quanto riguarda il MSNA, è chiaro l'intento di consentire (anche coattivamente) l'accertamento dell'età. Sennonché, come rilevato dal Garante per la *privacy* (chiamato ad esprimersi quando il decreto era in corso di conversione in legge, ma senza che nessuna delle sue osservazioni sia poi stata recepita), il minore è destinatario di una disciplina complessivamente molto più garantistica di quella riservata allo straniero adulto: alla luce di ciò, il silenzio delle fonti sovraordinate in ordine alla possibilità di procedere all'ispezione degli effetti personali anche con specifico riferimento al MSNA potrebbe risultare significativa in senso impeditivo (evidenziando dunque un contrasto tra la disciplina appena varata e quella sovranazionale)[45].

La seconda categoria soggettiva potenzialmente interessata da un accesso immediato al dispositivo è invece costituita dalla moltitudine di persone tradotte in un *hotspot* (ai sensi dell'art. 10-*ter* comma 1 TU) e di quelle a vario titolo trattenute nel medesimo *hotspot* o in un CPR.

In forza di questa disciplina, si assiste ad una sensibile amplificazione degli effetti della scelta – in concreto marcata da ampia discrezionalità – di decidere se destinare o meno uno straniero a un CPR. È infatti importante osservare come la norma menzioni le persone trattenute, e non quelle suscettibili di esserlo. Il distinguo non è di poco conto, visto che, se i presupposti per poter disporre il trattenimento – in tutte le sue diverse declinazioni – sono alquanto estesi, l'istituto, regolato nella prospettiva di attingere un numero assai significativo di persone, almeno per ora vede un'applicazione ben più contenuta di quella astrattamente ipotizzabile sulla scorta del nudo dato positivo[46].

In proposito, lo iato tra diritto scritto e diritto vivente è notevole, tanto da aver indotto il legislatore a inserire dei veri e propri criteri di priorità per guidare la scelta dell'autorità di pubblica sicurezza in ordine alla decisione di quali persone trattenere. Stando al comma 1.1 dell'art. 14 TU – inserito dal d.l. 21.10.2020, n. 130, conv. con mod. con l. 18.12.2020, n. 173, e a cui fanno rinvio tanto l'art. 6 quanto l'art. 6-*bis* del d.lgs. n. 142/2015 – il trattenimento deve infatti trovare applicazione prioritaria nei confronti degli stranieri che: siano cittadini di (o comunque provengano da) Paesi coi quali viga un accordo di riammissione; siano condannati, anche con sentenza non definitiva, per uno dei reati ostativi al rilascio del visto di ingresso (art. 4, comma 3, terzo periodo, TU) o del permesso di soggiorno (art. 5, comma 5-*bis*, TU); costituiscano una minaccia per l'ordine e la sicurezza pubblica.

Potendo operare nei riguardi di chi sia trattenuto e non di chi sia nella condizione di esserlo, l'accesso al *device* delle persone in stato di detenzione amministrativa – consentito grazie alle interpolazioni degli artt. 14 TU (con l'innesto del comma 1.2), 6 (v. il nuovo comma 4-*bis*) e 6-*bis* d.lgs. n. 142/2015 – finisce dunque per amplificare il tasso di discriminazione

44. L'unica eccezione sembra essere quella dei trattenuti ai sensi dell'art. 6-*ter* d.lgs. n. 142/2015.

45. Audizione del professor Pasquale Stanzione, che in proposito prende in esame anche la disciplina racchiusa nel nuovo "regolamento procedure" (reg. (UE) 2024/1348, il quale «esige – in particolare agli artt. da 22 a 25 – garanzie rafforzate, evitando accertamenti irragionevoli, contrastanti con il loro superiore interesse e con la presunzione di minore età nei casi dubbi, nonché contemplando in via residuale una valutazione multidisciplinare ai fini accertativi dell'età» (p. 2 della relazione in pdf). In generale, sul tema v. R. Bendinelli, *Le norme sul trattamento dei dati personali dei richiedenti asilo nell'Unione europea: talune criticità rispetto al caso dell'interessato minorenne*, in questa *Rivista*, n. 1.2024.

46. In proposito, si rinvia alle considerazioni già svolte in E. Valentini, *Il proteiforme apparato coercitivo allestito per lo straniero*, in F. Curi-F. Martelloni-A. Sbraccia-E. Valentini, *I migranti sui sentieri del diritto*, II ed., Torino, Giappichelli, 2021, p. 243 ss.

tra chi è trattenuto e chi non lo è, enfatizzando gli effetti di una scelta – quella di imporre l'ingresso in un Centro detentivo – nella sostanza affidata all'autorità di pubblica sicurezza[47].

Sulla scorta di ciò, è facile scorgere le premesse anche per eventuali abusi dell'istituto. Infatti, l'idea che la detenzione amministrativa debba attingere in via preferenziale soggetti già condannati (anche in via non definitiva) per un reato ostativo al rilascio del permesso di soggiorno o costituenti una minaccia per l'ordine e la sicurezza pubblica rischia di trasformare l'ispezione del *device* del trattenuto in uno strumento di controllo di natura preventiva nei suoi confronti; e ciò, oltretutto, senza che necessariamente egli sia stato valutato come pericoloso all'esito di un procedimento di prevenzione o di un processo penale[48].

Infine, si consideri un aspetto ulteriore. La circostanza che l'«accesso immediato» ai dispositivi elettronici a prescindere dal consenso dell'interessato sia circoscritto ai soli migranti condotti in un *hotspot* e a quelli (a vario titolo) trattenuti si salda alla perfezione con la pratica – totalmente sguarnita di base legale[49] – che vede i migranti privati del proprio *smartphone* all'ingresso nei punti di crisi e nei CPR: tale prassi, evidentemente ingenerata da una istintiva (e quasi freudiana) equiparazione tra il regime detentivo tipico del carcere e quello destinato a svolgersi all'interno dei CPR, finisce infatti per risultare del tutto confacente alla novella di nuovo conio.

9. L'accesso immediato: profili procedurali

Anche nei confronti delle persone sottoposte a detenzione amministrativa e per i minori stranieri non accompagnati la disciplina prevede un primo tipo di approccio da parte della pubblica autorità, improntato a modalità non coattive, e che dunque si sostanzia in una richiesta di consegna del *device* del tutto analoga a quella prevista dal novellato art. 11 del "decreto Procedure" (di cui s'è detto sopra).

Solo in seconda battuta, e dunque una volta constatata la mancata collaborazione da parte dello straniero, può scattare – appunto solo nei confronti dei MSNA a degli stranieri condotti negli *hotspot*, come pure dei trattenuti *ex* artt. 14 TU, 6 e 6-*bis* del "decreto Procedure" – il ricorso alle maniere forti, attraverso un'apprensione da attuarsi in forma coattiva.

In proposito, va segnalato il ricorso alla consueta edulcorazione semantica da parte del legislatore, che, quando si tratta di usare la forza nei confronti degli stranieri (come avviene con il trattenimento) evita di chiamare le cose con il loro nome: quello che è un sequestro coattivo (poiché effettuato a prescindere dalla consegna spontanea del *device*) finalizzato a

47. In proposito, va detto che la corretta applicazione dei criteri di priorità nell'applicazione del trattenimento è difficilmente sindacabile. Infatti, oggetto di sindacato da parte del giudice della convalida non è il rispetto dei criteri di priorità nell'applicazione della misura, ma la sussistenza dei presupposti applicativi del trattenimento, che vedono una definizione normativa decisamente più ampia.

48. E anzi anche quando il processo penale abbia escluso la pericolosità, appunto per effetto dell'automatismo insito nel richiamo ai reati che ostano al rilascio del visto di ingresso o del permesso di soggiorno. Sull'istituto (il cui perimetro operativo è peraltro in corso di ridimensionamento da parte della Corte costituzionale), v. le ancora attuali considerazioni di M. Savino, *L'incostituzionalità del c.d. automatismo espulsivo*, su questa *Rivista*, n. 3.2013, p. 37 ss.

49. Dopo essere stata stigmatizzata dalla giurisprudenza (V. Trib. Milano, sez. specializzata, ordinanza 23.2.2021, che si può leggere in www.sistemapenale.it, 15.9.2021, con nota adesiva di G. Mentasti), tale prassi è stata "codificata" dagli artt. 4 e 5 della cosiddetta "direttiva Lamorgese" (d.m. interno del 19.5.2022, che ha soppiantato il «regolamento unico C.I.E.» del 2014 e che affronta i principali profili concernenti la gestione dei Centri); tuttavia, essa tuttora continua a non essere in linea con il principio della riserva di legge *ex* art. 15 Cost.

svolgere un'ispezione informatica contro la volontà dell'interessato, diventa, nella terminologia impiegata dal nuovo comma 3-*bis* dell'art. 10-*ter* TU, un ben più generico «accesso immediato»[50]. Sennonché, sulla possibilità di usare la forza non si possono avanzare dubbi, visto che l'accesso immediato scatta «in caso di inosservanza dell'obbligo di cooperazione di cui al comma 2-*bis*» (del medesimo art. 10-*ter* TU).

Se il migrante è riottoso, dunque, e fermo restando lo scopo dell'ispezione del dispositivo – che resta improntato alla sola ricerca dei medesimi «elementi indicati nel medesimo comma 2-*bis*» dell'art. 10-*ter* TU –, il questore può disporre «che gli ufficiali o agenti di pubblica sicurezza procedano all'accesso immediato ai dati identificativi dei dispositivi elettronici e delle eventuali schede elettroniche (S.I.M.) o digitali (eS.I.M.) in possesso dello straniero, nonché ai documenti, anche video o fotografici, contenuti nei medesimi dispositivi o supporti elettronici o digitali».

Nell'aprire (molto pericolosamente e problematicamente) alla possibile osservazione anche di documenti (compresi quelli video o fotografici), il legislatore pone poi un limite ben preciso, vietando «in ogni caso» «l'accesso alla corrispondenza e a qualunque altra forma di comunicazione».

I rapporti tra i due commi introdotti nel corpo dell'art. 10-*ter* TU (oggetto di rinvio anche da parte delle ulteriori disposizioni inserite dall'art. 12 del medesimo "decreto flussi", concernenti i trattenuti e i MSNA) risultano poco chiari, essendo la seconda disposizione molto più dettagliata della prima. Esattamente come abbiamo già osservato rispetto alla consegna "spontanea" di cui all'art. 11 del d.lgs. n. 25/2008, nell'ipotesi di accesso "assecondato" non risulta espressamente stabilita la necessità di documentare le operazioni, e, ancor prima, non viene neppure adeguatamente specificato cosa possa essere fatto oggetto di osservazione.

Tuttavia, nel corpo dell'art. 10-*ter* (come pure degli artt. 14 TU, 6 e 6-*bis* del "decreto procedure") questa possibile divaricazione può essere risolta attraverso una lettura sistematica di due precetti posti in successione topografica fra loro (appunto i commi 2-*bis* e 2-*ter*), considerando la seconda disposizione atta a completare anche i *deficit* contenutistici del precetto subito precedente[51].

Ciò posto, i profili procedimentali (appunto descritti solo in relazione all'accesso coattivo) denotano uno *standard* di garanzia davvero basso, testimoniato innanzitutto dalla circostanza che, *as usual*, lo straniero è posto al cospetto di attività poste in essere direttamente dall'autorità di pubblica sicurezza, con il coinvolgimento solo postumo dell'autorità giudiziaria, peraltro incarnata dal Giudice di pace [52] (e nel Tribunale dei minorenni, ove l'ispezione attinga il telefono di un MSNA).

A tale specifico proposito, e al netto di ciò che diremo in ordine alle ragioni che hanno comunque indotto il legislatore a contemplare una parvenza di giurisdizione, l'assetto complessivo delle competenze risulta a dir poco irrazionale. L'assegnazione del compito di

50. In realtà, la parola «ispezione» campeggia nella rubrica dell'art. 12 d.l. n. 145/2024. Tuttavia, essa non risulta mai impiegata dai singoli commi che compongono la disposizione nel suo complesso (forse per non evocare la necessità di rispettare le garanzie prescritte dagli artt. 244 ss. c.p.p.).

51. Per quanto più ardua da prospettarsi, come già rilevato *retro* la medesima esegesi risulta peraltro doverosa anche rispetto all'innesto operato nel primo comma del d.lgs. n. 25/2008 (che ha un contenuto corrispondente al solo comma 2-*bis d*ell'art. 10-*ter* TU e al contempo non richiama il comma 2-*ter*).

52. Difficile non mettere in dubbio l'utilità di un presidio rappresentato dalla necessaria convalida del giudice di pace, storicamente mostratosi molto accondiscendente dinanzi alle richieste dell'autorità di pubblica sicurezza (così com'è testimoniato dall'altissimo tasso di convalide dei trattenimenti e degli accompagnamenti coattivi alla frontiera disposti ai sensi dell'art. 14 TU).

convalidare l'accesso allo *smartphone* al Giudice di pace potrebbe infatti spiegarsi sulla scorta del fatto che proprio a tale organo – non togato – è affidata la competenza in ordine alla convalida del trattenimento *ex* art. 14 TU. Tuttavia, il trattenuto a fini di rimpatrio (e dunque l'espulso o il "respinto differito") è solo uno dei possibili destinatari dell'ispezione coattiva del *device*. Ad esso si affiancano infatti, oltre alle persone condotte nei punti di crisi per ivi essere sottoposte alle attività menzionate dal comma 1 dell'art. 10-*ter* TU, anche i richiedenti protezione internazionale che siano trattenuti *ex* art. 6 e 6-*bis* del "decreto Accoglienza". Ebbene: per questi ultimi pare del tutto insensata l'attribuzione della competenza alla convalida in capo al Giudice di pace; tanto più considerando che, proprio con il medesimo "decreto flussi" in cui è situata la novità normativa sulla quale stiamo ragionando, il compito di convalidare i trattenimenti dei richiedenti protezione internazionale è stato assegnato alle Corti d'appello[53].

Entrando *in medias res*, questa è la sequenza tratteggiata dalla disciplina in esame: sulla scorta delle indicazioni ricevute dal questore, gli ufficiali o gli agenti di polizia procedono all'accesso, previo avviso all'interessato del diritto di assistere alle operazioni alla presenza di un mediatore culturale (o, qualora nominato, dell'esercente dei poteri tutelari per il MSNA). Dopodiché, testualmente: «il verbale delle operazioni compiute, che dà atto anche delle disposizioni del questore, indica le finalità, i criteri e le modalità dell'accesso, i dati controllati e l'esito delle operazioni, riporta le eventuali dichiarazioni rese dall'interessato e, unitamente alla eventuale documentazione fotografica allegata, è trasmesso per la convalida, entro il termine di quarantotto ore dall'avvio delle operazioni, al Giudice di pace territorialmente competente che, entro le successive quarantotto ore, decide sulla convalida con provvedimento motivato. Il provvedimento è comunicato all'autorità di pubblica sicurezza, che consegna allo straniero copia del medesimo provvedimento e del verbale delle operazioni compiute. In caso di non convalida o di convalida parziale, i dati illegittimamente controllati sono inutilizzabili e il giudice dispone la cancellazione della documentazione ad essi relativa».

9.1. Segue: l'inevitabile contrasto con l'art. 15 Cost.

Gli aspetti problematici di questa disciplina sono numerosi ed evidenti.

Il primo salta immediatamente agli occhi, ed è costituito dal coinvolgimento meramente postumo del giudice, chiamato a convalidare l'accesso al dispositivo solo una volta che questo si è già realizzato.

In proposito, pare che il legislatore abbia pavlovianamente ribadito anche in questo contesto lo schema ricorrente a proposito delle restrizioni della libertà personale dello straniero nella prospettiva di patrocinarne l'allontanamento: ossia quello che, in origine previsto per il trattenimento *ex* art. 14 TU, è stato esteso al trattenimento del richiedente asilo (già a far data dal 2002, con una scelta normativa poi ribadita anche dalle numerose successive metamorfosi che hanno investito l'istituto), nonché all'accompagnamento coattivo alla frontiera (con riforme che si sono succedute in tempi diversi, a partire dal 2002 e fino al 2018).

53. V. art. 16 d.l. n. 145/2024 alla luce delle modifiche operate con la legge (di conversione) n. 187/2024. Sulla scorta di tale assetto, il richiedente asilo in stato di trattenimento si trova dunque sottoposto alle valutazioni di tre diversi giudici: la Corte d'appello (deputata a convalidare il trattenimento), il Giudice di pace (chiamato a convalidare l'accesso al *device*), la sezione specializzata in materia di immigrazione e protezione internazionale del Tribunale avente sede nel capoluogo del distretto (a sua volta competente a decidere nel caso di rigetto della domanda di protezione).

Il necessario coinvolgimento di un giudice è senz'altro dovuto alla consapevolezza del possibile impatto sull'inviolabilità della corrispondenza, conseguente alla possibilità di accedere a documenti, «anche video o fotografici». Sennonché, il legislatore del "decreto flussi" mostra di trascurare che lo *standard* garantistico disegnato dall'art. 15 Cost. è per almeno un aspetto superiore a quello preteso dall'art. 13: l'art. 15 identifica infatti nella sola autorità giudiziaria l'organo legittimato a violare la corrispondenza, e non affida alcun potere provvisorio in capo all'autorità di pubblica sicurezza (peraltro da esercitarsi in via di eccezionalità ed urgenza), sulla falsariga di quanto stabilito dal terzo comma dell'art. 13 Cost.[54].

L'anomalia della disciplina approntata dal "decreto-flussi" è testimoniata dal confronto con l'art. 254 c.p.p., che, disciplinando il sequestro di corrispondenza, è attento a mantenere ben distinte le prerogative della polizia da quelle dell'autorità giudiziaria: infatti, mentre l'ufficiale di polizia giudiziaria può procedere al cosiddetto "fermo postale" – bloccando il recapito di «lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato» –, è la sola autorità giudiziaria a poter procedere all'apertura dei plichi o a prendere altrimenti conoscenza del loro contenuto.

La disciplina dell'art. 254 c.p.p. costituisce un *tertium comparationis* illuminante, tanto più significativo ove si consideri che la suddivisione delle competenze – distribuite tra autorità giudiziaria e ufficiale di polizia giudiziaria – opera in via preventiva, ovvero quando ancora non è chiara la natura dell'elemento probatorio che verrà sottoposto ad osservazione, e dunque quando ancora non è dato sapere (appunto perché non lo si è ancora "aperto") se tale elemento sia riconducibile o meno alla nozione di «oggetto di corrispondenza»[55].

La circostanza che, anche nella versione definitivamente varata con la legge di conversione del d.l. n. 145/2024, possano essere fatti oggetto di ispezione del *device* pure i «documenti, anche video o fotografici» rende oltremodo calzante il richiamo agli artt. 254 c.p.p., ben potendo tali documenti configurare «oggetti di corrispondenza». Basti pensare, come già rilevato, all'esempio dello *screenshot* di un messaggio (tipo *whatsapp*) o di una *e-mail*[56]. La fisionomia dell'art. 254 c.p.p. dimostra che è l'astratta possibilità di incappare in un «oggetto di corrispondenza» a determinare il necessario coinvolgimento dell'autorità giudiziaria nell'attività di ricerca della prova; coinvolgimento ineludibile anche rispetto all'ipotesi di corrispondenza non in via trasmissione ma anche "giacente" nel *device*, così come chiarito (e opportunamente preteso) dalla sentenza costituzionale n. 170 del 2023.

9.2. Segue: ulteriori aspetti critici

Ciò detto in relazione all'assetto di fondo della disciplina in esame, tale da renderla radicalmente inconciliabile con l'art. 15 comma 2 Cost., gli aspetti più di dettaglio sono destinati a risultare assorbiti. Tuttavia, essi meritano comunque di essere segnalati. Riepiloghiamoli, sulla scorta di considerazioni sparse, a prima lettura.

54. Tale constatazione è di per sé assorbente, poiché in grado di superare un'altra possibile fonte di perplessità, insita nel difetto di ragioni di eccezionalità e urgenza in grado di giustificare, per di più come regola generale, un intervento da parte dell'autorità di pubblica sicurezza che vada oltre la fisica apprensione del *device*, e riferito anche alla relativa ispezione, che ben potrebbe – e dovrebbe – essere affidata all'autorità giudiziaria.

55. Espressione ripresa testualmente dal primo comma dell'art. 254 c.p.p.

56. Audizione del professor Pasquale Stanzione, cit., p. 3 del pdf.

Le operazioni da compiersi sul *device* possono essere demandate, dal questore, non solo ad ufficiali (come prescritto dall'art. 254 c.p.p.), ma anche ad agenti di polizia.

Non è prescritta la presenza di un difensore. Il fatto che l'interessato possa assistere allo svolgimento delle operazioni avendo al proprio fianco il solo mediatore culturale – di per sé privo delle competenze necessarie a presidiare il rispetto della legge in ordine alla tutela dei numerosi diritti suscettibili di risultare compressi dall'accesso al dispositivo elettronico – non può non suscitare perplessità. Perplessità scaturenti non solo dal tangibile rischio di abusi, insito nella possibilità di un'azione debordante da parte dell'autorità di polizia (la quale, una volta in possesso del *device*, ben potrebbe andare oltre i limiti imposti dalla legge, in ipotesi spingendosi fino a un'ispezione – e a un'estrazione di copia – di tutti i contenuti custoditi nello *smartphone*). Infatti, le preoccupazioni scaturiscono già sulla scorta del dato normativo, il quale, anche ove rispettato, appunto permette l'osservazione pure di documenti, anche video o fotografici[57].

L'unica forma di partecipazione accordata al possessore del dispositivo elettronico è rappresentata dal diritto di assistere allo svolgimento dell'ispezione (cui si associa l'obbligo di verbalizzare le sue eventuali dichiarazioni), alla presenza di un mediatore culturale. Peccato, tuttavia, che, oltre a quella di un difensore, non sia prevista neppure la presenza di un interprete (figura comunque non omologabile a quella del mediatore culturale), come pure quella di un consulente tecnico che possa assistere alle operazioni[58].

Ancora: avviso del diritto di presenziare alle operazioni non significa presenza necessitata; da ciò discende che, là dove il diretto interessato non dichiari di voler essere presente mentre si svolge l'accesso al proprio *device*, il personale di polizia possa procedere "in solitudine" (e dunque, parrebbe, anche senza coinvolgere il mediatore culturale).

Secondo quanto testualmente stabilito, oltre a dover dare atto delle disposizioni del questore (e delle eventuali dichiarazioni rese dal possessore del dispositivo elettronico), il verbale delle operazioni compiute «indica le finalità, i criteri e le modalità dell'accesso, i dati controllati e l'esito delle operazioni», e vede l'allegazione di «eventuale documentazione fotografica». Le modalità di svolgimento dell'operazione non sono dunque meglio specificate, non essendo previsto che debba essere effettuata una copia forense, e senza che

57. In generale, la mancata previsione di assistenza difensiva stride con il complessivo disegno approntato dalla novella. Infatti, se la delicatezza dell'accertamento (appunto in grado di coinvolgere anche la corrispondenza) ha indotto il legislatore ad imporre il necessario intervento di un giudice, analoga "premura" avrebbe dovuto suggerire anche l'obbligatoria presenza del difensore.

58. Eccettuate le ipotesi di contenzioso strategico, è arduo immaginare che un migrante in procinto di subire l'ispezione del telefono possa trovarsi nelle condizioni (economiche e di consapevolezza in ordine ai propri diritti, essendo egli appunto sguarnito di difensore) di nominare un consulente tecnico che possa presenziare all'estrazione dei dati dal suo *smartphone*. Tuttavia, com'è ovvio, è il dato giuridico che conta; e l'inadeguatezza del quadro si staglia anche ponendo mente ai contenuti del d.d.l. n. 806/2023, rubricato «Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, *smartphone* e memorie digitali», e approvato dal Senato il 10 aprile 2024. Come noto ai processualpenalisti, tale disegno di legge si prefigge di innalzare le garanzie concernenti il sequestro dei dispositivi elettronici e dei successivi accertamenti sui relativi contenuti disposti a fini penali, proprio in considerazione dell'alto tasso di intrusività che caratterizza simili mezzi d'indagine (non così distante da quello caratteristico delle intercettazioni). Oltre ad individuare nel g.i.p. l'organo titolare del potere di disporre il sequestro del *device* (o comunque la convalida del sequestro disposto in via urgente dal pubblico ministero o dalla polizia giudiziaria: v. l'idea di un inedito art. 254-*ter* c.p.p. racchiusa nel disegno di legge), tale potenziamento delle garanzie dovrebbe realizzarsi anche attraverso il necessario coinvolgimento dei soggetti interessati e dei propri difensori in vista del conferimento dell'incarico tecnico per la duplicazione del contenuto dei dispositivi informatici: conferimento da attuarsi in contraddittorio, con facoltà, per l'indagato e gli altri soggetti colpiti dall'estrazione dei dati, di nominare un proprio consulente.

esista alcuna indicazione (neppure a livello regolamentare, almeno per ora) in ordine al *software* utilizzato per procedere all'analisi[59].

Il giudizio di convalida demandato al Giudice di pace (come pure al Tribunale dei minorenni, nel caso di accesso allo *smartphone* del MSNA) ha natura meramente cartolare. Non solo: anch'esso, al pari delle operazioni sul *device*, si svolge senza che sia contemplata anche solo l'astratta possibilità di un'assistenza difensiva. Non è infatti prevista neppure la possibilità di presentare memorie onde orientare la decisione del giudice, e dunque nella prospettiva di ottenere la declaratoria di inutilizzabilità e la cancellazione di dati indebitamente fatti oggetto di osservazione (e di documentazione fotografica).

La mancata assistenza difensiva desta preoccupazione ove si consideri che il vaglio cartolare rimesso al giudice – chiamato a pronunciarsi con un provvedimento motivato – sembra individuare l'unico momento preposto a constatare e a dichiarare l'inutilizzabilità degli elementi «illegittimamente controllati» (destinata appunto a sfociare in un rigetto della richiesta di convalida o in un suo accoglimento solo parziale), e a decretare la cancellazione della documentazione ad essi relativa. La preoccupazione aumenta ponendo mente al fatto che per il provvedimento di convalida non è previsto alcun mezzo di impugnazione, e che per di più non risulta neppure chiaro se l'inutilizzabilità dei dati «illegittimamente controllati» possa essere fatta valere anche in un contesto diverso e successivo rispetto a quello della convalida dinanzi al giudice di pace (o al tribunale dei minorenni)[60].

Benché la norma non vi faccia espresso riferimento, una doverosa valorizzazione del principio di proporzionalità porta a suggerire che il giudice debba ritenersi tenuto a rigettare la richiesta di convalida non solo quando sia stata violata la segretezza delle comunicazioni, ma anche là dove l'accesso al *device* non fosse davvero *necessario*, così come richiesto dalla disciplina in esame; e dunque qualora la pubblica autorità abbia deciso di dar luogo all'ispezione nonostante la determinazione dell'identità, della nazionalità, dell'età e del percorso migratorio dello straniero possano essere raggiunte in altro modo, e dunque sulla scorta delle informazioni rese dal diretto interessato (che si sia rifiutato di consegnare il proprio dispositivo elettronico ma che abbia al contempo offerto elementi sufficienti ai fini dell'accertamento da svolgersi nel caso concreto). In sostanza, e come ritenuto anche dalla giurisprudenza tedesca, al giudice va necessariamente demandata una valutazione in ordine al fatto che l'accesso immediato al *device* abbia realmente costituito l'*extrema ratio*: solo in questo modo risulterebbe rispettato il principio di proporzionalità prescritto dall'art. 52 CDFUE (oltre a quello della minimizzazione nel trattamento dei dati personali, *ex* art. 5, § 1, lett. *c* GDPR, art. 4, § 1, lett. *c* dir. (UE) 2016/680, art. 3, comma1, lett. *c* d.lgs. 18.5.2018, n. 51[61]). Ebbene: anche in considerazione di tale delicato compito giudiziale – compito che sarebbe comunque stato opportuno esplicitare (come ha fatto il legislatore tedesco nel 2024) –, sarebbe stato opportuno prevedere l'assistenza difensiva del migrante, così da mettere l'interessato nella condizione di portare argomenti per sollecitare il rigetto della convalida.

Non è chiara la conseguenza del mancato rispetto dei tempi prescritti per la convalida; in proposito, risulta difficile ipotizzare un'inutilizzabilità non esplicitata dalla legge. Ad ogni modo, la tempistica prescritta (48 + 48 ore) impone un'azione celere; l'unico modo per

59. Inoltre, non risulta chiarita neppure la conseguenza di un eventuale diniego della *password* di accesso al dispositivo.

60. Infatti, il comma 3-*ter* dell'art. 10-*ter* TU ricollega l'inutilizzabilità (e la conseguente cancellazione) dei dati illegittimamente controllati alla mancata convalida o alla convalida parziale.

61. La necessità di rispettare questi precetti è stata segnalata in sede di audizione dal professor Pasquale Stanzione (v. la relazione scritta, p. 2 del pdf).

attribuirle senso sembra quella di associare al suo mancato rispetto l'obbligo di immediata restituzione dello *smartphone* all'avente diritto[62], così da contrastare fenomeni come quelli ad esempio verificatisi in Gran Bretagna, dove i migranti sono stati privati del proprio telefono addirittura per mesi[63].

La disciplina parla di inutilizzabilità, così menzionando una categoria squisitamente processualpenalistica, ma con una scelta lessicale che potrebbe rivelarsi foriera di dubbi in ordine all'esatto perimetro di tale divieto d'uso. La risposta più garantistica – nel senso, dunque, di un divieto d'uso a 360 gradi – dovrebbe essere indiscutibile, essendo dimostrata dal fatto che, nel caso di elementi «illegittimamente controllati», il giudice di pace, rigettando la convalida, debba, oltre a dichiarare l'inutilizzabilità, pure disporre la cancellazione di tali elementi.

Ciò detto, va poi segnalato un aspetto ulteriore, concernente il perimetro di utilizzabilità dei dati che siano stati controllati (e documentati) in modo legittimo. Tali elementi sono spendibili solo nell'ambito del procedimento in cui si colloca l'ispezione – e dunque i procedimenti di rimpatrio o di protezione internazionale – oppure anche in seno a un eventuale rito penale (o ai fini dell'applicazione di una misura di prevenzione)? In una logica di garanzia, lo scopo che orienta l'ispezione del *device* (anche nei casi in cui questa avvenga con il consenso dell'interessato) dovrebbe marcare anche i confini di utilizzabilità del risultato probatorio: tale ricostruzione è l'unica in grado di limitare usi distorti ed abusivi di una disciplina che, nata per esigenze totalmente diverse, in via di fatto può prestarsi a diventare una formidabile forma di controllo di polizia a fini preventivi (un rischio, quest'ultimo, che peraltro non sarebbe affatto escluso – ma solo ridimensionato – dall'affermazione di inutilizzabilità se non ai fini della corretta identificazione del migrante).

In proposito, il legislatore meglio avrebbe fatto a mettere nero su bianco la risposta a questa domanda, tutt'altro che peregrina; e non solo con una sanzione espressa di inutilizzabilità (simile, per intenderci, a quella che si può rinvenire nell'art. 226 disp. att. c.p.p. per le intercettazioni preventive); ma, ancor prima, e *in primis* a tutela della corrispondenza e della riservatezza del migrante, con un obbligo di cancellazione dei dati acquisiti a fini identificativi simile a quello vigente in Germania, destinato a scattare non appena i dati utilizzati per stabilire l'identità e la nazionalità dello straniero non siano più necessari per tali scopi.

In mancanza di una previsione espressa di inutilizzabilità (che peraltro non riuscirebbe comunque ad evitare che le conoscenze apprese tramite l'accesso agli *smartphone* possano fungere da spunto per avviare delle indagini, preventive o anche penali[64]), è facile prevedere che la giurisprudenza possa incasellare i dati acquisiti mediante l'accesso al *device* nella nozione di documento *ex* art. 234 c.p.p. Non solo. Una conclusione di segno analogo potrebbe

62. Una simile esegesi, che peraltro non trova conforto nella lettera della legge, sarebbe destinata a scontrarsi con la prassi (di cui più volte si è detto) che vede i telefoni cellulari "requisiti" ai migranti trattenuti nei Centri detentivi.

63. V. *retro*, nota 14.

64. Si pensi, per analogia, proprio all'art. 226 disp. att. c.p.p. testé citato nel testo: disposizione che, pur sancendo l'inutilizzabilità, nel processo penale, degli «elementi acquisiti attraverso le attività preventive», ne accorda comunque il possibile impiego per «fini investigativi» (comma 5): e dunque quale «stimolo per l'esercizio dei poteri di ricerca delle notizie di reato attribuiti al pubblico ministero o alla polizia giudiziaria (art. 330 c.p.p.)» (così F. Caprioli, *Le disposizioni in materia di intercettazioni e perquisizioni*, in Aa. Vv., *Il processo penale tra politiche della sicurezza e nuovi garantismi*, a cura di G. Di Chiara, Giappichelli, Torino, p. 25), o, comunque, per lo sviluppo di indagini penali già in precedenza avviate (similmente a quanto è possibile in relazione ad altri atti, come le dichiarazioni rese dall'indagato sul luogo e nell'immediatezza del fatto *ex* art. 350 commi 5 e 6, che non solo sono inutilizzabili, ma, ancor prima, neppure documentabili).

essere estesa anche al verbale descrittivo delle operazioni svolte sul *device*, ove si pensi che, ammettendo l'acquisizione al processo penale di documentazione di atti che non sono ripetibili, l'ambiguo tenore del terzo comma dell'art. 238 c.p.p. non specifica *expressis verbis* che questi debbano essere stati compiuti nell'ambito di un procedimento penale[65].

10. Una novità dirompente: la sentenza della Corte di giustizia del 4 ottobre 2024

Constatata la dubbia compatibilità della nuova disciplina con l'art. 15 Cost., è ora necessario tornare ad interrogarsi sui suoi rapporti con il diritto comunitario, in particolare alla luce delle sue più recenti evoluzioni giurisprudenziali.

In proposito, si è già dato atto di come, pur replicando il contenuto dell'art. 13 della direttiva 2013/32/UE, il considerando n. 22 del nuovo "regolamento Procedure" (UE/2024/1348, destinato a operare dal 12 giugno 2026) precisi che, tra gli effetti personali del richiedente asilo assoggettabili a ispezione a scopo identificativo, possano rientrare anche dispositivi elettronici quali *laptop*, *tablet* o telefoni cellulari. Al contempo, esso si premura quantomeno di richiamare gli Stati membri al rispetto di determinati presupposti, ossia che la perquisizione del cellulare sia «necessaria e debitamente giustificata», e si svolga «nel rispetto dei diritti fondamentali e del principio di proporzionalità».

Quanto sin qui esposto dimostra tuttavia il mancato rispetto di tali presupposti da parte del legislatore italiano[66], in particolare alla luce di una recente pronuncia della Corte di giustizia dell'Unione europea, non a caso evocata anche dal Garante della *privacy* espressosi sul contenuto dell'art. 12 d.l. n. 145 del 2024.

Tale decisione – del 4 ottobre 2024[67], e dunque di pochi giorni precedente il d.l. n. 145/2024 – ha subito attirato l'attenzione dei processualpenalisti, poiché in grado di scardinare le tecniche investigative finora seguite una volta ottenuto il sequestro del telefono cellulare nell'ambito di un'indagine penale[68].

Chiamata ad esprimersi su un rinvio pregiudiziale promosso dal Tribunale amministrativo regionale del Tirolo (Austria), la Corte di giustizia ha infatti riconosciuto la possibilità di accedere ai dati contenuti in un telefono cellulare – a fini di prevenzione, indagine, accertamento e perseguimento di reati in generale – solo là dove tale attività di

65. In proposito, e su opposte posizioni: R. Orlandi, *Atti e informazioni della autorità amministrativa nel processo penale. Contributo allo studio delle prove extracostituite*, Giuffré, Milano, 1992, p. 142 ss., secondo cui, malgrado le previsioni dell'art. 238 siano dettate per i soli procedimenti giurisdizionali, la disposizione del 3º co. sarebbe comunque suscettibile di essere estesa in via interpretativa anche ai verbali formati da altre pubbliche autorità; *contra*, fra gli altri, C. Cesari, *L'irripetibilità sopravvenuta degli atti d'indagine*, Giuffré, Milano, 1999, p. 433 ss., che esclude la possibilità di riferire il terzo comma dell'art. 238 c.p.p. ad atti irripetibili diversi da quelli provenienti da un procedimento penale.

66. Come già osservato, oltre a non ricorrere mai alla parola «perquisizione» (che nel nostro sistema evoca un istituto, proprio della procedura penale, preposto alla ricerca del corpo del reato e delle cose pertinenti al reato), il legislatore ha preferito l'espressione «accesso immediato» piuttosto che «ispezione» (che campeggia solo nella *rubrica legis* dell'art. 12 d.l. n. 145/2024); impiegando un lessico diverso da quello usato nel considerando 22 del regolamento Procedure, è come se avesse inteso eludere la necessità di rispettare le condizioni ivi indicate.

67. Si tratta di CGUE, 4.10.2024, n. 171, resa nella causa C-548/21. A commento della pronuncia, v. S. De Francesco, *Corte di giustizia e accesso ai dati degli smartphone: nuovi problemi di (in)compatibilità tra diritto interno e diritto dell'Unione europea*, in www.dirittodidifesa.it, 6 novembre 2024.

68. Infatti – e al netto degli importanti effetti scaturiti dalla sentenza costituzionale n. 170 del 2023, che però riguardano la sola corrispondenza telematica presente nei dispositivi elettronici – la giurisprudenza di legittimità è solita etichettare come attività di indagine atipica della polizia giudiziaria (che può essere svolta anche in via autonoma, senza neppure la delega del Pubblico ministero) quella di ispezione dello *smartphone* che consenta l'osservazione e l'estrazione di copia di dati non riconducibili alla nozione di corrispondenza.

acquisizione probatoria ottemperi ad alcune rigorose condizioni. In particolare, la relativa disciplina dovrebbe: definire in modo sufficientemente preciso la natura o le categorie delle infrazioni per cui tale tecnica d'indagine può operare; garantire il rispetto del principio di proporzionalità; subordinare l'esercizio di tale possibilità (salvo in casi di urgenza debitamente giustificati) al controllo preventivo di un giudice o di un organo amministrativo indipendente.

Inoltre, il possessore del *device* va informato dei motivi sui quali si fonda l'autorizzazione ad accedere ai dati, appunto rilasciata da un giudice o da un organo amministrativo indipendente, a partire dal momento in cui la comunicazione di tali informazioni non sia più suscettibile di compromettere i doveri che incombono su tali autorità. Un'affermazione, quest'ultima, resa necessaria per salvaguardare il diritto a presentare un ricorso effettivo.

Naturalmente, le ricadute immediate della pronuncia riguardano l'accesso ai dispositivi elettronici disposto per esigenze di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali di cui alla direttiva (UE) 2016/680 (fonte che la Corte di giustizia ha ritenuto pertinente al caso specifico al posto della direttiva 2002/58/CE, viceversa relativa alla vita privata e alle comunicazioni elettroniche, che era stata evocata dal Tribunale austriaco).

Tuttavia, la circostanza che i giudici di Lussemburgo abbiano fatto leva su disposizioni racchiuse non solo nella direttiva (UE) 2016/680 ma *in primis* nella Carta di Nizza, induce, *mutatis mutandis*, a ritenere tali conclusioni riferibili anche all'ispezione di dispositivi elettronici disposta per esigenze legate alla tutela delle frontiere[69].

Tale constatazione porta a condividere le osservazioni già espresse dal Garante della *privacy*, che aveva messo in guardia il legislatore circa il possibile contrasto tra la disciplina racchiusa nel d.l. n. 145/2024 e il diritto comunitario anche e soprattutto alla luce della pronuncia della Corte di giustizia; osservazioni che si erano concentrate sulla necessità di modificare la disciplina varata in sede di decreto onde renderla più rispettosa del principio di proporzionalità.

Oltre che con quello alla segretezza della corrispondenza (tutelata dall'art. 15 Cost.), l'ispezione dello *smartphone* si presta ad interferire anche con il diritto al rispetto della vita privata (diritto non a caso oggetto di attenzione da parte del legislatore tedesco, che esclude l'accesso al *device* dei migranti in presenza di «indicazioni concrete per supporre che l'analisi dei dati porterebbe all'acquisizione di informazioni tutelate dal diritto alla riservatezza»).

Tuttavia, nel vietare l'accesso alla corrispondenza e a qualunque altra forma di comunicazione (con un precetto peraltro esplicitato nella sola disposizione dedicata all'accesso coattivo e non anche in quella concernente la consegna "spontanea" del *device*), la disciplina introdotta con il "decreto flussi" mostra di preoccuparsi di proteggere la sola segretezza delle comunicazioni (in modo peraltro non conforme all'art. 15 Cost.). A differenza di quelli tedeschi, i riformatori italiani non hanno neppure preso in considerazione l'esigenza di proteggere la riservatezza dei dati racchiusi nel *device* diversi dalla corrispondenza; dati che, stando alla nuova normativa, rischiano dunque di rimanere alla mercé della pubblica autorità, oltretutto senza che sia prevista alcuna forma di impugnazione idonea a fungere da rimedio effettivo.

69. Il che – si badi – vale sia per la situazione oggi vigente sia per l'assetto destinato a divenire operativo il 12 giugno 2026; infatti, per quanto il *considerando* 22 del regolamento Procedure faccia riferimento ai dispositivi elettronici «quali *laptop*, *tablet* o telefoni cellulari», le norme della CDFUE menzionate dalla sentenza del 4 ottobre del 2024 hanno una valenza generalizzata, riferibile anche alla posizione giuridica degli stranieri.

La pronuncia della Corte di giustizia dimostra l'insostenibilità di un simile assetto, in particolare alla luce della nozione di «dato personale» a cui la decisione pretende vada assicurato il livello di protezione sopra descritto. Per la Corte, le condizioni di legittimità per poter accedere ai contenuti del *device* devono trovare applicazione ai dati riguardanti il traffico telefonico (costituiti dalle chiamate in entrata e in uscita), come pure a quelli concernenti l'ubicazione del telefono; altri «dati personali» da tutelarsi (sempre secondo le indicazioni della pronuncia del 4 ottobre) sono poi la cronologia di navigazione in *internet* e anche le fotografie custodite nella memoria del telefonino.

L'esigenza di confrontarsi con la decisione della Corte di giustizia avrà ricadute significative sull'acquisizione dei dati serbati nella memoria dei dispositivi elettronici sottoposti a sequestro probatorio penale[70]. Circoscriverne le ricadute alla sola attività di accertamento penale sarebbe però alquanto riduttivo, appunto perché tale pronuncia si fonda soprattutto su una valorizzazione dell'art. 52 CDFUE.

Inoltre, un simile approccio determinerebbe un esito paradossale (ancorché tutt'altro che sconosciuto in questa branca dell'ordinamento): mentre i dati personali contenuti degli *smarthpone* in uso ai MSNA e agli stranieri trattenuti sarebbero acquisibili in forza della disciplina (così scarna di tutele) qui oggetto di esame, un eventuale procedimento volto ad accertare la commissione di un reato proprio di uno straniero irregolare potrebbe non consentire affatto ispezioni o perquisizioni telematiche, se non nel rispetto delle condizioni pretese dai giudici di Lussemburgo (che oltretutto, come noto, hanno negato la natura di autorità amministrativa indipendente al Pubblico ministero, sia pure rispetto a ordinamenti diversi da quello italiano). La divaricazione dei livelli di garanzia sarebbe eclatante, e difficilmente giustificabile sul piano della ragionevolezza.

11. Conclusione

Sulla scorta delle riflessioni svolte in questo scritto, la disciplina appena varata mette in fila una cospicua serie di difetti.

La frequente tendenza ad un uso promiscuo del medesimo telefono da parte di più persone durante il viaggio migratorio, unita alla presa d'atto dei risultati raggiunti nei Paesi in cui tale pratica opera già da anni, inducono a sollevare più di un dubbio circa l'adeguatezza dell'accesso al *device* a soddisfare lo scopo per il quale tale pratica è stata concepita. Tanto

70. Come già rilevato, finora la giurisprudenza penale aveva ricondotto le operazioni di osservazione dei dati racchiusi in un *device* alle attività ed operazioni di cui all'art. 348 c.p.p. V. ad esempio Cass. pen., sez. VI, 27.3.2018, in *C.E.D. Cass.*, n. 273273, secondo cui «l'acquisizione da parte della polizia giudiziaria del numero di utenza telefonica mobile attraverso l'esame, all'insaputa dell'indagato, dell'apparecchio cellulare a lui in uso rientra tra gli atti urgenti e "innominati" demandati agli organi di polizia giudiziaria, ai sensi degli artt. 55 e 348 c.p.p., e, come tale, non è soggetta ad una preventiva autorizzazione dell'autorità giudiziaria e neppure alla necessaria documentazione prevista dall'art. 357 c.p.p., che non fa riferimento alle attività ed operazioni di cui all'art. 348 c.p.p.» (in motivazione la Corte ha aggiunto che detta attività non è qualificabile come perquisizione, non essendo finalizzata alla ricerca del corpo del reato o di cose pertinenti al reato, né come ispezione di cose, atteso che l'utenza non è qualificabile come traccia o altro effetto materiale del reato, né è assimilabile alla acquisizione dei dati del traffico telefonico). V. anche sez. 1, 13.3.2013, *ivi*, n. 255973 («la rilevazione del numero di una utenza contattata, conservato nella memoria di un apparecchio di telefonia mobile, è una operazione non assimilabile all'acquisizione dei dati di traffico conservati presso il gestore dei servizi telefonici e non necessita, quindi, del decreto di autorizzazione dell'autorità giudiziaria, potendo conseguire ad una mera attività di ispezione del telefono da parte della polizia giudiziaria»), nonché sez. 3, 21.10.2020, *ivi*, n. 280022. In prospettiva *de iure condendo*, v. il d.d.l. n. 806/2023 (cui già s'è fatto cenno *retro*, nota 58).

da far ritenere che essa non sia in grado di superare neppure il primo criterio del test di proporzionalità.

Volendo ritenere non dirimente questa prima obiezione – la quale, per essere superata, postula quantomeno che la valutazione dei risultati dell'ispezione non venga fideisticamente delegata ad un algoritmo, prestandosi ad essere contrastata anche garantendo allo straniero la possibilità di confutarne i risultati dimostrativi –, la disciplina appena allestita dal legislatore italiano andrebbe comunque riscritta, garantendo un controllo preventivo di natura giurisdizionale, consono a salvaguardare non solo l'art. 15 Cost., ma anche la riservatezza dei dati personali, tutelata dall'art. 8 CEDU e 7 CDFUE.

In particolare, la circostanza che l'art. 15 Cost. non ammetta che la decisione di violare la segretezza della corrispondenza possa essere assunta (neppure in via provvisoria) da autorità diverse da quella giudiziaria dimostra la necessità di rivedere la disciplina di nuovo conio: o espungendo il riferimento ai «documenti, anche video o fotografici», oppure prescrivendo un intervento *ex ante* (e non meramente *ex post*) da parte dell'autorità giudiziaria.

La seconda soluzione – e dunque quella di anticipare l'intervento del giudice rispetto allo schema procedimentale viceversa privilegiato dalla novella (basato su una convalida *ex post*) – sarebbe l'unica in grado di ottemperare anche alle indicazioni racchiuse nella sentenza resa il 4 ottobre dalla Corte di giustizia.

Il richiamo al criterio di proporzionalità operato dalla recente pronuncia lussemburghese induce inoltre a sollecitare una rivisitazione dei presupposti per permettere l'accesso al dispositivo elettronico, onde circoscriverlo ai soli casi in cui realmente costituisca l'*extrema ratio* e imponendo la doverosa cancellazione dei dati una volta che non siano più indispensabili allo scopo (sul modello della soluzione tedesca). E ciò non solo nei casi di accesso forzato, ma anche in quelli di accesso "acconsentito": in relazione al quale, parimenti, andrebbe salvaguardato il principio di trasparenza, attraverso una più chiara comunicazione del tipo di trattamento cui il dispositivo verrà sottoposto e assicurando la necessaria assistenza difensiva.

La disciplina di nuovo conio non ha poi le carte in regola neppure da un altro punto di vista, dato che non prevede alcun ricorso dotato di una qualche effettività.

Infine, andrebbe espunta la possibilità di accesso al dispositivo elettronico in uso al MSNA, del tutto sguarnita di addentellati nella normativa europea e scarsamente compatibile con la legislazione dedicata agli stranieri minori.