medialaws
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 7/2016

ANNALISA REGI*

La Corte Costituzionale tedesca affronta il tema dei limiti alle investigazioni compiute con strumenti di sorveglianza occulta: come contemperare il dovere dello Stato di proteggere la popolazione dalle gravi forme di criminalità con la garanzia dei diritti fondamentali della persona?

Nota a Bundesverfassungsgericht, I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09

1. *Premessa.*

Bene innanzitutto rappresentare che, con sentenza del 20 aprile 2016, la Corte Costituzionale Federale tedesca (*Bundesverfassungsgericht* - BVerfG) ha preso in

* Avvocato in Milano, specializzanda presso il Corso di perfezionamento e di specializzazione in Diritto penale "Giorgio Marinucci"

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

considerazione il tema dei limiti alle investigazioni compiute dalla polizia federale, ricorrendo a misure di sorveglianza occulte, al fine di proteggere la società dalle minacce del terrorismo internazionale.

Al riguardo, la Corte ha rilevato che il ricorso alle predette misure da un lato risulta compatibile con i diritti fondamentali riconosciuti all'individuo dalla Costituzione; dall'altro viola, sotto alcuni specifici aspetti, il principio di proporzionalità, in forza del quale va condotto il bilanciamento tra interessi contrapposti, *id est* prerogative individuali e poteri pubblici.

Nella sentenza sono state inoltre affrontate anche altre due rilevanti questioni: il trasferimento dei dati raccolti dalla polizia federale ad altre autorità nazionali e, per la prima volta, i presupposti per la consegna dei dati raccolti ad autorità di Paesi terzi[2].

Come vedremo, al termine del proprio *iter* argomentativo, la Corte ha dichiarato l'incostituzionalità di alcune disposizioni della *Bundeskriminalamtgesetz* (BKAG), ossia della legge federale che disciplina i compiti e l'attività del *Bundeskriminalamt* (BKA - Ufficio Criminale Federale), nonché la cooperazione in materia penale tra i governi statali e quello federale e con i Paesi terzi.

Al fine di poter meglio comprendere la pronuncia in commento, è opportuno rammentare che il diritto di polizia in Germania è stato caratterizzato negli anni da alcune modifiche e tendenze evolutive, che riflettono le problematicità derivanti dall'assenza di un'autorità di pubblica sicurezza attiva a livello federale, ma anche dalla necessità di adeguare periodicamente l'organizzazione delle predette autorità di pubblica sicurezza alle differenti esigenze emerse nelle diverse fasi storiche attraversate dalla Repubblica Federale[3].

In primis, tra gli anni '60 e '80 dello scorso secolo, si è assistito ad una «*soggettivizzazione del* modus operandi *delle forze di polizia*», atteso che a queste ultime è stato concesso di

[2] Bene sin da subito chiarire che la dicitura "Paesi terzi" non intende fare riferimento agli Stati membri dell'Unione europea.

[3] A. DE PETRIS, *Le forze di pubblica sicurezza in Germania. Tra necessità di coordinamento, effettività di intervento e rispetto dell'organizzazione federale*, in *ds*, anno III, n. 1, 2013, 12 aprile 2013, 5.

procedere sulla base non solo di pericoli oggettivamente esistenti, ma anche di valutazioni erronee, in grado di giustificare tuttavia il sospetto di una situazione di pericolo per la sicurezza pubblica. Siffatta modifica ha comportato, a sua volta, «*una soggettivizzazione normativa rispetto alle forme di intervento delle autorità di sicurezza*», le quali hanno dovuto iniziare a considerare (nell'assumere le proprie decisioni) non solo la collettività complessivamente intesa, ma anche i singoli individui.

In terzo luogo, sono mutate anche le modalità operative da seguire nell'attività di contrasto preventivo della criminalità organizzata. Al riguardo, la prassi abituale prevedeva «*una legittimazione normativa e giurisdizionale delle sole informazioni raccolte nell'attività di* intelligence *direttamente finalizzata all'eliminazione di organizzazioni criminali*»: conseguentemente, tutti i dati personali raccolti in iniziative non qualificabili come indagini di polizia esulavano dal predetto obbligo di legalizzazione, malgrado costituissero comunque un'intrusione nella sfera dei diritti fondamentali del soggetto interessato. In seguito, atteso che «*la moderna lotta all'illegalità non può più legittimarsi come esclusiva reazione a reati già commessi*», è stata valorizzata anche la funzione di contrasto preventivo contro possibili azioni criminali. Ed è così che si è iniziato a raccogliere dati e informazioni «*su persone e situazioni sospette a prescindere dall'effettiva presenza di delitti al momento delle investigazioni*», con conseguente «*indebolimento di quelle forme di tutela dei diritti individuali che le iniziative delle forze di polizia erano in precedenza tenute molto più strenuamente ad osservare*»[4].

Infine, tra le più attuali tendenze evolutive in tema di sicurezza pubblica in Germania, merita rilevare «*la spinta all'accentramento delle competenze in materia*», ovvero il loro trasferimento dagli ambiti inferiori a quelli superiori dell'ordinamento. In particolare, si è recentemente assistito «*ad una continua trasmigrazione di potestà di polizia dalle amministrazioni comunali ai* Länder*, e da questi alla Federazione*».

In riferimento alla pronuncia in commento, è bene precisare che al *Bundeskriminalamt* sono stati riconosciuti poteri sempre più ampi nell'ambito della lotta contro la criminalità

[4] *Ivi*, spec. 5-7.

organizzata, quali la funzione di coordinamento della cooperazione tra Federazione e *Länder*, e tra le autorità di polizia nazionali ed internazionali.

Il trasferimento verso l'alto di siffatte competenze è riconducibile ai seguenti motivi: a) la difficile situazione finanziaria dei *Länder* (i quali non erano particolarmente interessati a conservare potestà il cui esercizio si traduceva in un onere particolarmente gravoso sui loro bilanci); b) il cambiamento della situazione ai confini nazionali (dal momento che i controlli non venivano più posti in essere sul fronte occidentale, mentre erano divenuti assai più blandi su quello orientale, le autorità federali non potevano validamente esercitare la loro funzione di protezione dei confini senza operare direttamente anche nel territorio interno, ovvero in quello che sarebbe originariamente lo specifico ambito di competenza dei *Länder*); c) il diverso agire della criminalità organizzata, che non si muove più in ambiti esclusivamente regionali o sub - statuali, richiedendo, per poter essere contrastata, un intervento delle pubbliche autorità che non può arrestarsi di fronte ai confini territoriali interni[5].

A ben vedere, le predette giustificazioni sono alla base non solo del trasferimento verso l'alto delle competenze, ma anche dello sviluppo della collaborazione e della razionalizzazione delle relazioni tra autorità nazionali e sovranazionali nella lotta alla criminalità organizzata.

2. *Bundesverfassungsgericht, I Senato, 20 aprile 2016: un unicum nel panorama giurisprudenziale della Corte Costituzionale tedesca?*

Bene precisare che la pronuncia qui in commento segue una storica sentenza della stessa Corte Costituzionale Federale tedesca del 27 novembre 2008[6], in cui per la prima volta è stato

[5] *Ivi*, spec. 7-10.
[6] *Bundesverfassungsgericht*, 27 febbraio 2008, in *Riv. trim. dir. pen. econ*., 2009, III, 679 ss.

riconosciuto un nuovo diritto costituzionale alla riservatezza ed integrità dei sistemi tecnologici di informazione.

La Corte era stata chiamata a valutare la costituzionalità di una legge che autorizzava i servizi segreti del Nord Reno–Westfalia a controllare ed investigare clandestinamente sulla rete internet. In particolare, la norma (art. 5, comma secondo, n. 11 della legge sulla protezione della Costituzione del Nord Reno–Westfalia) avrebbe garantito ai servizi segreti il diritto di intercettare e cercare in modo occulto comunicazioni via internet ed accedere segretamente ai sistemi tecnologici di informazione.

Ad avviso della Corte, siffatte attività investigative interferivano con diritti costituzionalmente garantiti e, pertanto, qualsiasi legge che le consentisse doveva dimostrare che le predette attività erano giustificate dalla protezione di altri diritti costituzionali, che le stesse erano necessarie per assicurare tale protezione e che erano proporzionate nel loro impatto.

Al riguardo, la sentenza in commento ha ritenuto la norma in questione non conforme alla Costituzione.

Ripercorrendo l'*iter* argomentativo seguito dalla Corte, occorre porre in evidenza che la stessa, «*dinnanzi alle potenzialità operative del nuovo strumento, non [ha] escluso in assoluto l'ammissibilità di tale strumento di indagine, ma [ha] ritenuto insufficienti le garanzie costituzionali a tutela della segretezza delle comunicazioni, dell'inviolabilità del domicilio*[7]».

La medesima, inoltre, non si è limitata ad applicare i principi costituzionali già esistenti,

ma ha riconosciuto un nuovo diritto costituzionale: il diritto fondamentale alla riservatezza ed integrità dei sistemi tecnologici, che è stato collocato all'interno del più esteso diritto all'integrità della personalità.

In particolare, la Corte, ritenendo che «*i principi costituzionali della segretezza delle comunicazioni, [del]l'inviolabilità della dimora e [de]l diritto all'autodeterminazione dell'informazione*

[7] L. GIORGANO, A. VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in www.penalecontemporaneo.it.

non coprissero di fatto la violazione ai diritti personali del caso [in esame],» atteso che tutti e tre i principi non considererebbero debitamente «*l'incidenza delle tecnologie nella formazione della personalità e l'incidenza delle operazioni sul computer come dato di per sè oggetto di valutazione*», ha colmato la lacuna normativa individuata, creando un nuovo diritto, che tutela «*l'interesse degli utenti di un sistema tecnologico di informazione a che i dati creati, trattati e memorizzati rimangano riservati*»[8].

Merita notare come l'organo supremo tedesco abbia applicato le garanzie del nuovo diritto ai sistemi tecnologici di informazione, ma non abbia fornito una «*definizione di tale sistema*». Il medesimo ha invece «*elenca[to] i sistemi che non sono protetti da questo diritto e [ha] forni[to] una descrizione delle capacità minime che un sistema tecnologico informatico deve possedere per rientrare nel campo di applicazione della tutela di questo diritto fondamentale. Così facendo, [ha] manten[uto] molto ampia la portata della protezione del diritto e volutamente [ha] evita[to] il riferimento a tecnologie specifiche. In tal modo, [ha] riconosc[iuto] chiaramente la rapida evoluzione tecnologica dei dispositivi tecnologici di informazione e con la sentenza in esame [ha] tenta[to] di creare una normativa neutrale per la tecnologia, cercando quindi di mantenere il nuovo diritto fondamentale a prova di futuro*»[9].

In ogni caso, il diritto alla segretezza ed integrità dei sistemi tecnologici di informazione non è assoluto, posto che lo stesso può essere limitato «*sia per motivi di prevenzione che per perseguire crimini*». Tuttavia, qualsiasi misura che limiti tale diritto deve essere proporzionata alla violazione e, al riguardo, la Corte ha precisato che il requisito di proporzionalità è soddisfatto solo laddove esistano «*prove sufficienti che significativi valori fondamentali di rango superiore [quali la vita e l'integrità degli altri cittadini, i fondamenti dello Stato e i valori essenziali di umanità] debbano essere protetti*»[10].

---

[8] F. BESEMER, *Un nuovo diritto costituzionale in Germania? Quale status per il diritto alla riservatezza ed integrità dei sistemi tecnologici di informazione?*, in www.dirittocomparati.it.
[9] A. WIEBKE, *La decisione della Corte Costituzionale tedesca sul diritto alla riservatezza ed integrità dei sistemi tecnologici d'informazione – un rapporto sul caso BVerfGE NJW 2008,* 822, in www.jei.it.
[10] *Ibidem.*

Successivamente, sempre nella sentenza, la Corte ha poi mitigato il predetto requisito, affermando che non è richiesto un alto grado di probabilità che un pericolo si verifichi in un prossimo futuro.

Ciascuna di tali misure deve essere inoltre esaminata e confermata da un giudice con una valutazione da compiere di volta in volta, al fine di assicurare un controllo oggettivo e indipendente prima dell'esecuzione.

Infine, ogni misura restrittiva del nuovo diritto costituzionale non deve violare l'area centrale della gestione privata della vita, la quale include, tra l'altro, la comunicazione e l'informazione a proposito di sentimenti intimi e relazioni profonde[11].

In sintesi: «*la soluzione tedesca al problema del bilanciamento di interessi tra la lotta alla criminalità e la riservatezza dei singoli nei sistemi informatici è stata l'introduzione del nuovo principio costituzionale*»[12]. Ed è proprio dal contrasto tra quest'ultimo principio e l'attività di *intelligence* disciplinata dall'art. 5, comma secondo, n. 11 della legge sulla protezione della Costituzione del Nord Reno–Westfalia che è scaturita la declaratoria di incostituzionalità di quest'ultima norma. Insomma, gli utenti, secondo siffatta pronuncia, «*godono di una legittima aspettativa di riservatezza rispetto ai dati ricavabili dall'uso della tecnologia informatica e devono essere tutelati contro l'accesso segreto*»[13].

[11] *Ibidem.*

[12] F. BESEMER, *Un nuovo diritto costituzionale in Germania? Quale status per il diritto alla riservatezza ed integrità dei sistemi tecnologici di informazione?*, cit.

[13] 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*, cit.

3. *Il principio di proporzionalità quale guida nel bilanciamento tra valori costituzionali contrapposti.*

Tanto premesso e rappresentato, occorre mettere in evidenza che nella sentenza del 20 aprile 2016 la Corte, da un lato, ha precisato che l'attribuzione all'Ufficio Criminale Federale del potere di raccogliere segretamente dati personali implica gravi interferenze nella vita privata; dall'altro, ha tuttavia riconosciuto che il ricorso a mezzi efficaci di raccolta delle informazioni risulta basilare per la protezione contro le minacce provenienti dal terrorismo internazionale all'ordine democratico e ai diritti fondamentali.

Alla luce di ciò, emerge con immediata evidenza quale sia compito del Legislatore: raggiungere un equilibrio tra il dovere dello Stato di proteggere la collettività dalla criminalità organizzata, prevenendo i reati, e la garanzia dei diritti fondamentali dell'individuo all'inviolabilità del domicilio, alla segretezza delle comunicazioni, nonché alla riservatezza e all'integrità dei sistemi informatici[14].

Ora, in siffatto scenario, il Legislatore deve effettuare il bilanciamento tra i contrapposti valori costituzionali in forza del principio di proporzionalità, in base al quale «*i poteri investigativi che incidono in maniera profonda sulla vita privata vanno limitati dalla legge alla tutela di interessi sufficientemente rilevanti nei casi in cui sia prevedibile un pericolo sufficientemente specifico a detti interessi*»[15].

Ed è proprio dal principio di proporzionalità che la Corte ha fatto discendere alcuni corollari, precisando innanzitutto che la raccolta segreta di dati personali può estendersi

[14] «*It is the legislature's task to find a balance between the severity of interferences with fundamental rights on the one hand and the duty of the state to protect the population on the other*» (così nella traduzione inglese del comunicato stampa della Corte Costituzionale Tedesca, comunicato stampa n. 19/2016 del 20 aprile 2016, consultabile su www.bundesverfassungsgericht.de.

[15] 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*, cit.; gli interessi rilevanti che legittimano l'utilizzo di misure di sorveglianza segrete sono individuati, a mero titolo esemplificativo, nella salute, nella vita e nella libertà della persona, così come nell'esistenza o nella sicurezza della Federazione o di un *Land*.

dall'individuo oggetto dell'indagine a soggetti terzi soltanto in condizioni particolari[16] e che occorre preservare in maniera rigorosa il nucleo della vita privata, ricorrendo a norme in grado di incrementare il livello di garanzia[17].

In secondo luogo, la medesima ha evidenziato la necessità di tutelare le persone che sono titolari del segreto professionale[18] e di esercitare i poteri investigativi con estrema trasparenza, sotto il controllo giurisdizionale[19].

L'organo supremo tedesco ha inoltre chiarito l'esigenza di informare le parti interessate e di metterle nelle condizioni di attivare un controllo giurisdizionale, una volta che le misure siano state attuate, nonché di prevedere un obbligo di relazione al Parlamento e all'opinione pubblica[20].

Da ultimo, lo stesso ha rappresentato che i requisiti per poter cancellare i dati personali raccolti dopo il loro impiego devono essere previsti *ex lege*[21].

4. *Analisi delle disposizioni impugnate.*

[16] «*Only under limited conditions may the investigative powers also extend to persons from whom the threat does not emanate and who belong to the target person's sphere*»: così, nella traduzione inglese del comunicato stampa della Corte, cit.

[17] «*With regard to powers which typically lead to interference with the strictly protected core area of private life, particular protective rules are needed*»: così nella traduzione inglese del comunicato stampa della Corte, cit.

[18] «*Sufficient protection of persons subject to professional confidentiality is also required*»: così nella traduzione inglese del comunicato stampa della Corte, cit.

[19] «*Moreover, the powers are subject to constitutionally required standards of transparency, individual legal protection and judicial review*»: così nella traduzione inglese del comunicato stampa della Corte, cit.

[20] «*Stemming from these standards are duties to inform the affected parties after the measures have been carried out, powers of judicial review, supervisory control on a regular basis, as well as reporting requirements vis-à-vis the Parliament and the public*»: così nella traduzione inglese del comunicato stampa della Corte, cit.

[21] «*Finally, these investigative powers must be supplemented by requirements to delete the recorded data*»: così nella traduzione inglese del comunicato stampa della Corte, cit.

Si rende ora opportuno esaminare le disposizioni della *Bundeskriminalamtgesetz* (BKAG) dichiarate incostituzionali dalla Corte Costituzionale Federale tedesca, disposizioni contenute nella sottosezione della legge relativa alla prevenzione delle minacce terroristiche internazionali, nei paragrafi da 20a a 20x, introdotte il 25 dicembre 2008, con efficacia dal 1 gennaio 2009.

4.1. Ripercorrendo l'*iter* seguito dalla Corte, quest'ultima ha preso innanzitutto in considerazione l'utilizzo di mezzi speciali di sorveglianza in luoghi differenti dal domicilio, quali l'osservazione, la registrazione audio-video, l'applicazione di dispositivi di localizzazione o l'uso di informatori della polizia – disciplinati nel paragrafo 20g, da 1 a 3, della BKAG -, rilevando che la legge non limita sufficientemente i poteri attribuiti all'Ufficio Criminale Federale in relazione a siffatti strumenti, atteso che:

- l'impiego dei predetti mezzi finalizzato alla prevenzione dei reati e non soltanto alla protezione da determinate minacce non è vietato in assoluto, ma è permesso nel rispetto di alcuni limiti, richiedendosi la prevedibilità di uno specifico fatto-reato, almeno per quanto attiene alla sua natura, o la probabilità specifica – desunta dal comportamento di un individuo – che quest'ultimo possa nel prossimo futuro commettere reati terroristici. Essendo tali limiti assenti nelle disposizioni in questione, risulta evidente come le stesse non consentano il controllo dei mezzi utilizzati da parte dell'autorità giudiziaria e non rispettino il principio di proporzionalità;

- le prescrizioni impugnate non prevedono, nel permettere la raccolta e l'analisi dei dati personali, misure volte a garantire la tutela dell'ambito rigorosamente riservato della vita privata, da preservare dall'ingerenza pubblica;

- quanto al monitoraggio a lungo termine o all'ascolto di conversazioni non pubbliche, le norme richiedono una preventiva autorizzazione giudiziaria soltanto in alcuni casi e comunque dopo un mese dall'inizio della misura.

4.2. La Corte si è poi soffermata sulla normativa della sorveglianza delle case private, che consente la raccolta di dati audio-video – contenuta nel paragrafo 20h della BKAG -, ritenendo che la medesima soddisfi soltanto parzialmente il principio di proporzionalità, in quanto:

- recando un grave pregiudizio alla riservatezza, la mancata limitazione della misura al solo individuo c.d. "bersaglio" (da cui proviene la minaccia) si pone in contrasto con l'art. 13 della Grundgesetz (GG, Legge Fondamentale). A ben vedere, è evidente che una tale misura non possa colpire i terzi estranei, se non in modo meramente indiretto;
- implicando un'ingerenza nell'ambito assolutamente riservato della vita privata, è necessario – al fine di appurare se i dati raccolti contengono informazioni strettamente private - che i medesimi vengano esaminati da un organismo indipendente, prima di essere utilizzati dall'Ufficio Criminale Federale, fatti ovviamente salvi i casi di pericolo immediato.

4.3. L'organo supremo tedesco si è in seguito occupato della disciplina che permette l'accesso ai sistemi informatici da remoto - paragrafo 20k della BKAG -, constatando come la stessa non protegga sufficientemente lo spazio rigorosamente riservato della vita privata, dal momento che al controllo sono preposti non soggetti esterni e indipendenti, ma componenti dell'Ufficio Criminale Federale.

4.4. La pronuncia si è inoltre soffermata sulla normativa – paragrafo 20l della BKAG - che estende l'impiego delle intercettazioni e della raccolta dei dati di traffico alla prevenzione dei reati. Siffatta disciplina risulta soltanto parzialmente compatibile con la Costituzione, dal momento che prevede un'estensione basata su presupposti generici e non ben definiti.

4.5. In riferimento a tutti i poteri di indagine e di sorveglianza, bene rappresentare che la Corte ha individuato l'assenza di alcune previsioni supplementari, in mancanza delle quali i limiti costituzionali non sono rispettati, posto che:

- la protezione delle persone che possono avvalersi del segreto professionale non è validamente tracciata, basandosi sulla distinzione tra il difensore e gli altri avvocati. Non avendo le misure di sorveglianza occulte in questione lo scopo di perseguire i reati, ma quello di proteggere dalle minacce, ben si comprende come tale distinzione non risulti idonea alla tutela dei consulenti legali;

- i requisiti costituzionali non sono completamente soddisfatti dalle norme finalizzate ad assicurare la trasparenza, la tutela legale e l'impugnazione. Non sono infatti presenti adeguate specificazioni sulla revisione obbligatoria delle misure, sulla documentazione che consenta la predetta revisione, nonché sui doveri informativi nei confronti del Parlamento e dell'opinione pubblica;

- la disposizione della cancellazione dei dati raccolti non è sufficiente, essendo possibile memorizzare dati in vista di ulteriori utilizzi a scopo preventivo o precauzionale per il futuro perseguimento di un reato di considerevole importanza (paragrafo 20v della BKAG).

4.6. Dopo la trattazione dei limiti alle investigazioni compiute dalla polizia federale ricorrendo a misure di sorveglianza occulte, la Corte è passata ad analizzare la questione relativa al trasferimento dei dati raccolti dall'Ufficio Criminale Federale ad altre autorità nazionali. Importante porre in evidenza che, prima di affrontare siffatta problematica, la stessa ha ritenuto opportuno sviluppare nuove distinzioni per poter utilizzare i dati raccolti in procedimenti diversi e, al riguardo, è ricorsa a due importanti principi: quello dello scopo e quello del mutamento dello scopo[22].

[22] «*The principles of purpose (Zweckbindung) and change in purpose (Zweckanderung) are relevant here*»: così nella traduzione inglese del comunicato stampa della Corte, cit.

Quanto all'ulteriore uso degli elementi raccolti entro l'ambito dello scopo originale, occorre rilevare che lo stesso è generalmente permesso, perseguendo come obiettivo la protezione del medesimo interesse del procedimento principale. Se le informazioni provengono dalla sorveglianza di abitazioni private o dall'accesso a sistemi informatici, alla base di qualsivoglia utilizzo ulteriore dei dati ottenuti tramite esse vi devono tuttavia essere gli stessi presupposti delle misure originarie.

Quanto invece all'uso delle informazioni per uno scopo differente da quello originario, il medesimo è consentito «*per perseguire reati diversi di gravità tale per cui l'adozione di misure analoghe sarebbe consentita sulla base dei medesimi presupposti delle misure applicate nel procedimento originario*» [23]. Anche in siffatto caso, laddove i dati provengano dalla sorveglianza di abitazioni private o dall'accesso a sistemi informatici, il loro utilizzo nell'ambito di procedimenti per reati diversi è permesse solo al ricorrere delle stesse condizioni giustificanti l'adozione delle misure originarie.

4.7. Tanto chiarito, la Corte Costituzionale Federale tedesca ha affrontato la questione relativa al trasferimento delle informazioni raccolte con gli strumenti di sorveglianza occulta ad altre autorità nazionali (paragrafo 20v della BKAG).

In primis, la medesima ha messo in evidenza che non sussistono rilievi circa il potere dell'Ufficio Criminale Federale di utilizzare i dati ottenuti da altre autorità per salvaguardare la popolazione dalle minacce del terrorismo internazionale. A ben vedere, il predetto potere risulta tuttavia sproporzionato in relazione alle informazioni provenienti dalla sorveglianza di abitazioni private o dall'accesso a sistemi informatici, atteso che, in siffatta ipotesi, un ulteriore utilizzo può essere consentito soltanto al ricorrere di un pericolo imminente o di una situazione di rischio sufficientemente specifica.

[23] Così 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*, cit.

In secondo luogo, ha ritenuto troppo generica e non in grado di soddisfare i requisiti costituzionali la previsione della possibilità di utilizzare ulteriormente le informazioni raccolte da altre autorità per la protezione dei testimoni o di altre persone.

Da ultimo, ha sostenuto l'incostituzionalità del potere di trasferire i dati raccolti per la prevenzione dei reati di terrorismo ad altre autorità nazionali, in quanto il trasferimento degli stessi è effettuato a prescindere dall'esistenza di una specifica base probatoria per ulteriori indagini. A siffatto proposito, occorre rilevare che: a) non sussiste alcuna garanzia volta a limitare alla persecuzione di gravi reati il trasferimento delle informazioni provenienti dalla sorveglianza di abitazioni private o dall'accesso da remoto a sistemi informatici; b) non è escluso il trasferimento dei dati dalla sorveglianza visiva di case private per le autorità di polizia, pur essendo, ai sensi della disposizione di cui all'art. 13 della Grundgesetz, tale sorveglianza visiva ammessa al solo fine della protezione contro specifiche minacce e non per le accuse penali; c) i poteri per il trasferimento delle informazioni agli uffici per la protezione della Costituzione, il controspionaggio militare Agenzia e il Servizio federale di *intelligence* risultano, a ben vedere, sproporzionatamente generici e, conseguentemente, non definiti in maniera circoscritta[24].

4.8. L'organo supremo tedesco si è infine occupato della questione relativa al trasferimento delle informazioni raccolte tramite le misure di sorveglianza occulta alle autorità di sicurezza di Paesi terzi e, al riguardo, ha richiamato alcuni principi-base cui la normativa in commento dovrebbe uniformarsi, quali: a) la soggezione del predetto trasferimento al rispetto dei diritti fondamentali e dei principi costituzionali dello scopo e del cambiamento dello stesso; b) la tutela dell'autonomia dell'ordine legale del Paese terzo ricevente le informazioni; c) la necessità che la legge garantisca che «*la tutela dei diritti fondamentali non sia lesa dal trasferimento dei dati raccolti dalle autorità tedesche verso Paesi terzi e*

[24] Sul punto, si vedano anche: L. GIORDANO, A. VENEGONI, *ibidem*.

organizzazioni internazionali»[25], dovendo gli Stati che ricevono siffatti dati assicurare un livello di protezione dei dati conforme al "modello tedesco"; d) la salvaguardia dei diritti umani da parte del Paese ricevente; e) l'esistenza di scopi sufficientemente importanti alla base del trasferimento di informazioni verso Paesi terzi.

Dopo aver brevemente richiamato siffatti principi di matrice costituzionale, la pronuncia non ha mancato di mettere in evidenza come la normativa della BKAG, oggetto di censura, non sia ad essi conforme. Del resto, non si può fare a meno di rilevare come la medesima si limiti a definire in maniera del tutto ampia e generica (e, conseguentemente, sproporzionata) gli scopi per il trasferimento, demandando all'Ufficio Criminale Federale l'autorizzazione. La stessa inoltre permette che le informazioni trasmesse siano trattate conformemente alla normativa di protezione dei diritti umani del Paese terzo e non richiede la sussistenza di interessi particolarmente importanti come requisito imprescindibile per poter procedere al trasferimento di dati provenienti da misure di sorveglianza comportanti interferenze particolarmente ampie nella sfera privata.

5. *Considerazioni conclusive.*

Tanto premesso e rappresentato, come recentemente osservato in dottrina, «*al di là delle questioni specifiche di diritto interno dello Stato tedesco, resta il fatto che la presente decisione (…) [costituisce] certamente un intervento significativo nella tematica del rapporto tra rafforzamento dei mezzi investigativi per la lotta a gravi reati, quali il terrorismo, e garanzie fondamentali della persona*»[26].

Si tratta di una pronuncia non esente da critiche e perplessità: alcuni l'hanno intesa come un ostacolo alla lotta contro il terrorismo; altri non l'hanno interpretata come un

[25] *Ibidem.*
[26] *Ibidem.*

impedimento a siffatta lotta *tout court*, ma hanno colto in essa il fine di limitare un utilizzo indiscriminato delle misure di sorveglianza occulta.

In ogni caso, la decisione affronta una tematica estremamente attuale anche nell'ordinamento italiano, sempre più attento ad occuparsi della «*demarcazione dei confini*» tra «*misure estremamente invasive, necessarie per la lotta a reati gravissimi*», da un lato, e «*diritti della persona*», dall'altro[27].

Tutto ciò considerato, si rende doverosa una riflessione finale.

A ben vedere, non si può non rilevare come il terrorismo che dobbiamo contrastare oggi – quello emerso anche dalle recenti drammatiche vicende in Francia e in Belgio – operi strutturalmente e operativamente oltre i confini nazionali ed europei e non possa, pertanto, essere sconfitto ricorrendo a mere politiche nazionali.

Del resto, è ovvio che in un mondo globalizzato – quale quello odierno – «*la criminalità – finanziaria, organizzata e terroristica – non conosce confini, specie in un'Europa che è divenuta un unico spazio economico*»[28]. In altri termini, se un reato «*ha caratteristiche transnazionali, esso deve trovare una risposta a livello transnazionale*»[29].

Al fine di poter efficacemente contrastare siffatte grave formi di criminalità, sarebbe assolutamente opportuno e necessario un intervento dell'Unione europea e, a tal proposito, occorre innanzitutto rilevare quanto segue.

Vero che il Trattato di Lisbona, entrato in vigore il primo dicembre 2009, ha innovato la materia della cooperazione nella giustizia penale nell'Unione europea: da un lato, è stata prevista la possibilità di introdurre misure legislative di armonizzazione attraverso direttive da approvare con un procedimento legislativo ordinario; dall'altro, sono state introdotte le basi giuridiche necessarie per espandere ulteriormente i poteri e le competenze di Eurojust e per procedere alla creazione dell'Ufficio del Procuratore europeo.

---

[27] *Ibidem.*
[28] Consultabile su www.questionegiustizia.it.
[29] *Ibidem.*

Vero anche che siffatte novità sono tuttavia «*rimaste in larga parte inattuate. Dopo una prima fase, tra il 2010 ed il 2012, positivamente caratterizzata dall'approvazione di alcune importanti direttive in materia di armonizzazione dei diritti minimi uniformi della difesa nel processo penale (che costituiscono la premessa necessaria per costruire la fiducia reciproca fra diversi ordinamenti e il riconoscimento delle decisioni), l'iniziativa legislativa in materia sembra si sia arenata tra grandi difficoltà in Consiglio, inerzie del Parlamento europeo ed una sostanziale paralisi propositiva della Commissione*»[30].

In relazione al tema qui oggetto di interesse, si segnala per completezza la pubblicazione in data 4 maggio 2016 sulla Gazzetta Ufficiale dell'Unione europea di tre provvedimenti in materia di trattamento dei dati personali per finalità (tra l'altro) di prevenzione e repressione dei reati: a) il Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; b) la Direttiva UE 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati; c) la Direttiva UE 2016/681, sull'uso dei dati del codice di prenotazione per finalità di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Si tratta in particolare della raccolta e del trattamento dei dati concernenti le persone che utilizzano vettori aerei per viaggi che riguardino Paesi esterni all'Unione. Peraltro, l'art. 2 della Direttiva consente agli Stati membri di applicare la disciplina anche a tutti o ad una parte dei voli interni al territorio dell'Unione.

Alla luce di tutto quanto sopra esposto, è stato recentemente osservato che ad oggi «*manca (…) una franca valutazione, empirica ed obiettiva, dello stato di attuazione e di funzionamento (e soprattutto di non-funzionamento) degli strumenti di cooperazione esistenti [in ambito penale]. Spesso si ha notizia di difficoltà insorte nello scambio effettivo, leale e completo tra autorità di diversi Paesi di*

[30] *Ibidem.*

notizie di reato e di atti di indagine. Non sempre le autorità nazionali collaborano effettivamente tra di loro». Insomma, si reputa «*che occorra reagire a questa inerzia*», atteso che «*pensare di poter(..) sconfiggere [il terrorismo] con politiche penali nazionali è una illusione pericolosa*»[31].

[31] *Ibidem.*