

DIRITTI COMPARATI

Comparare i diritti fondamentali in Europa

SERVIZI DI COMUNICAZIONE E MISURE ANTITERRORISMO IN PARZIALE ATTUAZIONE DI DIRETTIVA COMUNITARIA: IL BVERFG DICHIARA LA NULLITÀ DELLA CONSERVAZIONE “IN BLOCCO” E DELLA TRASMISSIONE DEI DATI DI TRAFFICO

Posted on 29 Maggio 2010 by [Alessandra Di Martino](#)

In seguito alla proposizione di ben 34.000 ricorsi diretti, con una sentenza resa il 2 marzo 2010 (BVerfG, sentenza 2 marzo 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) il BVerfG ha dichiarato nulli, per violazione della libertà e segretezza delle comunicazioni (art. 10 GG), i §§ 113a, 113b della legge sulle telecomunicazioni (TKG) e 100g del codice di procedura penale (StPO), introdotti dalla legge 21 dicembre 2007 “sulla nuova regolazione della sorveglianza nelle telecomunicazioni ed altre misure istruttorie effettuate segretamente, e sull’attuazione della direttiva 2006/24/CE”.

Tali norme riguardano rispettivamente: l’obbligo di conservazione dei dati di traffico – ma non di quelli di contenuto – generati o trattati nell’ambito della fornitura di servizi di telecomunicazione accessibili al pubblico (telefonia fissa e mobile, accesso ad Internet e posta elettronica) per un periodo di sei mesi (§ 113a); gli scopi che giustificano la trasmissione dei dati alla pubblica autorità – ossia il “perseguimento dei reati, la difesa da

rilevanti pericoli per la pubblica sicurezza e l'adempimento dei compiti legislativamente previsti per i servizi segreti" (§ 113 b) –; la disciplina della rilevazione dei dati ai fini dell'esercizio dell'azione penale, consentita, anche senza la consapevolezza dell'interessato, qualora sussistano elementi concreti tali da fondare il sospetto della commissione di un reato dal "rilevante" significato o comunque realizzato attraverso uno strumento di comunicazione (§ 100g StPO).

I profili di particolare interesse della pronuncia sono principalmente due. In primo luogo, la controversia, che investe una normativa di attuazione di una direttiva comunitaria, viene risolta a prescindere dalla formulazione di un conflitto diretto tra il diritto comunitario, con il relativo primato, e i diritti fondamentali della Legge fondamentale. In secondo luogo, il Tribunale costituzionale prende chiaramente posizione, sulla scia di recenti pronunce (cfr. BVerfG, 1 BvR 370/07, 595/07, sentenza del 27 febbraio 2008, sulla ricognizione di comunicazioni on-line all'insaputa dell'interessato), contro una disciplina di conservazione e trasmissione dei dati adottata nel contesto delle misure antiterrorismo successive all'11 settembre: avvalendosi di uno stringente giudizio di bilanciamento, il BVerfG fa valere le ragioni della protezione della sfera privata, in particolare della libertà di comunicazione, su quelle della sicurezza.

Con riguardo al primo aspetto, il Tribunale non ritiene che il caso di specie rientri nell'ambito della giurisprudenza *Solange*, pronunciandosi pertanto a favore dell'ammissibilità del ricorso; non accoglie tuttavia la richiesta di sollevare un rinvio pregiudiziale alla Corte di Giustizia, poiché il giudizio non riguarda l'interpretazione di una norma del diritto comunitario o dell'Unione, ma una sfera del diritto interno che corrisponde al margine di conformazione lasciato al legislatore nazionale dalla direttiva. Quest'ultima, infatti, si riferisce soltanto agli obblighi di conservazione dei dati (lo precisa CGCE, sentenza 10 febbraio C-301/06, che respinge un ricorso volto ad invalidare la direttiva poiché fondata su un erroneo fondamento normativo), mentre la legge impugnata regola anche l'accesso a tali dati da parte delle autorità preposte al perseguimento dei reati, oltre al loro uso e scambio tra le medesime autorità. Inoltre, mentre la direttiva comunitaria prevede la conservazione dei dati solo in relazione

a reati "gravi", tale limite cade nella legislazione tedesca.

Con riguardo al secondo aspetto, bisogna anzitutto rilevare che esso viene tematizzato con una costante presa in considerazione della cornice europea. Significativamente, richiamando la recente sentenza sul Trattato di Lisbona, il BVerfG afferma che "la percezione della libertà, da parte dei cittadini, di non essere registrati e schedati nella totalità appartiene alla identità costituzionale della Repubblica federale tedesca, per la cui conservazione la Repubblica federale si deve impegnare nei contesti europei e internazionali", aggiungendo che "attraverso una prudente conservazione (*vorsorgliche Speicherung*) dei dati di traffico delle telecomunicazioni" - alla luce di criteri che lo stesso Tribunale si appresta ad enucleare in maniera molto puntuale - "si restringe considerevolmente il margine di ulteriori raccolte generiche (*anlasslos*) di dati per il tramite dell'Unione europea" (Rn. 218).

Conformemente ad una nota giurisprudenza - cfr. in particolare, BVerfGE, 65, 1, sul c.d. "diritto all'autodeterminazione informativa" rispetto al quale l'art. 10 GG è considerato norma speciale (Rn. 191) - il Tribunale costituzionale prevede una serie di requisiti, volti a rendere eccezionali le raccolte generiche dei dati e comunque a limitarne gli abusi. Tali requisiti costituiscono degli indici tali da valutare il rispetto del principio di proporzionalità in senso stretto - *in primis* da parte del legislatore -, delineando uno specifico contenuto per la riserva di legge posta a presidio della segretezza delle comunicazioni, e quindi sostanzialmente rinforzandola (o, secondo la terminologia tedesca, "qualificandola"). Essi riguardano nell'ordine

- a) la previsione legislativa di uno standard elevato di sicurezza dei sistemi informatici, di proprietà dei privati fornitori, secondo le più recenti acquisizioni tecnologiche, unitamente all'inasprimento degli strumenti della responsabilità civile (questo aspetto investe, nella dogmatica tedesca, i c.d. obblighi di protezione).
- b) la disciplina legislativa, puntuale e non generica, delle circostanze, dello scopo e dell'estensione relativi ad ogni atto di utilizzazione dei dati. Ne consegue l'insufficienza di clausole generali e la necessità di elementi oggettivi tali da qualificare un reato come "grave"; la

delimitazione della finalità di prevenzione mediante la sussistenza di un pericolo concreto per beni quali corpo, vita e libertà di una persona; l'applicazione di tali criteri anche alle rilevazioni effettuate dai servizi di sicurezza ed alle utilizzazioni successive ai primi trasferimenti; il favor per un generale divieto di trasmissione di dati relativi a comunicazioni particolarmente confidenziali (soprattutto la consulenza telefonica, in ambito sociale o religioso).

- c) la previsione legislativa di strumenti idonei ad assicurare la trasparenza delle rilevazioni e delle trasmissioni dei dati, in particolare con riferimento all'obbligo di notifica successiva all'interessato.
- d) la specifica conformazione della riserva di giurisdizione (non prevista dal testo costituzionale, ma enucleata dalla giurisprudenza), con riguardo agli atti di prelievo e di trasmissione dei dati da parte dell'autorità, nonché la predisposizione di un meccanismo successivo di controllo sul rispetto dei fini di utilizzazione (cfr. art. 19, comma 4, sulla tutela effettiva dei diritti).

Direttive meno stringenti sono formulate rispetto alla comunicazione agli organi inquirenti, da parte dei fornitori dei servizi, dei dati corrispondenti a singoli indirizzi IP già identificati.

Sulla base di tali rilievi di carattere generale, il BVerfG pronuncia la nullità delle norme impugnate, non ravvisando per esse una rispondenza ai requisiti di cui ai punti a-d). Va peraltro rilevato che le indicazioni formulate dal Tribunale costituzionale in questa sentenza appaiono destinate non solo ad orientare nel prossimo futuro l'attività del legislatore tedesco, ma anche, qualora il circolo tra i sistemi di protezione dei diritti in Europa si inneschi virtuosamente in questo settore – il che attualmente richiede una maggiore attenzione delle Corti europee per il valore democratico espresso dalla riserva di legge in materia penale – a ripercuotersi sulla giurisprudenza di queste ultime e di quelle nazionali.