ISSN 2384-9169
Fascicolo n. 3 - 2023
rivista.eurojus.it

L'uso dei dati personali di ubicazione e relativi al traffico per la ricerca di persone scomparse nel sistema dell'Unione europea

DI SERENA CRESPI*

Sommario: 1. L'uso dei dati di ubicazione e relativi al traffico per la ricerca di persone scomparse: inquadramento dell'indagine. – 2. L'accesso mediato ai dati di ubicazione dello scomparso da parte delle autorità di soccorso, di polizia e giurisdizionali: l'applicabilità della direttiva *e-privacy* (e non del GDPR o della direttiva LED). – 3. *Segue*: l'art. 10 della direttiva *e-privacy* e l'accesso mediato ai dati di ubicazione dello scomparso da parte delle autorità di soccorso, di polizia e giurisdizionali. – 4. *Segue*: l'art. 15 della direttiva *e-privacy* e l'accesso mediato ai dati relativi al traffico dello scomparso da parte delle autorità di soccorso, di polizia, giurisdizionali. – 5. L'accesso diretto ai dati di ubicazione e relativi al traffico dello scomparso da parte delle autorità di soccorso, di polizia e giurisdizionali: l'inquadramento della fattispecie giuridica tra direttiva *e-privacy*, LED e GDPR. – 6. Le condizioni di accesso diretto ai dati di ubicazione da parte delle autorità di soccorso. – 7. Le condizioni di accesso diretto ai dati di ubicazione e relativi al traffico da parte delle autorità di polizia e giurisdizionali operanti in materia penale tra l'altro nella ricerca degli scomparsi. – 8. Conclusioni.

1. Nel corso di una trasmissione televisiva che ha come obiettivo quello di aiutare a rintracciare le persone scomparse [1], il fratello di una di queste aveva rivendicato la facoltà di localizzare il telefono del congiunto che da alcuni giorni immotivatamente non dava più notizie di sé. Secondo quest'ultimo, l'acquisizione di tali informazioni in tempi brevi avrebbe permesso di risalire alla posizione dello scomparso – presupponendo la coincidenza di ubicazione tra quest'ultimo e il suo telefono cellulare – o quantomeno avrebbero fornito una traccia degli spostamenti dello stesso, i quali erano conservati nella memoria dell'apparecchio terminale di quest'ultimo, e dunque degli utili tasselli per ricostruire il contesto ove era maturata la

* Professore associato di Diritto dell'Unione europea, Università degli Studi di Milano-Bicocca.
[1] Trasmissione "*Chi l'ha visto*", RAI3, nel corso di due puntante del dicembre 2022.

sparizione. Almeno in base a quanto riferito nel corso della predetta trasmissione, a ciò si sarebbe tuttavia opposta la (genericamente qualificata) legislazione sulla *privacy*, la quale avrebbe impedito alle autorità pubbliche coinvolte nelle ricerche – di soccorso, di polizia e/o giurisdizionali – di avere accesso, anche a seguito della denuncia di allontanamento presentata dai familiari, ai predetti dati in mancanza del consenso dello scomparso o di una consistente ipotesi di reato. E ciò sebbene l'acquisizione tempestiva di questi ultimi fosse essenziale per condurre efficacemente le ricerche soprattutto nell'immediatezza dell'irreperibilità. La *privacy* sarebbe stata, in altri termini, oggetto di una protezione eccessiva e lesiva di diritti, parimenti se non maggiormente importanti, alla vita e alla sicurezza personale e pubblica.

Questo episodio è stata la fonte di ispirazione del presente contributo che, ricostruendo il quadro normativo, invero tutto UE, in materia di tutela dei dati – il regolamento generale GDPR,[2] nonché le direttive LED[3] ed *e-privacy*[4] che ne completano la disciplina – è volto ad accertare la possibilità e, se del caso, le condizioni alle quali le predette autorità pubbliche possono usare i dati personali, conservati tra l'altro nell'apparecchio terminale di uno scomparso, per rintracciare quest'ultimo senza il consenso dello stesso, nonché prescindendo da una, quantomeno solida, prova di reato. Si tratta, in altri termini, di verificare se, ed eventualmente in che misura, questa esigenza possa comprimere il diritto alla *privacy* e alla tutela dei dati personali di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea,[5] nonché derogare alla disciplina positiva dello stesso prevista nei predetti atti di diritto derivato comune. In effetti, come si avrà modo di vedere nel prosieguo, il GDPR e le direttive LED ed *e-privacy*, proprio al fine di tutelare il diritto fondamentale alla riservatezza dei dati, subordinano, almeno in linea di principio, l'accesso ai dati da parte di terzi – e dunque anche

---

[2] Il regolamento 2016/679 (di seguito: GDPR) del Parlamento europeo e del Consiglio del 27 aprile 2016 è volto a tutelare il trattamento dei dati personali delle persone fisiche residenti nell'UE, nonché la circolazione di tali dati sia all'interno dell'unione europea sia in paesi terzi (*GUUE* L 119 del 4 maggio 2016). Per un'analisi delle disposizioni del GDPR, C. KUNER, L.A. BYGRAVE, C. DOCKSEY (eds), *The EU General Data Protection Regulation: A Commentary*, Oxford, 2020. L'aggiornamento del 2021, C. KUNER, L.A. BYGRAVE, C. DOCKSEY, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839645.

[3] Direttiva 2016/680 (di seguito: LED) del Parlamento europeo e del Consiglio del 27 aprile 2016 disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (*GUUE* L 119 del 4 maggio 2016). Per un'analisi della direttiva LED anche congiuntamente al GDPR, R. JAY, *Data Protection Law and Practice*, 5th ed., London, 2020.

[4] La direttiva 2002/58 (di seguito: *e-privacy*) del Parlamento europeo e del Consiglio del 12 luglio 2008, che disciplina il trattamento dei dati personali nel settore delle comunicazioni elettroniche anche al fine di tutela la vita privata degli individui (*GUUE* L 201 del 31 luglio 2002), è stata modificata in ultimo dalla direttiva 2009/136 del 25 novembre 2009 (*GUUE* L 337 del 18 dicembre 2009), nonché rettificata nel 2017 (*GUUE* L 162 del 23 giugno 2017). Sotto la presidenza francese del Consiglio (2021) è stato avviato un procedimento di revisione dell'atto in esame. Sulla proposta di regolamento del Parlamento europeo e del Consiglio del 10 febbraio 2021 sul rispetto della vita privata e sulla protezione dei dati nelle comunicazioni elettroniche in sostituzione della predetta direttiva, https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states, nonché https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states.

[5] Sulla Carta dei diritti fondamentali dell'Unione europea, A. TIZZANO, *L'application de la Charte des droits fondamentaux dans les États membres à la lumière de son article 51, paragraphe 1*, in *Diritto dell'Unione europea*, 2014, p. 429 ss.; R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017; B. NASCIMBENE, *Carta dei diritti fondamentali, applicabilità e rapporti fra giudici: la necessità di una tutela integrata*, in *europeanpapers.eu*, vol. 6, n. 1, 2021, p. 81 ss.

delle autorità pubbliche di soccorso, di polizia o giurisdizionali – al previo consenso dell'interessato, ossia ad un elemento per definizione mancante nel caso di sparizione di un individuo. La prevenzione, la ricerca, l'accertamento e il perseguimento dei reati, anche al fine di salvaguardare la sicurezza pubblica e quella nazionale, sono tra le poche eccezioni che giustificano l'accesso ai dati da parte di autorità pubbliche senza il previo consenso dell'utente.

Al fine di fornire una risposta realmente utile, l'indagine analizzerà in particolare l'accesso ai dati non solo di ubicazione, vero e proprio oggetto del caso di cronaca che ha motivato la presente riflessione, ma anche di quelli relativi al traffico, i quali forniscono informazioni complementari ai primi. Mentre in effetti i dati di ubicazione indicano «la posizione geografica dell'apparecchio terminale dell'utente» (art. 2, let. *c*, della direttiva *e-privacy*) e consentono di ricostruire la latitudine, longitudine, altitudine e direzione di viaggio di quest'ultimo con riguardo tra l'altro alle celle di rete agganciate in un determinato momento (considerando 14 della direttiva *e-privacy*), quelli relativi al traffico sono «i dati sottoposti a trattamento ai fini della trasmissione di una comunicazione» (art. 2, let. *b*, della direttiva *e-privacy*) e permettono di conoscere il «chi, dove, quando e come» di un flusso di informazioni. Nel caso di irreperibilità di un individuo, i primi permettono allora di individuare la posizione geografica, anche *in itinere*, solo del telefono cellulare dello scomparso, quelli relativi al traffico consentendo invece di ricostruire l'insieme dei contatti e delle abitudini di una persona anche in relazione ad altri soggetti e dunque il contesto ove è maturata la scomparsa, il che appare essenziale tra l'altro per indagarne la natura volontaria, suicidaria, accidentale o criminale.

L'analisi differenzierà inoltre a seconda del tipo di autorità pubblica – di soccorso, di polizia ovvero giurisdizionale – che accede ai dati di ubicazione o relativi al traffico di un certo individuo. Gli atti comuni che regolano la protezione dei dati (GDPR, direttive LED ed *e-privacy*) hanno ambiti di applicazione soggettivi differenti, cosicché la possibilità e le condizioni di acquisizione di questi ultimi in caso di sparizione di una persona possono divergere in funzione dell'autorità presa in considerazione e dunque della legislazione UE soggettivamente applicabile, la quale peraltro lascia ampi spazi a normative nazionali di trasposizione e attuazione.

L'acquisizione dei dati di ubicazione o relativi al traffico da parte delle predette autorità pubbliche può poi essere realizzata in forma diretta o mediata.[6] Quantomeno nel caso in esame, essa sarebbe avvenuta secondo quest'ultima modalità, ossia richiedendo e poi ottenendo l'accesso ai dati, peraltro esclusivamente di ubicazione, dai fornitori dei servizi di comunicazione, i quali raccolgono queste informazioni nell'ambito della loro tradizionale attività economica. Sempre al fine di offrire un quadro giuridico completo, la presente indagine analizzerà tuttavia non solo quest'ultima modalità di accesso ai dati, ma altresì quella diretta, peraltro relativamente anche ai dati sul traffico. In quest'ultimo caso, le autorità di soccorso, di polizia ovvero giurisdizionali ottengono entrambi i tipi di dati attraverso propri ed autonomi mezzi di intercettazione e di geo-localizzazione. Come si avrà modo di vedere meglio nel prosieguo, la carenza dell'intermediazione e della collaborazione degli operatori economici determina così la comprensione dell'operazione in esame in un atto UE diverso (direttiva *e-*

[6] Sulla distinzione tra accesso diretto e mediato ai dati personali si permetta il rinvio a S. CRESPI, *L'influenza del diritto dell'Unione europea sulla sicurezza nazionale: l'art. 4, par. 2, TUE alla prova della recente giurisprudenza UE tra l'altro in materia di privacy*, in questa Rivista, fasc. 4, 2022, p. 85 ss., spec. p. 88.

privacy) da quelli che disciplinano invece l'accesso diretto ai dati (GDPR e direttiva LED), le condizioni che regolano l'acquisizione degli stessi variando anche in funzione della modalità – diretta o mediata – ivi prescelta.

2. La facoltà e le condizioni alle quali le autorità pubbliche di soccorso, di polizia ovvero giurisdizionali coinvolte nella ricerca di uno scomparso possono acquisire in via mediata le informazioni relative all'ubicazione o al traffico di quest'ultimo rientrano nell'ambito di applicazione della direttiva *e-privacy*. Quest'ultima disciplina *ogni* trattamento di dati effettuato dai fornitori dei servizi di comunicazione e quindi anche le circostanze, le condizioni e le modalità alle quali i dati raccolti da questi ultimi per motivi commerciali possono essere eccezionalmente divulgati a terzi tra l'altro per ragioni differenti da quelle che ne hanno ispirato l'originaria raccolta – ad esempio, proprio la localizzazione dello scomparso o la ricostruzione delle sue abitudini e dei suoi contatti al fine di rintracciarlo – nonché senza il consenso dell'utente. Come già anticipato, infatti, uno scomparso non può per definizione apporre quest'ultimo. Il fatto poi che la direttiva *e-privacy* regoli la divulgazione a terzi dei dati raccolti dagli operatori economici nel settore delle comunicazioni a prescindere dal soggetto "terzo" che effettivamente ne richieda l'accesso (considerando 39 della direttiva *e-privacy*) permette l'applicazione delle norme di quest'ultima allorché la richiesta di acquisizione dei dati provenga da *ogni* autorità pubblica e dunque anche di quelle di soccorso, di polizia o giurisdizionali.

Anche al fine di garantire la coerenza del sistema legislativo UE in materia di tutela dei dati personali, l'applicabilità della direttiva *e-privacy* relativamente a tali aspetti esclude di conseguenza la regolamentazione degli stessi da parte degli altri atti comuni inerenti la privacy e la protezione del diritto di cui agli artt. 7 e 8 della Carta, ossia il GDPR e/o la direttiva LED. Il GDPR – che norma il trattamento dei dati da parte di ogni persona fisica e giuridica, nonché autorità pubblica (art. 2, par. 1 GDPR) diverse da quelle oggetto della disciplina di dettaglio di cui alle direttive *e-privacy* (fornitori di servizi di comunicazione) e LED (autorità operanti in ambito penale), nonché menzionate all'art. 4, par. 2, TUE (sicurezza nazionale) – e la direttiva LED – che invece disciplina il trattamento dei dati da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati – regolano *a contrario* l'accesso (solo) diretto ai dati da parte rispettivamente dalle autorità di soccorso e di quelle di polizia/giurisdizionali coinvolte nella sparizione di un individuo.

Tali conclusioni trovano peraltro conferma nelle pronunce UE del 2020 *Privacy International, La Quadrature du Net, French Data Network* e *Ordre des barreaux francophones et germanophone*.[7] Con riferimento alla compatibilità con la direttiva *e-privacy*

[7] Così, Corte giust., 6 ottobre 2020, C-511/18, C-512/18, C-520/18, *La Quadrature du Net, French Data Network e Ordre des barreaux francophones et germanophone*, ECLI:EU:C:2020:79; 6 ottobre 2020, C-623/17, *Privacy International*, ECLI:EU:C:2020:790. In dottrina, I. CAMERON, *Metadata retention and national security : Privacy International and La Quadrature du Net : Case C-623/17*, in *Common Market Law Review*, 2021 p. 1433 ss. ; S. J. ESKENS, *The ever-growing complexity of the data retention discussion in the EU : an in-depth review of La Quadrature du Net and others and Privacy International : joined cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and others [2020], case C-623/17 Privacy International,* in *European Data Protection Law Review*, 2022, vol. 8, nº 1, p. 143 ss.; M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net : one step forward two steps back in the data retention saga? : case C-623/17 Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, joined cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v. Premier Minister and Others*, in *European Public Law*, 2022, n° 1, p. 123 ss.

di talune legislazioni nazionali (quelle britannica, francese e belga[8]) che autorizzavano tra l'altro i propri servizi di *intelligence* ad accedere ai dati raccolti dagli operatori nel settore delle comunicazioni al fine di salvaguardare la sicurezza dello Stato, la Corte di giustizia, respingendo le argomentazioni di taluni paesi membri (Regno Unito, Irlanda, Francia Svezia, Cipro, Repubblica ceca, Ungheria, Estonia, Polonia) che ritenevano ivi inapplicabile il diritto UE per effetto dell'art. 4, par. 2, TUE secondo cui «la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro», ha viceversa ritenuto le predette normative comprese nella sfera attuativa del diritto comune e, più in particolare, della direttiva *e-privacy*. Esse imponevano ai predetti operatori di raccogliere, conservare e divulgare ai servizi di *intelligence* i dati degli utenti in deroga alle regole di misura stabilite dalla direttiva *e-privacy* – prevedendo invece quest'ultima il trattamento dei dati solo effettivamente necessari, i quali potevano essere conservati esclusivamente per un tempo congro e non illimitato – cosicché tali legislazioni nazionali eccentriche rispetto alla disciplina comune, proprio in quanto comprese nella sfera attuativa di quest'ultima, erano compatibili con il diritto UE unicamente qualora esse rispettassero le condizioni derogatorie previste all'art. 15 della direttiva *e-privacy*. Al fine di bilanciare il diritto fondamentale alla tutela dei dati personali con l'esigenza di salvaguardare rilevanti interessi securititari collettivi, quest'ultimo autorizza, infatti, gli Stati membri, seppur a determinate condizioni ispirate ai principi UE di necessità e proporzionalità, ad adottare legislazioni interne di deroga a (solo) taluni diritti previsti dalla direttiva *e-privacy* (ossia quelli di cui agli artt. 5, 6, 8 e 9) per salvaguardare gli interessi della sicurezza dello Stato, della difesa, della sicurezza pubblica, nonché la prevenzione, ricerca, accertamento e perseguimento dei reati[9].

Il fatto inoltre che in tali occasioni il giudice di Lussemburgo, pur prendendo in considerazione la disciplina generale del GDPR in quanto richiamata dagli Stati membri intervenuti nelle procedure pregiudiziali *Privacy International, La Quadrature du Net, French Data Network* e *Ordre des barreaux francophones et germanophone*, abbiano invero concentrato la propria analisi giuridica solo sulla direttiva *e-privacy*, limitandosi a brevi cenni con riguardo al primo,[10] conferma l'inapplicabilità del GDPR ai casi di acquisizione mediata dei dati. Quest'ultimo concerne, infatti, solo l'accesso diretto delle autorità pubbliche ai dati personali degli utenti.

---

[8] Quanto alla Francia (C-511/18 e C-512/18), *décrets 2015-1185 del 28 settembre 2015 portant désignation des services spécialisés de renseignement* (*JORF* del 29 settembre 2015) ; 2015-1211 del 1 ottobre 2015 *relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* (*JORF* del 2 ottobre 2015) ; 2015-1639 del 11 dicembre 2015 *relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure* (*JORF* del 12 dicembre 2015) ; 2016-67 del 29 gennaio 2016 *relatif aux techniques de recueil de renseignement* (*JORF* du 31 gennaio 2016) ; nonché l'art. R. 10-13 *Code des postes et des communications électroniques* e il *décret* 2011-219 del 25 febbraio 2011 *relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* (*JORF* del 1 marzo 2011). Con riferimento al Belgio (C-520/18), legge del 29 maggio 2016 *relative à la collecte et à la conservation des données dans le secteur des communications électroniques* (*Moniteur belge* del 18 luglio 2016, p. 44717). Quanto al Regno Unito (C-623/17), *Art. 94 del Telecommunications Act* del 1984 e gli artt. 21, par. 4, 6, 65-69 del *Regulation of Investigatory Powers Act* del 2000.

[9] Sull'applicazione in particolare del principio di proporzionalità nell'ambito dell'art. 15 della direttiva e-privacy, Corte giust. 16 febbraio 2023, C-349/21, *HYA*, punto 43.

[10] Corte giust. *Privacy International* cit., punto 47; *La Quadrature du Net* cit., punto 102.

Tali conclusioni sono state corroborate anche dalle successive sentenze *G.D.* e *SpaceNet* del 2022 con riguardo alla compatibilità con la direttiva *e-privacy* dell'obbligo imposto dalle normative irlandese e tedesca agli operatori di comunicazione di conservare in modo generalizzato i dati degli utenti al fine di metterli nella disponibilità delle autorità questa volta di polizia per ragioni inerenti il contrasto della criminalità.[11] Anche tali legislazioni interne, proprio in quanto derogavano alle regole inerenti la raccolta e la conservazione dei dati previste dalla direttiva *e-privacy*, rientravano parimenti nell'ambito applicativo di quest'ultima. Esse erano allora compatibili con il sistema UE solo allorché rispettassero le condizioni di equilibrio previste dal già menzionato art. 15 della direttiva *e-privacy*. Il fatto poi che in tal caso, e a differenza delle cause *Privacy International, La Quadrature du Net, French Data Network* e *Ordre des barreaux francophones et germanophone*, né i paesi membri intervenuti nella procedura pregiudiziale né la Corte di giustizia in sentenza abbiano richiamato la direttiva LED, che norma tra l'altro proprio il trattamento dei dati da parte delle autorità di polizia per il contrasto della criminalità, esclude *a fortiori* l'applicabilità della stessa all'accesso mediato ai dati. Non diversamente da quanto osservato con riguardo al GDPR, la direttiva LED disciplina cosi unicamente l'accesso diretto agli stessi da parte delle autorità pubbliche operanti in ambito penale.

Ora, le legislazioni nazionali che autorizzano l'accesso mediato ai dati di uno scomparso da parte delle autorità di soccorso, di polizia ovvero giurisdizionali coinvolte nelle ricerche dello stesso richiedono, similmente a quelle oggetto di analisi nelle cause *Privacy International, La Quadrature du Net, French Data Network*, *Ordre des barreaux francophones et germanophone, G.D.* e *SpaceNet,* di derogare alla disciplina prevista dalla direttiva *e-privacy*, ossia il consenso dell'utente per l'accesso ai dati, nonché l'acquisizione di questi ultimi per ragioni (la ricerca della scomparso) diverse da quelle invece economiche che ne hanno motivato l'originaria raccolta da parte dei fornitori di servizi di comunicazioni. In virtù della predetta giurisprudenza UE, esse rientrano allora parimenti nell'ambito applicativo della direttiva *e-privacy*. Né invero a tale tesi si potrebbe opporre che in questi casi la richiesta provenga da autorità pubbliche (in particolare quelle di primo soccorso) e per motivazioni (ossia la ricerca di una persona scomparsa) almeno parzialmente differenti da quelle invece oggetto delle controversie *Privacy International, La Quadrature du Net, French Data Network*, *Ordre des barreaux francophones et germanophone, G.D.* e *SpaceNet*, le quali concernono l'accesso ai dati UE da parte dei servizi di *intelligence* e di polizia per salvaguardare la sicurezza dello Stato e contrastare la criminalità anche grave. Dal combinato disposto di queste ultime si deduce anzi che l'applicazione della direttiva *e-privacy* in caso di accesso mediato ai dati prescinde proprio

[11] In tal senso, Corte giust., 20 settembre 2022, C-793/ e 794/19, *SpaceNet*, ECLI:EU:C:2022:702, spec. punto 48. Per un'analisi della sentenza in aggiunta a S. CRESPI, *L'influenza del diritto dell'Unione europea sulla sicurezza nazionale* cit., spec., p. 87-92, D. SIMON, *Droits fondamentaux - Protection des données numériques*, in *Europe*, 11 Novembre 2022, p. 357 ss.; X. TRACOL, *The joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The judgments of the Grand Chamber about data retention continue falling on deaf ears in Member States*, in *Computer law&security review*, 2023, vol. 48, p. 14 ss. Tale conclusion erano peraltro già state confermate nella di poco precedente pronuncia *G.D.*, del 5 aprile 2022, C-140/20, ECLI:EU:C:2022:258, quanto alla legislazione irlandese che autorizzava le autorità di polizia ad accedere ai dati personali per lottare contro la criminalità. In dottrina, S. CRESPI, *L'influenza del diritto dell'Unione europea sulla sicurezza nazionale* cit., spec. p. 98-99; D. SIMON, *Droits fondamentaux - Protection des données*, in *Europe Europe*, 2022, n° 6, p. 186 ss.

.

dalla natura dell'autorità pubblica che ne faccia richiesta agli operatori di comunicazione, nonché dalla motivazione ivi sottesa. In tali occasioni, la Corte di giustizia è, infatti, giunta alle medesime conclusioni (l'applicabilità della direttiva *e-privacy*) ed ha applicato le stesse condizioni (quelle dell'art. 15 direttiva *e-privacy*) sia qualora l'accesso ai dati personale sia stato richiesto dai servizi di *intelligence* per la salvaguardia della sicurezza dello Stato (*Privacy International, La Quadrature du Net, French Data Network* e *Ordre des barreaux francophones et germanophone*) sia quando invece tale acquisizione sia stata introdotta da quelle di polizia per il contrasto della criminalità anche grave (*G.D.* e *SpaceNet*). L'elemento che comporta l'applicabilità della direttiva *e-privacy* è allora la previsione di discipline nazionali in deroga a quella UE, ossia un fattore oggettivo presente anche nel caso in cui le autorità pubbliche di soccorso, di polizia o giurisdizionale richiedano ai fornitori dei predetti servizi l'accesso, al fine di cercare un individuo inaspettatamente irreperibile, ai dati di quest'ultimo senza il previo consenso dello stesso.

3. Una volta accertato che l'acquisizione mediata dei dati rientra nell'ambito di applicazione della direttiva *e-privacy* – e non del GDPR o della direttiva LED – è allora necessario indagare se, ed eventualmente a quali condizioni, quest'ultima autorizzi le autorità di soccorso, di polizia ovvero giurisdizionali a richiedere e poi ottenere, al fine di condurre le ricerche di uno scomparso, l'accesso ai dati di quest'ultimo attraverso l'intermediazione dei fornitori dei servizi di comunicazione, i quali raccolgono questi ultimi per motivi commerciali.

In particolare, quanto all'*an*, la direttiva *e-privacy* prevede, quale regola generale, la riservatezza di ogni comunicazione (art. 5) e dei relativi dati inerenti sia il traffico (art. 6) sia l'ubicazione (art. 9). Posto che questi ultimi contengono informazioni sulla vita privata delle persone fisiche o sui legittimi interessi di quelle giuridiche, l'atto UE in esame, proprio al fine di dare concretezza al principio di cui all'art. 5 della stessa, pone così dei limiti al trattamento che i fornitori dei predetti servizi possono imporre ai dati ricavati nell'ambito della loro attività economica. Questi ultimi sono autorizzati a trattare tali dati esclusivamente per stabilire i collegamenti tra gli apparecchi telefonici e trasmettere le relative comunicazioni, nonché a memorizzarli, anche se solo nella misura del necessario e per un periodo di tempo limitato (in Italia, ad esempio, da 3 a 6 mesi), ai fini del pagamento o della fatturazione (considerando 22 e 26). Qualsiasi ulteriore trattamento di dati che l'operatore economico voglia effettuare – ad esempio, per la commercializzazione dei servizi di comunicazione o per la fornitura di servizi a valore aggiunto, ossia consigli su pacchetti tariffari meno costosi, l'orientamento stradale, le informazioni sul traffico o ancora le previsioni meteorologiche – è autorizzato solo se l'utente abbia espresso il proprio specifico consenso, in base peraltro ad informazioni esaurienti ed accurate date dal fornitore dei predetti servizi circa la natura dei successivi trattamenti che egli intende effettuare. In tale contesto, l'abbonato ha poi sempre il diritto di non apporre o revocare il consenso a ogni trattamento ulteriore (considerando 26). I dati devono inoltre essere cancellati o resi anonimi quando essi non siano più necessari (considerando 26 e 28, artt. 6 e 9).

Quanto alla divulgazione dei dati a terzi – e quindi anche alle autorità pubbliche coinvolte nella ricerca di scomparsi – la direttiva *e-privacy* permette tale operazione solo quando l'utente abbia fornito il proprio consenso (art. 5), peraltro specifico ed informato. L'apposizione di quest'ultimo, già essenziale per ogni trattamento dei dati, è in tal caso ancora più importante, avendo la Corte di giustizia al riguardo più volte affermato che l'accesso di terzi ai dati raccolti

dai fornitori di servizi di comunicazione nell'ambito della loro attività comporta gravi rischi per il diritto alla *privacy* e alla tutela dei dati personali di cui agli artt. 7 e 8 della Carta e costituisce una autonoma ingerenza in questi diritti fondamentali, e ciò a prescindere dal fatto che le informazioni di cui trattasi abbiano o meno carattere sensibile, o che gli interessati abbiano o meno subito inconvenienti in seguito a siffatta ingerenza, ovvero ancora che i dati siano o meno stati utilizzati successivamente.[12]

Almeno a prima vista, in un quadro che, come quello appena delineato, permette di apportare limitazioni al diritto alla riservatezza delle comunicazioni e dei dati solo una volta ottenuto il previo consenso informato dell'utente, il quale rappresenta così la base giuridica naturale e privilegiata dal legislatore UE, l'accesso a questi ultimi da parte di ogni autorità pubblica dovrebbe, anche quando si tratti di rintracciare delle persone scomparse, essere in linea di principio escluso, non potendosi per definizione ottenere il previo consenso dell'utente in situazioni di improvvisa ed inspiegabile irreperibilità. Anzi, l'utilità di tale accesso verrebbe meno qualora l'abbonato fosse in condizioni di apporre il proprio consenso e di autorizzare così l'acquisizione dei dati di ubicazione o relativi al traffico da parte delle predette autorità pubbliche.

Le regole appena illustrate fondate sul consenso dell'utente non sono tuttavia priva di eccezioni, gli artt. 10 e 15 della direttiva *e-privacy* illustrando taluni casi, invero tassativi e da interpretarsi restrittivamente, nei quali i terzi possono essere autorizzati, seppur a determinate condizioni, ad accedere ai dati relativi all'ubicazione e/o al traffico di un individuo anche in mancanza del consenso di quest'ultimo, il che ne permetterebbe l'uso tra l'altro in caso d'improvvisa scomparsa di un utente. Limitando per il momento l'analisi all'art. 10, let. *b*, della direttiva *e-privacy*, esso autorizza i paesi membri a concedere, con legge, al fornitore di una rete o di un servizio di comunicazione la facoltà di «sottoporre a trattamento i dati personali relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, linea per linea, per gli organismi che trattano chiamate di emergenza, riconosciuti come tali da uno Stato membro, in particolare per le forze di polizia, i servizi di ambulanza e i vigili del fuoco, affinché questi possano reagire a tali chiamate». Pur in mancanza di una giurisprudenza comune interpretativa di tale norma, quest'ultima – e il sostanzialmente corrispondente par. 4 dell'art. 127 del Codice in materia di protezione dei dati che ha trasposto in Italia la direttiva *e-privacy*[13]– nella misura in cui consente ai predetti operatori di selezionare, estrapolare e condividere («trattare») con le autorità di soccorso, di polizia o giurisdizionali i dati (in realtà solo) di ubicazione di un singolo individuo («linea per linea») anche senza il consenso di quest'ultimo, e addirittura qualora esso abbia già rifiutato od omesso di prestare il consenso, sembra costituire allora una base giuridica adeguata per permettere la geo-localizzazione degli apparecchi terminali anche degli scomparsi.[14]

---

[12] Così, Corte giust., *La Quadrature du Net* cit., punti 114-116; nonché *G.D.* cit., punti 44 e 47.

[13] D.leg. del 30 giugno 2003 n. 196, in *G.U.* della Repubblica italiana del 29 luglio 2003 n. 174. Il testo è reperibile anche sul sito del nostro Garante della protezione dei dati personali all'indirizzo: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.

[14] L'uso dell'art. 10, let. b), della direttiva *e-privacy* cit. quale base giuridica non solo non è mai stato interpretato dalla giurisprudenza UE, ma è stato solo limitatamente oggetto dell'attenzione della dottrina. Relativamente a un impiego della stessa per accedere e usare i dati dei migranti nell'ambito di attività di soccorso umanitario da parte di organizzazioni non governative (NGOs), T. GAZI, *Data to the rescue: how humanitarian aid NGOs should*

Il fatto che l'art. 10, let. *b*, della direttiva *e-privacy*, nel definire il proprio ambito applicativo oggettivo, si limiti poi a richiedere la sussistenza (o meglio la convinzione della sussistenza) di una situazione di pericolo – «gli organismi che trattano chiamate di emergenza […] affinché questi possano reagire a tali chiamate» – sembra permetterne l'uso a prescindere dalla qualificazione dell'irreperibilità come un evento suicidario, un incidente o un'ipotesi di reato e dunque in situazioni di scomparsa anche disgiunte da quest'ultimo. E in effetti la disposizione in esame, nell'elencare le autorità che possono richiedere ai fornitori di rete o di servizi di comunicazione l'accesso ai dati di ubicazione di un individuo senza il consenso di quest'ultimo, pone, accanto a quelle di polizia, le autorità di primo soccorso, le quali intervengono per definizione anche in assenza di ipotesi delittuose.

La norma in esame subordina tuttavia l'uso della stessa alla sussistenza di una chiamata di emergenza. L'uso dell'art. 10, let. *b*, della direttiva *e-privacy* come base giuridica per accedere ai dati di un individuo è certamente possibile qualora quest'ultima sia effettuata dal soggetto che si trovi in difficoltà. Seppur a determinate condizioni, essa sembra invero utilizzabile anche allorché la chiamata giunga alle autorità pubbliche di soccorso e di polizia da parte di terzi. Ciò pare dedursi dal testo del considerando 36 della direttiva in esame che stabilisce, in modo generale, che «gli Stati membri possono limitare il diritto alla vita privata degli utenti e degli abbonati riguardo [tra l'altro] ai dati relativi all'ubicazione allorché ciò sia necessario per consentire ai servizi di emergenza di svolgere il loro compito nel modo più efficace possibile», senza cioè richiedere che la chiamata di emergenza giunga dall'utente o dall'abbonato.

Tuttavia, al fine però di escludere una compressione eccessiva del diritto fondamentale alla *privacy* e tutela dei dati del soggetto (preteso) scomparso o in difficoltà, le predette autorità pubbliche dovrebbero, in quest'ultimo caso, intervenire unicamente a seguito di una denuncia di scomparsa che, attraverso elementi oggettivi, attesti l'eccezionalità e l'effettiva pericolosità della situazione, nonché escludano la volontarietà dell'allontanamento. La sussistenza della condizione d'allarme sottesa all'art. 10, let. *b*, della direttiva *e-privacy* esclude in effetti dal suo spazio attuativo circostanze che invece ne prescindono come per l'appunto quelle ove sia stata accertata l'intenzione, quantomeno di adulti che non presentano indici di vulnerabilità, di distaccarsi dal proprio contesto abituale e di non essere più cercati. Pur nel silenzio della direttiva *e-privacy* e dell'atto di trasposizione italiano, non sembra in effetti che l'allontanamento, ancorché volontario, di minori, anziani o individui in condizioni di fragilità anche solo temporanea possa indurre ad escludere l'applicabilità del regime previsto all'art. 10, let. *b*, della direttiva *e-privacy*. Anche quando poi si tratti di adulti capaci, l'intenzione di andarsene dovrebbe inoltre essere valutata con accuratezza al fine di evitare che l'accesso ai dati personali di ubicazione dello scomparso sia escluso solo semplicemente invocandone la pretesa intenzionalità, e ciò anche allorché la sparizione sia sorprendente ed inspiegabile per le persone vicine allo scomparso.

Quanto all'applicazione della norma in esame allorché le autorità coinvolte nella ricerca siano convinte che la scomparsa sia da ricondursi a un ipotesi delittuosa (ad esempio, un omicidio pur in assenza di un cadavere), la convinzione della morte dello scomparso ben

collect information based on the GDPR, in *Journal of International Humanitarian Aid*, 2020, p. 1 ss.; N. BEHNAM, K. CRABTREE, *Big data, little ethics: confidentiality and consent*, in *Forced Migration Review*, 2019, p. 61 ss.

potrebbe escludere l'emergenza invece alla base dell'art. 10, let. *b*, della direttiva *e-privacy*. In realtà, considerata l'importanza del ritrovamento del cadavere per le condanne criminali,[15] l'esigenza di rintracciare in ogni caso il corpo della persona scomparsa ben potrebbe giustificare l'uso di questa norma anche nel caso in esame.

Né invero un uso parsimonioso dell'art. 10, let. *b*, della direttiva *e-privacy* risponderebbe all'esigenza di applicare quest'ultimo, in quanto norma derogatoria, solo in casi eccezioni e dunque, per tale via, di tutelare meglio i diritti fondamentali previsti agli artt. 7 e 8 della Carta. Il rischio di un uso troppo disinvolto della clausola in esame pare in effetti scongiurato dalla previsione di una serie di elementi che controbilanciano, già a livello normativo, l'accesso ai dati ivi previsto. Quest'ultimo non soltanto è permesso, come già ricordato, esclusivamente in «condizioni di emergenza» solo agli «organismi che trattano chiamate di emergenza riconosciuti come tali da uno Stato membro», ma è anche limitato alla possibilità d'acquisire unicamente i dati di ubicazione, quelli relativi al traffico restando invece esclusi dall'ambito applicativo della norma in esame. Questa scelta del legislatore UE pare condivisibile, la richiesta d'acquisizione di questo secondo tipo di dati essendo coerente non tanto con l'emergenziale ricerca di una persona scomparsa in condizioni di pericolo, quanto con un'indagine penale di lungo periodo. Come già ricordato, infatti, i dati relativi al traffico permettono, a differenza di quelli di ubicazione, di ricostruire il contesto fattuale della sparizione anche in relazione ad altri soggetti coi quali lo scomparso abbia interagito. Il riferimento poi alla transitorietà del mancato consenso – «nonostante il rifiuto o il mancato consenso *temporanei* dell'abbonato o dell'utente» – lascia intendere che la geo-localizzazione dell'apparecchio terminale di questi ultimi debba essere temporalmente circoscritta all'emergenza in atto. Ciò è invero comprensibile dato che quest'ultima non può essere infinita o particolarmente lunga, il perdurare di una condizione di allarme non essendo più qualificabile come un'emergenza in senso stretto.

L'apposizione delle predette condizioni – soggettive (solo alcuni tipi di autorità autorizzate dai singoli Stati membri), oggettive (unicamente in condizioni di emergenza, nonché a seguito di una apposita chiamata/denuncia di allontanamento), qualitative (soltanto i dati personali di ubicazione), temporali (esclusivamente per il tempo dell'emergenza) – risponde all'esigenza di circoscrivere l'eccezionale accesso ai dati da parte di autorità di primo soccorso, di polizia o giurisdizionali senza il consenso dell'interessato solo quando effettivamente necessario, nonché mediante misure equilibrate. Attraverso i classici principi UE di necessità e di proporzionalità, i diritti fondamentali alla *privacy* e alla tutela dei dati sono, in altri termini, bilanciati con l'esigenza di garantire la vita, la sicurezza personale e quella pubblica, l'incapacità di ricostruire la sorte degli scomparsi creando tra l'altro (in)sicurezza nella collettività, e ciò anche quando essa non sia da ricondursi all'ambito penale. L'applicazione di tali condizioni di misura permettono peraltro di preservare il contenuto essenziale dei diritti fondamentali di cui agli artt. 7 e 8 della Carta come prescritto dall'art. 52 di quest'ultima. Secondo tale norma, infatti, «eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta [e dunque anche di quello alla protezione dei dati e della

[15] Proprio a fronte delle tradizionali difficoltà giuridiche di condanne penali in assenza di cadavere le pronunce nazionali di condanna in tali circostanze sono ancora un'eccezione. In tal senso, *ex multiis*, Cass. Penale (Sez. prima) del 10 luglio 2019 n. 48673 (c.d. caso Ragusa).

privacy] devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

L'osservanza delle condizioni di temperanza di cui tra l'altro all'art. 10 let. *b*, della direttiva *e-privacy* è ancora più importante considerato che, seppur con riguardo all'art. 15 del medesimo atto, i giudici di Lussemburgo, soprattutto negli ultimi dieci anni, non hanno esitato a dichiarare incompatibili con gli artt. 7, 8 e 52 della Carta, e ad annullare con effetti *erga omnes* ed *ex tunc*, alcuni atti UE in materia di protezione dei dati – ossia la direttiva 2006/24 inerente la conservazione dei dati generati nell'ambito dei servizi di comunicazione elettronica per il contrasto alla criminalità grave[16] nella pronuncia *Digital Right Ireland*,[17] le decisioni di adeguatezza UE-USA *Safe Harbour* e *Privacy Shield*[18] nelle sentenze *Schrems I*[19] e *Schrems*

[16] La direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, la quale modifica la direttiva 2002/58/CE (c.d. *e-privacy*) già cit., è pubblicata in *GUUE*, 13 aprile 2005 L 105/54.

[17] Corte giust., 8 aprile 2014, C-293/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238. In dottrina, M. COLE, F. BOEHM, *EU Data Retention – Finally abolished? Eight years in light of Article 8*, in *Critical Quarterly for Legislation and Law*, 2014, p. 58 ss.; D. LYNSKEY, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Common Market Law Review*, 2014, p. 1789 ss.; O. POLLICINO, *Diritto all'oblio e conservazione di dati. La Corte di giustizia a piedi uniti: verso un digital right to privacy*, in *Giurisprudenza costituzionale*, 2014, p. 2949 ss.; S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto Pubblico Comparato ed Europeo*, 2017, p. 687 ss. La già citata pronuncia *G.D.* del 2022 riguardava la ricevibilità (poi ammessa seppur a condizione di rispettare i principi UE di equivalenza e di effettività) nell'ambito di un procedimento penale di elementi di prova fondati su dati raccolti in base alla legislazione irlandese di trasposizione della direttiva 2006/24 già cit. dichiarata per l'appunto invalida nella sentenza UE *Digital Rights Ireland*.

[18] Sulle decisioni di adeguatezza *Safe Harbour* e *Privacy Shield*, G. VERMEULEN, *Eyes Wide Shut*: *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities*, in G. VERMEULEN, E. LIEVENS (ed.), *Data protection and privacy under pressure. Transatlantic tensions, EU surveillance and Big Data, Antwerp,* 2017, p. 45 ss. A seguito dei negoziati condotti dalla Commissione europea e l'amministrazione USA nel 2021 e dell'accordo di principio raggiunto a marzo 2022 tra queste ultime, la Commissione europea, anche sulla base dell'*Executive Order* USA di ottobre 2022, sta redigendo una nuova decisione di adeguatezza tra UE e USA (https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045) che sostituirà il *Privacy Shield* dichiarato nullo dalla Corte giust., 16 luglio 2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems* (c.d. *Schrems II*), ECLI:EU:C:2020:559. Su tali aspetti, G. RUGANI, *Gli ultimi sviluppi della saga sui trasferimenti di dati personali UE-USA: l'Executive Order firmato dal Presidente USA Biden il 7 ottobre 2022 e la proposta di decisione di adeguatezza presentata dalla Commissione UE il 13 dicembre 2022*, in AISDUEblog.

[19] Corte giust., 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* (c.d. *Schrems I*), ECLI:EU:C:2015:650. In dottrina, L. COLONNA, Schrems vs. Commissioner*: A Precedent for the CJEU to Intervene in the National Intelligence Surveillance Activities of Member States?*, in *Europarättslig tidskrift*, 2016, nº 2, p. 208 ss.; R.A. EPSTEIN, *The ECJ's Fanal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European Constitutional Law Review*, 2016, vol. 12, p. 330 ss.; A. DEBET, *L'invalidation du* Safe Harbor *par la CJUE: tempête sur les transferts de données vers les États-Unis*, in *La Semaine Juridique – éd. gén.*, 2015, nº 46-47, p. 2108 ss.

II,[20] l'Accordo PNR tra Canada e Unione europea nel parere 1/15[21] – proprio in quanto essi apportavano limitazioni non necessarie e non proporzionate al predetto diritto fondamentale UE. Pur se fino ad ora la Corte di giustizia sembra essere stata meno severa con le legislazioni degli Stati membri che, sulla base delle condizioni derogatorie previste nella direttiva *e-privacy* (art. 15), autorizzavano le autorità (di polizia e di *intelligence*) ad accedere e usare, per ragioni di contrasto alla criminalità o di tutela della sicurezza dello Stato, i dati raccolti dagli operatori economici delle comunicazioni per motivi commerciali – l'incompatibilità con gli artt. 7, 8 e 52 della Carta essendo stata accertata nei casi *Tele2 Sverige* (Svezia), *G.D.* (Irlanda) *Spetsializirana prokuratura* (Bulgaria)[22] – essa ha ripetutamente dimostrato la volontà di controllarne scrupolosamente il rispetto proprio alla luce dei principi UE di necessità e proporzionalità.[23] A fronte di ciò, non sembra allora possibile escludere in futuro più frequenti declaratorie di incompatibilità UE anche di normative interne che, a prescindere dal motivo di deroga al diritto alle riservatezza dei dati personali – la lotta alla criminalità, la salvaguardia della sicurezza nazionale o anche la ricerca di persone improvvisamente irreperibili – autorizzino i fornitori di servizi di comunicazione a divulgare ad autorità pubbliche (di soccorso,

[20] Per un commento alla pronuncia *Schrems II*, già cit., F. D'ATH, *Arrêt «* Schrems II *» : sur la légalité d es transferts de donnéespersonnelles fondés sur une décision d'adéquation ou moyennant des garanties appropriées*, in *Journal de droit européen*, 2020, nº 10, p. 442 ss. ; E. FLETT, J. WILSON, J. CLOVER, *Schrems strikes again: EU-US privacy shield suffers same fate as its predecessor*, in *Computer and Telecommunications Law Review*, 2020, p. 161 ss.; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, p. 733 ss.; M. ROTENBERG, Schrems II*, from Snowden to China: toward a new alignment on transatlanticdata protection*, in *European Law Journal*, 2020, p. 141 ss.; C. SELLARS, Schrems II *and Standard Contractual Clauses – the Advocate-General's*
Opinion, in *Computer Law Review International*, 2020, p. 29 ss.

[21] Corte giust., parere 1/15 *Canada/UE* del 27 luglio 2017, pubblicato nella Raccolta digitale della Corte di giustizia dell'Unione europea. In dottrina, N. LE BONNIEC, *L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne : une délicate conciliation entre sécurité nationale et sécurité numérique*, in *Revue trimestrielle de droit européen*, 2018, n. 3, p. 617 ss. ; C. KUNER, *International agreement, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR,* in *Common Market Law Review*, 2018, p. 857 ss.; E.A. ROSSI, *Gli accordi PNR (Passenger Name Record) nella lotta al terrorismo internazionale. Conseguenze del parere n. 1/15 della Corte di giustizia del 26 luglio 2017 per la legittimità della direttiva n. 2016/681/UE*, in *Diritto comunitario e degli scambi internazionali*, 2018, p. 395 ss.

[22] Fino ad ora la Corte di giustizia ha concluso per l'incompatibilità delle legislazioni nazionali che autorizzavano le autorità di polizia all'accesso indiscriminato ai dati relativi al traffico e all'ubicazione solo nei casi Corte giust. G.D. cit (Irlanda); 21 dicembre 2016, C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970 (Svezia) e Corte giust. 17 novembre 2022, C-350/21, *Spetsializirana prokuratura*, ECLI:EU:C:2022:896 (Bulgaria). Per un commento a *Tele2 Sverige*, I. CAMERON, *Balancing data protection and law enforcement needs:* Tele2 Sverige and Watson, in *Common Market Law Review*, 2017, p. 1467 ss.; X. TRACOL, *The judgement of the Grand Chamber dated 21 December 2016 in the two joint* Tele2Sverige and Watson *cases: the need for a harmonized legal framework on the retention of data at EU level*, in *Computer Law & Security Review*, 2017, p. 1 ss.

[23] Pur concludendo in questo caso per la compatibilità delle legislazioni nazionali, tale controllo dei giudici dell'unione europea è stato esercitato nelle già menzionate sentenze *Privacy International, La Quadrature du Net, French Data Network* e *Ordre des barreaux francophones et Germanophone* relativamente alle normative britannica, francese e belga (in merito, nota n. 7 del presente contributo) che autorizzavano le autorità di *intelligence* ad accedere e usare per salvaguardare la sicurezza dello Stato i dati raccolti dai fornitori di servizi di comunicazione per ragioni commerciali. Analogamente, pur se con riguardo a legislazioni interne che permettevano l'accesso ai dati UE da parte delle autorità di polizia per ragioni di contrasto alla criminalità anche grave, Corte giust. 2 dicembre 2018, C-207/16, *Ministerio Fiscal,* ECLI:EU:C:2018:788 (Spagna); *SpaceNet* cit. (Germania); *G.D* cit. (Irlanda). Per un'analisi della pronuncial *Ministerio Fiscal*, C. DOCKSEY, Ministerio Fiscal*: holding the line on ePrivacy*, in *Maastricht Journal of European and Comparative Law*, 2019, p. 585 ss.; X. TRACOL, Ministerio Fiscal*: access of public authorities to personal data retained by providers of electronic communications services*, in *European Data protection Law Review*, 2019, p. 127 ss.

di polizia ovvero giurisdizionali) i dati degli utenti in assenza di adeguate condizioni di misura e ragionevolezza.

La ricostruzione qui proposta – e dunque l'uso degli artt. 10, let. *b*, della direttiva *e-privacy* e 127, comma 4, del Codice italiano in materia di protezione dei dati come basi giuridiche abilitanti le autorità coinvolte nelle ricerche di uno scomparso a richiedere, seppur a determinate condizioni, ai servizi di comunicazione i dati di ubicazione di quest'ultimo anche senza il suo consenso – trova parziale conferma nella prassi decisionale del Garante della *privacy* italiano con riguardo all'impiego dei dati di ubicazione raccolti dagli operatori di comunicazione per localizzare persone infortunate o disperse in montagna da parte di unità di ricerca e soccorso (il Corpo nazionale del soccorso alpino e speleologico).[24] Nel provvedimento n. 1580543 del 19 dicembre 2008,[25] quest'ultimo, pur fondando la legittimità di tale uso dei dati sull'art. 24, comma 1, *let. e)* del Codice italiano sulla protezione dei dati che, trasponendo nel nostro paese l'art. 7 della (ormai abrogata) direttiva 95/46,[26] autorizzava il trattamento degli stessi senza il consenso dell'utente allorché ciò fosse necessario per la salvaguardia della vita e dell'incolumità fisica di un terzo o dell'interessato, ha precisato che «i servizi abilitati in base alla legge a ricevere chiamate di emergenza possono [proprio in base al considerando 36 e all'art. 10, par. 1, *let. b)* della direttiva *e-privacy*] in ogni caso trattare i dati relativi all'ubicazione degli apparecchi relativi ai chiamanti, anche quando l'utente o l'abbonato abbiano già rifiutato o omesso di prestare il consenso». Peraltro, come si avrà modo di vedere nel prosieguo, gli artt. 6, par. 1*, let. d)* GDPR e 8 della direttiva LED, che hanno un contenuto analogo agli artt. 7 della direttiva 96/46 e 24, comma 1, *let. e)* del Codice italiano sulla protezione dei dati, paiono applicabili solo relativamente all'acquisizione diretta dei dati, cosicché l'uso di tali norme nel caso di accesso mediato agli stessi, invece oggetto del provvedimento n. 1580543 del 19 dicembre 2008, avrebbe dovuto essere esclusa, il considerando 36 e all'art. 10, par. 1, *let. b)* della direttiva *e-privacy*, nonché l'art. 127, par. 4, del predetto Codice italiano essendo disposizioni più adeguate per giustificare l'accesso, per l'appunto mediato, ai dati nel caso in esame.

4. A differenza dell'art. 10, let. *b*, della direttiva *e-privacy* che autorizza l'accesso delle autorità di soccorso, di polizia o giurisdizionali ai dati di ubicazione di un utente anche senza il consenso di quest'ultimo, nessuna disposizione della direttiva in esame concerne, quantomeno espressamente, la possibilità per le medesime autorità di accedere in via mediata ai dati relativi al traffico. E ciò sebbene questi ultimi, permettendo di ricostruire le abitudini e i contatti di un certo individuo, siano strumenti essenziali per ricostruire il contesto nel quale è maturata la sparizione, nonché indagarne la natura volontaria, suicidaria, accidentale o violenta.

[24] Non sono invece state trovate analoghe decisioni tra quelle adottate *dall'European Data Protection Board* (EDPB), nonché da talune Autorità garanti della *privacy* prese in esame, ossia quelle di Spagna, Francia, Belgio, Regno Unito, Irlanda, Malta.

[25] Il testo della decisione è disponibile sul sito del Garante della *privacy* italiano, Persone disperse in montagna: si può localizzare il cellulare per... - Garante Privacy.

[26] La 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, è stata pubblicata in *GUCE* L 281 del 23 novembre 1995, p. 31-50. La presente direttiva è stata abrogata a seguito dell'entrata in vigore del già citato GDPR a maggio 2018.

Pur nel silenzio della direttiva *e-privacy*, questo accesso ai dati sembra essere in ogni caso ammesso in virtù e alle condizioni stabilite dall'art. 15 della stessa. Come già anticipato, questa norma autorizza gli Stati membri ad introdurre, mediante lo strumento legislativo, talune deroghe al regime di tutela della riservatezza dei dati personali previsto dalla direttiva *e-privacy* tra l'altro relativo alla divulgazione degli stessi a terzi – e dunque potenzialmente anche alle autorità pubbliche coinvolte nelle ricerche di uno scomparso – ogni volta in cui ciò sia necessario per «la salvaguardia della sicurezza nazionale, della difesa e della sicurezza pubblica, o per la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati».[27] L'impiego di tale norma per giustificare l'eccezionale acquisizione mediata dei dati relativi al traffico da parte delle predette autorità pubbliche presuppone allora che l'esigenza di rintracciare le persone irreperibili rientri tra gli obiettivi d'interesse generale UE ivi menzionati, così come peraltro interpretati dalla Corte di giustizia. A differenza dell'art. 10, let. *b*, della direttiva *e-privacy* che non è mai stato oggetto di valutazione da parte di quest'ultima, l'art. 15 della stessa è stato, infatti, ripetutamente oggetto di attenzione da parte dei giudici dell'Unione. E' in effetti proprio su questa base giuridica che, nei già citati casi *Tele2*, *Ministerio Fiscal*, *Privacy International, La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophone, G.D., SpaceNet*, *VD e SR* e *Spetsializirana prokuratura*, gli Stati membri avevano adottato normative interne che eccezionalmente autorizzavano le proprie autorità di polizia o *intelligence* ad accedere in via mediata ai dati di ubicazione e relativi al traffico degli utenti vuoi per lottare contro la criminalità (*Tele2*, *Ministerio Fiscal*, *G.D., SpaceNet*, *VD e SR* e *Spetsializirana prokuratura*) vuoi invece per salvaguardare la sicurezza dello Stato (*Privacy International, La Quadrature du Net, French Data Network e Ordre des barreaux francophones et germanophone*).

Ora, anche alla luce di questa giurisprudenza comune, non pare innanzitutto che la ricerca degli scomparsi possa rientrare in quest'ultima esigenza. Secondo la Corte di giustizia, l'obiettivo di preservare la sicurezza interna corrisponde all'interesse di tutelare le funzioni essenziali di un paese e gli interessi fondamentali della società mediante la prevenzione e/o la repressione di attività in grado di destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese.[28] Esso permette, in altri termini, di reagire a minacce – peraltro reali, attuali o quanto meno prevedibili – di eccezionale gravità dirette contro la società, la popolazione o lo Stato, il che accade, ad esempio, quando sia necessario contrastare attività di terrorismo interno o internazionale.[29] Il fatto poi che, per i giudici di Lussemburgo, nemmeno le attività di lotta contro la criminalità anche grave abbiano un grado di eccezionalità e pericolosità sufficientemente elevato da essere assimilabili ad una minaccia per la sicurezza nazionale – rientrando queste ultime nella diversa nozione di rischio alla «sicurezza pubblica»[30] – induce a ritenere a maggior ragione esclusa dalla categoria in esame anche l'esigenza di non lasciare insoluta la scomparsa di membri della propria collettività.

Meno immediato è invece accertare – questa volta in positivo – se tale motivo sia compreso nell'interesse generale UE di salvaguardare «la sicurezza pubblica» o in quello

[27] Per una disamina dettagliata della norma in esame da parte dei giudici di Lussemburgo, Corte giust. *G.D.* cit., punto 32 e la giurisprudenza UE ivi citata.
[28] Corte giust., *La Quadrature du Net* cit., punto 135; *G.D.* cit., punto 61.
[29] Corte giust., *La Quadrature du Net* cit., punti 136-137; *G.D.* cit., punto 62.
[30] Corte giust., *G.D.* cit., punto 63.

diverso di favorire «la prevenzione, ricerca, accertamento e perseguimento dei reati». Che invero la ricerca degli scomparsi ben possa rientrare almeno in una di queste due nozioni pare dedursi dal tenore del considerando 11 e 35 e dell'art. 8 della direttiva LED. Nel definire le basi giuridiche che rendono lecito il trattamento dei dati effettuato dalle autorità in materia penale, tali norme stabiliscono che «la prevenzione, l'indagine, l'accertamento e il perseguimento di reati», la quale include la tutela della «sicurezza pubblica», «dovrebbe comprendere anche la salvaguardia degli interessi vitali dell'interessato». In altri termini, le nozioni di «prevenzione, indagine, accertamento, perseguimento di reati o esecuzione di sanzioni penali» e di «sicurezza pubblica», tra loro collegate, includono la salvaguardia degli interessi vitali degli individui, ossia di un bene giuridico che è parimenti alla base dell'esigenza di ricercare le persone irreperibili. Né invero a una diversa conclusione – ossia l'esclusione di quest'ultima dalle nozioni di «sicurezza pubblica» o di «prevenzione, ricerca, accertamento e perseguimento dei reati» e dunque dall'art. 15 della direttiva *e-privacy* – sembra condurre il fatto che, secondo i giudici di Lussemburgo, «una misura legislativa adottata ai sensi di detta disposizione deve *rispondere in modo effettivo e rigoroso* ad uno di questi obiettivi»,[31] tutte e tre le categorie in esame avendo come obiettivo primario proprio quello di salvaguardare il medesimo bene giuridico della vita degli individui.

Quanto alla questione di sapere se l'esigenza di ricercare le persone scomparse ricada nella nozione di «sicurezza pubblica» o di «prevenzione, ricerca, accertamento e perseguimento dei reati», è da rilevare che, almeno quando il contesto fattuale nel quale si è verificata l'irreperibilità di un individuo lasci spazio a ipotesi di rilevanza penale (ad esempio, omicidio, occultamento di cadavere, sequestro di persona, sottrazione di minore), l'accesso ai dati relativi al traffico pare giustificato dall'obiettivo di favorire «l'accertamento e il perseguimento» del reato che si presume ivi sotteso. Ma anche quando l'allontanamento, pur inaspettato e sorprendente, possa essere la conseguenza di un gesto suicidario o di un accidente, esso sembra poter in ogni caso rientrare nella categoria in esame, l'accesso delle autorità di polizia e/o giurisdizionali ai dati relativi al traffico permettendo «la ricerca» di reati anche solo eventualmente sottostanti la scomparsa. Anzi, proprio in caso d'incertezza sulla natura della sparizione, l'accesso e l'analisi dei predetti dati pare costituire uno strumento indispensabile per orientarne la qualificazione (volontaria, suicidaria, accidentale o criminale), e ciò anche al fine di escludere un'ipotesi di reato.

La ricerca degli scomparsi potrebbe invero essere compresa anche nell'ambito della diversa categoria della necessità di salvaguardare la «sicurezza pubblica». Come già ricordato, infatti, l'incapacità di ricostruire la sorte di un membro della collettività – l'essere ancora in vita o la sua morte e, in quest'ultimo caso, le circostanze di quant'ultima anche quando non violenta – ben può rappresentare un fattore di "insicurezza pubblica". Ciò pare a maggior ragione vero posto che l'analisi delle pronunce UE che hanno interpretato il concetto di «sicurezza pubblica» anche se in ambiti diversi dalla protezione dei dati e dalla *privacy* mostra come quest'ultimo abbracci esigenze anche non connesse a situazioni penalmente rilevanti.[32]

[31] Corte giust. *G.D.* cit., punto 41; *SpaceNet* cit., punto 58.

[32] Quanto alla possibile (ma non necessaria) correlazione giuridica tra sicurezza pubblica e reati, v., ad esempio, Corte giust. 21 giugno 2022, *Ligue des droits humains c. Conseil des ministres*, C-817/19, ECLI:EU:C:2022:491, punto 162 relativamente all'uso dei dati PNR per evitare turbamenti alla sicurezza pubblica; 27 febbraio 2020,

Secondo la Corte di giustizia, esso è stato, ad esempio, a ragione invocato per approvare in via straordinaria progetti di costruzione in zone protette abitate da specie prioritarie,[33] di abbattere alberi moribondi o infestati soprattutto lungo le vie di comunicazione e gli itinerari turistici,[34] di vigilare sulla qualità dei prodotti ed eventualmente di limitarne la circolazione nel mercato unico,[35] di escludere la vendita di fuochi d'artificio il cui contenuto in miscela sia superiore a un kilogrammo,[36] o di circoscrivere il commercio delle armi da fuoco.[37] Anche considerato che la ricerca degli scomparsi non risponde a considerazioni di ordine economico o commerciale, ossia a motivazioni certamente escluse dalla nozione di «sicurezza pubblica»,[38] essa, nella misura in cui genera un'insicurezza sociale, sembra poter giustificare la comprensione, in ogni caso solo proporzionata e laddove necessario, del diritto fondamentale alla riservatezza dei dati tra l'altro relativi al traffico sulla base dell'art. 15 della direttiva *e-privacy*. L'eccezionalità dell'uso di quest'ultima norma per comprimere dei diritti fondamentali UE, da un lato, e la necessità di utilizzare i dati relativi anche al traffico per la ricerca delle persone scomparse tra l'altro in assenza di una prova certa di reato, dall'altro lato, dovrebbe in ogni caso indurre il legislatore UE, in sede di revisione della direttiva *e-privacy*, a contemplare quest'ultima possibilità, anche coordinando in modo più fluido gli artt. 10 e 15 della stessa.

Similmente poi a quanto osservato con riferimento all'art. 10, let. *b)* della direttiva *e-privacy*, anche quest'ultimo, sempre al fine di rispettare il contenuto dell'art. 52 della Carta, subordina l'eventuale deroga agli artt. 7 e 8 della stessa al rispetto di condizioni ispirate ai principi UE di necessità e proporzionalità. In particolare, ogni eccezione al regime generale di tutela dei dati personali di cui alla direttiva in esame deve essere stabilito con legge, può riguardare solo i diritti di cui agli artt. 5, 6, 8 e 9 della direttiva *e-privacy*, nonché deve rispettare i valori (art. 2 TUE) e i diritti fondamentali dell'Unione (art. 6 TUE). L'attenzione verso questi requisiti è inoltre sottoposto allo scrupoloso apprezzamento dei giudici di Lussemburgo, i quali, come già osservato, non hanno esitato a dichiarare incompatibili con l'art. 15 della direttiva *e-privacy* non solo atti UE (*Digital Right Ireland*, *Schrems I*, *Schrems II*, parere 1/15), ma anche talune normative nazionali (quella svedese in *Tele2 Sverige*, quella irlandese in *G.D.* e quella bulgara in *Spetsializirana prokuratura*).

La qualificazione dell'esigenza di ricerca degli scomparsi nella categoria giuridica della «sicurezza pubblica» consentirebbe peraltro un accesso più ampio ai dati relativi al traffico

---

Subdelegación del Gobierno en Ciudad Real c. RH, C-836/18, ECLI:EU:C:2020:119 quanto alla facoltà di negare il diritto di soggiorno nell'Unione europea a un cittadino di un paese terzo che abbia commesso pregressi reati.

[33] Corte giust. 16 luglio 2020, *WWF Italia Onlus*, C-411/19, ECLI:EU:C:2020:580; 22 giugno 2022, *Commissione europea c. Slovacchia*, C-661/20, ECLI:EU:C:2022:496.

[34] Corte giust. 17 aprile 2018, *Commissione europea c. Polonia*, C-441/17, ECLI:EU:C:2018:255.

[35] Corte giust. 6 maggio 2021, *Analisi G. Caracciolo Srl*, C-142/20, ECLI:EU:C:2021:368.

[36] Corte giust. 26 settembre 2018, *Van Gennip BVBA*, C-137/17, ECLI:EU:C:2018:771.

[37] Corte giust. 24 novembre 2022, *A*, C-296/21, ECLI:EU:C:2022:918; 3 dicembre 2019, *Repubblica ceca c. Parlamento europeo e Consiglio*, C-482/17, ECLI:EU:C:2019:1035; 23 gennaio 2018, *The Queen c. Minister of Justice*, C-267/16, ECLI:EU:C:2018:26.

[38] Corte giust. 17 settembre 2020, *Autoritatea națională de reglementare în domeniul energiei (ANRE) c. Societatea de Producere a Energiei Electrice în Hidrocentrale Hidroelectrica SA*, C-648/18, ECLI:EU:C:2020:723, punto 43; nonché *Subdelegación del Gobierno en Ciudad Real c. RH* cit., punto 47 quanto al requisito di possedere risorse sufficienti per rifiutare il diritto di soggiorno a un cittadino di un paese terzo, familiare di un cittadino dell'Unione. Un siffatto obiettivo meramente economico, infatti, si distingue fondamentalmente da quello inteso a tutelare la pubblica sicurezza e non consente di giustificare lesioni così gravi al godimento effettivo del contenuto essenziale dei diritti che derivano dallo *status* di cittadino dell'Unione.

rispetto a quello permesso ad obiettivi inclusi nel diverso concetto di «prevenzione, ricerca, accertamento e perseguimento dei reati». Secondo la Corte di giustizia, infatti, tra gli obiettivi d'interesse generale UE che possono giustificare una misura adottata ai sensi dell'art. 15 della direttiva *e-privacy* esiste una gerarchia in funzione della loro rispettiva importanza, la quale condiziona la gravità dell'ingerenza nei diritti fondamentali di cui agli artt. 7 e 8 della Carta e dunque l'ampiezza – quantitativa, qualitativa e temporale – dell'accesso ai dati da parte di terzi diversi dall'utente.[39] Mentre la sicurezza dello Stato giustifica, seppur a determinate condizioni di equilibrio, l'imposizione ai fornitori dei servizi di comunicazione situati all'interno dell'Unione europea di procedere ad una conservazione generalizzata dei dati relativi al traffico e all'ubicazione,[40] la prevenzione di minacce alla sicurezza pubblica autorizza le autorità nazionali a ingiungere loro solo il prolungamento, peraltro a tempo determinato, della conservazione dei dati accumulati per ragioni di fatturazione o al fine di offrire servizi di valore aggiunto. La prevenzione, la ricerca, l'accertamento e il perseguimento di reati legittima invece ingerenze nei diritti fondamentali comuni che non presentano un carattere grave,[41] il che pare accedere nel caso di divulgazione a terzi dei dati già raccolti in virtù delle regole di minimizzazione previste dalla direttiva *e-privacy* (artt. 5, 6 e 8 della stessa).

5. Come già anticipato, l'accesso ai dati di ubicazione o relativi al traffico da parte delle autorità di soccorso, di polizia e giurisdizionali può avvenire in modo non solo mediato, ma anche diretto, ossia mediante l'impiego da parte di queste ultime di appositi strumenti di localizzazione e di intercettazione nella disponibilità delle stesse. Posto tuttavia che, in tal caso, i dati sono acquisiti senza la collaborazione dei fornitori dei servizi di comunicazione, la facoltà, ed eventualmente le condizioni, di accesso diretto agli stessi da parte delle predette autorità pubbliche non sono certamente disciplinate dalla direttiva *e-privacy*. Quest'ultima regola il trattamento dei dati solo se effettuato dai predetti fornitori, cosicché l'assenza di questo elemento collaborativo determina l'inapplicabilità dell'atto UE in discussione.

Questa ricostruzione trova indiretta conferma nelle già menzionate sentenze *Privacy International* e *La Quadrature du Net*, seppur con riguardo all'accesso diretto ai dati da parte dei servizi di *intelligence* di taluni Stati membri (Regno Unito, Francia e Belgio) al fine di salvaguardare la sicurezza nazionale. Secondo la Corte di giustizia, mentre le legislazioni interne che disciplinano l'accesso mediato ai dati rientrano nella sfera attuativa della direttiva *e-privacy*, quelle che regolano l'acquisizione diretta degli stessi sono comprese nell'ambito applicativo del diritto nazionale (e dunque CEDU) per effetto dell'art. 4, par. 2, TUE.[42] Pur non concordando pienamente con i giudici dell'Unione quanto a tale seconda valutazione allorché l'operazione riguardi dati "vecchi", ossia conservati nelle banche dati dei fornitori di servizi di comunicazione o in transito da un operatore ad un altro, i quali paiono rientrare nell'ambito

[39] Corte giust. *La Quadrature du Net* cit., punti 136-140; *G.D.* cit., punto 56; *SpaceNet* cit., punto 71.
[40] Corte giust. *La Quadrature du Net* cit., punto 168; *G.D.* cit., punti 57-58; *SpaceNet* cit., punto 72. Ciò purché lo Stato membro interessato affronti una minaccia *grave e reale* per la sicurezza nazionale, nonché il provvedimento che prevede tale ingiunzione possa essere oggetto di un controllo effettivo da parte di un giudice o un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante.
[41] Corte giust. *La Quadrature du Net* cit., punto 140; *G.D.* cit., punto 59; *SpaceNet* cit., punto 73.
[42] Corte giust., *La Quadrature du Net* cit., punto 103; *Privacy International* cit., punto 48.

applicativo della direttiva *e-privacy*,[43] l'esclusione dalla sfera attuativa di quest'ultima dell'accesso diretto ai dati quantomeno "nuovi" da parte di autorità pubbliche (e dunque anche di quelle di soccorso, polizia ovvero giurisdizionali coinvolte nella ricerca di persone scomparse) appare invero condivisibile. In tal caso, l'acquisizione dei dati è effettuata dalle predette autorità attraverso autonomi strumenti di localizzazione e intercettazione, cosicché, prescindendo dalla divulgazione degli stessi da parte dei fornitori dei servizi di comunicazione, essa difetterebbe di un contatto soggettivo con la disciplina della direttiva *e-privacy*, ossia la mediazione di questi ultimi nell'accesso ai dati. Anche presupponendo poi che tali autorità, impiegando proprie tecnologie, sfruttino le reti di comunicazione dei predetti operatori (così, ad esempio, nel caso dell'invio di messaggi che consentono la trasmissione automatica della posizione dell'apparecchio terminale o del veicolo di un utente), essi non accederebbero in ogni caso a dati "vecchi". La fattispecie in esame, nella misura in cui prevede l'uso della rete al fine di ricavare dati alternativi rispetto a quelli già nella disponibilità dei predetti operatori, mancherebbe allora anche dell'elemento di contatto oggettivo con la disciplina della direttiva *e-privacy*, ossia l'accesso a dati invece già raccolti dai fornitori dei servizi di comunicazione o in transito da un operatore a un altro, in tal modo dovendo essere a maggior ragione esclusa dell'ambito attuativo della stessa.

A differenza tuttavia di quanto affermato dai giudici di Lussemburgo nelle pronunce *Privacy International* e *La Quadrature du Net* relativamente ai servizi di sorveglianza degli Stati membri, l'accesso diretto a dati "nuovi" quantomeno da parte delle autorità di soccorso, di polizia ovvero giurisdizionali coinvolte nella ricerca degli scomparsi non rientra nell'ambito attuativo del diritto interno e CEDU, ma invece in quello dell'Unione europea e, più in particolare, di quello del GDPR o della direttiva LED, a seconda del soggetto pubblico autorizzato ad accedere ai dati. In particolare, il GDPR disciplina ogni trattamento di dati – e dunque anche l'accesso agli stessi – posto in essere non solo da ogni persona fisica e giuridica, ma anche da ogni autorità pubblica (artt. 2, par. 1, e 4, parr. 2, 7 e 8 GDPR) purché diversa da quelle che operano in materia penale e di sicurezza nazionale.[44] I trattamenti di dati realizzati da queste ultime con riguardo a dati "nuovi" raccolti con propri mezzi di intercettazione rientrano in effetti nell'ambito attuativo del diritto interno e CEDU per effetto dell'art. 2, par. 2, lett. *a)* GDPR, il quale esclude dalla sfera attuativa di quest'ultimo i trattamenti «effettuati per attività che non rientrano nell'ambito di applicazione del diritto» UE e dunque, anche alla luce del considerando 16 GDPR, di quelle «riguardanti la sicurezza nazionale». Seppur impiegando la dicitura di sicurezza «dello Stato» – la quale è in ogni caso sinonimo di «nazionale» (art. 15 direttiva *e-privacy*) – quest'ultima esclude parimenti dal proprio ambito di applicazione le attività securitarie (art. 1, par. 3). Le esclusioni dell'art. 2, par. 2, lett. *a)* GDPR

[43] In tal senso, si permetta di rinviare all'analisi svolta in S. CRESPI, *L'influenza del diritto dell'Unione europea sulla sicurezza nazionale* cit., spec. p. 101 ss.

[44] Sull'art. 2 GDPR, H. KRANENBORG, *Article 2*, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY (eds), *The EU General Data Protection Regulation* cit., p. 60 ss. , spec. pp. 69-70, nonché ID., *Article 8*, in S. PEERS, T. HERVEY, J. KENNER, A. WARD (eds.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford, 2021. Piu in generale sulla divisione di competenze UE e nazionali, S. GARBEN, I. GOVAERE (eds.), *The Division of Competences between the EU and the Member States. Reflections on the Past, the Present and the Future*, Oxford, 2017, spec. il contributo di C. TIMMERMANS, *The Competence Divide of the Lisbon Treaty Six Years After*, p. 19 ss. Quanto all'art. 4, parr. 2, 7 e 8, GDPR, L.A. BYGRAVE, L. TOSONI, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY (eds), *The EU General Data Protection Regulation* cit., p. 116 ss.

e dell'art. 1, par. 3, della direttiva *e-privacy* riproducono così a livello derivato il contenuto dell'art. 4, par. 2, TUE, il quale attribuisce alla competenza interna e dunque CEDU) la materia della sicurezza nazionale.[45] In tale ambito, il diritto comune (GDPR e i principi comuni di necessità e proporzionalità) è allora applicabile solo in via residuale, ossia al fine di escludere abusi della competenza degli Stati membri in materia di sicurezza nazionale, nonché salvaguardare l'effetto utile della disciplina UE in materia di tutela dei dati personali.[46]

Sono inoltre parimenti esclusi dall'ambito applicativo del GDPR i trattamenti di dati – e dunque l'accesso agli stessi – effettuati dalle autorità operanti in ambito penale, prevedendo l'art. 2, par. 2, lett. *d)* GDPR che il regolamento generale in materia di *privacy* «non si applic[hi per l'appunto] ai trattamenti di dati effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati od esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse». Tale esclusione si spiega in ragione dell'inclusione di questi aspetti nella direttiva LED, la quale è ivi applicabile quale *lex specialis*. In tale ambito, il GDPR può allora operare esclusivamente in via residuale per le questioni non regolate dalla direttiva LED o allorché quest'ultima richiami o rinvii al primo così come accade, ad esempio, ai considerando 11, 12 e 34 e l'art. 9 della direttiva LED ove si dice che «il trattamento dei dati effettuato dalle autorità competenti nella prevenzione, indagine, accertamento o perseguimento di reati per finalità ulteriori rientri nell'ambito applicativo del GDPR».[47]

In tale contesto a geometria variabile soggettiva, mentre allora sono disciplinati dalla direttiva LED l'accesso e, se del caso, le condizioni alle quali le autorità di polizia e giurisdizionali operanti in ambito penale possono acquisire in via diretta dati "nuovi" di ubicazione e relativi al traffico tra l'altro in occasione della ricerca di persone scomparse, il GDPR regola tali aspetti quanto alle autorità pubbliche diverse da quelle operanti nella sfera attuativa della direttiva LED (ambito penale) e dell'art. 4, par. 2, TUE (sicurezza nazionale) e dunque tra l'altro con riguardo a quelle di primo soccorso.

---

[45] Su tale norma dei trattati, G. MARTINICO, *What lies behind article 4(2) TEU?*, in A.S. ARNAIZ, C.A. LLIVINA (eds.), *National Constitutional Identity and European Integration*, 2013, p. 93 ss; ID., *Taming National Identity: A Systematic Understanding of Article 4.2 TEU*, in *European Public Law*, 2021, n. 3, p. 447 ss.; T. TRIDIMAS, *The General Principles of EU Law*, Oxford, 3rd ed., 2013; G. DI FEDERICO, *L'identità nazionale degli Stati membri nel diritto dell'Unione europea. Natura e portata dell'art. 4, par. 2, TUE*, Napoli, 2017; ID., *Il ruolo dell'art. 4, par. 2, TUE nella soluzione dei conflitti interordinamentali*, in *Quaderni costituzionali*, fasc. 2, 2019, p. 333 ss.; A. KACZOROWSKA-IRELAND, *What Is the European Union required to Respect under Article 4(2) TEU?: The Uniqueness Approach*, in *European Public Law*, 2019, vol. 25, p. 57 ss.; B. DE WITTE, *Article 4(2) TEU as a Protection of the Institutional Diversity of the Member States*, in *European Public Law*, 2021, n. 3, p. 559 ss.; M. CLAES, *National Identity and the Protection of Fundamental Rights*, in *European Public Law*, 2021, vol. 27, p. 517 ss. Più in generale sull'equilibrio tra diritto UE e diritto interno, M.E. BARTOLONI, *Ambito di applicazione del Diritto dell'Unione europea e ordinamenti nazionali. Una questione aperta*, Napoli, 2018, spec. p. 224 ss.

[46] In merito, S. CRESPI, *L'influenza del diritto dell'Unione europea sulla sicurezza nazionale* cit., spec. p. 101 ss.

[47] In tal senso, L. GEORGIEVA, *Article 10. Processing of personal data relating to criminal convinctions and offences*, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY (eds), *The EU General Data Protection Regulation* cit., p. 385 ss., spec. p. 389; nonché FRA (*European Union Agency for Fundamental Rights*), EUROPEAN COURT OF HUMAN RIGHTS, COUNCIL OF EUROPE, AND EUROPEAN DATA PROTECTION SUPERVISOR (eds.), *Hanbook on European Data Protection Law*, Bruxelles, 2018, spec. p. 282. Il par. 2 dell'art. 2 GDPR esclude dal proprio ambito di applicazioni anche i trattamenti dei dati personali UE nell'ambito PESC («b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE»), nonché « c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico».

6. La facoltà delle autorità di soccorso di raccogliere, conservare e poi usare i dati di ubicazione attraverso proprie applicazioni di localizzazione sembra permessa dall'art. 6 GDPR, il quale elenca le basi giuridiche (lett. *a)-f)*) che giustificano il trattamento dei dati da parte di ogni persona ed autorità rientrante nell'ambito di applicazione soggettivo dello stesso.[48] In particolare, il par. 1, lett. *d*) dell'art. 6 GDPR stabilisce che tali operazioni sono lecite allorché «è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica».[49] Tale motivazione è richiamata anche all'art. 9, par. 2, let. *c*) GDPR per giustificare il trattamento di dati particolarmente sensibili, ossia quelli che rivelano l'origine etnica o razziale, le opinioni politiche, le convinzioni religiose, l'appartenenza sindacale, nonché trattano dati genetici, biometrici o relativi alla salute, il quale è di regola vietato (par 1 dell'art. 9 GDPR).[50] Analogamente, i trasferimenti di dati UE verso paesi terzi od organizzazioni internazionali, in linea di principio permessi solo quando la Commissione europea abbia adottato una decisione di adeguatezza (art. 45 GDPR) o in presenza di appropriate garanzie alternative (art. 46 GDPR), sono eccezionalmente permessi allorché ciò «sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso» (art. 49 GDPR).[51]

Anche alla luce dei considerando 46 e 112 GDPR che qualificano gli «interessi vitali» come «un interesse essenziale per la vita», gli artt. 6, 9 e 49 GDPR paiono allora giustificare a buon diritto una compressione del diritto alla protezione dei dati e della *privacy* previsti agli art. 7 e 8 della Carta – come si avrà modo di vedere nel prosieguo, in ogni caso solo proporzionata e laddove necessario – al fine di garantire il rispetto del diritto, parimenti fondamentale, alla vita di cui all'art. 2 della stessa. Posto che anche la ricerca degli scomparsi è volta a tutelare quest'ultimo bene giuridico, essa sembra allora rientrare a giusto titolo nella nozione di «interessi vitali», in tal modo giustificando, pur se ancora una volta a determinate condizioni di equilibrio UE, l'accesso in via diretta ai dati (solo) di ubicazione da parte delle autorità di soccorso, quelli relativi al traffico esorbitando le funzione delle autorità pubbliche oggetto di analisi nel presente paragrafo. L'art. 6 GDPR riguarda peraltro *ogni* trattamento di dati personali, cosicché esso pare motivare l'uso del par. 1, lett. *d*) dello stesso anche relativamente ai dati relativi al traffico, seppur con riguardo ad autorità pubbliche diverse da quelle di soccorso rientranti nell'ambito attuativo del GDPR. Né invero a una diversa conclusione sembra condurre il fatto che, anche in ragione della natura derogatoria degli artt. 6, 9 e 49 GDPR, il trattamento dei dati su tali basi possa effettuarsi esclusivamente nel caso di un pericolo di vita concreto ed imminente per l'interessato o per un'altra persona fisica. L'improvvisa e inspiegabile irreperibilità di un individuo può, infatti, sottintendere proprio un tale rischio.

L'applicabilità delle disposizioni in esame nel caso di specie non sembra neppure esclusa dalla circostanza che quantomeno gli artt. 9, par. 2, let. c) (dati sensibili) e 49, par. 1, let. f)

---

[48] W. KOTSCHY, *Article 6. Lawfulness of proceeding*, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY, *The EU General Data Protection Regulation* cit., p. 321 ss.

[49] Sull'uso di questa norma per la localizzazione da parte delle organizzazioni non governative (NGO) nelle operazioni di salvataggio per ragioni umanitarie, T. GAZI, *Data to the rescue* cit.

[50] Sull'art. 9 GDPR, L. GEORGIEVA, C. KUNER, *Article 9. Processing of special categories of personal data*, in in C. KUNER, L.A. BYGRAVE, C. DOCKSEY, *The EU General Data Protection Regulation* cit., p. 365 ss., spec. pp. 377-378.

[51] Su tale disposizione, C. KUNER, *Article 49. Derogations for specific situations*, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY (EDS.), *The EU General Data Protection Regulation* cit., p. 841 ss., spec. p. 852.

(trasferimento internazionale di dati) GDPR subordinino espressamente l'uso di queste basi giuridiche al previo accertamento dell'incapacità fisica (ad esempio, una grave malattia) o giuridica (ad esempio, nel caso di minori o di incapaci) dell'interessato di prestare il proprio specifico consenso («qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il consenso»).[52] Anche quando, come pare corretto fare, si ritenga quest'ultima condizione applicabile perfino alla let. *d)* del par. 1 dell'art. 6 GDPR (legittimità del trattamento dei dati), la quale manca di una analoga precisazione,[53] l'accertamento di quest'ultima non sembra porre difficoltà applicative nei casi di irreperibilità di un individuo, l'incapacità fisica e/o giuridica dell'interessato di apporre il proprio previo consenso al trattamento dei dati essendo connaturata all'inspiegabile (e dunque non volontaria) scomparsa dello stesso. Se peraltro la prova della predetta incapacità permette, ai sensi dell'art. 9, par. 2, let. *c)* GDPR, a taluni enti (ospedali) che raccolgono dati sensibili (stato di salute psico-fisico) di comunicarli a terzi (forze di polizia) in caso di rischio degli interessi vitali di un individuo,[54] essa deve a maggior ragione consentire la divulgazione a terzi (autorità di soccorso) di dati meno sensibili (quelli di ubicazione) oggetto dell'art. 6 GDPR.

Il considerando 46 GDPR esclude inoltre l'uso della let. *d)*, par. 1 dell'art. 6 GDPR qualora il trattamento dei dati possa essere «manifestamente» fondato su un'altra base giuridica. La ricerca degli scomparsi anche mediante l'accesso diretto ai dati di ubicazione da parte delle autorità di soccorso non pare tuttavia poter essere meglio fondata su basi giuridiche alternative all'art. 6, par. 1, let. *d)* GDPR. Non sembra, ad esempio, esserlo l'art. 6, par. 1, let. *e*) GDPR, il quale prevede che il trattamento dei dati è lecito se «necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento», e ciò sebbene l'incapacità di risalire alla sorte di individui irreperibili crei un indubbio nocumento alla collettività. La ricerca degli scomparsi ha come obiettivo principale la salvaguardia della vita dei singoli, quello della protezione dell'interesse collettivo alla ricostruzione della sorte degli stessi essendo un effetto solo secondario. In tale contesto, la base giuridica privilegiata per fondare l'accesso ai dati di ubicazione di un individuo in caso di scomparsa sembra allora essere quella preordinata a tutelare gli interessi vitali di un certo soggetto (art. 6, par. 1, let. *d)* GDPR) rispetto a quella che invece mira alla tutela di un interesse collettivo (art. 6, par. 1, let. *e*) GDPR). Ciò pare a maggior ragione vero posto che, come già ricordato, il considerando 46 GDPR esclude l'uso della let. *d)*, par. 1 dell'art. 6 GDPR solo qualora il trattamento dei dati possa essere «*manifestamente*» fondato su un'altra base giuridica, il che non accade, quantomeno con tale grado di certezza, nel caso in esame. La potenziale

[52] Secondo, W. KOTSCHY, *Article 6. Lawfulness of proceeding* cit, p. 321 ss., spec. p. 334, tale condizione non pare invero applicabile nel caso l'interesse vitale in discussione sia quello di una terza persona. Diversamente, un certo individuo potrebbe, autorizzando o meno l'accesso ai propri dati, influire sulla vita o la morte di altri soggetti. In tal senso anche l'*European Data Protection Board* (EDPB) e l'*European Data Protection Supervisor* (EDPS), *Joint Response to LIBE Commitee on the impact of the US Cloud Act on the Eyropean Legal Framework for personal data protection*, del 10 luglio 2019, spec. p. 4 con riguardo al trattamento dei dati personali UE nell'ambito del trasferimento internazionale negli USA.

[53] Così, seppur con riferimento all'art. 49 GDPR, C. KUNER, *Article 49* cit., spec. p. 852. In tal senso, EDPB, *Guidelines 2/2018 on Derogation of Article 49 under Regulation 2016/679*, del 25 maggio 2018, spec. p. 13.

[54] In tal senso, la *National Crime Agency* del Regno Unito, *Police information requests to NHS Organisations, GPs and other healthcare providers in respect of potential homicide investigation, proof of life enquiries and more general enquiries to trace missing persons*, disponibile sul sito web https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/802433/Information_sharing_between_police_and_health_and_care.pdf

sovrapposizione tra le fattispecie di cui alle lett. *d*) ed *e)* del par. 1 dell'art. 6 GDPR è peraltro riconosciuta dallo stesso legislatore europeo, i considerando 46 e 112 GDPR prevedendo proprio che «alcuni tipi di trattamento di dati [– quelli, ad esempio, necessari a fini umanitari per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione, in casi di emergenze umanitarie e catastrofi di origine naturale e umana –] possono rispondere sia agli interessi vitali dell'interessato [(let. *d)*)] sia a motivi di interesse pubblico [(let. *e)*)] ».[55]

Non pare neppure che la ricerca degli scomparsi possa rientrare nell'ambito di applicazione dell'art. 6, par. 1, let. *f)*, il quale prevede che « il trattamento è lecito […se] è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi [...]». Per espressa previsione dell'art. 6, par. 1, GDPR, quest'ultimo «non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti» – in quanto esso è compreso nella lett. *e)* della medesima norma – il quale è così applicabile solo in ambito privatistico. Tale circostanza esclude allora l'applicabilità della norma in esame alle autorità di soccorso, le quali sono per l'appunto autorità pubbliche.

La legittimità dell'accesso diretto ai dati di ubicazione di uno scomparso da parte delle autorità di soccorso è stata peraltro ammessa dal nostro Garante nel provvedimento n. 3736199 del 22 gennaio 2015[56] quanto all'uso da parte del Corpo Nazionale Soccorso Alpino e Speleologico di apposite tecnologie – l'invio di messaggi che consentono la trasmissione automatica dei dati GPS dell'apparecchio terminale di un utente – che, rispetto a quelle autorizzate con il già menzionato provvedimento del 2008, avevano proprio «il pregio di non richiedere l'intermediazione dell'operatore telefonico e di rendere ancora più rapide ed efficienti le operazioni di soccorso, senza che ci [fosse] bisogno di una particolare configurazione del *software* del terminale». L'uso di questa tecnologia nel caso di specie, fondata sull'accesso diretto delle autorità di soccorso ai dati di ubicazione di un individuo, era giustificato dall'art. 24 del Codice italiano di protezione dei dati, il quale, abrogato a seguito dell'entrata in vigore del GDPR, aveva un contenuto analogo all'attuale art. 6 , par. 1, let. *d)* GDPR. Trasponendo nel nostro ordinamento l'art. 7 del precedente regime di tutela dei dati (ossia quello della già menzionata direttiva 95/46), l'art. 24 del predetto Codice italiano stabiliva, infatti, che il trattamento dei dati anche senza il consenso dell'interessato è possibile quando ciò è «necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il consenso per impossibilità fisica, incapacità di agire o incapacità di intendere o volere, il consenso è manifestato da chi esercita legalmente la potestà, o da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato». Considerata l'assonanza giuridica tra quest'ultimo e l'art. 6, par. 1, let. *d*) GDPR, è allora plausibile ritenere che il Garante italiano, qualora venisse nuovamente consultato quanto all'impiego di autonome tecnologie per la localizzazione di persone disperse tra l'altro in montagna da parte delle unità di soccorso, confermerebbe le conclusioni raggiunte nel

[55] Sulla difficoltà di distinguere queste due nozioni anche L. GEORGIEVA, C. KUNER, *Article 9* cit., spec. p. 378.
[56] Decisione n. 3736199 del Garante italiano della *privacy* del 22 gennaio 2015, *Utilizzo di tecnologie di geo-localizzazione di persone infortunate o disperse in montagna da parte del Corpo Nazionale Soccorso Alpino e Speleologico (CNSAS)*, reperibile sul sito del predetto Garante: Utilizzo di tecnologie di geolocalizzazione di persone infortunate o... - Garante Privacy.

provvedimento n. 3736199 del 2015, autorizzando l'accesso diretto ai dati da parte di queste ultime sulla base proprio dell'attuale art. 6, par. 1, let. *d*) GDPR.

Ulteriore conferma della legittimità di quest'ultima modalità di acquisizione dei dati pare poi doversi rintracciare nel regolamento 2015/758 del Parlamento europeo e del Consiglio e in quello delegato 2019/320 della Commissione europea, i quali prevedono regole comuni per la produzione rispettivamente di veicoli e telefoni cellulari già dotati di una apposita tecnologia (GNSS) che permette, in caso di pericolo (ad esempio, incidente stradale) e mediante un uso dei dati minimizzato, di avvertire i servizi di emergenza, trasmettendo in modo automatico la posizione dell'utente in difficoltà.[57] Almeno secondo il Garante europeo della protezione dei dati (EDPS),[58] l'impiego di questi strumenti di localizzazione è compatibile con la legislazione UE in materia di tutela dei dati personali e *privacy* in quanto esso è rispettoso dei principi UE di necessità e proporzionalità, nonché delle condizioni di misura previste all'art. 5 GDPR. Tale norma stabilisce che i dati «devono essere trattati in modo lecito, corretto e trasparente; raccolti per finalità determinate, esplicite e legittime, nonché trattati in modo coerente con queste finalità; essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati; esatti ed aggiornati, cosicché devono essere cancellati o rettificati tempestivamente i dati inesatti; conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti; trattati in maniera da garantire un'adeguata sicurezza dei dati».[59]

E in effetti, come si evince dal provvedimento n. 736199 del 2015 del Garante italiano, i dati raccolti dal nostro Corpo Nazionale Soccorso Alpino e Speleologico, proprio nel rispetto dell'art. 5 GDPR, devono riguardare solo la posizione geografica del terminale della persona dispersa, non potendo tali autorità avere accesso a dati relativi al traffico o ad altre tipologie di dati per natura eccedenti le finalità di soccorso e dunque non pertinenti; tali dati devono poi essere utilizzati soltanto per lo scopo di salvaguardare la vita o l'integrità fisica delle persone disperse, nonché esclusivamente quando siano state formalmente attivate le ricerche da parte

---

[57] Il regolamento 2015/758 del Parlamento europeo e del Consiglio del 29 aprile 2015 relativo ai requisiti di omologazione per lo sviluppo del sistema *eCall* di bordo basato sul servizio 112 (*GUUE* L 123 del 19.5.2015, pag. 77) è completato dal regolamento delegato 2017/79 della Commissione del 12 settembre 2016 che stabilisce in dettaglio prescrizioni tecniche e procedure di prova per l'omologazione dei veicoli per quanto riguarda i relativi sistemi *eCall* di bordo basati sul servizio 112 (*GUUE* L 12, 17.1.2017, p. 44-85). Il regolamento delegato 2019/320 della Commissione europea del 12 dicembre 2018 stabilisce invece regole comuni per la localizzazione del chiamante nelle comunicazioni di emergenza da dispositivi mobili (*GUUE* L 55/1 del 25 febbraio 2019). Per prossimi cambiamenti in merito, v. la proposta di regolamento delegato della Commissione europea del 16 dicembre 2022 (SWD(2022)430 final). In dottrina quanto al regolamento 2015/758, T.H.A. WISMAN, *eCall and the Quest for Effective Protection of the Right to Privacy*, in EDPL 1/2016, p. 59 ss.

[58] In tal senso, *l'European Data Protection Supervisor* (EDPS), *Comments on the Commission Recommendation and the accompanying impact assessment on the implementation of the harmonised EU-wide in-vehicle emergency call ("eCall")*, https://edps.europa.eu/sites/edp/files/publication/11-12-12_ecall_en.pdf; ID., *Formal comments on the draft Commission Delegated Regulation supplementing Directive (EU) 2018/1972 of the European Parliament and of the Council with measures to ensure effective access to emergency services through emergency communications to the single European emergency number '112'*, https://edps.europa.eu/system/files/2022-11/2022-1092_draft_formal_comments_en.pdf

[59] In dottrina, C. DE TERWANGNE, *Article 5. Principles relating to processing of personal data*, in C. KUNER, L.A. BYGRAVE, C. DOCKSEY (EDS.), *The EU General Data Protection Regulation* cit., spec. p. 309 ss.; W. KOTSCHY, *The proposal for a new General Data Protection Regulation – Problems Solved?*, in *International Data Privacy Law*, 2014, p. 274 ss. Quanto a questi aspetti ma nel regime precedente di cui alla direttiva 95/46 già cit., M.E. BOULANGER ET AL., *La protection des données è caractère personnel en droit communautaire*, in *Journal des tribunaux. Droit européen*, 1997, p. 145 ss.

delle centrali operative del 118 (Sanità), 115 (Vigili del fuoco) o delle autorità di pubblica sicurezza; i dati devono inoltre essere raccolti unicamente da parte del personale delle autorità di soccorso appositamente incaricate delle ricerche; le tecnologie di localizzazione devono essere attivate sull'apparecchio dei dispersi esclusivamente per il tempo necessario all'individuazione dell'apparecchio terminale, dovendo i dati raccolti essere inibiti una volta realizzato l'intervento di soccorso. Analogamente, i regolamenti 2015/758 e 2019/320 prevedono che i dati di ubicazione raccolti possano essere usati esclusivamente per affrontare situazioni di emergenza; siano conservati solo per il periodo di tempo necessario a gestire l'emergenza e siano in ogni caso immediatamente cancellati una volta conclusa la situazione di pericolo. Le aziende produttrici devono inoltre garantire che il sistema non sia tracciabile né oggetto di controllo costante; che i dati personali siano automaticamente e costantemente eliminati dalla memoria interna del sistema; e che le informazioni sull'uso dei dati siano incluse nel manuale di istruzioni del conducente.

Al fine di garantire la massima tutela dei dati personali degli individui potrebbero ritenersi applicabili alla let. *d)* dell'art. 6, par. 1, GDPR anche le condizioni esplicitamente previste – e dunque probabilmente circoscritte – al par. 3 dell'art. 6 e dall'art. 21 GDPR quanto ai trattamenti di dati basati rispettivamente sulle lett. *e)* ed *f)* del par. 1 dell'art. 6 GDPR. In particolare, il par. 3 dell'art. 6 GDPR richiede che «la base su cui si fonda il trattamento dei dati di cui al par. 1, let. […] *e)*, deve essere stabilita dal diritto UE o da quello dello Stato membro cui è soggetto il titolare del trattamento», la quale deve definire la finalità del trattamento, le tipologie di dati oggetto dello stesso, i soggetti a cui possono essere comunicati i dati e le finalità per cui essi sono comunicati, le limitazioni della finalità, i periodi di conservazione, nonché le procedure di trattamento. L'art. 21 GDPR garantisce all'interessato «il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati che lo riguardano ai sensi dell'art. 6, par. 1, lett. *e)* o *f)* […]».

7. Quanto all'accesso diretto ai dati di ubicazione e, questa volta anche di quelli, relativi al traffico di uno scomparso da parte delle autorità di polizia e giurisdizionali è stato già osservato come il considerando 35 e l'art. 8 della direttiva LED stabiliscono che «per essere lecito, il trattamento dei dati dovrebbe essere necessario per l'esecuzione di un compito svolto nell'interesse pubblico da un'autorità competente a fini della prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, [e che] tali attività dovrebbero comprendere la salvaguardia degli interessi vitali dell'interessato». Similmente all'art. 6, par. 1, let. *d)* GDPR quanto alle autorità di soccorso, tale esigenza giustifica così l'acquisizione in via diretta dei dati da parte delle autorità pubbliche operanti in ambito penale. L'improvvisa irreperibilità di una persona ben può sottintendere una minaccia agli interessi vitali di quest'ultima, cosicché la ricerca dello scomparso anche mediante l'uso della tecnologia rientra nell'ambito attuativo della direttiva LED ed è in linea di principio autorizzato dall'art. 8 della stessa. A differenza di quanto osservato con le autorità di soccorso, quelle operanti in ambito penale possono peraltro accedere, su tale base giuridica, ai dati non solo di ubicazione ma anche relativi al traffico.

Né invero a una diversa conclusione pare dover indurre il fatto che, nell'ambito della discrezionalità lasciata dal legislatore UE a quello nazionale («…tali attività *dovrebbero*

comprendere la salvaguardia degli interessi vitali dell'interessato»), l'art. 5 del d.leg. n. 51 del 18 maggio 2018, che ha trasposto in Italia la direttiva LED, un po' sorprendentemente non abbia riprodotto l'inciso inerente la salvaguardia degli interessi vitali dell'interessato di cui al considerando 35 e all'art. 8 della predetta direttiva. Quest'ultimo è invece previsto – e pare allora circoscritto – quanto al trattamento di particolari categorie di dati, ossia quelli che rivelano l'origine etnica e razzale, le opinioni politiche, le convinzioni religiose, l'appartenenza sindacale di cui all'art. 10 della direttiva LED e all'art. 7 del d.leg. n. 51 del 18 maggio 2018, nonché al trasferimento internazionale di dati UE in mancanza di una decisione di adeguatezza o di appropriate garanzie alternative di cui all'art. 38 della direttiva LED e all'art. 34 del d.leg. n. 51 del 18 maggio 2018. Se in effetti la necessità di tutelare gli interessi vitali dell'interessato permette di derogare a divieti di trattamento di dati in casi particolarmente delicati – l'uso di dati sensibili o il trasferimento di ogni dato UE in paesi extra-UE con un livello di tutela della *privacy* e dei dati più basso di quello europeo – tale esigenza sembra allora giustificare a maggior ragione una dispensa dal, certamente meno grave, trattamento dei dati allorché l'interessato sia o si sospetti essere in condizioni di emergenza.

In attesa della modifica del quadro legislativo italiano così da adeguarlo ai (invero legittimi) *desiderata* UE, l'obbligo di interpretare il diritto interno conformemente a quello derivato comune dovrebbe permettere di autorizzare in ogni caso il trattamento dei dati dello scomparso anche senza il consenso di questo ultimo in virtù e alle condizioni di cui all'art. 8 della direttiva LED, in tal modo evitando il vuoto giuridico che si creerebbe in caso di scomparsa.[60] Ciò permetterebbe inoltre di allineare il contenuto della direttiva LED a quello del GDPR, il quale prevede, con norme in questo caso direttamente applicabili negli ordinamenti giuridici nazionali che non lasciano quindi spazio alla discrezionalità degli Stati membri, la correlazione tra il trattamento legittimo dei dati personali e la necessità di salvaguardare gli interessi vitali degli individui.

Non diversamente poi da quanto già osservato relativamente al GDPR, il rischio di un uso troppo disinvolto da parte delle autorità in materia penale delle norme in esame – e dunque dell'accesso diretto ai dati di ubicazione e relativi al traffico degli individui – è compensato dall'applicabilità, anche quanto alla direttiva in esame, dei principi UE di necessità e proporzionalità di cui tra l'altro all'art. 4 della direttiva LED. Analogamente all'art. 5 GDPR, questa norma stabilisce, infatti, che «gli Stati membri dispongono che i dati siano trattati in modo lecito e corretto; siano raccolti per finalità determinate, esplicite e legittime, nonché siano trattati in modo non incompatibile con tali finalità; i dati devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati; esatti ed aggiornati, cosicché devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti; conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; trattati in modo da garantire un'adeguata sicurezza dei dati personali. Infine, il trattamento dei dati per una finalità diversa da quella per cui questi ultimi sono stati raccolti, è consentito solo nella misura

[60] Sull'obbligo di interpretazione conforme, Corte giust. 13 novembre 1990, C-106/89, *Marleasing SA contro La Comercial Internacional de Alimentación SA*, ECLI:EU:C:1990:395. Per un commento a questa pronuncial storica, P. MEAD, *The Obligation to Apply European law: Is Duke Dead?*, in *European Law Review*, 1991, p. 490 ss.; A. BERNARDI (a cura di), *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico*, Napoli, 2015.

in cui il titolare del trattamento sia stato autorizzato in tal senso dal UE o nazionale, nonché quando il trattamento è necessario e proporzionato».

8. L'analisi, anche alla luce della giurisprudenza UE e della prassi decisionale del nostro Garante, delle pertinenti disposizioni del GDPR, della direttiva LED e di quella *e-privacy* sembra dissipare l'equivoco emerso nella predetta trasmissione televisiva che pareva escludere *in toto* la possibilità di usare i dati di ubicazione e/o relativi al traffico per cercare persone immotivatamente e inaspettatamente irreperibili. Pur se a determinate condizioni di garanzia, la legislazione UE in materia di protezione dei dati personali permette, infatti, l'accesso da parte delle autorità pubbliche coinvolte nella ricerca degli scomparsi (di soccorso, di polizia o giurisdizionali) ai dati di questi ultimi, peraltro relativi sia al traffico sia all'ubicazione, non solo in forma mediata ma anche in via diretta. Ciò è invero comprensibile dato che il sistema comune non concepisce il diritto alla *privacy* e alla tutela dei personali di cui alla Carta come un diritto assoluto, senza cioè prendere in esame la naturale – e invero necessaria – interferenza di quest'ultimo con altri diritti anche fondamentali (ad esempio, la libertà d'impresa, d'espressione, il diritto alla salute o quello alla vita) o importanti esigenze pubbliche (ad esempio, la ricerca scientifica; la salvaguardia della sicurezza nazionale, la sicurezza pubblica, le attività in ambito penale). La legislazione comune che dà attuazione agli artt. 7 e 8 della Carta (GDPR, direttive LED ed *e-privacy*) è anzi proprio volta a bilanciare, già a livello normativo e attraverso principi UE ispirati all'equilibrio e alla ragionevolezza (*rectius*: di necessità e proporzionalità), il primo con i secondi in caso di frizioni o conflitti.

L'analisi svolta mette inoltre in luce la complessiva coerenza del sistema UE quanto alle modalità e alle condizioni di accesso ai dati da parte delle diverse autorità pubbliche coinvolte nelle ricerche degli scomparsi. Anche quando queste ultime sono regolate da atti UE differenti per ragioni vuoi soggettive vuoi oggettive, il che non rende sempre agevole la lettura e la comprensione del sistema nel suo insieme, la disciplina di questi profili risulta tendenzialmente logica, garantendone una sufficiente prevedibilità applicativa per le autorità pubbliche ed i cittadini europei. In attesa di intervento legislativo UE più puntuale che, anche attraverso un miglior coordinamento degli artt. 10 e 15 della direttiva *e-privacy*, permetta l'uso, seppur circoscritto, anche dei dati relativi al traffico per la ricerca delle persone scomparse tra l'altro in situazioni non penalmente rilevanti, l'uso della tecnologia e dei relativi dati è allora lasciata ad un apprezzamento fattuale da parte delle predette autorità pubbliche, da condursi caso per caso secondo criteri di misura (*rectius*: di necessità e di proporzionalità) in grado di escludere tanto abusi dei diritti fondamentali UE della *privacy* e alla protezione dei dati, quanto un impiego troppo parsimonioso di questi ultimi nella ricerca delle persone scomparse.