federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

30 NOVEMBRE 2016

Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)

di Massimo Rubechi
Ricercatore in Diritto costituzionale
Università degli Studi di Urbino Carlo Bo

Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi) *

di Massimo Rubechi
Ricercatore in Diritto costituzionale
Università degli Studi di Urbino Carlo Bo

Sommario: **1.** Sicurezza e *privacy*: Un confronto antico, delle sfide moderne. **2.** La dimensione costituzionale della sicurezza e le limitazioni ai diritti di libertà. **3.** Dignità della persona, diritto alla riservatezza e protezione dei dati personali in epoca di terrorismo. **4.** Le nuove sfide nel contesto degli ordinamenti statuali europei. **5.** Sicurezza e tutela della riservatezza nella giurisprudenza delle Corti sovranazionali. **6.** Sicurezza e *privacy* dopo i più recenti attacchi terroristici: considerazioni di sintesi.

1. Sicurezza e *privacy*. Un confronto antico, delle sfide moderne.

È una reazione fisiologica quella degli ordinamenti democratici adottare misure emergenziali e di polizia per fronteggiare minacce alla sicurezza dei propri cittadini, soprattutto se provenienti dal terrorismo, interno o internazionale. Una sfida che risulta più complessa e meritevole d'attenzione nello studio del costituzionalismo moderno poiché non è semplice applicare al terrorismo le tradizionali categorie del diritto. Si tratta infatti di un fenomeno – pur nelle sue diverse accezioni – caratterizzato da una dimensione storica e politica e che tende, da un lato, a scardinare proprio lo stato di diritto e, dall'altro, a limitare il godimento dei tradizionali diritti individuali.

In generale, il modo con cui gli ordinamenti reagiscono a queste situazioni si concreta nel ricorso a interventi di carattere emergenziale che consistono primariamente nell'inasprimento delle misure di polizia. Ciò è stato particolarmente vero negli Stati Uniti[1] all'indomani degli attacchi terroristici dell'11

* Articolo sottoposto a referaggio.

[1] Per una discussione sul rapporto tra terrorismo e Costituzione sia in generale che con specifico riguardo all'ordinamento statunitense si veda C. BASSU, *Terrorismo e costituzionalismo. Percorsi comparati*, Torino, 2010. All'indomani degli attentati terroristici dell'11 settembre 2001, l'attenzione degli studiosi si è concentrato proprio sul tema del rapporto fra misure di sicurezza e garanzie delle libertà fondamentali. Almeno il commento in prima lettura di F. LANCHESTER, *Gli Stati Uniti e l'11 settembre 2001*, in Rivista Aic. Si vedano altresì in tal senso le relazioni al Convegno annuale 2003 dell'Associazione italiana costituzionalisti proprio dedicato al tema, e in particolare per la dottrina italiana DE SIERVO U., *Informazione, comunicazione globale e privacy* e G. DE VERGOTTINI, *La difficile convivenza fra libertà e sicurezza: la risposta delle democrazie al terrorismo. Gli ordinamenti nazionali*, tutte reperibili sul sito internet dell'Associazione. Parimenti si veda P. BONETTI, *Terrorismo, emergenza e costituzioni democratiche*, Bologna, 2006. Sul più ampio tema della protezione della democrazia sotto il profilo del diritto

settembre 2001 ma è una reazione ben visibile anche nel continente europeo sia in seguito agli attacchi di Madrid e Londra degli anni successivi sia in particolare dopo le stragi di Parigi del novembre 2015 o di Bruxelles del marzo 2016. E allora sia gli organi di vertice dello stato, sia l'opinione pubblica sono chiamati ad interrogarsi sull'efficacia delle misure volte ad assicurare la sicurezza individuale e collettiva nonché l'integrità dello stesso Stato.

Le tradizionali libertà negative – a partire dalla libertà personale – sono i primi diritti fondamentali dell'uomo a risultare potenzialmente compressi dall'inasprimento delle misure di sicurezza. In seguito agli attentati terroristici più recenti, invece, sono emerse nuove, ulteriori, sfide.

Le esigenze di controllo e prevenzione hanno infatti dei punti di contatto sia con gli ambiti di tutela delle libertà fondamentali nella loro forma di esercizio più classica e tradizionale, sia nella declinazione che si potrebbe definire come «digitale», con riferimento all'impiego dei mezzi di comunicazione soprattutto attraverso la rete *internet*. Un impiego quest'ultimo che era senza dubbio più massiccio quando stati effettuati i recenti attacchi terroristici rispetto ai primi anni duemila – è questa la parziale novità –, in ragione di una diffusione e di un potenziamento degli strumenti tecnologici ed informatici molto vasta e pressoché generalizzata in ampie fasce della popolazione.

Le prime misure invasive della privacy sono state adottate negli Usa già a partire dal *Patriot Act* del 2001, assieme, naturalmente, a misure che incidono su libertà costituzionali più tradizionali. Il famoso scandalo *Datagate* – nato dalle rivelazioni di Edward Snowden – trae origine proprio dall'impiego delle norme introdotte negli Stati Uniti dopo l'11 settembre: la rivelazione della massiccia attività di raccolta di dati personali di cittadini di tutto il mondo (e quindi anche europei) da parte delle autorità federali degli Usa e per ragioni di sicurezza nazionale, fu resa possibile grazie all'accesso ai server delle tantissime e rilevanti società di *Information and Communications Technologies* (cd. Ict) collocate sul suolo americano.

Me è negli ultimi due anni che anche i Paesi europei hanno deciso di intervenire in maniera parimenti incisiva, e in un contesto caratterizzato da più elevati livelli di tecnologizzazione e di informatizzazione rispetto ad allora, che offrono nuove sfide sia alle modalità di prevenzione e di controllo, sia alle limitazioni cui devono essere sottoposte.

Se è vero che si aprono nuovi scenari, non vuol dire tuttavia che le tradizionali frontiere non debbano essere presidiate. Si pensi ad esempio alla limitazione della libertà di domicilio in forza delle perquisizioni domiciliari in assenza di autorizzazione dell'autorità giudiziaria, effettuate in Francia nell'ambito delle

comparato v. invece, del medesimo periodo, S. CECCANTI, *Le democrazie protette e semi-protette da eccezione a regola. Prima e dopo le Twin Towers*, Torino, 2004. Più in generale sul rapporto tra conflittualità internazionale e principi costituzionali cfr. almeno G. DE VERGOTTINI, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, 2004 e P. CARNEVALE, *La Costituzione va alla guerra?*, Napoli, 2013.

misure attuative dello stato d'urgenza[2]. O ancora basta far riferimento alla compressione potenziale della libertà di manifestazione del pensiero, determinata dal blocco amministrativo dei siti *internet* inneggianti al terrorismo, ancora una volta resa possibile dalle scelte del legislatore francese[3], così come le limitazioni alla libertà di circolazione determinate dall'obbligo di dimora per soggetti ritenuti pericolosi per l'ordine pubblico e la sicurezza (*assignation à résidence*)[4].

Ma il potenziamento delle tradizionali misure di polizia è recentemente andato di pari passo con l'introduzione di nuovi strumenti e il rafforzamento delle misure di sorveglianza occulta e di prevenzione, che dunque pongono in primo piano la necessità di concentrarsi anche sulla tutela dei dati personali, a partire dal loro impiego. Oltre all'ampliamento delle misure di intercettazione, si pensi ad esempio all'installazione di sistemi di videosorveglianza sempre più capillari[5], così come alla creazione delle grandi banche dati per finalità di sicurezza, nonché alla possibilità di aggregare e analizzare enormi quantità di dati attraverso le nuove tecnologie.[6]

In questa sede, dunque, si tenterà di tracciare le nuove sfide alla tutela della *privacy* che vengono poste nel nuovo scenario aperto dai recenti attentati terroristici di matrice islamista, alla ricerca di un possibile equilibrio fra le diverse esigenze che consenta di non comprimere oltremodo gli spazi dei diritti fondamentali nonostante le tendenze restrittive in atto.

La ricerca di un bilanciamento è possibile tuttavia solo se preliminarmente viene delineata la dimensione costituzionale della sicurezza e, dunque, è a questo primo profilo che verrà dedicato il primo paragrafo del presente lavoro (§2). Ci si concentrerà poi (§3) su una sistematizzazione della natura del diritto alla *privacy* alla luce dell'evoluzione ad opera sia di numerosi interventi giurisprudenziali sia di importanti novelle legislative.

---

[2] Introdotte con la l. 20 novembre 2015, n. 1501 che prorogava, tra l'altro, lo stato di urgenza inizialmente previsto per soli dodici giorni. Si tratta di misure che il *Conseil constitutionnel* ha per gran parte dichiarato conformi a Costituzione, con la sola eccezione della misura relativa al sequestro di dati informatici, perché privo delle garanzie legali in grado di assicurare il corretto bilanciamento tra il valore costituzionale di tutela dell'ordine pubblico e il diritto al rispetto della vita privata, anche in considerazione del fatto che alcuni dati potrebbero appartenere a soggetti terzi che verrebbero casualmente coinvolti nell'operazione (*Décision n.* 2016-536 QPC del 19 febbraio 2016).

[3] L'articolo 9 della legge n. 2014/1353, approvata invero prima degli attacchi di Parigi. Per un commento si veda C. GAZZETTA, *Sicurezza, terrorismo e cittadinanza: la nuova legislazione francese anti-terrorismo e l'impegno internazionale contro i cd. foreign fighters*, in *Democrazia e sicurezza*, n. 3/2015.

[4] Il *Conseil constitutionnel* ha stabilito la conformità a Costituzione di tale misura, perché proporzionata rispetto ai benefici che derivano in termini di tutela dell'ordine e della sicurezza pubblica (*Décision* n. 2015-527 QPC del 22 dicembre 2015).

[5] Sul punto v. L. CALIFANO, V. FIORILLO, *Videosorveglianza*, in R. BIFULCO – A. CELOTTO – M. OLIVETTI (a cura di), *Digesto delle discipline pubblicistiche* (aggiornamento), Torino, 2015 e relativi esempi citati; v. anche M. MANETTI – R. BORRELLO (a cura di), *Videosorveglianza e privacy*, Firenze, 2010.

[6] Si veda, specificamente dedicato al tema, L. SCAFFARDI, *Nuove tecnologie, prevenzione del crimine e privacy: alla ricerca di un difficile bilanciamento*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, 2013.

Nel successivo paragrafo (§4), l'analisi sarà focalizzata sulle nuove sfide inerenti il rapporto fra il potenziamento delle misure di sicurezza e la potenziale compressione del diritto alla *privacy*, a partire da alcuni spunti provenienti dalle misure recentemente introdotte da taluni degli stati membri dell'Unione europea.

Nella sezione successiva (§5), invece, ci si concentrerà sulle decisioni più recenti delle Corti di Lussemburgo e di Strasburgo che consentono di apprezzare i principi comuni nello spazio giuridico europeo riguardanti il rapporto fra le misure di contrasto al terrorismo e la tutela della *privacy*.

Infine, si tenterà di tratteggiare delle linee di sintesi di un possibile percorso di risposta al terrorismo nel contesto contemporaneo, che tenga conto sia delle nuove sfide, sia dei "vecchi diritti" (§6).

2. La dimensione costituzionale della sicurezza e le limitazioni ai diritti di libertà.

La dottrina costituzionalistica si è lungamente interrogata sulla definizione di sicurezza e sul suo fondamento costituzionale, a partire dai molteplici significati che ad essa possono essere assegnati[7]. Senza la pretesa di ricostruire un dibattito sì autorevole e ricco, in questa sede ci si limiterà ad affrontare il problema principale ai fini di un possibile bilanciamento fra sicurezza e *privacy*, vale a dire la sua dimensione costituzionale.

Premettendo che nella Costituzione italiana un diritto alla sicurezza non trova un esplicito riferimento e che, parimenti, non viene menzionato l'ordine pubblico come possibile limite ai diritti di libertà[8], è necessario qui chiedersi – tentando di schematizzare il dibattito dottrinario cui si è fatto riferimento – se sia giuridicamente più congruo considerare la sicurezza come un diritto ovvero come configurarlo come un interesse collettivo.

Preliminarmente, va però rilevato come il termine sicurezza possa assumere diverse declinazioni, ciascuna delle quali con una specifica rilevanza giuridica. Ragionando in termini di binomi per comprendere le sue differenti connotazioni, si può parlare di «sicurezza esterna» o di «sicurezza interna» qualora si prenda in considerazione la provenienza delle minacce al gruppo sociale di riferimento; oppure si possono contrapporre una «sicurezza individuale» ad una «sicurezza collettiva», distinguendo dunque una *sicurezza da*, nel primo caso, e *sicurezza di,* nel secondo, a seconda di quanto venga sottolineato il ruolo dell'ordinamento giuridico nell'adempiere a determinate prestazioni per i cittadini; si può infine ragionare in termini di «sicurezza materiale» o di «sicurezza ideale», intesa con la prima la tutela dell'incolumità di

[7] Ricostruendone i diversi significati, M. DOGLIANI, *Il volto costituzionale della sicurezza*, in G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 2012, pp. 1ss. parla di «termine polisenso».
[8] Cfr in questo senso L. CALIFANO, V. FIORILLO, *Videosorveglianza*, *op. cit.*, p. 505.

beni e persone, con la seconda la necessità di preservare principi e valori fondamentali di un ordinamento[9].

Per quanto riguarda la distinzione fra sicurezza interna e sicurezza esterna, se rimane rilevante dal punto di vista dell'organizzazione delle differenti tipologie di attività e della distribuzione dei compiti tra i vari corpi dello Stato, si viene oggettivamente a sfumare a fronte alla peculiarità della minaccia terroristica, in particolare quella islamista radicale, poiché viene messa in atto da cittadini o comunque residenti del Paese, i quali magari hanno trascorso solo brevi periodi di addestramento all'estero presso le milizie organizzate.[10]

E inoltre, il crescente utilizzo da parte delle organizzazioni terroristiche delle cd. *Information and Communications Technologies* e, in particolare dei *social networks* non solo possono compromettere l'efficacia delle misure di prevenzione della diffusione dei messaggi di istigazione al terrorismo ma rendono strumenti di lotta gli stessi mezzi di comunicazione, nella misura in cui le organizzazioni terroristiche possono mirare anche a colpire la sicurezza dei sistemi informatici e l'inviolabilità delle banche dati[11].

Entrambi questi profili rendono, dunque, più complesso inquadrare anche teoricamente il tema della sicurezza con le schematizzazioni riportate nonché, in ultima analisi, con le classiche categorie dello Stato nazionale e del monopolio della forza legittima.

Con riguardo ai fondamenti costituzionali della sicurezza, le due posizioni prevalenti richiamate in avvio sono quelle che tendono a individuare, da un lato, la sicurezza come interesse collettivo riconosciuto, e dall'altro, la sicurezza come vero e proprio diritto fondamentale proprio di ciascun individuo. È evidente come dalla configurazione della sicurezza secondo l'una o l'altra ipotesi dipenda la definizione dei termini corretti – e prima ancora forse l'opportunità e fors'anche la possibilità stessa – di tratteggiare un'operazione di bilanciamento.

Coloro che non qualificano la sicurezza come diritto individuale supportano questa posizione rilevando primariamente che una tale situazione giuridica soggettiva sarebbe priva di un elemento imprescindibile

---

[9] V. T. GIUPPONI, *La sicurezza e le sue dimensioni costituzionali* in *Forum on line di Quaderni costituzionali*.

[10] Si tratta dei cd. *foreign fighters*, rispetto ai quali il Consiglio di sicurezza delle Nazioni Unite ha adottato la Risoluzione S/RES/2178(2014). Anche al fine di dare seguito a tale risoluzione recentemente anche l'Italia ha adottato (al pari di Belgio, Francia, Germania e Regno Unito), il decreto legge 18 febbraio 2015, n. 7, convertito con modificazioni dalla legge 17 aprile 2015, n. 43. Per un commento si vedano C. GAZZETTA, *Sicurezza*, *op. cit.* e E. BONINI, *Foreign fighters, ecco come in Europa si risponde alla minaccia*, 9 febbraio 2015, in http://www.eunews.it/2015/02/09/foreign-fightersrisponde-minaccia/29894

[11] Si pensi al fenomeno del cd. *cyber crime*, su cui v., tra gli altri, S. W. BRENNER, *Cybercrime, cyberterrorism and cyberwarfare*", in *Revue internationale de droit penal*, 2007, 453 ss; F. R. FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in Diritto penale e processo, 2009, 5, 639 ss; GRUPPO DI LAVORO ASTRID, *La sicurezza dei domini digitali*, 28.5.2015, in www.astrid.it; C. SARZANA DI SANT'IPPOLITO, *Sicurezza informatica e lotta alla cybercriminalità: confusione di competenze e sovrapposizione di iniziative amministrative e legislative*, in Diritto dell'Internet, 2005, 5, 437 ss.

affinché essa possa essere qualificata come diritto dell'individuo: la sua giustiziabilità. Secondo questa impostazione, la sicurezza rappresenterebbe un valore costituzionale di tipo settoriale, nel senso che essa potrebbe essere concepita come l'aspetto soggettivo dell'ordine pubblico. E, dunque, essa assume una precisa connotazione, tanto da condurre alla considerazione secondo cui «la sicurezza di cui si occupa la Costituzione negli artt. 13, 14, 15, 16, 17, 18, 117 comma 2, lettera d) e h) non può essere confusa con altri tipi di sicurezza»[12].

Non di interesse settoriale bensì di interesse della collettività parlano poi altri Autori, i quali riconoscono un significato più ampio al concetto di sicurezza, estendendola in vario modo all'insieme della tutela dei beni costituzionali[13] e a più settori dell'*agere* pubblico[14]. In quest'ottica, secondo una delle impostazioni che si riconoscono in questo filone, la sicurezza avrebbe sia un «volto repressivo» che una «sembianza promozionale»: a tenere uniti questi capi apparentemente piuttosto distanti sarebbe l'evoluzione del bisogno umano che, partendo dalla statica difesa della «*tranquillitas*» civile, andrebbe oggi dinamicamente a ricomprendere anche l'«istanza di realizzazione di una società che consenta l'espressione delle potenzialità di sviluppo degli individui». In altre parole, la sicurezza sarebbe strettamente collegata alla «rimozione degli ostacoli che si frappongano all'effettivo godimento dei diritti»: e dunque si dovrebbe parlare più appropriatamente di «sicurezza dei diritti» piuttosto che di «diritto alla sicurezza» nella forma di Stato sociale[15].

Diametralmente opposte alle impostazioni sin qui richiamate, vi sono le teorie che considerano la sicurezza come un diritto costituzionale – o addirittura come un «valore superprimario»[16] – le quali, prendendo le mosse dal pensiero contrattualista, tendono a qualificarla come un «bene inscindibilmente legato alla vita, alla incolumità fisica, al benessere dell'uomo e alla qualità della sua esistenza, nonché alla dignità della persona». Se questo è il presupposto, allora non si starebbe parlando solo di un compito da riconoscere in capo allo Stato, ossia quello di garantire la pace sociale, ma si sarebbe dinnanzi a un «diritto a un'esistenza protetta, indispensabile al godimento degli altri diritti di cui [l'individuo] è titolare in condizioni di sicurezza»[17]. In questo senso si potrebbe leggere anche l'articolo 6 della Carta di Nizza, dove

---

[12] Cfr. A. PACE, *Libertà e sicurezza. Cinquant'anni dopo*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, 2014, pp. 547 ss., secondo cui «sicurezza pubblica e ordine pubblico costituiscono non già concetti diversi tra loro ma i due lati della stessa medaglia, il primo soggettivo, il secondo oggettivo» (p. 551).

[13] M. DOGLIANI, *Il volto costituzionale della sicurezza*, op. cit.

[14] P. RIDOLA, *Libertà e diritti nello sviluppo del costituzionalismo*, in P. RIDOLA – R. NANIA (a cura di), *I diritti costituzionali*, Torino, 2006.

[15] Cfr. M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, in G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 2012, in particolare pp. 18 ss., nonché, ID., *Diritto alla sicurezza e sicurezza dei diritti*, in Democrazia e Sicurezza, n. 2/2013.

[16] Il quale, in quanto tale, non si presterebbe a bilanciamento secondo i canoni tradizionali. V. in questo senso G. CERRINA FERONI – G. MORBIDELLI, *La sicurezza: un valore superprimario*, in Percorsi costituzionali, n. 1/2008

[17] T. E. FROSINI, *Il diritto costituzionale alla sicurezza*, in Forum on line di Quaderni costituzionali.

è stabilito che «Ogni individuo ha diritto alla libertà e alla sicurezza», pur non definendone la natura e le caratteristiche nel dettaglio.

Nel contesto attuale, risultano meno diffuse le interpretazioni che troppo fortemente si riconnettono alle teorie contrattualiste che giustificavano la nascita dello stato stesso in un contesto di riconoscimento dei diritti assai più embrionale rispetto al nostro. Oggi, infatti, gli ordinamenti democratici garantiscono un livello di sicurezza incomparabilmente più robusto rispetto all'epoca in cui esse furono formulate, tanto da permettere di poter considerare intrinsecamente superato il profilo individualistico della sicurezza, poiché sottinteso alla caratterizzazione stessa degli ordinamenti come democratici e liberali. E, dunque, il contesto attuale consente di potersi concentrare sull'interesse collettivo in cui la sicurezza si concreta, poiché non si sostituisce al profilo individuale, ma anzi ne costituisce una evoluzione e un potenziamento.

Impiegando in questa sede una definizione di sicurezza di carattere restrittivo, vale a dire limitata solo al suo tradizionale profilo preventivo e repressivo e dunque intesa nel senso di garanzia dell'ordine pubblico, si può allo stato convenire sul fatto che essa «non si connota per un ambito specifico di attività garantite, ma si pone come scopo che può giustificare misure restrittive delle libertà» e si configura dunque come una «ragione di limiti dei diritti riconosciuti»[18].

E, dunque, parrebbe più congruo riferirsi al tema della definizione del rapporto fra sicurezza e diritti fondamentali in termini di proporzionalità ed equilibrio dei limiti introdotti per perseguire gli scopi posti.

A prescindere dall'utilizzo della nozione tecnica di bilanciamento fra due diritti o fra diritti e valori, e dunque a prescindere da come la sicurezza possa essere configurata nel contesto delle opzioni dottrinarie in precedenza esposte, è dunque certamente ammissibile che in talune circostanze emergenziali (e non) dalla sicurezza possano discendere limiti legittimi per i diritti fondamentali[19].

Saranno però il *quantum* e il *quomodo* di tale operazione di limitazione a fare la differenza nella tenuta complessiva dello stato di diritto.

3. Dignità della persona, diritto alla riservatezza e protezione dei dati personali in epoca di terrorismo.

Il diritto alla *privacy* viene configurato dalla dottrina, in maniera pressoché unanime, come un diritto fondamentale della persona, anche se la Costituzione italiana non lo contempla esplicitamente. Questa

[18] A. CERRI, *Diritto alla riservatezza e videosorveglianza*, in M. MANETTI – R. BORRELLO (a cura di), *Videosorveglianza e Privacy*, Firenze, 2010, p. 18.

[19] M. RUOTOLO, *Costituzione e sicurezza tra diritto e società*, A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, 2014, p. 588. Il riferimento dell'A. è agli artt. 13, commi 2 e 3, 14, commi 2 e 3, 25 comma 3, 16, 17, comma 3, 41 della Costituzione.

sua accezione discende dal collegamento intimo con la dignità dell'uomo[20], principale fondamento su cui si basa l'ordinamento costituzionale di stampo liberaldemocratico nel contesto europeo[21].

Nel nostro testo costituzionale, il principio della dignità della persona trova esplicazione nell'articolo 2 quale clausola «a fattispecie aperta»[22], e dunque anche il diritto alla *privacy* si connota ontologicamente come diritto fondamentale.

Si tratta di una considerazione che mette bene in luce il motivo per cui esso ha legami forti con altre fattispecie di libertà più tradizionali[23], quali quelle negative, il che mette in luce una tendenza espansiva che si è andata rafforzando nel corso del tempo, sia in seguito agli apporti della dottrina sia, in particolare, della giurisprudenza.

In questo senso, il legame stretto con la tutela della libertà personale (art. 13)[24], con l'inviolabilità del domicilio (art. 14) e con la libertà e segretezza della comunicazione (art. 15)[25] rappresentano le connessioni più evidenti, poiché strettamente connaturate all'essenza della persona[26].

Ma vanno altresì ricordati, in un'ottica di circolarità interpretativa, i casi opposti, vale a dire le situazioni in cui la tutela della riservatezza ha prodotto un ampliamento del contenuto dei diritti fondamentali classici, come ad esempio la libertà personale che si espande anche della dimensione della tutela della libertà morale del singolo[27].

---

[20] Come affermava in altri tempi M. MAZZIOTTI DI CELSO, *Diritto all'immagine e Costituzione*, in *Giurisprudenza costituzionale*, 1970, p. 1533, l'interesse alla riservatezza rappresenta infatti una vera e propria «condizione necessaria perché la persona sia libera di svilupparsi autonomamente, il che non potrebbe avvenire se tutti gli aspetti della sua vita potessero essere noti al pubblico».

[21] Sul tema v. almeno P. GROSSI, *Dignità umana e libertà nella Carta dei diritti fondamentali dell'Unione europea*, in M. SICLARI (a cura di), *Contributi allo studio della Carta dei diritti fondamentali dell'Unione europea*, Torino, 2003 nonché M. DI CIOMMO, *Dignità umana e Stato costituzionale*, Firenze, 2010 e relativa appendice giurisprudenziale.

[22] Sulla teorizzazione di questo concetto, cfr. A. BARBERA, *Art. 2*, in G. Branca (a cura di), *Commentario della Costituzione. Principii fondamentali, art. 1-12*, Bologna-Roma, 1975, p. 66.

[23] Cfr. G. BUSIA, *Riservatezza (diritto alla)*, in *Digesto delle discipline pubblicistiche*, agg., 2000, p. 481.

[24] Cfr. A.M. SANDULLI – A. BALDASSARRE, *Profili costituzionali della statistica in Italia*, in *Diritto e società*, 1973, p. 383; P. CARETTI, *I diritti fondamentali: libertà e diritti sociali*, Torino, 2005, pp. 243-244.

[25] Cfr. A. CERRI, *Riservatezza (diritto alla)*, *Diritto costituzionale*, in *Enciclopedia giuridica*, vol. XXVIII, Roma, 1995, p. 5.

[26] Non si possono inoltre trascurare gli inevitabili richiami a profili più peculiari, quali del diritto all'esercizio privato del culto religioso (art. 19), del diritto al nome (art. 22), dell'inviolabilità del diritto di difesa (art. 24), dei diritti propri alla formazione familiare (art. 29), del diritto alla salute, anche come rispetto della persona nell'assoggettamento ai trattamenti sanitari obbligatori (art. 32).

[27] L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, p. 14.

Così come rafforza la sua connotazione come diritto fondamentale il fatto che il diritto alla *privacy* possa fungere, in taluni casi, da limite alle stesse libertà costituzionalmente riconosciute e tutelate[28], come nel caso, ad esempio, della libertà di manifestazione del pensiero (art. 21)[29].

A conferma del riconoscimento di questa natura, si registra inoltre il contributo fornito dalle principali Carte dei diritti di carattere internazionale e sovranazionale: partendo dalla Dichiarazione universale dei diritti dell'uomo del 1948 (art. 12) e dalla Convenzione europea dei diritti dell'uomo del 1950 (art. 8); passando per la Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata dal Consiglio d'Europa nel 1981; per arrivare, in tempi più recenti, alla Carta dei diritti fondamentali dell'Unione europea del 2000 (artt. 7 e 8) e, infine, al Trattato sul funzionamento dell'Unione europea (art. 16), come riscritto dal Trattato di Lisbona del 2007.

Va inoltre nella medesima direzione anche l'opera ermeneutica svolta dalle supreme corti italiane, qualificabile spesso come una costante attività di trasformazione di istanze provenienti dalla società in veri e propri diritti tutelati dall'ordinamento e azionabili di fronte ai giudici[30], spesso impiegando gli accordi internazionali sui diritti come strumento ermeneutico del diritto interno.

Tratteggiata brevemente la natura del diritto alla *privacy* nella sua evoluzione, ai fini del presente lavoro è necessario concentrarsi anche sul contenuto del diritto, poiché è stato oggetto anch'esso di una significativa trasformazione[31].

La configurazione originale del diritto alla *privacy* era notoriamente riconducibile al «*right to be let alone*», quel «diritto ad essere lasciato solo» teorizzato dagli statunitensi Warren e Brandeis sul finire del XIX secolo. Esso dunque nasceva come diritto alla «riservatezza», ossia come tutela della sfera personale e intima dalle aggressioni esterne.

---

[28] Sul «vincolo alla riservatezza» quale limite inteso come «costellazione di diritti», cfr. F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Torino, 1995, pp. 20-21.

[29] Cfr. A. PACE, in A. PACE – M. MANETTI, *Rapporti civili: la libertà di manifestazione del proprio pensiero*, in G. BRANCA – A. PIZZORUSSO (a cura di), *Commentario della Costituzione*, Bologna-Roma, 2006, p. 146; A. CATAUDELLA, *La tutela civile della vita privata*, Milano, 1972, p. 34.

[30] Meritano pertanto una particolare menzione le sentt. nn. 122/1970, 38/1973, 139/1990, 366/1991, 81/1993, 135/2002 e 271/2005 della Corte costituzionale. ~~MA~~ Tuttavia giova qui richiamare anche la pronuncia sul cd. "caso Soraya" della Corte di Cassazione (Cass., sez. I civ., 27 maggio 1975, n. 2129).

[31] Sul tema del diritto alla riservatezza, la bibliografia è sconfinata e dunque si vedano almeno A. BALDASSARRE, *Privacy e costituzione: l'esperienza statunitense*, Roma, 1974; G. BUTTARELLI, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1997; L. CALIFANO, *Privacy: affermazione, op. cit.*; ID., *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. CALIFANO – C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, 2014; U. DE SIERVO, *Tutela dei dati personali e riservatezza*, in AA. VV., *Diritti, nuove tecnologie, trasformazioni sociali: scritti in memoria di Paolo Barile*, Padova, 2003; S. RODOTÀ, *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 1974 e ID., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 1997; G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza,* in R. NANIA – P. RIDOLA (a cura di), I diritti fondamentali, vol. II, Torino, 2006, pp. 619 ss.

A questo profilo antico del diritto si è andato affiancando un significato nuovo, in considerazione soprattutto di uno sviluppo tecnologico tanto imponente (nella portata e velocità del progresso) quanto esteso (nella sua capacità di toccare e influenzare la vita di qualunque abitante del pianeta), che ha moltiplicato le forme di comunicazione e potenziato le memorie di archiviazione.

Oggi, infatti, l'aspetto della tutela della riservatezza viene ad essere affiancato ed integrato dai profili riguardanti la protezione dei dati, in ragione del fatto che i dati, soprattutto se personali, rappresentano un presupposto irrinunciabile per lo svolgimento delle attività umane.

Con questo cambiamento, muta dunque anche in parte sia l'oggetto della tutela, che evolve da sfera privata a contenuto inerente le informazioni dell'individuo, sia la qualità della stessa: da tradizionale libertà negativa (liberi da ingerenze esterne) ora viene ad essere integrata da un diritto all'autodeterminazione informativa posto in capo all'individuo.

Viene infatti riconosciuta a ciascun soggetto la facoltà di scegliere che cosa fare dei dati che lo riguardano, quali e quanti di questi mettere a disposizione degli altri, quali operazioni su di essi possono essere svolte, a quale ambito di circolazione essi possono essere destinati. Questo «concetto di autodeterminazione informativa»[32] viene a trovare una sua dimensione concreta attraverso l'istituto del consenso al trattamento dei dati, come peraltro sancito anche dall'art. 8 della Carta di Nizza[33]. Il consenso potrebbe dunque costituire il presupposto principale per la tutela dei diritti, divenendo l'«elemento centrale nella garanzia per l'effettività del diritto fondamentale»[34].

La positivizzazione della disciplina sulla tutela dei dati personali nel contesto europeo ha preso avvio con la direttiva 95/46/CE, la cd. direttiva madre su cui si sono poi stratificati ulteriori, successivi, interventi[35]. Sulla base dell'impulso comunitario – in parte anche obbligato, in seguito alla necessità di rendere operativo il trattato di Schengen – anche l'Italia ha introdotto una disciplina organica sulla protezione dei dati personali[36], mentre sino ad allora la nostra normativa era caratterizzata solo da alcuni interventi

[32] L. CALIFANO, *Privacy: affermazione*, *op. cit.*, p. 15.

[33] L'articolo 8, dedicato proprio alla «Protezione dei dati di carattere personale» merita di essere riportato testualmente: «1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[34] L. CALIFANO, *Privacy: affermazione*, *op. cit.*, p. 92 e vedi anche pp.ss.

[35] Si vedano le seguenti direttive: 2002/58/Ce sulla protezione dati nel settore delle comunicazioni elettroniche; 2006/24/Ce sulla conservazione dei dati sul traffico telefonico; dir. 2009/136/Ce di modifica della 2002/58/Ce. Si aggiunga il regolamento Ue 611/2013 sulla violazione dei dati personali (il c.d. *data breach*).

[36] Per una ricostruzione del diritto anche alla luce delle evoluzioni legislative nel nostro ordinamento v. M. TIMIANI, *Un contributo allo studio sul diritto alla riservatezza*, in Studi parlamentari e di politica costituzionale, n. 176/2012, pp. 51ss.

limitati, sia come settori interessati che come livello di garanzie riconosciuto. Si fa naturalmente riferimento alla legge 675/1996 che è confluita di lì a poco nel d.lgs. 196/2003, il Codice in materia di protezione dei dati personali (cd. Codice *privacy*), a carattere generale e trasversale.

Si tratta di una normativa che veicola nel nostro Paese i principi fondamentali che reggono il sistema della protezione dati (necessità, finalità, proporzionalità, liceità, ecc.), i diritti riconosciuti agli individui (accesso, cancellazione, aggiornamento, opposizione, ecc.), gli istituti di garanzia (informativa, consenso, sistema delle autorizzazioni, ecc.); ma che istituisce altresì l'Autorità preposta alla vigilanza sull'effettiva tutela di questo diritto fondamentale, il Garante per la protezione dei dati personali.

Questo quadro è tuttavia destinato a mutare a breve, sia nel nostro ordinamento sia nel contesto europeo: nel maggio 2016 è stato adottato il Regolamento generale in materia di protezione dei dati personali (Ue) 2017/679, che sostituisce le vecchie direttive, innovando significativamente la disciplina[37].

Esso contiene infatti dei significativi passi in avanti in termini di garanzie, con la positivizzazione di nuovi diritti (uno su tutti, il diritto all'oblio) e l'irrobustimento di strumenti conosciuti (come informativa e consenso); pone l'accento sulla responsabilizzazione di chi i dati li tratta (sul solco del principio di *accountability*); ridisegna l'architettura delle istituzioni, con il rafforzamento dei poteri delle Autorità di controllo e l'avvio di forme stringenti forme di cooperazione, estendendo addirittura l'applicazione della disciplina e, dunque, i corrispondenti controlli, anche ai fornitori di servizi *internet* che abbiano sede al di fuori dell'Ue (se destinati a cittadini dell'Ue).

Si tratta di un passo in avanti non solo dal punto di vista del contenuto ma anche sul piano degli strumenti impiegati per la tutela del diritto: la scelta dell'Unione europea di disciplinare la materia con lo strumento del regolamento sottintende infatti la volontà di uniformare l'effettività del diritto stesso, riducendo i margini di differenziazione fra i singoli stati ma al contempo determinando la necessità di verificare la compatibilità delle norme di diritto interno vigenti.

In sintesi, l'espansione del contenuto del diritto alla *privacy* è caratterizzata da un dialogo costante fra giudici e legislatore nel contesto italiano, ma si è intrecciata più volte e in maniera sempre più intensa con la dimensione europea, anche per quanto concerne le ricadute e gli effetti di una tutela multilivello dei diritti sempre più robusta. E oggi deve affrontare le sfide che l'entrata in vigore di un Regolamento europeo unitario pone anche all'interno dei singoli stati membri.

Per quanto riguarda invece il quadro normativo in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, al contrario si è deciso di impiegare lo strumento

[37] Per un primo e articolato commento v. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016.

della direttiva (Ue) 2016/680) per introdurre un'importante revisione: in questi settori il legislatore europeo ha preferito lasciare un più ampio margine di discrezionalità in capo agli Stati membri.

E dunque la differenza fra un diritto fondamentale che deve essere garantito su tutto il territorio e a tutti i cittadini, e una esigenza di sicurezza, un interesse collettivo, che viene considerata come fondamentale ma comunque territorialmente differenziabile, in ragione di scelte sovrane dei singoli Stati che tengano conto di diverse peculiarità, pare emergere anche sotto il profilo degli strumenti impiegati per la disciplina dei rispettivi ambiti.

4. Le nuove sfide nel contesto degli ordinamenti statuali europei.

Le nuove sfide al diritto alla *privacy* in epoca di terrorismo evocate in precedenza derivano sia da recenti decisioni delle istituzioni dell'Unione europea sia da interventi normativi dei singoli stati membri.

Partendo dalle disposizioni di natura sovranazionale, un primo esempio è contenuto nel nuovo pacchetto protezione dati, ed è costituito in particolare dalla direttiva 2016/681 in materia di acquisizione e conservazione del Codice di prenotazione dei passeggeri (Pnr, *Passenger name record*).

Essa istituisce un enorme database contenente i dati di tutti coloro che salgono su voli aerei la cui partenza ovvero destinazione si trovi all'interno del territorio europeo[38].

Il rischio percepito in maniera più netta è che l'accesso a tale archivio possa essere effettuato anche da autorità di Paesi terzi[39], dove le garanzie di *privacy* potrebbero essere minori. In questo senso naturalmente riaffiorano alla mente le preoccupazioni suscitate dal cd. scandalo Datagate di cui si è detto in avvio.

Ma altri, chiari, esempi, arrivano di nuovo dalla Francia[40], dove, nei mesi successivi alla strage presso la redazione di Charlie Hebdo e all'interno del supermercato Hyper Cacher nella periferia parigina (gennaio

[38] I dati raccolti sono di vario genere, tra cui l'itinerario di viaggio, le informazioni sul biglietto, i contatti forniti dal viaggatore, sino alle modalità di acquisto e pagamento e alle informazioni sul bagaglio.

[39] Vi è da dire che il nuovo strumento della direttiva va ad inserirsi nella già lunga e controversa vicenda degli accordi con gli Stati Uniti in tema di PNR. Un primo accordo negoziato all'indomani dell'11 settembre 2001 e che consentiva il trasferimento dei dati di viaggio di tutti i passeggeri europei alle autorità statunitensi è stato invalidato dalla Corte di Giustizia dell'Unione europea il 30 maggio 2006, nelle cause riunite C-317/04 e C-318/04. Successivamente vi sono stati altri due accordi rispettivamente nel 2007 e nel 2011. Per uno dei primi commenti sul tema si veda F. CLEMENTI – G. TIBERI, *Sicurezza interna, diritti e cooperazione internazionale nella lotta al terrorismo: i casi Pnr e Swift*, in *Astrid Rassegna*, n. 1/2013.

[40] Per un commento si rinvia a R. CASELLA, *La Francia dopo gli attentati di Parigi. La dichiarazione dello stato d'urgenza e la proposta di revisione costituzionale del Presidente Hollande*, in *Nomos*, n. 3/2015. In seguito agli attentati dell'autunno del 2015 e dopo un tentativo fallito per via legislativa negli anni precedenti – su cui sia consentito il rinvio a M. RUBECHI, *La "déchéance de nationalité" nelle proposte di modifica della normativa sulla cittadinanza e l'immigrazione francese*, in Democrazia e Sicurezza, n. 1/2011 – in Francia si è tentato di disciplinare direttamente in Costituzione la perdita della nazionalità per coloro che avessero commesso crimini che attentassero gravemente alla vita della nazione. Il progetto di revisione costituzionale, che conteneva un più ampio pacchetto di misure per la «protezione della Nazione» tra cui la costituzionalizzazione dello stato d'urgenza, è decaduto: il Presidente della Repubblica, constatata la mancanza d'accordo su un testo condiviso tra i due rami del Parlamento, ha dichiarato la sua

2015), il Consiglio dei Ministri aveva presentato un progetto di legge di riforma complessiva dei servizi segreti e del sistema di intercettazioni telefoniche e conservazione dei dati di traffico telematico, chiedendo che il Parlamento lo esaminasse secondo la procedura accelerata[41].

a. Prima della presentazione in Consiglio dei Ministri, il Governo aveva tuttavia consultato la *Commission nationale informatique et libertés* (Cnil), l'Autorità di protezione dati francese, e da questo primo confronto erano emerse numerose criticità. Le preoccupazioni riguardavano soprattutto l'indeterminatezza e la mancanza di criteri nell'individuazione dei tipi di dati di navigazione che i servizi segreti potevano captare direttamente presso i fornitori di servizi di comunicazioni elettroniche, con una raccolta di metadati pressoché illimitata e praticamente automatica. In secondo luogo, l'Autorità di protezione dati francese era apparsa molto scettica rispetto al silenzio del testo sulle modalità di conservazione dei dati recuperati nell'ambito delle operazioni di sorveglianza[42].

Anche al fine di placare le varie voci critiche dentro e fuori il Parlamento, il Presidente della Repubblica Hollande aveva dunque intrapreso una iniziativa alquanto inedita, pur se costituzionalmente prevista (articolo 61, comma 2 della Costituzione), ovvero la decisione di adire egli stesso, per la prima volta rispetto a una legge ordinaria, il *Conseil constitutionnel*. Anche in questo caso, in coerenza con una serie di decisioni più inclinate sul versante della sicurezza che non su quello della *privacy*, il *Conseil* ha poi stabilito che la legge era conforme a Costituzione, fatta eccezione per alcune disposizioni in tema di geolocalizzazione e alle misure di "sorveglianza internazionale" (intercettazione di conversazioni effettuate o ricevute all'estero)[43].

Ancor più recentemente, il Governo Valls ha deciso, tramite decreto[44], di istituire il TES (*titres électroniques sécurisés*,), un unico database – contenente foto, dati biometrici e impronte digitali di ogni cittadino francese, unitamente all'indirizzo di residenza e a dati di contatto come la posta elettronica – che unifica tutti i dati contenuti in due registri che sino ad alla sua introduzione erano sempre stati separati: quello

intenzione di non convocare il Parlamento in seduta comune per procedere con l'approvazione della riforma, facendo così di fatto decadere la proposta di revisione (art. 89, commi 1 e 2 della Costituzione).

[41] Il progetto è poi divenuto legge n. 2015-912 del 24 luglio 2015, cd. "*loi relative au renseignement*".

[42] *Délibération n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement*. Vi è da dire che alcuni dei rilievi formulati dall'Autorità di protezione dati francese sono poi stati superati dal testo legislativo definitivo. Il parere è reperibile sul sito della Cnil al seguente link https://www.cnil.fr/fr/publication-de-lavis-sur-le-projet-de-loi-relatif-au-renseignement.

[43] *Décision n.* 2015-713 DC del 23 luglio 2016. Solo successivamente, una volta adito dal Consiglio di Stato su sollecitazione originaria di alcune associazioni, lo stesso *Conseil* si è spinto a dichiarare non conforme a Costituzione la disposizione della medesima legge che consentiva «*la surveillance et le contrôle des transmissions empruntant la voie hertzienne*» senza particolari autorizzazioni né giudiziarie né amministrative. V. per completezza anche *Décision n.* 2016- 590 QPC del 21 ottobre 2016

[44] *Décret* n. 2016-1460 del 28 ottobre 2016.

dei passaporti e quello della *Carte Nationale d'Identité*[45]. La misura, introdotta nell'ottica di un rafforzamento delle misure anti-contraffazione e anti-falsificazione, ha stabilito tuttavia che a poter accedere al TES potranno essere i funzionari pubblici incaricati della realizzazione di passaporti o carte d'identità, ma anche la polizia giudiziaria, i servizi segreti, la *Police Nationale* o i gendarmi esclusivamente per «bisogni legati alle loro funzioni», senza che venga configurato alcun particolare onere di motivazione a cui subordinare l'accesso.

Consultata prima dell'emanazione del decreto, l'Autorità di protezione dati francese, ha espresso alcune remore sul nuovo sistema, in particolare riguardo alle scarse misure di sicurezza volte a tutelare i dati biometrici, nonché alla indeterminatezza delle finalità e delle categorie di soggetti che possono avere accesso a TES e, infine, ha invitato il Governo a coinvolgere anche il Parlamento in merito a delle disposizioni dall'indiscutibile impatto sulla tutela dei diritti fondamentali.[46]

Ma le recenti innovazioni non riguardano solo la Francia, vittima di una sanguinosa serie di attacchi terroristi, ma anche altri importanti paesi europei, come la Gran Bretagna, dove il Parlamento sta esaminando l' *Investigatory powers bill*[47], un disegno di legge dal grande impatto sulla tutela della libertà e segretezza delle comunicazioni nonché della *privacy* dei cittadini: se approvato nei contenuti originari, sarà permesso alle autorità investigative di svolgere intercettazioni telefoniche e telematiche sostanzialmente a tappeto, senza che i fornitori dei relativi servizi possano disattendere tale ordine; inoltre, potranno essere acquisite e conservate per un anno le informazioni concernenti i siti web oggetto di navigazione.

Ma si pensi anche alla Germania dove, a poco più di due mesi dagli attentati di Monaco, il 21 ottobre 2016 il Bundestag ha approvato una legge di riforma dei poteri investigativi dell'Agenzia per la sicurezza esterna tedesca (BND), che riguarda in particolare il potenziamento della possibilità di intercettare le conversazioni via *internet* di stranieri non solo per contrasto ad atti di terrorismo ma anche a fini di prevenzione, con il rischio peraltro di introdurre una discutibile differenziazione fra cittadini tedeschi e cittadini stranieri.

---

[45] L'obiettivo era di accentrare a livello nazionale la procedura, riducendo così il coinvolgimento degli uffici territoriali, e operare controlli più stringenti soprattutto tra i dati biometrici di chi richiede l'emissione di nuovi documenti di identità.

[46] *Délibération n° 2016-292 du 29 septembre 2016 portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité* (saisine n° 1979541). Pubblicato sulla Gazzetta Ufficiale del 30 ottobre 2016.

[47] Originariamente HC Bill 143, attualmente all'esame della Camera dei Lords.

Il legislatore italiano finora è intervenuto in materia di antiterrorismo solo affrontando la questione dei cd. *foreign fighters* con il decreto legge 18 febbraio 2015, n. 7, che contiene primariamente[48] disposizioni di carattere penalistico, anche in attuazione della Risoluzione del Consiglio di sicurezza dell'Onu del 2014[49] che obbligava gli Stati membri ad adottare misure di contrasto a questo fenomeno.

Uno spunto interessante sul versante della tutela della *privacy* ci giunge invece dalla giurisprudenza di legittimità.

In un recente pronunciamento, la Corte di Cassazione ha, infatti, avallato una significativa restrizione delle libertà fondamentali per fini di accertamento dei reati. La Corte ha ammesso che captatori informatici, o agenti intrusivi – comunemente definiti, nel gergo informatico, *trojan* – vengano veicolati sotto forma di *virus* tramite l'invio di email, messaggi o il *download* di applicazioni dalla rete e installati da remoto sui telefoni cellulari e *tablet* delle persone sospettate, al fine di registrare le conversazioni captate[50]. In altre parole, si tratta di una moderna forma di intercettazione ambientale, che rappresenta una sorta di superamento delle tradizionali microspie.

La Suprema Corte ha acconsentito al ricorso, da parte degli investigatori, a questo nuovo mezzo, attenuando probabilmente così alcune garanzie tradizionalmente richieste per le intercettazioni. Nonostante l'impiego dello strumento del *trojan* debba essere preventivamente autorizzato dal giudice come per le tradizionali intercettazioni, le conversazioni raccolte potrebbero infatti svolgersi all'interno di una privata dimora, senza che tale luogo debba essere preventivamente individuato nel decreto che dispone l'intercettazione ovvero senza, ad esempio, che sia necessariamente in corso l'attività criminosa. Insomma, appare evidente come l'aver considerato legittimo uno strumento d'indagine così potente comporti, per lo meno sotto il profilo che qui maggiormente rileva, l'aver sposato una visione che assegna un peso diverso (minore che in passato) alla tutela delle libertà costituzionali dell'individuo (libertà e segretezza della corrispondenza, inviolabilità del domicilio, tutela della sfera intima e privata) di fronte a

[48] Sotto il profilo più strettamente inerente la *privacy*, il decreto ha modificato l'art. 53 del d.lgs. 196/2003 (Codice *privacy*). Sino ad allora infatti le forze di pubblica sicurezza potevano effettuare trattamenti di dati personali in deroga a diverse garanzie contenute nel Codice solo se tale possibilità era prevista da una norma di legge. La novella prevede invece che questi trattamenti in deroga possano essere disposti anche sulla base di una fonte regolamentare.

[49] Risoluzione S/RES/2178 per contrastare i *foreign fighters*, ovvero cittadini europei di fede islamica che hanno trascorso periodi di addestramento all'estero. In esecuzione della risoluzione Italia, Belgio, Francia, Germania, Regno Unito, Paesi Bassi e Danimarca hanno adottato misure legislative anti-terrorismo. Il decreto legge italiano, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, contiene disposizioni inerenti soprattutto il versante penalistico, quindi di repressione del fenomeno, oltre a prevedere misure emergenziali attuabili anche dal Questore, come il ritiro del passaporto per chi è sospettato di volersi recare all'estero con finalità di addestramento. Per una definizione del concetto di *Foreign terrorist fighter* v. M. SOSSAI, Foreign terrorist fighters*: una nozione ai confini del diritto internazionale*, in Federalismi.it, 25 settembre 2015.

[50] Cassazione Penale, Sezioni Unite, 1 luglio 2016, n. 26889. Per un primo commento sui risvolti penalistici si veda M. T. ABBAGNALE, *In tema di captatore informatico*, in *Archivio penale*, n. 2/2016.

interessi ritenuti oggi prioritari come la sicurezza in generale e, nel caso di specie, le attività di prevenzione svolte dalle autorità di pubblica sicurezza.

Anche se il caso sottoposto alla Corte di cassazione era relativo a fattispecie connesse alla criminalità organizzata di stampo mafioso, la prevalenza data alle ragioni di sicurezza ben potrebbe consentire, a voler leggere tra le righe della sentenza, l'applicazione di questi nuovi strumenti di indagine al contrasto del fenomeno terroristico[51].

I cd. captatori informatici e gli strumenti di accesso ai sistemi informatici da remoto hanno, invece, finora ricevuto un trattamento più prudente da parte di tribunali di altri paesi membri dell'Unione europea. Si riporta qui il caso del Tribunale costituzionale federale tedesco[52], il quale, in un'articolata sentenza resa il 20 aprile 2016, ha sottoposto ad un rigido scrutinio di proporzionalità una serie di disposizioni della legge federale tedesca sull'attività delle forze di polizia (Bundeskriminalamtgesetz – BKAG) che rendevano possibili forme di sorveglianza occulta e impiego di mezzi informatici per acquisire dati da remoto[53].

In particolare le disposizioni relative alla sorveglianza delle case private con raccolta di dati audio-video e l'impiego dei *trojan* sono stati ritenuti strumenti non in grado di assicurare una protezione sufficiente della sfera privata, anche perché i dati raccolti avrebbero dovuto essere esaminati direttamente dall'ufficio federale di polizia, invece che da soggetti esterni e indipendenti.

Nei singoli Stati sembra dunque prevalere una tendenza all'inasprimento delle misure di prevenzione e sicurezza analoga a quella che si registrò dopo gli attentati dell'11 settembre 2001 a partire dal *Patrioct Act* americano, seppur con modalità diverse rispetto ad allora e più inerenti la sfera personale e la protezione dei dati del singolo, nel contesto digitale in cui tali sfide vengono avanzate.

5. Sicurezza e tutela della riservatezza nella giurisprudenza della Corti sovranazionali.

Data il maggio 2016 l'adozione del cd. «pacchetto protezione dati», costituito dal nuovo Regolamento generale (2016/679), nonché dalla direttiva che specificamente declina questi principi all'interno delle

[51] Ecco un passaggio significativo della sentenza in tal senso: «è invece consentita la captazione nei luoghi di privata dimora ex art. 614 cod. pen., pure se non singolarmente individuati e se ivi non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica, secondo la previsione dell'art. 13 d.l. n. 152 del 1991».

[52] BVerfG del 20 aprile 2016, 1 BVR 966/09, 1BVR 1140/09. Un primo commento in L. GIORDANO – A. VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *Diritto penale contemporaneo*, 2016.

[53] Non si dimentichi, peraltro, che il 27 febbraio 2008 il *Bundesverfassungsgericht* aveva affermato in maniera forte la tutela della *privacy* a confronto con le esigenze di indagine, dichiarando l'illegittimità costituzionale di una legge che consentiva di accedere da remoto ai sistemi informatici dei privati per visionarne i contenuti e nonché le pagine relative alla navigazione sul *web*. BVerfG del 27 febbraio 2008, 1BVR 370/97.

attività giudiziarie e di polizia (2016/680)[54]. Il che di per sé mette in evidenza, come illustrato *supra* (§3), un volontà di positivizzazione del diritto alla *privacy* e la necessità di una sua tutela omogenea su tutto il territorio europeo.

Ma a livello europeo anche gli interventi di carattere giurisprudenziale mostrano come tale diritto si sia evoluto e affermato in maniera molto decisa, in un dialogo costante fra legislatore e corti che ha permesso di estendere la portata del diritto alla *privacy*, pur nel contesto delle gravi sfide terroristiche.

In quest'ottica, la Corte di giustizia dell'Unione europea ha emesso negli ultimi anni alcune pronunce dall'impatto rilevante rispetto alle politiche securitarie finora attuate. Tralasciando in questa sede la nota sentenza cd. Google Spain del 2014[55] – molto importante sul piano dell'affermazione di nuove forme di protezione dei dati personali, ma non pertinente ai fini della trattazione in oggetto –, sono due le pronunce cui ci si riferisce.

L'8 aprile 2014 nella sentenza comunemente richiamata come il caso *Digital Rights Ireland*[56], i giudici hanno dichiarato invalida la direttiva 2006/24/CE del Parlamento europeo e del Consiglio – che modifica la direttiva 2002/58/CE – 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 (cd. *data retention*)[57].

La decisione è rilevante sia nel merito, sia perché costituisce un precedente procedurale importante: si tratta infatti del primo caso in cui la Corte ha annullato per intero un atto di diritto derivato perché in contrasto con disposizioni della Carta dei diritti fondamentali.[58]

Il caso sorgeva su due domande di pronuncia pregiudiziale avanzate, rispettivamente, dalla *High Court of Ireland* e dal *Verfassungsgerichtshof* austriaco. La Corte ha verificato una netta incompatibilità delle

[54] Deve essere collocata in questo contesto l'approvazione della direttiva (Ue) 2016/681 sul già citato Pnr: quest'ultima normativa, da tempo bloccata da dubbi e discussioni, proprio a causa della sua portata estremamente invasiva (il fenomeno della «sorveglianza di massa»), oggi ha potuto beneficiare del veicolo fornito dal «pacchetto protezione dati» quale suo ideale contrappeso, approfittando delle pressioni inevitabilmente fattesi più forti a causa della violenza ed efferatezza raggiunta dalle azioni del terrorismo internazionale.

[55] Corte di giustizia dell'Unione europea, sentenza della Corte (Grande Sezione), 13 maggio 2014 nella causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Espanola de Protection de Datos (AEPD), Mario Costeja Gonzalez*.

[56] Corte di giustizia dell'Unione europea, sentenza della Corte (Grande Sezione), 8 aprile 2014 nelle cause riunite *Digital Rights Ireland Ltd* (C-293/12), *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a.* (C-594/12). La rilevanza di tale sentenza è messa in evidenza in S. BONFIGLIO, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in Democrazia e Sicurezza, n. 3/2014.

[57] Si tratta in buona sostanza di tutti i dati relativi al traffico riguardante la telefonia fissa, la telefonia mobile, l'accesso a *internet*, la posta elettronica su *internet* nonché la telefonia via *internet*, relativi a tutti gli abbonati e gli utenti registrati in Europa. Sono esclusi i contenuti delle suddette comunicazioni.

[58] Come evidenzia O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi*.it, n. 3/2014, p. 9.

disposizioni contenute nella direttiva con quelle della Carta dei diritti fondamentali dell'Unione europea riguardanti la tutela della vita privata e familiare (art. 7) e la protezione dei dati personali (art. 8).

Per la Corte, la finalità della direttiva consisteva nel garantire la disponibilità dei dati «a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale», al fine di «contribuire alla lotta contro la criminalità grave e, di conseguenza, in ultima analisi, alla sicurezza pubblica» (art. 1, par. 1). E dunque si trattava di finalità legittime, poiché rispondevano ad un rilevante interesse pubblico.

La compatibilità con il diritto dell'Unione europea di tali misure, tuttavia deve, secondo la Corte essere valutata applicando un severo *test* di proporzionalità. Che nel caso di specie, ha ritenuto non potesse essere superato.

In primo luogo, veniva prevista una raccolta e conservazione di una vasta mole di dati personali, senza contestualmente stabilire alcun criterio per una differenziazione tra i vari strumenti di comunicazione né, soprattutto, tra i diversi tipi di reati da perseguire e non tenendo conto dei profili soggettivi degli individui coinvolti.

Riguardo alla conservazione, la direttiva non delimitava in maniera proporzionata e ragionevole la possibilità per le Autorità nazionali di accedere a tali dati, mancando di indicare criteri o procedure atte a regolamentare tanto l'accesso ai dati conservati quanto il loro riutilizzo da parte delle Autorità medesime. E in ogni caso avrebbe dovuto stabilire, secondo la Corte, anche dei criteri che, in fase applicativa, fossero atti a garantire che la conservazione dei dati fosse limitata al tempo strettamente necessario.

La Corte ha continuato poi rilevando che non sono stati introdotti i necessari requisiti di sicurezza nelle modalità di conservazione dei dati da parte degli operatori, al fine di scongiurare possibili violazioni e che la conservazione dei dati in database e server collocati al di fuori del territorio dell'Unione europea, resa possibile dal silenzio della direttiva sul punto, sostanzierebbe una violazione delle garanzie che le Autorità di protezione dati europee devono assicurare agli interessati rispetto al loro diritto di autodeterminazione informativa[59].

In sintesi, la compressione del diritto alla protezione dati in nome della sicurezza interna e internazionale è risultato secondo la Corte sproporzionato rispetto alle finalità perseguite[60].

---

[59] Sempre in tema di conservazione, è importante inoltre ricordare che la direttiva ha fissato poi un termine generale di almeno sei mesi, (estendibili a un massimo di 24 mesi), applicabile indistintamente a tutti i dati «senza che venga effettuata alcuna distinzione tra le categorie di dati [*omissis*] a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate» e «senza che venga precisato che la determinazione della durata di conservazione debba basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario».

[60] Sul caso *Digital Rights Ireland* v. G. FINOCCHIARO, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Il diritto dell'informazione e dell'informatica,* 2015, p. 779 e O. POLLICINO, *Diritto all'oblio*

Lo scrutinio della Corte è stato particolarmente rigoroso anche in una successiva e rilevante sentenza, relativa al cd. *Safe Harbour.*[61] Anche nota come *caso Schrems* o caso *Facebook*, dal nome delle parti coinvolte, in questa decisione dell'ottobre 2015 la Corte ha invalidato l'intero meccanismo cd. di «approdo sicuro» che, basandosi su un accordo tra Commissione europea e Governo americano (decisione 2000/520 della Commissione), consentiva il trasferimento dei dati personali dei cittadini europei trattati da imprese e multinazionali verso gli Stati Uniti [62]. Il *Safe Harbour* era, dunque, la base legale che consentiva alle grandi multinazionali del *web* di operare in Europa mantenendo i propri *server* principali negli Stati Uniti.[63]

Il caso ha origine da un ricorso presentato da un utente austriaco di *Facebook*, Maximilian Schrems, il quale ha contestato presso l'Autorità di protezione dati irlandese il fatto che Facebook Ireland Ltd trasferisse negli Stati Uniti i dati personali dei propri utenti e li conservasse su *server* ubicati negli Usa[64].

Partendo, dunque, ancora una volta da un rinvio pregiudiziale – circostanza significativa se si considera che la Corte dovrebbe, per quella strada, fornire prevalentemente interpretazioni degli atti derivati – la Corte ha deciso di invalidare la decisione della Commissione sulla base di due motivazioni principali.

In primo luogo, anche se gli Stati membri sono tenuti a dare attuazione alla decisione della Commissione, nulla può impedire che un'Autorità di controllo di uno Stato membro possa esaminare la domanda di una persona relativa alla protezione dei suoi dati personali, anche se sono stati trasferiti da uno Stato

---

e conservazione di dati. La Corte di giustizia a piedi uniti verso un digital right to privacy, in *Giurisprudenza costituzionale,* 2014, p. 2949.

[61] Sentenza della Corte (Grande Sezione) del 6 ottobre 2015, *Maximillian Schrems contro Data Protection Commissioner* nella causa C-362/14.

[62] La Commissione può adottare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, una decisione che constata che un paese terzo garantisce un livello di protezione adeguato per i dati personali che vi giungono tramite trasferimento. La decisione della Commissione, poi, si applica a tutti gli Stati membri che dovranno conformarvisi.

[63] La decisione ha destato grande interesse in dottrina e numerosi sono stati i commenti. V. in particolare R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale*, 2016, p. 289-307; P. FALLETTA, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14)*, in *Federalismi.it*, n. 24/2015; V. ZENO ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Il diritto dell'informazione e dell'informatica,* 2015, p. 683. Un commento più incentrato sugli aspetti tecnologici è quello di C. COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa. A margine della sentenza "Safe harbour" della Corte di giustizia dell'Unione Europea*, in *Il diritto dell'informazione e dell'informatica,* 2015, p. 719.

[64] Schrems riteneva che, alla luce delle rivelazioni fatte da Edward Snowden in merito alle attività dei servizi di intelligence americana e alla facilità con cui questi accedevano a dati e metadati – come i riferimenti su mittente e ricevente, data e ora della conversazione, durata, ecc., oggetto in caso di comunicazione di posta elettronica –, gli Stati Uniti non offrissero ai cittadini europei delle garanzie sufficienti per i propri dati personali. Dal rifiuto dell'Autorità irlandese di dare corso alla denuncia presentata da Schrems, l'alta Corte d'appello irlandese ha poi interpellato in via pregiudiziale la Corte di Lussemburgo riguardo a come interpretare quelle disposizioni della direttiva privacy 95/46/CE che, rappresentando la base giuridica della decisione della Commissione, consentono il trasferimento verso paesi terzi. Conseguentemente ha inoltre richiesto se e in che misura si possano far valere i diritti degli interessati, qualora questi nutrano dei dubbi sull'adeguatezza e sicurezza dei propri dati personali all'interno del paese presso cui sono stati trasferiti.

membro verso un Paese terzo. Questo purché la persona interessata, come nel caso del ricorrente, «faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.» (par. 37).

I giudici poi entrano nel merito della valutazione della decisione della Commissione, alla luce non solo dei principi stabiliti all'interno della direttiva privacy del 1995 ma, soprattutto, delle disposizioni della Carta di Nizza a tutela della *privacy*. Il vaglio è inclemente e la decisione viene dichiarata incompatibile con le garanzie minime dei diritti fondamentali in più punti.

Oltre ad esprimere dei dubbi sui meccanismi di auto-certificazione in materia di *data protection* adottati dalle aziende americane, la Corte si concentra sulle deroghe che la decisione prevede possano applicarsi al rispetto della *privacy* in ragione del «primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» sui principi dell'approdo sicuro, giungendo a stabilire che in quell'ordinamento non sussistono le garanzie minime richieste nel continente europeo, poiché non si riscontrano specifiche fonti di rango legislativo in grado di assicurare che l'accesso e le ingerenze sui dati conservati avvengano alla luce di particolari procedure e garanzie; e non viene inoltre previsto alcun meccanismo di rimedio giudiziale per i cittadini europei in caso di violazione dei propri dati.

Infine, in maniera ancora più netta la Corte ricorda, proprio menzionando il richiamato caso *Digital Rights Irlanda*, come le deroghe e restrizioni alla *data protection* debbano essere limitate allo stretto necessario. La normativa americana, invece, consente una raccolta massiva e indiscriminata di dati, a cui, altrettanto indiscriminatamente, le autorità pubbliche possono accedere in qualsiasi momento e questo certamente non risponde al requisito di necessità appena richiamato.

Si è riportato in maniera diffusa il contenuto della decisione, poiché essa ha avuto un effetto deflagrante nei rapporti commerciali e politici tra Europa e Stati Uniti, tanto che si sono immediatamente messi in moto i nuovi negoziati diplomatici per giungere ad una nuova versione dell'accordo il quale, almeno attenendoci al piano normativo-istituzionale, è intervenuto sotto due profili.

Da una parte, gli Stati Uniti hanno approvato, il 2 giugno 2015, il *Freedom Act*, cioè la nuova e più liberale legge che disciplina l'attività di sorveglianza da parte delle autorità federali, sostitutivo del *Patriot Act* del 2001[65]. Dall'altra, è stato approvato il nuovo accordo tra Ue ed Usa, adottato dalla Commissione europea il 12 luglio 2016, sostitutivo del *Safe Harbour*, definito *Privacy Shield*, dai contenuti più garantistici nei

[65] Significativo, in quest'ottica, è l'intervento restrittivo sulla raccolta e sull'uso delle intercettazioni, e in particolare dei metadati (testo reperibile sul sito del Congresso: https://www.congress.gov/bill/114th-congress/house-bill/2048/text).

confronti dei cittadini europei i cui dati finiscono negli Stati Uniti per effetto di trasferimenti interni ai colossi americani delle Ict che operano sul nostro territorio[66].

Ma se il giudice di Lussemburgo negli ultimi anni ha accentuato la sua attenzione verso i diritti fondamentali – soprattutto a partire dal Trattato di Lisbona in poi, per effetto della definitiva "costituzionalizzazione" della Carta dei diritti di Nizza –, forse a ciò ha contribuito anche l'influenza esercitata dal giudice di Strasburgo, forte di decenni di esperienza nel campo proprio della difesa dei diritti inviolabili della persona.

Anche nella giurisprudenza della Corte europea per i Diritti dell'uomo si ritrovano difatti solidi argini alla proliferazione di restrizioni al godimento delle libertà dovute ad un potenziamento delle politiche di sicurezza[67].

Con particolare riferimento al delicato rapporto fra sicurezza e *privacy*, risulta di fondamentale importanza la sentenza resa il 12 gennaio 2016, nella causa *Szabò e Vissy c. Ungheria*, con cui ha pesantemente censurato il *Police Act* approvato nel 2011 dal Parlamento magiaro. E ciò non solo, naturalmente, per il tema cui si riferisce, ma anche poiché questa decisione è stata presa all'indomani degli attentati terroristici di Parigi e dunque sull'onda emotiva suscitata da tali eventi[68].

Il giudice dei diritti è tuttavia stato infatti severo, censurando il sistema intrusivo di perquisizione, intercettazione e registrazione, da effettuarsi sia fisicamente che tramite strumenti informatici, che la normativa magiara introduceva senza la previsione di adeguate garanzie a tutela della persona interessata. Nello specifico, la legge antiterrorismo metteva in pratica un'attività di sorveglianza indiscriminata, deliberata su decisione del Ministro della Giustizia, senza che fosse necessario produrre prove in grado di comprovarne la necessità. Il tutto era accompagnato da una durata sostanzialmente illimitata delle

[66] In sintesi, le principali tutele consistono in: «obblighi di protezione stringenti per le imprese che trasferiscono dati; misure di sicurezza in materia di accesso ai dati da parte del Governo degli Stati Uniti; strumenti specifici per la tutela delle persone; la revisione annuale congiunta dell'accordo per monitorarne l'attuazione». (Tratto dal sito del Garante per la protezione dei dati personali, http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5306161).

[67] La Corte europea per i diritti dell'uomo ha da sempre posto una particolare attenzione alla tutela del «diritto al rispetto della vita privata e familiare» (come recita l'art. 8 della Convenzione), soprattutto nel rapporto con le esigenze di prevenzione e accertamento dei reati, nonché di sicurezza: cfr. sent. 2 agosto 1984, *Malone c. Regno Unito*; sent. 24 aprile 1990, *Kruslin c. Francia*; sent. 4 maggio 2000, *Rotaru c. Romania*; sent 22 ottobre 2002, *Taylor-Sabori c. Regno Unito*; sent. 28 gennaio 2003, *Peck c. Regno Unito*; sent. 17 luglio 2003, *Perry c. Regno Unito*; sent. 29 marzo 2005, *Matheron c. Francia*; sent. 31 maggio 2005, *Vetter c. Francia*; sent. 3 aprile 2007, *Copland c. Regno Unito*; sent. 2 dicembre 2008, *K. c. Finlandia*; sent. 4 dicembre 2008, *S. e Marper c. Regno Unito*; sent. 27 ottobre 2009, *Haralambie c. Romania*; sent. 17 dicembre 2009, *Bouchacourt c. Francia*, *Gardel c. Francia* e *M.B. c. Francia*; sent. 18 aprile 2013, *M.K. c. Francia*.

[68] È giusto infatti sottolineare come il giudice dei diritti abbia voluto rimarcare la perdurante valenza dei principi di necessità, finalità e proporzionalità proprio in un momento fortemente critico, quando i diritti inviolabili della persona appaiono sotto l'attacco dei nemici della democrazia, ma sono altresì – e come conseguenza – esposti al rischio di sospensione/minimalizzazione da parte delle stesse autorità pubbliche.

misure di controllo (per effetto del meccanismo delle proroghe), in assenza di qualsiasi forma di controllo giudiziario a tutela da eventuali abusi.

E dunque sia la Corte di Giustizia dell'Unione europea con decisioni di impatto interno e internazionale rilevantissime, sia la Corte europea per i diritti dell'Uomo con decisioni in controtendenza rispetto al sentimento comune, hanno arginato i tentativi di potenziamento degli strumenti di sicurezza che avrebbero potuto determinare una eccessiva compressione del diritto alla *privacy*. Sul tema della *privacy*, dunque, le Corti sovranazionali sono recentemente intervenute quasi all'unisono, in difesa di un diritto fondamentale potenzialmente a rischio come quello in oggetto.

Ma al contempo hanno anche proceduto a dare chiare indicazioni di merito ai legislatori, fissando principi in maniera decisamente dettagliata, in modo tale da consentire anche il loro recepimento in successivi atti normativi deliberati a livello europeo: è il caso, per l'appunto, del nuovo regolamento europeo approvato nel 2016.

Qualche spunto ulteriore e qualche supporto alla causa della tutela del diritto alla *privacy* nel contesto del potenziamento delle politiche di prevenzione potrebbero, infine, giungere anche da Corti che stanno dall'altra parte dell'Oceano Atlantico.

La scorsa primavera, la nota azienda di prodotti informatici Microsoft ha infatti intentato un'azione giudiziaria nei confronti del Dipartimento di Giustizia degli Stati Uniti, denunciando l'aumento esponenziale di richieste di accesso, da parte delle autorità federali, agli innumerevoli dati personali da essa detenuti, e associati a milioni e milioni di persone, tra cui, inevitabilmente, tantissimi europei, fruitori dei suoi servizi informatici[69]. A luglio 2016 la Corte d'appello federale[70] ha dichiarato inaccessibili alle autorità statunitensi i dati custoditi in *server* posti al di fuori del territorio Usa, come, ad esempio, in Europa.

E l'azione di Microsoft non è risultata isolata, poiché si è mossa sugli stessi binari del conflitto che ha interessato un altro colosso dell'informatica: Apple, nei confronti dell'Fbi. Un conflitto che probabilmente si ricorderà poiché l'agenzia federale di sicurezza è riuscita a violare, avvalendosi di consulenti *hacker* esterni, il sistema di decrittazione da Apple ai propri telefoni cellulari, al fine di accedere allo *smartphone* utilizzato dall'autore della strage di San Bernardino dello scorso dicembre, dopo che la stessa Apple si era opposta all'ordinanza ingiuntale dal magistrato federale appositamente interpellato dal Fbi.

[69] I dati rappresentati dall'azienda Microsoft sono particolarmente significativi: delle 5.624 richieste di accesso intentate, quasi la metà (2.576) erano accompagnate dal divieto (anche a tempo indeterminato) di informare gli interessati degli accessi stessi.

[70] v. *U.S. Court of Appeals*, 2nd Cir., del 14 luglio 2016 (Docket No. 14-2985).

Non sfugge naturalmente che dietro queste azioni giudiziarie ci siano interessi economici precisi, che hanno spinto queste multinazionali dell'industria informatica ad appellarsi alla tutela della *privacy* per difendersi dalle richieste di accesso delle forze di pubblica sicurezza. Ciò nonostante, è innegabile che il fenomeno della regolamentazione dell'accesso ai dati sensibili, sotto il profilo del diritto alla *privacy*, stia assumendo anche negli Stati Uniti un rilievo crescente, in ragione di interventi sempre più decisi dell'autorità di pubblica sicurezza, giustificati dall'emergenza (ormai perdurante[71]) di vincere la lotta al terrorismo.

Il che, non da ultimo, potrebbe certamente offrire nuovi spunti di approfondimento nella ricerca di un equilibrio dinamico fra sicurezza e *privacy*.

6. Sicurezza e privacy dopo i più recenti attacchi terroristici: considerazioni di sintesi.

Sicurezza e privacy si confrontano su sfide antiche. Ma in un contesto nuovo, caratterizzato dalla generalizzazione dell'impiego della rete *internet* da parte di alcune fasce della popolazione e da nuove modalità informatiche di comunicazione, che le declina in maniera diversa.

Di fronte all'avvento del terrorismo internazionale che di quei nuovi mezzi fa ampio uso per superare le barriere statuali ed eludere le tradizionali tecniche di polizia, il potenziamento degli strumenti di prevenzione e di controllo occulto da parte delle autorità di pubblica sicurezza è importante al fine di garantire la sicurezza della popolazione.

Ma al contempo è necessario che vengano individuati nuovi limiti e nuove tutele per il diritto alla *privacy* sia per ciò che concerne il suo profilo più tradizionalmente riconducibile alla riservatezza, sia per quel che riguarda la tutela dei dati personali e la loro, dunque, diffusione indiscriminata.

Si tratta di una nuova modalità di leggere la tradizionale tensione fra la necessità di potenziare gli strumenti di polizia per garantire maggiore sicurezza da un lato e le eventuali compressioni ai diritti fondamentali dell'uomo derivanti da questa operazione. Ed è necessario trovare un punto di equilibrio di non semplice momento.

Soprattutto in circostanze storiche in cui episodi terroristici mettono a repentaglio la vita dei cittadini e di conseguenza il sentimento della popolazione si indirizza verso una maggiore richiesta di misure di polizia e di prevenzione, si tende a considerare favorevolmente il potenziamento degli strumenti di controllo e protezione.

In tempo di pace, invece, le misure legislative si concentrano maggiormente sulla tutela dei diritti, imponendo limiti stringenti all'azione delle forze di pubblica sicurezza.

[71] Si sottolinea la perduranza nel tempo dello stato di allerta per il terrorismo in G. DE MINICO, *Libertà fondamentali in tempo di ordinario terrorismo*, in Federalismi.it, n. 10/2015.

La necessità di garantire la sicurezza dei cittadini da un lato e tutelare i loro diritti dall'altro oscillano dunque fra loro come un pendolo, che si sposta verso la tutela dei diritti quando le condizioni economiche e sociali sono più stabili o va nella direzione di una maggiore attenzione alle problematiche relative alla sicurezza, quando più decise sono le richieste in tal senso da parte della popolazione.

Ma mai un ordinamento democratico può tollerare che, anche in presenza di gravi minacce, possano venire compressi i diritti fondamentali riconosciuti e garantiti a tutti i cittadini, in ossequio alla necessaria salvaguardia della dignità umana, da cui discendono tutti i diritti di libertà che il nostro ordinamento tutela direttamente o indirettamente.

Più che di un bilanciamento fra diritti in senso tecnico, è dunque necessario individuare la proporzionalità delle misure introdotte, rispetto alla necessaria salvaguardia del nucleo centrale del diritto interessato. Diritto alla *privacy* e interesse collettivo alla sicurezza pari non sono dal punto di vista della dimensione costituzionale, e allora è necessario commisurare il loro rapporto in termini di ragionevolezza e proporzionalità, essendo il limite al diritto certamente giustificato in ossequio ad un interesse collettivo, ma senza che esso si possa mai estendere oltre la compressione del nucleo essenziale del diritto.

Per quanto riguarda il rapporto fra il diritto alla *privacy* e sicurezza, nel contesto dei singoli stati dell'Unione europea sono state recentemente introdotte normative più marcatamente orientate ad un potenziamento degli strumenti di controllo e prevenzione, soprattutto delle telecomunicazioni e del traffico *internet*. Le risposte sono naturalmente diverse e differenziate sono state anche le modalità con cui i corrispettivi tribunali delle leggi si sono orientate rispetto ad esse: da soluzioni più restrittive delle libertà in Francia avallate in tutto o in parte dal *Conseil constitutionnel* a orientamenti più prudenti come nel contesto tedesco, caratterizzato da una Corte costituzionale storicamente attenta alla tutela dei diritti.

Ma un elemento di interesse si riscontra nel fatto che la *privacy*, da «diritto giurisprudenziale» sia divenuto un diritto codificato, grazie ad un dialogo virtuoso tra giudice e legislatore. E questo sia a livello di Unione europea, sia nell'entrata del diritto medesimo nell'ambito dell'ordinamento costituzionale italiano attraverso la lettura a fattispecie aperta dell'articolo 2 della Costituzione.

A livello europeo, l'incisività delle decisioni della Corte europea di giustizia a tutela del diritto alla *privacy* è stata elevata, proprio nei confronti di misure limitative del diritto giustificate da ragioni di sicurezza e nonostante il contesto favorevole ad un inasprimento delle misure di prevenzione e controllo. Sia che si sia trattato di tutelare i rapporti fra cittadini dell'Unione europea nei confronti di stati terzi che intendevano impiegare i loro dati, sia che si fosse di fronte ad una valutazione sulle modalità di conservazione dei dati raccolti dalle autorità all'interno del continente, gli interventi della Corte di Lussemburgo sono stati nettamente orientati verso la limitazione degli spazi di intervento delle autorità, a tutto vantaggio della tutela del nucleo essenziale del diritto. Che nel corso delle sue decisioni ha definito

in maniera sempre più puntuale, a partire dalle tempistiche di conservazione dei dati, sino alle modalità di accesso e di eventuale trasmissioni a terzi.

E questo, peraltro, intervenendo in merito quasi con gli strumenti tipici di una corte interna, trasformando dei giudizi pregiudiziali, che in genere vengono impiegati per fornire interpretazioni di atti di legislazione derivata, in giudizi di merito basati su parametri contenuti nella Carta di Nizza[72].

E adesso il diritto alla *privacy*, così come interpretato dalle Corti, ritorna negli ordinamenti nazionali in maniera omogenea, attraverso l'approvazione del regolamento europeo nella primavera del 2016: lanciando così una sfida di adeguamento a tutti i paesi europei.

In particolare nel nostro ordinamento, le sfide potranno risultare particolarmente affascinanti sotto il profilo giuridico, considerando il modo con cui il diritto alla *privacy* si è affermato in via giurisprudenziale, spesso appoggiandosi sul suo riconoscimento formale nelle Carte dei diritti sovranazionali.

Spesso le decisioni delle Corti europee sono andate inoltre ad integrare l'interpretazione del diritto nazionale, estendendo il diritto alla *privacy* ben oltre la tradizionale connotazione di libertà negativa, sino a trasformarlo anche in parte in un diritto di disporre dei propri dati. Ma andando altresì ad ampliare la portata di altri diritti per suo tramite o a costituire la ragione di una loro limitazione.

Insomma, il diritto alla *privacy*, nonostante le sfide del terrorismo e anzi, probabilmente anche grazie alle compressioni che ha subito in ragione delle risposte repressive al terrorismo stesso, non ha cessato di estendere la sua portata contenutistica.

Anche quando il pendolo oscilla dalla parte della sicurezza, infatti, il sistema di tutela multilivello dei diritti nel continente europeo ha mostrato – al momento in cui si scrive – di avere gli anticorpi per tutelare il nucleo essenziale, incomprimibile, dei diritti fondamentali, «con entrambe le Corti sovranazionali […] che paiono concorrere alla costruzione dei tasselli di un vero e proprio sistema di garanzie dei diritti»[73].

E ciò risulta a maggior ragione importante perché la minaccia al terrorismo, seppur con modalità differenziate, perdura ormai da molti anni, ed è dunque necessario trovare un equilibrio stabile, ancorché flessibile, tra politiche di sicurezza e prevenzione e tutela delle libertà fondamentali in generale e della *privacy* in particolare.

---

[72] In questo senso v. anche O. POLLICINO, *Interpretazione*, *op. cit.*, p. 9, il quale nota come la Corte di giustizia dell'Unione europea abbia messo in evidenza con questa decisione «la sua mal celata vocazione di giudice para-costituzionale e quindi di custode della legalità, per l'appunto costituzionale, in Europa»

[73] Così E. MALFATTI, *I "livelli" di tutela dei diritti fondamentali nella dimensione europea*, Torino, 2015, p. 271.