PASQUALE COSTANZO

NOTE PRELIMINARI SULLO STATUTO GIURIDICO DELLA GEOLOCALIZZAZIONE (A MARGINE DI RECENTI SVILUPPI GIURISPRUDENZIALI E LEGISLATIVI)

SOMMARIO: 1. Premessa. — 2. Il GPS sul tavolo delle Corti. — 3. La soluzione francese. — 4. Alcune conclusioni sul quadro italiano.

1. Premessa.

Con la l. n. 2014-372 del 28 marzo 2014, la Francia s'è dotata di una disciplina specifica delle attività di geolocalizzazione, quando svolte nel corso di indagini giudiziarie. Nell'ordinamento transalpino, infatti, tali attività erano in precedenza assoggettate solo alle più generiche disposizioni del codice di procedura penale, mentre, in via ordinaria, al fenomeno erano e restano applicabili le previsioni recate dalle normative di tutela della *privacy*. In questo quadro, il riferimento più immediato va, infatti, operato all'art. 34-1, c. 5, del Codice francese delle poste e delle comunicazioni elettroniche, che concerne il divieto sia di utilizzazione dei dati in grado di localizzare il terminale comunicativo di un utente proprio nel bel mezzo della comunicazione (cd. tempo reale) se non esclusivamente per le ragioni tecniche necessarie ad instradare la comunicazione medesima, sia di trattamento dei relativi dati senza il consenso informato dell'utente (non meno pertinente resta la più specifica disciplina del trattamento dati: dalle condizioni della sua correttezza al cd. diritto all'oblio, passando per il diritto di opposizione [1]).

La nuova legge francese offre, peraltro, un ulteriore spunto d'interesse, dal momento che, della questione della sua legittimità

* Il presente scritto è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

** Questo scritto è destinato agli studi per Maurizio Pedrazza Gorlero.

[1] Nell'ordinamento francese, cfr., principalmente, la legge n. 78-17, relativa all'informatica, alle banche dati e alle libertà, del 6 gennaio 1978, e la legge n. 2004-575, per l'affidamento sull'economia digitale, del 21 giugno 2004.

costituzionale, è stato investito il *Conseil constitutionnel* che, con la decisione n. 2014/693 DC del 25 marzo 2014, ha risposto ai sessanta deputati ricorrenti, i quali, pur facendo solidalmente parte della maggioranza governativa favorevole al testo, avevano manifestato, dalla cd. via *a priori* [2], apprensioni nei confronti di parte della legge: in ciò, per vero, sostenuti dallo stesso Ministro Guardasigilli, cui si doveva il relativo progetto [3].

Quanto alla geolocalizzazione (il lemma è uno dei non pochi neologismi prodotti dall'imporsi delle più recenti tecnologie comunicative), è, probabilmente, appena il caso di ricordare che essa consiste nell'attività e nel risultato dell'applicazione di tecnologie capaci di determinare, con un (sempre più) trascurabile margine di approssimazione, l'ubicazione nello spazio di un oggetto o di una persona, principalmente attraverso un sistema di posizionamento satellitare (*Global Positioning System* - GPS) o mediante la rete cellulare (*Global System Mobiles* - GSM). Operazioni, queste, che, realizzandosi a mezzo della rete telecomunicativa (*General Packet Radio Service* - GPRS; o *Universal Mobile Telecommunication Services* - UMTS), consentono anche l'invio al terminale dell'utente geolocalizzato di informazioni concernenti rotte di viaggio (cd. sistemi *Automated Vehicle Location* - AVL), itinerari turistici, aggiornamenti meteorologici, ecc., rivelandosi particolarmente preziose per la predetta rilevazione "in tempo reale" della posizione di persone e di veicoli (cd. sistemi *Automatic Vehicle Monitoring* - AVM) [4].

A dispetto di una simile complessità, la geolocalizzazione ha, com'è noto, cessato di appartenere solo ad ambiti specialistici, riguardando ormai "passivamente" situazioni del tutto abituali,

[2] Ossia l'impugnativa delle leggi prima della stessa promulgazione (cfr., *amplius*, *infra*, al par. 3).

[3] L'iniziativa legislativa è stata particolarmente seguita dal Guardasigilli Christiane Taubira, fruendo, altresì, della procedura accelerata: varato in Consiglio dei Ministri il 23 dicembre 2013, il d.d.l. è stato approvato in via definitiva l'11 febbraio 2014.

[4] Anche se la necessità di sapere dove ci si trova può dirsi sorta con l'uomo stesso non appena abbandonata l'esperienza sedentaria, la geolocalizzazione di cui si tratta è alquanto recente, essendo stata concepita anch'essa, come internet, negli anni '60 e sviluppata negli anni '70, nel quadro della difesa militare degli Stati Uniti, i quali, non casualmente, restano i proprietari del sistema satellitare di riferimento. Questo, tuttavia, dal 1980, è liberamente accessibile, per usi civili, da chiunque sia dotato di un ricevitore idoneo. I satelliti GPS trasmettono due segnali radio a bassa potenza, designati L1 e L2. Il GPS per uso civile utilizza la frequenza L1 di 1.575,42 MHz nella banda UHF; i segnali, con la tecnica della commutazione di pacchetto, viaggiano sulle onde radio "a vista", così da attraversare nuvole, vetro e materiale plastico, ma non la maggior parte degli oggetti solidi come edifici e montagne. Più nel dettaglio, la tecnologia GPS è in grado d'individuare sulla superficie terrestre un terminale comunicativo dedicato (integrato) contenente, cioè, una *Smart Card* dotata di un *microchip* compatibile con i segnali emessi da una "costellazione" di satelliti orbitanti, tanto da poterne identificare la posizione su una carta geografica in termini di longitudine e latitudine, quando non anche di altitudine. La localizzazione geografica può, però, anche avvenire grazie a terminali (ibridi) concepiti per altre utilizzazioni (pc, palmari, *smartphone*, ecc.), ma anch'essi, tutti, ormai, variamente arricchiti di un ricevitore

quali, ad es., le comunicazioni telefoniche e telematiche o le transazioni di *e-banking*, mentre le stesse operazioni di geolocalizzazione "attiva" sono divenute di pressoché generale dominio [5]. Così che se, non da ora, è stata posta la questione dello statuto giuridico del trattamento dei dati rilevati mediante un tale sistema, lo sviluppo di nuove generazioni di cellulari [6] e il moltiplicarsi di applicazioni di tipo "*social*" [7] hanno reso la stessa questione assai più critica per la vulnerabilità di libertà individuali (quali la libertà personale, *sub specie* della *privacy*, e la libertà di circolazione) e collettive (particolarmente, lavorative e sindacali). Sul piano processuale, poi, è soprattutto il diritto di difesa ad essere sotto osservazione, se si riflette sul fatto che i risultati di attività di geolocalizzazione acquisiti *a posteriori* spesso non sono stati reperiti con le garanzie eventualmente connesse all'attività investigativa [8].

2. Il GPS sul tavolo delle Corti.

Della problematica suscitata dalla geolocalizzazione, ha avuto, del resto, già modo di occuparsi la Corte di Strasburgo, per cui il *leading case* va individuato nell'ormai notissima decisione *Uzun c. Repubblica federale tedesca* (*req.* n. 35623/05, Quinta Sezione della Corte) del 2 settembre 2010.

Nella specie, la Corte EDU era stata adita da un cittadino tedesco sospettato d'essere implicato in fatti di natura terroristica e, per tale ragione, sottoposto, dal dicembre 1995 al giorno del suo arresto nel febbraio 1996, a geolocalizzazione mediante l'installazione di una ricevente GPS nella sua autovettura. Il ricorso,

GPS. Nel caso del GSM, la geolocalizzazione avviene attraverso la conversione in misure di distanza dei tempi di percorrenza del segnale tra punti predeterminati.

[5] Mediante appositi *software* (*GeoIP*), può, infatti, rilevarsi la collocazione geografica di una risorsa internet tramite l'indirizzo IP assegnato dal *provider*, tanto da poterne risalire alla tipologia di utente e alla sua velocità di connessione.

[6] Ad esempio, gli utilizzatori di terminali *iPhone*, *iPad* e *iPod touch* sono, senz'altro, al corrente della possibilità di far ricorso al servizio fornito da Apple per essere geolocalizzati ai più diversi scopi o di consentire l'attivazione di programmi (*trackers*) che permettano di ritrovare l'apparecchio in caso di perdita. L'attivazione di tali programmi avviene, peraltro, dopo preavviso all'utente che deve volontariamente aderirvi: di qui la necessità di una consapevole vigilanza nel ricorrere alle varie applicazioni.

[7] Ad esempio, i frequentatori di *Facebook* e *LinkedIn* possono scegliere di farsi localizzare, cliccando su un apposito tasto. Addirittura *Foursquare* è un *social network* basato sulla geolocalizzazione tramite *web* e dispositivi mobili. Basandosi, su un username di *Twitter*, il software *Creepy* è, poi, in grado d'identificare il luogo geografico di una fotografia o di *tweet*.

[8] Ovviamente, nessuno ignora le straordinarie applicazioni di segno positivo della geolocalizzazione nel campo dell'assistenza medica, del soccorso o di ritrovamento di persone o della sicurezza pubblica, costituendo, in quest'ultimo caso, una sorta di "evoluzione" della videosorveglianza, della quale non potrebbe, pertanto, non mutuare le regole di base. A quest'ultimo proposito, spunti di riflessione in P. Costanzo, *Videosorveglianza e Internet*, in AA.VV., *Videosorveglianza e Privacy*, Angelo Pontecorboli Editore, Firenze, 23 ss.

avviato dopo il prescritto esaurimento dei rimedi giurisdizionali interni, era stato, peraltro, anche preceduto dalla chiamata in causa del Tribunale federale costituzionale. In quest'ultima sede, le doglianze del ricorrente, che protestava violate a suo danno le garanzie offerte dagli artt. 1, c. 1 (intangibilità della dignità umana) e 2, c. 1 (diritto al libero sviluppo della personalità individuale) del *Grundgesetz* erano essenzialmente motivate dall'utilizzo di prove a suo carico raccolte illegittimamente, ossia grazie ad un'attività di geolocalizzazione sprovvista dell'indispensabile base legale e sguarnita del necessario controllo giurisdizionale, nonché, comunque, "smodatamente" lesiva della propria *privacy*.

Il Tribunale di Karlsruhe, con la sentenza 2 *BvR* 581/01 [9], ha, però, ritenuto in primo luogo adeguata la generica formula del codice penale di rito tedesco [10], che aveva consentito di avvalersi, a fini dell'indagine, di non meglio precisati speciali mezzi tecnici di sorveglianza. Ha stimato poi proporzionata la misura adottata in ragione della gravità dei reati perseguiti, del limitato lasso di tempo interessato dalla geolocalizzazione, nonché della sua ritenuta minore invasività rispetto ad altre tecniche di sorveglianza (quali l'intercettazione, che permette di apprendere le informazioni più recondite su una persona, o l'installazione domiciliare di dispositivi di registrazione, che può documentarne anche i momenti d'intimità). Dal percorso logico che sorregge la pronuncia, sembrerebbe, tuttavia, trapelare un qualche imbarazzo nei confronti di una tecnica di sorveglianza che è, per la verità, idonea a mettere una persona sotto un'osservazione totale del suo modo di agire, ma che, appunto, per questa sua grande "potenza di fuoco", probabilmente, non ci si è sentiti di avversare più di tanto, in un tempo in cui la sicurezza pubblica ed individuale si configura, in determinate situazioni, sempre più come un bene scarso. Così che, di fronte all'esigenza di non indebolire ed, anzi, di rafforzare, la persecuzione di reati caratterizzati da particolare efferatezza il giudice costituzionale tedesco è parso, per un verso, mostrare di acquietarsi nell'accertamento di un quadro generico di garanzie, ma, dall'altro, di non rinunciare ad allertare nei confronti dei rischi che sopravvenienti tecnologie potrebbero comportare per l'inviolabilità dei diritti fondamentali, gravando sul legislatore il compito di apportare senza sosta i necessari aggiornamenti alla normativa [11]. E se, in un tale quadro, la geolocalizzazione sembrerebbe, in principio, esser man-

[9] 2 *BvR* 581/01 vom 12.4.2005, in *http://www.bverfg.de/entscheidungen/rs20050412_2bvr058101.html.*

[10] Si tratta dell'art. 100c, § 1.1 b, di tale codice.

[11] Par. 51: "*Das Bestimmtheitsgebot verlangt vom Gesetzgeber, dass er technische Eingriffsinstrumente genau bezeichnet und dadurch sicherstellt, dass der Adressat den Inhalt der Norm jeweils erkennen kann*

data assolta, non deve sfuggire la riserva, formulata nella decisione, circa l'inammissibilità, sul piano costituzionale, di una sorveglianza (a cui la stessa geolocalizzazione, si noti, apporterebbe un decisivo contributo), che fosse di portata totale (*Rundumüberwachung*), in quanto idonea a disegnare un profilo completo della personalità individuale.

Analoghe aporie *in subiecta materia* sembrano, peraltro, caratterizzare anche qualche altra illustre Corte giudiziaria. Ne è un chiaro, e altrettanto noto, esempio la sentenza *United States v. Jones* [12], che ha destato, in Italia soprattutto, l'attenzione della dottrina processualpenalistica [13]. Ricordiamo come la Corte Suprema fosse stata chiamata, nella specie, a valutare la costituzionalità dell'installazione, a fini di indagini di polizia giudiziaria, di un dispositivo GPS nell'autovettura di un soggetto coinvolto nel traffico di droga. L'interessato aveva lamentato l'avvenuto superamento dei limiti spaziali e temporali legalmente connessi con l'atto investigativo, ottenendo, a differenza del caso tedesco, il consenso unanime da parte giudici americani, che hanno, infatti, ritenuto incoerenti, rispetto alle garanzie del IV Emendamento, le attività di geolocalizzazione contestate [14]. La Corte Suprema si è, tuttavia, spaccata (5 a 4) su quale dovesse ritenersi l'esatta *ratio decidendi*. La maggioranza s'è mostrata, infatti, dell'avviso che fosse stata violata l'integrità degli effetti personali del ricorrente, secondo una visione, per così dire, risalente e proprietaria, mentre la minoranza ha fatto leva, può asserirsi, più modernamente, sulla lesione di una libertà, chiarendo che la sorveglianza GPS di lungo termine aveva provocato la violazione della «*reasonable expectation of privacy*» [15] del prevenuto [16]. Altre titu-

(...). Das Bestimmtheitsgebot verlangt aber keine gesetzlichen Formulierungen, die jede Einbeziehung kriminaltechnischer Neuerungen ausschließen. Wegen des schnellen und für den Grundrechtsschutz riskanten (...) informationstechnischen Wandels, dessen Gefahren für das Recht auf informationelle Selbstbestimmung auch der Sachverständige Prof. Dr. G. in der mündlichen Verhandlung vor dem Senat beschrieben hat, muss der Gesetzgeber die technischen Entwicklungen aufmerksam beobachten und bei Fehlentwicklungen hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe durch die Strafverfolgungsbehörden und die Strafgerichte notfalls durch ergänzende Rechtssetzung korrigierend eingreifen" (sottolineato nostro).

[12] *United States v. Jones*, 132 S. Ct. 949, 565 U.S (2012).

[13] Una pregevole e circostanziata ricostruzione del caso è operata da V. Fanchiotti, U.S. v. Jones: *una soluzione tradizionalista per il futuro della* privacy?, in *Dir. pen. e proc.*, 2012, 381 ss., Al medesimo proposito, cfr. anche M. Cerase, *Il GPS innanzi alla Corte suprema degli Stati Uniti tra originalismo interpretativo e progresso tecnologico*, in *Cass. pen*, 2012, 1936 ss.; F. Iovene, *Pedinamento satellitare e diritti fondamentali della persona*, ivi, 3556 ss.; nonché L. Filippi, *Il GPS è una prova "incostituzionale"? Domanda provocatoria, ma non troppo, dopo la sentenza Jones della Corte Suprema U.S.A.*, in *Arch. pen.*, 2012, 309 ss.

[14] Com'è noto, è stato il ricorso a tale Emendamento che ha consentito alla Corte Suprema di fondare un livello costituzionale di protezione della *privacy* a partire almeno da *Schmerber v. Califormie*, 384 U.S. 757 (1966).

[15] Su tale concetto, rileva particolarmente la decisione *Katz v. United States*, 389 U.S. 347 (1967), nella *concurring opinion* del giudice John Marshall Harlan jr.

banze hanno caratterizzato, poi, la rinuncia ad affrontare il problema *funditus* (allegandosi una mancata richiesta in tal senso... [17]), così da non fornire una risposta al quesito se potrebbero mai darsi ragionevoli motivi per legittimare un'indagine basata sulla geolocalizzazione [18], o, ancora, a quali condizioni diventerebbe lecito utilizzare i dati già raccolti, ad esempio, da *providers* di servizi *wireless* o in occasione del monitoraggio dei veicoli o dell'erogazione di servizi di navigazione [19].

C'è, tuttavia, luogo a ritenere che la Corte USA abbia solo preso tempo, non potendosi escludere che, tra non molto, sia chiamata ad occuparsi del caso risolto dalla Corte suprema del New Jersey (*State v. Earls*, A-53-11 del 18 luglio 2013), dove, a riforma del giudizio di primo grado, è stato affermato l'obbligo della polizia di munirsi di un mandato per poter utilizzare il tracciamento geografico fornito da un telefono cellulare, atteso che, tra l'altro, "*cell-phone use has become an indispensable part of modern life. The hundreds of millions of wireless devices in use each day can often be found near their owners — at work, school, or home, and at events and gatherings of all types. And wherever those mobile devices may be, they continuously identify their location to nearby cell towers so long as they are not turned off*" [20].

Nel frattempo, il dibattito si è trasferito (finalmente) nelle aule del Congresso, anche se il progetto consegnato al *Geolocation*

[16] Nel dettaglio, il dispositivo aveva fornito la posizione del signor Jones ogni 10 secondi per un periodo di quattro settimane.

[17] Per il giudice Antonin Scalia, icasticamente "*We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had to* Katz *analysis* [v. la nota 14]; *but there is no reason for rushing forward to resolve them here*": cfr. *http://www.law.cornell.edu/supremecourt/text/10-1259#writing-10-1259_OPINION_3*.

[18] Specie a fronte di contrasti giurisprudenziali tra le Corti di circuito circa la portata del principio della *reasonable expectation of privacy:* esemplarmente, v. *United States v. Maynard* 615 F.3d 544, 558–59 (D.C. Cir. 2010), rispetto a cui, tra l'altro, la sentenza *United States v. Jones* ha costituito la decisione di ultimo grado, confermandone, dunque, l'orientamento circa la sussunzione dell'uso del GPS sotto la garanzia del IV emendamento, e, invece, *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir 2010); *United States v. Garcia*, 474 F.3d 994 (7° Cir 2007.) e *United States v. Marquez*, 605 F.3d 604 (2010), che hanno escluso che il ricorso al GPS costituisca una ricerca investigativa in senso proprio, almeno con riguardo agli spazi pubblici. D'altro canto, la stessa Corte Suprema, nella decisione *United States v. Knotts*, 460 US 276 (1983) aveva avallato l'uso di un dispositivo acustico che permetteva di seguire un veicolo a breve distanza, ritenendo, nella specie, non indispensabile un mandato (*warrant*), tanto più che non v'era stato alcun atto di perquisizione o di sequestro; laddove, però, sembra difficile omologare l'offensività di un flebile *beep* con quella della geolocalizzazione.

[19] In proposito, un'altra occasione, per così dire, mancata, ma davanti ad una diversa Corte (District Court Western of Washington at Seattle) e per differenti ragioni processuali (accordo transattivo), può essere ritenuta la causa *Goodman v. HTC America*, originata da una *class action* per l'uso abusivo dell'*app AccuWeeather*, in origine concepita per fornire informazioni metereologiche all'utente geolocalizzato, ma poi sfruttata a fini di *marketing*.

[20] Reperibile *in http://caselaw.findlaw.com/nj-supreme-court/1639239.html.* Superfluo rimarcare che, anche al proposito, le Corti di circuito sono divise: v., ad., es., per una posizione contraria a quella citata nel testo, *United States v. Skinner*, 690 F.3d 772 (6° Cir. 2012).

Privacy and Surveillance Act (GPS Act) non sembra avere avuto, per il momento, una grande accoglienza, se si pensa che esso giace dal 2011 alla Commissione Giustizia del Senato: forse perché il d.d.l. si presenta ispirato ad un grande garantismo e appoggiato, non a caso, da associazioni come *ACLU* [21] ed *Electronic Frontier Foundation* [22], stentando a decollare anche sotto l'amministrazione Obama attestata, in genere, su posizioni progressiste (pur se, nei fatti, non ha, per vero, offerto grandi prove per quanto riguarda la tutela dei dati personali [23]). È, pertanto, da ritenersi che una decisiva scossa possa provenire solo da una chiara presa di posizione dei *nine sages in black robes* che siedono a First Street, a Washington.

Ritornando, però, ora, sulla già citata decisione *Uzun* della Corte europea dei diritti dell'uomo, essa sembra, idealmente (oltreché temporalmente), situarsi tra i due precedenti snodi giurisprudenziali, muovendosi, però, all'evidenza, nell'ambito della tutela di quei soli diritti che, per la tradizione europea, sono indiscutibilmente ritenuti fondamentali, giusta le previsioni degli artt. 6 (giusto processo) e 8 (rispetto della vita privata) della Convenzione di Roma del 1950. In questo senso, anche nella prospettiva dei giudici di Strasburgo, le attività di geolocalizzazione non sono in principio innocenti; tuttavia, il ricorso ad esse può trovare giustificazione qualora sia positivamente superato il *test* di legittimazione fondato sul concorso di tre requisiti:

— la previsione legislativa di tali attività (intesa, anche più sostanzialmente, come prevedibilità da parte dei sottoposti);

— l'esistenza di garanzie operative adeguate, tra cui la possibilità di un riscontro giudiziale ed

— il carattere proporzionale della misura adottata.

Applicando immediatamente il *test* alla fattispecie tedesca, la Corte EDU, ne sembra, però, diluire la capacità scriminante, valutando senza assoluto rigore sia l'adeguatezza della base legale fornita dal codice di procedura (non del tutto convincente, infatti, in quanto silente a proposito delle attività di geolocalizzazione — pur se già ritenuta, come s'è detto, congrua dal Tribunale di Karlsruhe), sia le garanzie previste (anche qui, non ritagliate sulla particolare misura investigativa), sia, ancora, la proporzionalità del provvedimento (criterio, questo, in fondo, sempre sfuggente, coincidendo con una valutazione prevalentemente di merito).

Lo statuto generale del ricorso al GPS sembra, insomma, registrare, nella giurisprudenza di Strasburgo, un chiaro arretra-

---

[21] *https://www.aclu.org/*

[22] *https://www.eff.org/*

[23] A giudizio, anzi, del noto Edward Snowden, la recente normativa, in cui si è impegnato il presidente USA, per la riforma della *National Security Agency*, non conterrebbe progressi particolari per la tutela della *privacy* degli americani (*http://time.com/37940/snowden-obama-nsa-reform/*).

mento rispetto al più minuzioso regime garantistico preteso per altre tecniche di sorveglianza. Di un simile arretramento (o di un mancato allineamento) è, peraltro, consapevole la stessa Corte quando (al § 63 della decisione *Uzunu*) afferma come i "*criteri piuttosto severi, stabiliti e applicati nello specifico contesto della sorveglianza delle telecomunicazioni (...), non siano applicabili ai casi come quello di specie, relativo alla sorveglianza via GPS di spostamenti in luoghi pubblici e, quindi, ad una misura che interferisce in misura minore nella vita privata della persona interessata rispetto all'intercettazione delle sue conversazioni telefoniche*".

Ciò fa tanto più riflettere, se si pensa che nella, di poco precedente, decisione *Kennedy c. Regno Unito* (*req.* n. 26839/05) del 18 maggio 2010, di differente Sezione (la Quarta), un copioso filone giurisprudenziale sulle misure di sorveglianza adottate ad insaputa del sorvegliato aveva trovato ancora espressa conferma, ribadendosi che "*la Corte ha sviluppate le seguenti garanzie minime, che dovrebbero essere previste negli ordinamenti per evitare abusi di potere: la natura dei reati che possono giustificare un ordine di intercettazione; una definizione delle categorie di persone che possono subire intercettazioni telefoniche; un limite alla durata delle intercettazioni telefoniche; le procedure da seguire per l'esame, l'utilizzazione e la conservazione dei dati ottenuti; le precauzioni che devono essere prese quando sono comunicati i dati alle altre parti; e le circostanze in cui le registrazioni potrebbero o dovrebbero essere cancellate o i nastri distrutti*".

Potrebbe, pertanto, destare qualche sorpresa il fatto che la Corte non manifesti esitazioni nell'ascrivere le attività di geolocalizzazione, al pari di quelle telecomunicative, al campo di operatività dell'art. 8 della CEDU; anche se le perplessità diminuiscono, tenendo presente l'idea, ricorrente nella giurisprudenza della Corte, della compatibilità convenzionale di un semplice controllo giudiziario *a posteriori* per ogni tipo di misura investigativa [24].

Ed è proprio su quest'ultimo profilo che la vicenda francese permette ora di fissare in modo specifico l'attenzione.

3. La soluzione francese.

Tutti questi precedenti sono certamente noti al legislatore francese quando mette mano a quella che diverrà la l. n. 2014-372,

[24] Sul punto, della Corte EDU, merita di essere ricordata esemplarmente la dec. *Smirnov c. Russia* (*req.* n. 71362/01, Prima Sezione) del 7 giugno per cui (al § 4) "*la non-exigence d'un mandat judiciaire préalable [peut se trouver], dans une certaine mesure, contrebalancée par la possibilité pour la personne visée par la perquisition de solliciter a posteriori un contrôle juridictionnel de la mesure*".

citata in esordio di queste osservazioni. Ma, il dialogo è aperto, soprattutto, con la Cassazione penale, che ha già avuto occasione di occuparsi ampiamente della problematica in parola. Non è, del resto, un caso isolato, specie a fronte degli esiti di tecnologie inedite, che la spinta propulsiva per un adeguamento legislativo provenga dal terzo potere, laddove, in un regime di fisiologica assunzione di responsabilità e di rispetto dei (propri) ruoli, il legislatore avveduto dovrebbe preoccuparsi di tracciare una rotta univoca per il futuro. Non è (ancora) questa, come si vedrà, la situazione italiana.

Restando alle sue ultime prese di posizione, sono le decisioni, di pari data (22 ottobre 2013) n. 13-81945 e n. 13-81949, ad esprimere in maniera netta il punto di vista della Cassazione francese [25]. Con esse, sono state, in particolare, rigettate le prospettazioni della Corte d'appello di Parigi, secondo cui la geolocalizzazione, similmente alla sorveglianza *de visu* ed ai pedinamenti, sarebbe da omologarsi ad un semplice atto investigativo, privo di lesività per la vita privata ed il segreto epistolare, anche in quanto realizzato senza atti di coercizione. Energica appare, in proposito, la smentita della Suprema Corte transalpina, secondo la quale, infatti, già a partire dalle operazioni preliminari dell'indagine, "*la technique dite de 'géolocalisation' constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge*". Evidenziandosi, inoltre, che il giudice al quale ci si riferisce de-

[25] In precedenza, poteva, per vero, segnalarsi il caso deciso dalla Cass. pen. il 2 novembre 2011, n. 11-84308, però, non particolarmente dirimente al nostro proposito, essendosi ritenuto senz'altro legittimo, in quell'occasione, il ricorso alla geolocalizzazione veicolare disposta direttamente dal giudice con modalità proporzionate al fine repressivo perseguito. Sicché, tutto sommato più interessanti paiono le pronunce della Suprema Corte francese concernenti attività di geolocalizzazione con riguardo a lavoratori dipendenti: cfr., in questo senso, già Cass. Chambre soc. 26 novembre 2002 n. 00-42401, per cui un siffatto tipo di sorveglianza sarebbe risultato illecito, a mente non solo delle normative nazionali, ma anche dell'art. 8 CEDU, rappresentando "*nécessairement une atteinte à la vie privée de ce dernier, insusceptible d'être justifiée, eu égard à son caractère disproportionné, par les intérêts légitimes de l'employeur*". Più di recente, viene in rilievo Cass. Chambre soc. 3 novembre 2011, n. 10-18036, che, meno perentoriamente, ha, da un lato, affermato "*qu'un système de géolocalisation ne peut être utilisé par l'employeur pour d'autres finalités que celles qui ont été déclarées auprès de la Commission nationale de l'informatique et des libertés, et portées à la connaissance des salariés*", e, dall'altro, precisato "*que l'utilisation d'un système de géolocalisation pour assurer le contrôle de la durée du travail, laquelle n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, n'est pas justifiée lorsque le salarié dispose d'une liberté dans l'organisation de son travail*".

Sulla medesima problematica, si registrano anche interventi della *Commission nationale de l'informatique et des libertés* (CNIL) sostanzialmente in linea con la predetta giurisprudenza, tra cui, la *Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public*, e la *Norme simplifiée n° 51 (délibération n° 2006-067 du 16 mars 2006 portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés)*.

v'essere tale in senso proprio (*juge du siége*) e non un generico magistrato, quale si presenta in Francia il Pubblico Ministero, a cui non sono assicurate né imparzialità né indipendenza. Ma ciò che, qui, particolarmente rileva è che, nell'enunciare questi principi di diritto, la Cassazione francese dichiara di rinvenirne il diretto fondamento nell'art. 8 della CEDU, mettendone, pertanto, in campo un'interpretazione più rigorosa rispetto alla stessa Corte di Strasburgo.

Dal canto suo, il legislatore francese ha mostrato di voler raccogliere senza indugi il monito della Cassazione: monito al quale sembrava saggio aderire anche in quanto emesso, come appena detto, con riferimento al quadro convenzionale EDU (non si trascuri il fatto che in Francia, in base all'art. 55 Cost., i giudici comuni sono abilitati direttamente ad eseguire un controllo di compatibilità delle leggi con i trattati, disapplicando quelle ritenute discordanti). Il punto è, però, che il medesimo legislatore ha ritenuto di poter reinterpretare in maniera autonoma quanto statuito dai giudici di *quai de l'Horloge* proprio circa la presenza di un giudice nell'ambito della procedura di predisposizione di attività investigative di geolocalizzazione, dal momento che l'ingresso di costui nella procedura non è stato fatto coincidere con l'attivazione stessa del meccanismo di geolocalizzazione, ma reso obbligatorio solo allo scadere del quindicesimo giorno successivo. Per il tempo anteriore, riconfigurato, *et pour cause*, come una fase di "flagranza prolungata", è il Pubblico Ministero a poter disporre nel senso considerato. Come risulta dai lavori preparatori, la giustificazione addotta è che la Cassazione non avrebbe ritenuto, in realtà, obbligata la soluzione integralmente giudiziaria, ma che sarebbe stato, per essa, giocoforza accedervi in presenza del "*vide juridique entourant la géolocalisation*".

Non imprevedibilmente, la questione è assurta a *punctum crucis* della vicenda, dato che la *Commission nationale de l'informatique et des libertés*, richiesta, nell'ambito della procedura legislativa, di emettere il suo parere, ha, senza esitazioni, censurato il periodo di "latenza" iniziale del giudice nella procedura di autorizzazione delle attività di geolocalizzazione [26] (proponendo, in subordine, la riduzione a otto giorni, peraltro, in maniera meglio corrispondente alla nozione di flagranza). La posizione della CNIL è andata, dunque, ad allinearsi con quella "letterale" della Cassazione penale francese, abbracciando anch'essa, così, un'interpretazione rigorosa delle garanzie pretese dall'art. 8 CEDU. In tale intervento, anche per la competenza in materia di tale Autorità indipendente, va rimarcata altresì la concezione assai

[26] Cfr. la *délibération n° 2013-404 du 19 décembre 2013 portant avis sur un projet de loi relatif à la géolocalisation (demande d'avis n° 13036690).*

più allarmata e critica, che, della geolocalizzazione, viene fornita come non semplicemente riducibile alla "*réalisation de filatures sur la voie publique telles que réalisées par les enquêteurs*", bensì capace di "*apporter des éléments relatifs à la vie privée qui n'auraient pas pu être portés à la connaissance des enquêteurs dans le cadre d'une filature traditionnelle*" [27].

Se potrebbe constatarsi come il dissidio tra legislatore e CNIL non si sia limitato a questo solo profilo, la menzionata *saisine* senatoriale al *Conseil constitutionnel* lo ha addirittura ignorato, pur avendo avuto il merito di offrire l'occasione al giudice costituzionale di una verifica a tutto campo della nuova disciplina [28]. Comunque sia, sul particolare punto considerato, la decisione del *Conseil* appare impressionantemente appiattita sulle scelte di politica criminale del legislatore, con una svalutazione alquanto acritica e assertoria delle potenzialità lesive della geolocalizzazione per talune libertà costituzionali.

Sembra lecito, pertanto, chiedersi se, in futuro, la Cassazione vorrà validare questa soluzione "al ribasso", o se, interpretando autenticamente se stessa, confermerà, anche nella lettera, le decisioni del 2013, giocando, per così dire, di anticipo rispetto alla Corte EDU, alla quale non si potrà certamente chiedere di censurare una protezione estesa di una libertà convenzionale.

4. Alcune conclusioni sul quadro italiano.

Qualche osservazione merita, infine, la situazione italiana, nella quale, come già accennato, è il formante giurisprudenziale a tenere il campo, pur non mancando, anche qui, rilevanti interventi dell'*autority* di settore.

Con riferimento a questi ultimi, possono, infatti, menzionarsi taluni Provvedimenti del Garante per la protezione dei dati personali, anche se di portata specifica, in quanto concernenti le condizioni di liceità del trattamento, da parte dei datori di lavoro, mediante geolocalizzazione satellitare, di dati afferenti a lavoratori dipendenti (5 giugno 2008 [29], 18 febbraio 2010 [30], 4 ottobre

[27] Dell'atteggiamento assai prudenziale della CNIL, testimonia anche la *fiche pratique* pubblicata sul relativo sito *web* a proposito dei rischi connessi con l'uso degli *smartphones:* in *http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/les-smartphones-en-questions/*.

[28] Assai sinteticamente, può ricordarsi che il giudice costituzionale francese, non legato come la Corte costituzionale italiana alla regola della corrispondenza tra chiesto e pronunciato, ha accertato l'invalidità, per motivi procedurali, dell'art. 3 della legge, e, per lesione del diritto di difesa, l'art. 1, nella parte in cui consentiva di fondare una condanna su elementi raccolti con la geolocalizzazione, ma rimasti ignoti al soggetto inquisito. Inoltre, la costituzionalità dello stesso art. 1 è stata sottoposta ad alcune riserve interpretative tendenti sempre a mantenere intatto il valore della difesa processuale. Sono state, invece, ritenute sufficienti, in quanto non sproporzionate rispetto alle finalità, a fronte dell'indubbio sacrificio di diritti costituzionalmente garantiti, le condizioni legittimanti il ricorso stesso alla geolocalizzazione, specie con riguardo al ruolo di garanzia assegnato all'autorità giudiziaria.

[29] Cfr. *http://www.garanteprivacy.i-*

2011 [31], 1° agosto 2012 [32] e 7 marzo 2013 [33]), se del caso, mediante esternalizzazione del servizio stesso di geolocalizzazione. Da questo complesso di prescrizioni, emerge chiaramente lo scrupolo di assicurare, a fronte di una non denegata necessità del rilevamento di persone e cose per fini legittimamente connessi all'attività d'impresa, la qualità dei dati trattati (nel senso della loro essenzialità e pertinenza), l'indispensabile informativa delle persone geosorvegliate e l'esclusione di forme di sorveglianza in ispregio allo Statuto dei lavoratori [34].

Sul piano più generale, dell'attenzione portata dal Garante alla problematica della geolocalizzazione, vi sono segni evidenti nella Relazione annuale del 2012 [35], emergendo anche la sintonia con gli orientamenti formulati dal cd. Gruppo di lavoro art. 29 [36], il cui Parere 13/2011 - WP 185, sui servizi di geolocalizzazione su dispositivi mobili intelligenti, del 16 maggio 2011 [37], al momento costituisce il più autorevole quadro di riferimento di livello europeo [38].

Nell'ordinamento nazionale, a parte l'attuazione delle direttive

t/web/guest/home/docweb/-/docweb-display/docweb/1531604.

[30] Cfr. *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1703103.*

[31] Cfr. *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1850581.*

[32] Cfr. *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1923293.*

[33] Cfr. *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2471134.*

[34] V. anche il Provvedimento di blocco del 7 ottobre 2010 (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1763071*).

[35] Cfr.. *http://194.242.234.211/documents/10160/2148177/Relazione+annuale+del+Garante+-+Testo.*

[36] Com'è noto, il riferimento è all'art. 29 della direttiva 95/46, che ha istituito un organismo indipendente, composto da un rappresentante delle autorità di tutela dei dati personali di Stato membro, del Garante europeo della protezione dei dati, e da un rappresentante della Commissione europea, incaricato, tra l'altro, di formulare pareri e raccomandazioni su questioni riguardanti la protezione dei dati personali nell'Unione europea.

[37] Preceduto nel tempo dal Parere 5/2005 - WP 115.

[38] A mente di tale Parere, alle attività di geolocalizzazione sono riferibili le normative recate dalle direttive 95/46/CE e 2002/58/CE, il cui art. 2 ragiona, tra l'altro, alla lett. c), di "dati relativi all'ubicazione", come quelli trattati in una rete di comunicazione elettronica, idonei ad indicare la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.

L'attenzione del documento è concentrata soprattutto sui soggetti che esercitano le attività in questione, individuati specificamente nei responsabili di infrastrutture geolocalizzanti, nei fornitori di servizi di geolocalizzazione e negli stessi sviluppatori dei sistemi d'uso di dispositivi mobili. A tali soggetti incombe munirsi del consenso informato degli interessati come condizione di legittimità del trattamento da geolocalizzazione, se del caso, richiedendolo dopo un certo lasso di tempo; mentre, a questi ultimi, deve essere assicurata la possibilità di una revoca efficace del consenso, senza il rischio di ricadute negative sull'uso del loro terminale mobile, oltreché quella di ottenere l'accesso ai dati di delocalizzazione che li concernono, nonché alle eventuali profilature basate su questi stessi dati. Resta, infine, obbligo dei titolari del trattamento determinare un tempo di conservazione dei dati non eccedente, assicurandosi della loro effettiva cancellazione.

concernenti, in via generale, la materia [39], non esistono riferimenti di livello primario pertinenti o specifici [40], sicché tutto risulta rimesso alle coordinate derivabili dal *milieu* giurisprudenziale, in cui campeggia, ovviamente, la posizione della Suprema Corte, che, peraltro, pare essersi assunta un assai critico compito di retroguardia nel settore.

Se confrontiamo tale posizione con quelle di cui s'è cercato di dare in precedenza conto a livello sia estero, sia sovranazionale, non possono, infatti, nutrirsi dubbi circa la formazione, nel tempo, di uno spesso filone giurisprudenziale attestato nel differenziare, sul piano investigativo, rispetto ad altre attività d'indagine, l'attività di geolocalizzazione in quanto stimata di minima invasività e di debole capacità di captazione di dati, ed assimilata (soprattutto a partire da Cass. pen., sez. V, 2 maggio 2002 n. 16130 [41]) ad una sorta di pedinamento mediante satellite, tanto da inferirne che i dati così ottenuti, poiché non attinenti né a conversazioni, né a comunicazioni, non richiedano il rispetto della disciplina di cui agli artt. 266 e ss. c.p.p. e delle garanzie proprie della *privacy* [42].

Nel contempo, sul piano processuale e probatorio, la medesima prospettiva conduce a considerare i dati raccolti con la geolocalizzazione alla stregua delle prove atipiche ricadenti sotto la disciplina dell'art. 189 c.p.p., la cui assunzione è del tutto rimessa al giudice, se ritenuta idonea ad assicurare l'accertamento dei fatti senza compromettere la libertà morale della persona [43].

Di tale atteggiamento svalutativo pare ancora segno il recente diniego della Suprema Corte di problematizzare la situazione, sollevando la questione di legittimità costituzionale della sua stessa interpretazione, in quanto (reputata) imposta dalla normativa penale di rito, favorevole alla collocazione dei sistemi di

[39] V. la nota precedente.

[40] Sul punto, v. S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.*, 2012, 588 s.

[41] In *Foro it.*, 2002, 2, 635, con nota adesiva di A. SCAGLIONE, *ibid.*; in senso critico, v., però, P. PERETOLI, *Controllo satellitare con GPS: pedinamento o intercettazione?*, in *Dir. pen. e proc.*, 2003, 94 ss.

[42] Così efficacemente A. SERRANI, *Sorveglianza satellitare GPS: un'attività investigativa ancora in cerca di garanzie*, in *http://www.archiviopenale.it/apw/wp-content/uploads/2013/12/questioni-Serrani-GPS.pdf.*, ed ivi pertinenti indicazioni giurisprudenziali. Peraltro, non manca chi, pur accedendo alla configurazione della Cassazione, ritiene auspicabile un intervento legislativo per tipizzare le attività in questione, postulando almeno l'intervento del P.M. per accertare la concreta ed effettiva indispensabilità delle indagini: cfr. M. STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova atipica*, in *Dir. pen. e proc.*, 2011. 213 ss..

[43] Derivandone un articolato dibattito dottrinale sulla gestione dei dati raccolti, che qui non si ha modo di riferire adeguatamente: cfr., comunque, ad es., A. LARONGA, *Il pedinamento satellitare: un atto tipico lesivo di diritti inviolabili?*, in *Questione giustizia*, 2002, 1153 ss., che auspica l'inserimento nel fascicolo del dibattimento anche del supporto informatico e non solo del verbale; o F. FALATO, *Sulla categoria dei mezzi atipici di ricerca della prova e le cd. intercettazioni GPS*, in *Giur. it.*, 2010, 2418 ss., che circoscrive le risultanze della geolocalizzazione al solo fascicolo del p.m. escludendole dal fascicolo del dibattimento, salvo il previo accordo delle parti.

rilevamento e acquisizione di dati, notizie e conversazione all'interno di luoghi riservati, pur in assenza di una specifica disciplina legislativa delle modalità d'intromissione nella vita privata [44].

Anche alla luce delle considerazioni pregresse, non sembra, pertanto, azzardato individuare in tale frangente una patologia rispetto al disposto dell'art. 8 CEDU, persino nel più blando orientamento interpretativo invalso a Strasburgo. Come si è potuto, infatti, osservare, secondo la Corte EDU, l'attività di geolocalizzazione deve giovarsi, in principio, anch'essa, delle tutele offerte dalla Convenzione di Roma, costituendo un dato di assoluta evidenza come siffatta attività incida in maniera considerevole sulla libertà e la riservatezza personali [45]. Una patologia probabilmente non più trattabile in via ordinaria a motivo del carattere ormai cronicizzato del dato giurisprudenziale, tale da rendere difficilmente praticabile anche il rimedio di interpretazioni convenzionalmente conformi [46], nonché persino poco pervio lo stesso intervento dei giudici della Consulta.

In questo senso, l'intervento della Corte europea dei diritti dell'uomo si collocherebbe in un quadro culturalmente e giuridicamente più maturo rispetto alla decisione *Uzun*, a cui la, tutto sommato compromissoria, soluzione francese potrebbe fornire motivi di ulteriore riflessione.

[44] Cass., pen., Sez. II, 21 maggio 2013 (ud. 13 febbraio 2013), Esposito, Presidente - Verga, estensore - Mazzotta, P.G. (conf.), Bellino ed altri in *Archivio penale* (*http://www.archiviopenale.it/apw/wp-content/uploads/2013/07/2013-cass-bellino.pdf*), con commento di A. Serrani, *Sorveglianza satellitare GPS*, cit.

[45] È di D. Gentile, Tracking *satellitare mediante gps: attività atipica di indagine o intercettazione di dati?, in Dir. pen. e proc.*, 2010, 1465 ss., l'esatta osservazione per cui, col progresso tecnologico è aumentata la necessità di protezione dei cd. dati sensibili, mentre la geolocalizzazione è molto più invasiva del classico pedinamento a motivo principalmente della sua capillarità e delle sue modalità temporali, conseguendone la necessità di una compiuta regolamentazione.

[46] È la condivisibile osservazione di F. Iovene, *Pedinamento satellitare e diritti fondamentali della persona*, in *Cass. pen*, 2012, 3556 ss.