Il Regolamento (UE) 2016/679 alla prova dei flussi migratori diretti verso l'Europa mediterranea. La tutela dei dati personali di rifugiati e migranti

Mirko Forti

Sommario: 1. Introduzione – 2. L'evoluzione del diritto alla privacy e il suo riconoscimento internazionale – 3. La tutela dell'identità personale dei migranti all'epoca del GDPR – 4. La tutela dei dati personali e la lotta al traffico illegale di esseri umani – 5. Conclusioni

1. Introduzione

Da diversi anni flussi migratori sempre crescenti, provenienti principalmente dall'Africa e dal Medio Oriente, si stanno dirigendo verso il continente europeo. Nel solo 2018 ben 17.258 persone, di cui 14.769 via mare, sono entrate nei confini dell'Unione europea. Nel 2017[1] furono invece in 186.768 ad arrivare nel territorio europeo, ma 3.116 perirono durante il pericoloso viaggio intrapreso dai loro Stati di origine, alla ricerca di una vita migliore. Le cause di un simile fenomeno migratorio sono molteplici; limitandosi a un breve accenno introduttivo e non esaustivo, possono essere menzionati elementi quali l'intensa crescita demografica e l'aumentata urbanizzazione avvenuta nelle regioni di provenienza, nonché l'instabilità politica ed economica di dette zone[2].

[1] Dati aggiornati al 1 aprile 2018, fonte *http://migration.iom.int/europe/* (consultato il 3 aprile 2018).

[2] M. Stoicovici, *Who are the migrants of today*, in *International Journal of Juridical Science*, 2010.

Un simile afflusso di persone pone numerose sfide che l'Unione europea non può esimersi dall'affrontare, e tra queste non deve essere trascurata la salvaguardia della privacy dei migranti. La raccolta e il trattamento dei dati personali di questi ultimi sono passi necessari per un controllo efficace dei movimenti migratori, per una loro facilitazione e per comprendere appieno le ragioni che hanno spinto così tante persone a intraprendere simili viaggi, nonché per rispettare la loro dignità umana. Le autorità nazionali e le agenzie europee, così come le Organizzazioni internazionali coinvolte nell'accoglienza dei migranti arrivati nel territorio europeo, devono infatti raccogliere dati sensibili di diversa natura: ad esempio, informazioni biografiche come il nome e la data di nascita, dati genetici e biometrici come le impronte digitali e campioni di DNA, documenti personali come la storia clinica[3].

La recente approvazione del Regolamento (UE) 2016/679[4] (di seguito, anche, il "Regolamento GDPR" o il "Regolamento") apre una nuova fase della normativa dell'Unione in materia di protezione dei dati personali, con importanti conseguenze anche nella gestione dei dati sensibili relativi ai migranti.

Il presente articolo si propone perciò di analizzare i profili di novità introdotti dal Regolamento, al fine di valutare la sua possibile incidenza sulla gestione della crisi migratoria. Dopo una breve introduzione sull'evoluzione del diritto alla privacy alla luce del costante progresso tecnologico, saranno infatti esaminati alcuni aspetti particolarmente rilevanti del GDPR nell'ambito della tutela dell'identità personale dei migranti. Il diritto alla riservatezza viene inoltre in rilievo nella lotta all'immigrazione illegale; sarà quindi valutato come l'utilizzo, a questo fine, di strumenti quali i droni o la geo-localizzazione possano porre a rischio la privacy dei soggetti coinvolti.

[3] R. Martens, *IOM data protection manual*, Ginevra, 2010, 14 e ss.

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GUUE n.119 del 4 maggio 2016, 1-88.

2. L'evoluzione del diritto alla privacy e il suo riconoscimento internazionale

Il continuo sviluppo delle nuove tecnologie di comunicazione ha fatto sì che ogni individuo sia costantemente connesso alla rete internet, condividendo le informazioni che lo riguardano con i restanti membri della comunità sociale. Il progresso tecnologico si è rivelato essere, come prevedibile, assai più rapido e incisivo della consapevolezza sociale e giuridica che avrebbe dovuto accompagnarlo di pari passo; le soluzioni normative previste per singoli casi specifici si stanno dimostrando inadeguate a rappresentare il continuo mutamento della società attuale, rendendo quindi necessaria l'individuazione di principi e valori riferibili al lungo periodo[5], che possono rimanere validi a prescindere dall'avanzamento delle nuove tecnologie. Questa continua connessione dei singoli a internet comporta la riduzione dei rispettivi spazi privati, provocando la moltiplicazione degli appelli alla privacy e la consapevolezza della necessaria evoluzione di questo concetto, al fine di adattarlo alle nuove e mutate esigenze della società attuale[6]. La privacy non è infatti più intesa solamente come *ius excludendi alios*, ossia come diritto individuale di escludere qualsiasi ingerenza esterna dalla propria sfera privata[7], ma anche come possibilità di ciascuno di controllare l'uso e la disponibilità dei propri dati personali[8]. Al centro della nuova concezione di privacy viene quindi posto l'individuo e il suo diritto ad avere l'ultima parola sulla raccolta e sul trattamento delle informazioni che lo riguardano, alla luce di una più ampia nozione di "protezione dei dati personali" che va a sostituire e integrare la sola tutela della riservatezza individuale, delineandosi inoltre come criterio di legalità dell'azione pubblica.

Si afferma perciò una sorta di diritto all'autodeterminazione informativa di ogni singolo individuo, da inserire in un più ampio

[5] S. Rodotà, *Tecnologie e diritti*, Bologna, Il Mulino, 1995, 19 e ss.

[6] S. Rodotà, cit.

[7] S.D. Warren-L.D. Brandeis, *The right to privacy*, in *Harvard Law Review*, 1890, 4, 193.

[8] A.F. Westin, *Privacy and freedom*, New York, Atheneum, 1970; A.R. Miller, *The assault on privacy*, University of Michigan Press, Ann Arbor, 1971; L. Lusky, *Invasion of privacy: a clarification of concepts*, in *Columbia Law Review*, 1972, 72, 693-710.

novero di prerogative che contribuiscono a salvaguardarne il diritto alla personalità[9], quali il diritto di «cercare, ricevere e diffondere informazioni e idee»[10] e il principio della riservatezza informatica. Il valore della privacy non viene più collegato al diritto di proprietà[11], bensì alla tutela della propria identità personale: controllare la, e influire sulla, circolazione delle proprie informazioni contribuisce a definire il ruolo dell'individuo nella società[12].

La disciplina giuridica attuale in materia di trattamento dei dati personali trova una sua prima espressione in due atti internazionali quali la Convenzione 108 del Consiglio d'Europa[13] e la Raccomandazione 131 dell'OCSE[14]; dall'analisi di questi documenti è possibile enucleare una serie di principi che caratterizzano ancora oggi la normativa attualmente in vigore. Alla stregua di tali principi, la raccolta dei dati personali deve essere condotta all'insegna della correttezza e dell'esattezza delle informazioni collezionate, a cui è collegato l'obbligo del loro aggiornamento periodico. Il soggetto interessato dal trattamento dei dati ha il diritto di essere informato sulle finalità alla base del suddetto trattamento prima che questo abbia luogo. Viene riconosciuto anche il principio della pubblicità delle banche dati che trattano informazioni personali, di cui deve esistere un registro accessibile[15], nonché il principio dell'accesso individuale che rende possibile a chiunque conoscere quali e quanti dati sul proprio conto sono stati raccolti. Ai fini della presente analisi, risulta particolarmente significativa proprio la Convenzione 108, il cui scopo principale è, ai sensi dell'articolo 1, garantire a ogni persona, indipendentemente da elementi quali la cit-

[9] D. Messinetti, voce *Personalità (diritti della)*, in *Enciclopedia del diritto*, vol. XXXIII, 355 e ss.

[10] Art. 19 della Dichiarazione Universale dei Diritti dell'Uomo, 1948.

[11] Y. Poullet, *Le fondement de la protection des donnés nominatives:"propriétes ou libertés"*, in *Nouvelles technologies et propriété*, LITEC, Montréal, 1991, 175; J. Rubenfeld, *The right of privacy*, in *Harvard Law review*, 1988-89, 102, 737

[12] S. Rodotà, cit.

[13] Convenzione del Consiglio di Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

[14] Raccomandazione del Consiglio OCSE relativa alle linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza, adottata dal Consiglio nel corso della sua 1037ma riunione, il 25 luglio 2002, C (2002)131/FINAL.

[15] S. Rodotà, cit.

tadinanza, sul territorio di ciascun Paese contraente, il rispetto della propria vita privata in relazione all'elaborazione automatica dei dati personali che la riguardano. Appare evidente, dal tenore di tale articolo, che l'attenzione degli Stati contraenti viene posta principalmente sulla protezione dei dati personali, come corollario e logica evoluzione del diritto alla privacy precedentemente inteso solo come diritto alla riservatezza. Ratificando la Convenzione 108, la stessa Unione europea ha mostrato di condividerne i valori, che informano quindi la produzione normativa UE in tale ambito.

Il diritto al rispetto della vita privata è inoltre riconosciuto dall'art. 8 della Convenzione europea sui diritti dell'uomo, che inoltre vieta interferenze in tale ambito da parte dei pubblici poteri, ad eccezione di quelle previste dalla legge e per salvaguardare l'ordine pubblico. L'art. 7 della Carta dei diritti fondamentali dell'Unione europea, come noto dotata del medesimo valore giuridico dei Trattati istitutivi in virtù dell'art. 6 TUE, garantisce a ogni individuo il valore irrinunciabile del rispetto della vita privata. L'art. 8 della Carta compie un passo ulteriore, garantendo il diritto alla protezione dei dati personali e stabilendo che il loro trattamento deve avvenire secondo il principio di lealtà e per finalità prestabilite dalla legge. I valori appena ricordati sono alla base del sopra citato Regolamento di recente approvazione e devono guidare l'azione dell'Unione europea anche nella gestione della crisi migratoria.

3. La tutela dell'identità personale dei migranti all'epoca del GDPR

3.1. Dalla Direttiva 95/46 al Regolamento (UE) 2016/679

Il valore della privacy e il diritto alla riservatezza sono ormai da tempo parte fondamentale dell'*acquis communautaire*; già nel 1995, infatti, l'Unione europea aveva adottato una direttiva in materia di protezione dei dati personali[16] per far sì che i vari Paesi membri aggiornassero la propria legislazione in tale ambito.

[16] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GUUE n.281 del 23 novembre 1995, 31-50.

La direttiva 95/46 rappresentava il testo di riferimento, a livello europeo, in materia di tutela della privacy e della riservatezza. Si riconosceva inoltre il valore della vita privata, sulla scia di quanto proclamato da atti internazionali quali la Convenzione 108: l'art. 1 della direttiva impegnava infatti gli Stati membri a riconoscere tale principio, con particolare attenzione alla tutela dei dati personali. Venivano fissati confini definiti alla raccolta di suddette informazioni, fissando inoltre per i Paesi membri l'obbligo di creare un'Autorità indipendente e garante della correttezza di tale raccolta. L'art. 29 della suddetta direttiva stabiliva la formazione di un gruppo di esperti a livello europeo, il cosiddetto art. 29 *Working Party*, formato da un rappresentante per Stato membro delle varie Autorità garanti e da un membro della Commissione, con un ruolo consultivo nei confronti delle istituzioni europee nella formulazione di proposte legislative in materia di trattamento dei dati personali.

Il continuo progresso tecnologico ha tuttavia messo a dura prova la menzionata direttiva in quanto l'esigenza di protezione non è rimasta costante nel corso degli anni e il livello di tutela accordato dalla normativa comunitaria si è rivelato inidoneo a salvaguardare le informazioni sensibili dai rischi posti dai nuovi mezzi di comunicazione[17]. Un ulteriore problema era costituito dalla diversità delle legislazioni nazionali in materia, considerato che una direttiva si limita a fissare un obbiettivo comune, lasciando ai vari Stati membri l'implementazione delle varie misure atte a raggiungerlo; alla luce di ciò, si comprende la decisione dell'Unione europea di emanare un regolamento, dato che – come noto – tale atto è obbligatorio nella sua interezza e immediatamente applicabile[18]. L'attuazione del regolamento non richiede quindi, in linea di principio, alcuna azione da parte dei vari Paesi UE.

Una simile caratteristica può rivelarsi assai utile nel trattamento dei dati personali dei migranti arrivati in territorio europeo, garan-

[17] B.A. Safari, *Intangible privacy rights: how Europe's GDPR will set a new global standard for personal data protection*, in *Seton Hall Law Review*, 2017, 47, 809-848.

[18] J.Wagner-A. Benecke, *National legislation within the framework of GDPR. Limits and opportunities of member State data protection law*, in *European data protection Law Review*, n.3/2016, 353-361.

tendo un'uniformità di applicazione che non subisce difformità secondo il Paese di sbarco.

3.2. Il criterio di applicazione territoriale del nuovo Regolamento

La sopra citata direttiva 95/46 stabilisce, all'art. 4 comma 1, il proprio campo di applicazione; rientrano in tale ambito le attività di trattamento dati svolte/espletate all'interno del territorio di uno Stato membro dell'Unione europea, o dello Spazio Economico Europeo (SEE). Tale previsione ha però limitato fortemente la tutela fornita dalla normativa europea rivelatasi, come detto, inadeguata a rispondere alle nuove esigenze di una connessione informatica globale. Le attività di aziende informatiche con sede negli Stati Uniti, si pensi a Google o Facebook a mero titolo di esempio, avrebbero potuto quindi evitare l'applicazione della normativa in questione. L'unico criterio determinante, secondo quanto previsto dal summenzionato art.4, è infatti il luogo fisico in cui vengono trattati i dati, non rilevando in alcun modo parametri alternativi quali la cittadinanza del soggetto interessato dal trattamento o la sua residenza abituale. Risulta evidente che una simile disposizione può condurre a una mancata tutela uniforme dei dati dei cittadini, europei e non, e che può essere facilmente aggirata. La direttiva non trovava inoltre applicazione relativamente alla cooperazione in materia penale e al trattamento di dati effettuato per finalità esclusivamente personale tra privati, come previsto dall'art. 3 punto 2.

La Commissione, attraverso una Comunicazione[19] del novembre 2010, evidenziava queste criticità, riconoscendo la necessità di una revisione normativa volta a determinare con certezza le competenze dei vari Paesi membri nell'ambito della protezione dei dati personali. Il nuovo Regolamento, prendendo spunto da quanto affermato nella recente giurisprudenza della Corte di giustizia[20], vuole invece tutelare

[19] Comunicazione, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM (2010) 609, 4 novembre 2010.

[20] Una su tutte, Corte di giustizia, sentenza del 13 maggio 2014, *Google Spain Sl*, causa C-131/12, ECLI:EU:C:2014:317. Nella suddetta sentenza la Corte ha specificato la nozione di "stabilimento" presente nella direttiva 95/46, chiarendo che, qualora i dati personali vengano trattati da una succursale o agenzia situata all'interno del territorio europeo, tale trattamento sarà sottoposto alla direttiva. La pronuncia in questione ha quindi spinto a una riforma della normativa, facendo sì che non venga applicata in base al luogo di trattazione dei dati personali, ma secondo

qualsiasi soggetto, indipendentemente dalla sua cittadinanza o residenza abituale, anche qualora la gestione delle informazioni venga portata avanti fuori dal territorio europeo. L'art. 3 del GDPR stabilisce l'applicabilità del nuovo Regolamento indipendentemente dal fatto che il trattamento dei dati personali sia condotto all'interno dell'Unione europea. Il trattamento di suddetti dati sarà soggetto alle disposizioni del GDPR qualora abbia ad oggetto l'offerta di beni o servizi a soggetti che si trovano nell'Unione, o il monitoraggio del loro comportamento se questo si esplica nei confini europei. Il considerando 22 del Regolamento spiega che qualsiasi trattamento effettuato da una succursale o filiale stabilita nel territorio UE, anche se la gestione delle informazioni viene poi concretamente effettuata al di fuori dei confini europei, deve essere sottoposto alle disposizioni del GDPR; è qui evidente l'influenza della pronuncia *Google Spain*.

Alla luce di quanto detto, si comprende che il Regolamento trova applicazione anche nei confronti dei migranti arrivati in territorio europeo, che potranno quindi godere delle tutele previste dal GDPR indipendentemente dalla loro nazione di provenienza e dal luogo del trattamento dei loro dati.

3.3. Il principio della portabilità dei dati nel nuovo GDPR. Riflessi applicativi nella gestione della crisi migratoria

Il nuovo Regolamento prevede, all'art.20, il cd. diritto alla portabilità dei dati, che consente al soggetto interessato di richiedere le proprie informazioni personali fornite al responsabile del trattamento dati in un formato strutturato, di uso comune e leggibile attraverso mezzi automatici, senza che il predetto responsabile possa ostacolare o rifiutarsi di soddisfare tale richiesta. L'articolo in questione riconosce la possibilità di valutare quali sono le informazioni condivise e di riappropriarsene. Una simile facoltà dovrebbe permettere una più agevole circolazione dei dati personali, a favore dei consumatori che potranno rientrare in possesso delle informazioni cedute a un gestore di servizi per l'ottenimento di una prestazione al fine di rivolgersi a un altro operatore del settore[21].

la posizione dei soggetti titolari delle informazioni gestite, ossia se si trovano all'interno dei confini europei.

[21] L. Valle-L. Greco, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di*

Il Regolamento sembra prevedere una sorta di "interoperabilità"[22] della lettura di tali dati da parte di qualsiasi gestore di servizi e porre dei requisiti minimi a cui i gestori del trattamento delle informazioni devono adeguarsi al fine di raggiungere l'obbiettivo della portabilità dei dati[23]. Lo stesso regolamento, tuttavia, al considerando 68 dispone altresì – apparentemente contraddicendosi – che il diritto del soggetto a trasmettere e ricevere i propri dati personali *non* crea un'obbligazione per il responsabile del trattamento ad adottare specifici sistemi tecnici e informatici.

L'applicazione di quanto previsto dall'art. 20 del Regolamento è soggetta inoltre a determinati requisiti legali, poiché può essere richiesta esclusivamente per i dati personali per cui il soggetto ha acconsentito al trattamento. Il diritto alla portabilità non viene esteso ai dati che il gestore del trattamento ha collezionato da altre fonti e che non provengono quindi dal diretto interessato. Si potrebbe perciò riscontrare una qualche contraddittorietà rispetto a quanto affermato dall'art. 15 (3) dello stesso Regolamento, che prevede il diritto per il soggetto interessato di richiedere una copia delle proprie informazioni trattate, senza però poterne domandare anche la portabilità. Al fine di ovviare a questa possibile discrasia, è stata proposta un'interpretazione del dettato normativo più ampia ed estensiva, includendo quindi anche dati generati da un fornitore di servizi attraverso processi quali l'utilizzo di algoritmi[24]. Un'ulteriore eccezione all'applicazione del diritto alla portabilità si ha quando il trattamento dei dati personali è necessario al perseguimento di finalità di pubblico interesse o quando è portato avanti da un'autorità pubblica nell'esercizio delle sue funzioni.

Quest'ultima previsione potrebbe rivestire una notevole importanza nella gestione delle informazioni sensibili dei migranti, specialmente se l'accoglienza di tali persone venisse qualificata, come

principi di diritto privato di formazione internazionale, in *Diritto dell'Informazione e dell'Informatica*, fasc. 2, 1 aprile 2017, 168 e ss.

[22] L. Scudiero, *Bringing your data everywhere: a legal reading of the right to portability*, in *European data protection Law Review*, 1/2017, 119-127.

[23] Article 29 Data Protection Working Party (A29 WP), *Guidelines on the right to data portability* (13 dicembre 2016) 16/EN WP 242, 4 http://ec.europa.eu/information-society/ newsroom/image/document/2016-51/wp242_en_40852.pdf

[24] Article 29 Data Protection Working Party (A29 WP), cit.

prevedibile, attività di pubblico interesse o esercizio di pubbliche funzioni. Una simile determinazione farebbe sì che il diritto alla portabilità dei dati non debba essere applicato alle informazioni raccolte durante l'accoglienza dei migranti, causando però un possibile detrimento al diritto all'identità personale dei migranti stessi, che vedrebbero la loro facoltà di conoscere i propri dati raccolti limitata a quanto previsto dall'art. 15 (3) del Regolamento, che garantisce il diritto a richiedere una copia di dette informazioni, escludendone però la portabilità.

L'interoperabilità dei sistemi di collezione dei dati personali potrebbe però essere utile per uniformare le procedure di accoglienza tra i vari Paesi dell'Unione, permettendo inoltre una veloce circolazione di tali dati all'interno del territorio europeo, seguendo i movimenti dei migranti tra i vari Paesi.

3.4. Il trasferimento dei dati all'estero sotto la normativa del GDPR

La diffusione globale della rete internet ha reso ormai possibile il trasferimento di dati e informazioni tra i vari Paesi, senza che confini territoriali e diverse disposizioni normative nazionali possano essere di ostacolo. La diffusione e la commercializzazione di dati sono ormai elementi fondamentali dell'economia odierna.

Secondo la disciplina prevista dall'art. 25 della direttiva 95/46, trasferimenti transfrontalieri di informazioni sensibili possono essere autorizzati solo verso Paesi terzi che, su giudizio della Commissione europea, presentano un livello di tutela della riservatezza adeguato rispetto agli standard europei. La normativa prevede delle deroghe, elencate tassativamente, al giudizio preventivo della Commissione, che può essere ovviato qualora il trasferimento dei dati è necessario per finalità quali la chiusura di un contratto, la salvaguardia di un interesse pubblico o di un interesse fondamentale della persona.

Il nuovo GDPR dedica diversi articoli, dal 44 al 50, alla regolazione dei trasferimenti dei dati personali oltre i confini nazionali; il testo del regolamento riconosce il diritto all'identità personale e alla salvaguardia della riservatezza delle informazioni sensibili trattate oltre frontiera, riprendendo e specificando inoltre, all'art. 45, il concetto di "adeguatezza" che caratterizzava il giudizio della Commissione ai sensi della previgente disciplina. Lo standard di protezione richiesto al Paese terzo non deve essere identico a quello previsto dalla normativa europea, ma deve essere a questo equivalente, ap-

plicandolo inoltre alla luce di quanto previsto dalla Carta dei diritti fondamentali dell'Unione europea[25]. Il Regolamento specifica che la Commissione, nel suo giudizio di adeguatezza, è tenuta a verificare ulteriori criteri politici e sociali che dovrebbero evidenziare l'attenzione del Paese terzo alla corretta tutela dell'identità personale dei soggetti coinvolti, oltre quelli prettamente tecnico-giuridici. Il GDPR prevede inoltre un riesame su base quadriennale delle conclusioni formulate dalla Commissione nel suo giudizio, al fine di valutare eventuali evoluzioni da parte del Paese esaminato. L'art.49 elenca le deroghe, riprese perlopiù dalla previgente direttiva, che permettono il trasferimento transfrontaliero dei dati anche in mancanza dei requisiti summenzionati; un'importante aggiunta che viene fatta è relativa al perseguimento dell'interesse del titolare del trattamento, qualora questo abbia valutato tutte le circostanze del caso e abbia fornito adeguate garanzie di tutela dell'identità personale del soggetto interessato.

Simili trasferimenti di dati tra diversi Stati sono altrettanto importanti per la corretta gestione dei flussi migratori; le varie autorità nazionali hanno difatti la necessità di sapere le caratteristiche di detti flussi, considerando che spesso i migranti non si stabiliscono nel primo Paese di sbarco. Una condivisione di tali informazioni si rivela fondamentale anche per combattere fenomeni illegali come il traffico di esseri umani. L'art. 44 del GDPR permette il trasferimento dati anche con Organizzazioni internazionali, alcune delle quali impegnate nella gestione della crisi migratoria, creando quindi la possibilità di una collaborazione con gli Stati di origine dei migranti.

4. La tutela dei dati personali e la lotta al traffico illegale di esseri umani

Il tema della salvaguardia dell'identità personale è di primaria importanza nell'ambito della lotta al traffico illegale di esseri umani, con particolare attenzione a quanto concerne le informazioni sensibili delle vittime di tali odiosi traffici, come prescritto anche

[25] C. Kuner, *Reality and illusion in EU data transfer Regulation post Schrems*, in *German Law Journal*, 2017, 18, 881-914.

dall'art. 6 del "Palermo Protocol"[26].

La direttiva 2011/36[27] non prevede alcuna disposizione specifica in materia di tutela dei dati personali, limitandosi a segnalare che la normativa rispetta quanto previsto dalla Carta dei diritti fondamentali dell'UE e che le vittime hanno specifici diritti nei procedimenti penali riguardanti i traffici di cui sono stati oggetto. La legislazione attuale pone infatti l'attenzione principalmente sul rapporto tra rispetto dell'identità personale e lotta all'immigrazione illegale limitatamente al profilo processual-penalistico, ossia agli interessi delle vittime all'interno del processo[28]. Un'analisi delle conseguenze che strumenti di sorveglianza e prevenzione dei suddetti traffici possono avere sulla privacy dei soggetti coinvolti deve però prendere in considerazione non solo la fase processuale, ma anche la fase di raccolta e catalogazione dei dati personali che avviene durante le operazioni di sorveglianza, cercando di trovare un equilibrio tra il rispetto della riservatezza delle vittime e la lotta al traffico di esseri umani.

La geo-localizzazione può essere uno degli strumenti sopra menzionati; il tracciamento della posizione attraverso strumenti elettronici è ormai una realtà diffusa, e viene utilizzato anche per rilevare la posizione dei sospetti trafficanti nell'ambito delle indagini penali. Gli stessi trafficanti possono però utilizzare pratiche di sorveglianza simili, con lo scopo di controllare le proprie vittime e far sì che non riescano a sfuggire dalla propria rete di abusi. Nonostante i rischi che la geo-localizzazione può arrecare alla privacy delle persone coinvolte, essa può costituire un ottimo aiuto alla lotta contro i trafficanti. Al fine di ridurre i predetti rischi, possono essere previsti degli accorgimenti come una limitazione dell'utilizzo degli strumenti di tracciamento della posizione solo a casi eccezionali, di fronte al concreto

[26] Protocollo per la prevenzione, soppressione e repressione del traffico di persone, adottato dall'Assemblea Generale dell'ONU con la Risoluzione 55/25 del 15 novembre 2000.

[27] Direttiva 2011/36/UE del Parlamento europeo e del Consiglio, del 5 aprile 2011, concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime, e che sostituisce la decisione quadro del Consiglio 2002/629/GAI, in GUUE, n.101, 15 aprile 2011, 180-190.

[28] F. Gerry-J. Muraszkiewicz-N. Vavoula, *The role of technology against human trafficking: reflections on privacy and data protection concerns*, in *Computer law e security review*, 2016, 32, 205-217.

sospetto di attività illegale. Il soggetto coinvolto può inoltre ritirare il proprio consenso alla condivisione dei dati relativi alla propria posizione in qualsiasi momento, anche durante il corso di un'indagine.

Le autorità nazionali utilizzano anche droni, ossia veicoli guidati a distanza che non necessitano di un pilota a bordo, nelle attività di pattugliamento dei confini e di prevenzione delle attività illegali come il traffico di esseri umani e l'immigrazione illegale. Lo spiegamento di droni da parte dei Paesi europei è ancora limitato[29], seppur si segnala il loro utilizzo da parte dell'Italia nell'ambito dell'operazione "Mare Nostrum"[30].

L'utilizzo di simili apparecchiature comporta però rilevanti rischi per l'integrità dell'identità personale, considerando che i droni sono spesso attrezzati con una telecamera per le riprese, che consente di raccogliere immagini idonee a identificare una persona. Alla luce di ciò, le azioni che vedono coinvolti tali strumenti devono essere compiute nel rispetto della normativa sulla privacy, ossia il GDPR per il territorio europeo. La sorveglianza operata dai droni si caratterizza per l'alta pervasività; possono essere infatti riprese immagini anche di soggetti non inclusi tra gli obbiettivi di dette operazioni. Deve inoltre esserci chiarezza nelle modalità di utilizzo di tali immagini, affinché non vi siano rischi di violazioni immotivate della privacy dei soggetti coinvolti.

5. Conclusioni

Il continuo progresso tecnologico ha portato a una costante evoluzione del diritto alla privacy, considerato ora come un diritto all'autodeterminazione informativa del singolo soggetto, che può quindi decidere quali dati personali rendere accessibili e secondo

[29] L. Marin-K. Krajcíková, *Deploying drones in policing European borders: constraints and challenges for data protection and human rights*, in A. Završnik (a cura di), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, Londra, Springer, 2016.

[30] Amnesty International, *LivesAdrift: Refugees and Migrants in Peril in the Central Mediterranean' https:// www.amnesty.org/fr/documents/document/?indexNumber =eur05%2F006%2F2014& language=en* accessed 15 October 2015 (consultato il 15 maggio 2018).

quali modalità. Questa evoluzione ha certamente influenzato anche la normativa più recente in materia di privacy, ossia il più volte citato Regolamento (UE) 2016/679, che pone infatti al centro del trattamento dati proprio il soggetto interessato, il quale ha l'ultima parola sulla condivisione delle proprie informazioni sensibili.

Il nuovo Regolamento andrà ad incidere anche sulle pratiche di tutela dell'identità personale dei migranti e rifugiati che arrivano sul territorio europeo, in particolar modo attraverso alcune sue previsioni. Il principio della portabilità dei dati, pur formalmente non applicabile alle attività di gestione della crisi migratoria, potrebbe infatti, considerata la loro finalità di interesse pubblico, spingere le varie autorità nazionali a modificare i propri sistemi informatici all'insegna dell'interoperabilità, velocizzando la condivisione delle informazioni relative ai migranti che si spostano da un Paese all'altro dell'Unione europea. Il Regolamento disciplina inoltre il trasferimento transfrontaliero di suddette informazioni, permettendo quindi una maggiore collaborazione tra gli Stati di origine dei migranti e quelli di destinazione, al fine di garantire un'accoglienza più efficace, nonché di valutare le cause primarie di tali flussi migratori. Una simile condivisione di informazioni è possibile anche con le Organizzazioni internazionali attive in tale ambito. La tutela dell'identità personale è un tema che viene in rilievo anche nella lotta al traffico illegale di esseri umani, dato che strumenti di sorveglianza quali i droni o la geo-localizzazione potrebbero collezionare e catalogare dati personali di soggetti non direttamente coinvolti in tali traffici, nonché delle vittime stesse. Pur a fronte della necessità di continuare ad utilizzare tali strumenti, indubbiamente efficaci e proficui nel prevenire e sopprimere tali odiosi traffici, non possono trascurarsi i profili di rischio per la riservatezza delle persone coinvolte, di cui la legislazione deve quindi tenere conto.