DIRITTI COMPARATI
Comparare i diritti fondamentali in Europa

DATI RELATIVI ALLE TELECOMUNICAZIONI E SICUREZZA IN UNA NUOVA PRONUNCIA DEL BVERFG

Posted on 12 Aprile 2012 by ***Alessandra Di Martino***

Il diritto alla protezione dei dati personali, in Germania, ha assunto tratti talmente specialistici da costituire ormai una materia a sé. Nonostante la cospicua crescita del corpo normativo e la costante presenza di soluzioni che ricercano una convergenza tra diritto e tecnica per far fronte ai rischi insiti nelle tecnologie informatiche, l'inquadramento costituzionale del *Datenschutz* è rimasto nel tempo relativamente stabile.
Punto di riferimento imprescindibile resta ancora la sentenza sul censimento del 1983, che ha elaborato il diritto all'autodeterminazione informativa (*Recht auf informationelle Selbstbestimmung: RiS*), definito come il diritto di decidere da sé in merito all'uso e alla comunicazione dei propri dati personali. Il RiS è una concretizzazione del diritto generale della personalità (art. 2 comma 1 e 1 comma 1 GG); la sua centralità – e al contempo la sua residualità – non è venuta meno dopo l'individuazione del nuovo e diverso (ma secondo alcuni superfluo) "diritto alla garanzia della riservatezza e dell'integrità dei sistemi informatici" (BVerfGE 120, 274, del 27 febbraio 2008).

Alla rinnovata centralità politica assunta negli ultimi anni dal tema della

sicurezza ha corrisposto una giurisprudenza del BVerfG che ha fatto salvo il principio di dignità-libertà. Diverse decisioni hanno toccato il RiS e la segretezza delle comunicazioni (BVerfGE 109, 279 e BVerfGE 110, 33, del 3 marzo 2004; BVerfGE 313, 348, del 27 luglio 2005; BVerfGE 115, 320, del 4 aprile 2006; BVerfGE 120, 274; BVerfGE 125, 260, del 2 marzo 2010); esse hanno posto una condivisibile enfasi sul rispetto della riserva di legge – specie con riguardo al principio di determinatezza e chiarezza delle norme –. In questo contesto, salta agli occhi lo zelo con cui il BVerfG si è impegnato in operazioni di sottile individuazione e differenziazione delle fattispecie rilevanti ai sensi della disciplina sulla protezione dei dati personali, indicando minuziosamente al legislatore non solo i principi cui ispirarsi, ma anche quali norme o frammenti di norme adottare per far fronte agli accertati vizi di incostituzionalità. Non a torto, la sentenza sulla *data retention* (BVerfGE 125, 260), senz'altro da condividersi per la decisione di accoglimento, è stata criticata per il dispositivo adottato (nullità secca e non incompatibilità con differimento degli effetti della decisione) e per un'ingerenza paternalistica nella sfera del potere legislativo (per un approfondimento rimando alle osservazioni svolte in *Giur. Cost*. 2010, 4059ss.)

Nel quadro che si è brevemente tracciato, l'ultima decisione in materia (1 BvR 1299/05, del 24 gennaio 2012), di cui si dà qui brevemente conto, si segnala prevalentemente per due profili. Da un lato, essa si mostra più in sintonia con le esigenze pratiche connesse alle attività di prevenzione e repressione dei reati, che nella ponderazione prevalgono a fronte della protezione di dati personali a basso contenuto informativo. Va, peraltro, rimarcata la significativa eccezione dei codici di sicurezza, per i quali la disciplina vigente è ritenuta costituzionalmente illegittima. Dall'altro, ritorna il dispositivo di incompatibilità con effetti differiti, affiancato ad una pronuncia di rigetto con obbligo di interpretazione conforme (che tuttavia sembra operare oltre il limite testuale della norma).

Ma osserviamo la questione più da vicino.

I ricorrenti impugnano con *Verfassungsbeschwerde* legislativa alcune norme della legge sulle telecomunicazioni (TKG), ritenute lesive della garanzia di segretezza delle comunicazioni (art. 10 GG) e del diritto di

autodeterminazione informativa. In particolare, il § 111 TKG obbliga i gestori dei servizi di telecomunicazione a raccogliere ed archiviare una serie di "dati relativi alle telecomunicazioni" (numeri di chiamata, dati di riconoscimento della connessione, numero dell'apparecchio di telefonia mobile, dati di riconoscimento della casella di posta elettronica, nonché informazioni del titolare della connessione: nome, indirizzo e data di nascita, data di inizio di decorrenza del contratto). I successivi §§ 112 e 113 TKG prevedono rispettivamente un procedimento automatizzato ed uno manuale di trasmissione delle informazioni ad altre autorità pubbliche. Secondo il § 112 TKG, i gestori dei servizi di telecomunicazione devono rendere disponibili tali dati per un prelievo riservato da parte dell'agenzia federale delle reti (*Bundesnetzagentur*). Quest'ultima, a sua volta, ha l'obbligo di prelevare i dati di telecomunicazione su richiesta di alcuni soggetti pubblici (organi inquirenti, autorità di polizia, servizi segreti, uffici doganali e autorità finanziarie di vigilanza). In questi casi, la trasmissione deve avvenire sempre se la richiesta è volta a soddisfare l'adempimento di un obbligo previsto per legge.
Quanto al procedimento di trasmissione manuale delle informazioni, che parimenti avviene all'insaputa degli interessati, il § 113 TKG pone il relativo obbligo direttamente in capo alle imprese (anche con riguardo alle comunicazioni che passano per le reti interne). La delimitazione delle autorità alle quali comunicare i dati non avviene nominativamente, ma funzionalmente, tramite l'indicazione dei compiti istituzionali (prevenzione dei reati, repressione di reati e contravvenzioni, attività informativa legata alla sicurezza nazionale e alla tutela dell'ordinamento costituzionale). Il paniere dei dati trasmissibili è più ampio rispetto a quello considerato dal paragrafo precedente, ricomprendendo le informazioni relative al rapporto contrattuale e, tra queste, le coordinate bancarie. Uno speciale obbligo di comunicazione è previsto in relazione ai dati volti ad impedire l'accesso non autorizzato agli apparecchi o alle relative memorie, come le password, i PIN o i PUK.
Il BVerfG rigetta preliminarmente le questioni di inammissibilità, anche con riferimento ad un'eventuale contrasto con il diritto UE: vale il criterio ormai consolidato secondo cui è salva la competenza del BVerfG laddove

residui alla Germania un margine per l'attuazione delle direttive (nella fattispecie, rileva di nuovo la direttiva 2006/24 sulla *data retention*).
Chiarisce, poi, che non è applicabile l'art. 10 GG sulla segretezza delle comunicazioni, ma il residuale diritto all'autodeterminazione informativa. Benché l'art. 10 GG tuteli la riservatezza dei dati di traffico, infatti, la relativa garanzia è circoscritta alle interferenze nei singoli percorsi comunicativi. Diversamente, il diritto all'autodeterminazione informativa è applicabile al trattamento di dati personali occorrenti al rapporto con i servizi di telecomunicazione (e generati nel relativo svolgimento), a prescindere da concreti itinerari comunicativi. Qualche perplessità suscita tale approccio nella misura in cui è il RiS – e non l'art. 10 GG – a rilevare quando il nesso con un singolo percorso comunicativo non sia diretto ma solo mediato (laddove il contenuto e i dati esterni di una determinata comunicazione risultino dal collegamento dei "dati di telecomunicazione" con altre informazioni di cui già si disponga o che si acquisiranno in seguito).
Un caso a parte è costituito dagli indirizzi IP-dinamici, che avevano dato luogo a contrasti giurisprudenziali: il BVerfG ritiene che la trasmissione di tali dati rientri nell'ambito dell'art. 10 GG, poiché l'impresa di telecomunicazione, ai fini dell'attribuzione di un indirizzo IP-dinamico, ha accesso ai dati generati nei singoli atti comunicativi.
Con l'esclusione dell'obbligo di trasmissione dei codici di accesso personali, le norme impugnate superano le censure di incostituzionalità. Quanto all'archiviazione indiscriminata dei dati di cui al § 111 TKG (stigmatizzatata dalla decisione sul censimento ed ammessa invece, salvo il rispetto di un più stringente onere di motivazione, dalla sentenza sulla *data retention*), la relativa legittimità è argomentata sulla base del basso potenziale informativo delle informazioni raccolte. Il Tribunale, peraltro, rileva che qualora dovesse avere luogo una modifica dei protocolli di navigazione on-line (con la funzione di identificazione svolta non più dagli indirizzi IP-dinamici bensì da quelli statici), l'inclusione degli indirizzi IP-statici nell'ambito del § 111 TKG sarebbe altamente problematica. Prescrive, dunque, al legislatore un obbligo – tipico per i settori che più risentono dell'evoluzione tecnica e scientifica – "di osservazione e

miglioramento" della disciplina.
Anche la trasmissione automatizzata dei dati di telecomunicazione (§ 112 TKG) è stata fatta salva: il BVerfG ha ritenuto soddisfatto il requisito della duplice previsione di una "doppia porta" legislativa (relativa, da un lato, alla messa a disposizione dei dati da parte della *Bundesnetzagentur* e, dall'altro, al prelievo di questi da parte di altre autorità). Nel giudizio di ponderazione tra il RiS e l'interesse alla sicurezza, il criterio di proporzionalità in senso stretto è stato rispettato per la sufficiente delimitazione sia delle autorità destinatarie dell
e informazioni, sia dei fini per i quali queste ultime possono essere impiegate.
Una lettura costituzionalmente conforme è richiesta invece per il § 113 comma 1 frase 1 TKG: per un verso tale norma, contenuta in una legge federale, non appare idonea a fondare l'autorizzazione al prelievo dei dati, effettuato da autorità non federali, presso imprese private, rimandando dunque ad un'integrazione da parte delle competenti leggi dei *Länder.* Ma anche nelle materie rientranti nella competenza del *Bund*, il principio di certezza del diritto richiede norme qualificate che autorizzino il prelievo dei dati. Per l'altro verso, il § 113 non chiarisce se tra i dati di telecomunicazione rientrino anche gli indirizzi IP-dinamici. Dato l'elevato contenuto informativo di questi ultimi (in grado di collegare la posizione dell'utente nella rete con i contenuti di ogni singola comunicazione), un'interpretazione adeguatrice della norma deve escludere gli indirizzi IP-dinamici dai dati oggetto del procedimento di trasmissione manuale.
La dichiarazione di incompatibilità costituzionale colpisce invece il § 113 comma 1 frase 2 TKG, relativo all'obbligo di trasmissione dei codici di accesso personali. La norma non supera infatti lo scrutinio di proporzionalità, nella misura in cui non specifica né differenzia i presupposti sottostanti i singoli atti di trasmissione. Ad esempio, l'impiego dei codici di accesso per realizzare una perquisizione on-line o per sorvegliare una comunicazione che non si è ancora conclusa richiede – oltre all'emissione di un mandato (o di un atto di convalida) da parte del giudice – l'osservanza di requisiti materiali più stringenti rispetto a quelli occorrenti per prendere visione di dati archiviati su un telefono cellulare

già sequestrato. Viceversa, il prelievo dei codici di accesso non può essere assoggettato genericamente alle condizioni più rigorose, le quali devono invece essere riservate alle utilizzazioni dei codici che colpiscono il RiS con maggiore intensità.
Come si è accennato, il BVerfG ha adottato una dichiarazione di incompatibilità. Tale scelta è il frutto di una ponderazione più articolata, alla luce della quale, nel caso di una dichiarazione di nullità, il pregiudizio sofferto dall'interesse generale alla sicurezza sarebbe comparativamente troppo gravoso. Per contro, l'incisione del diritto all'autodeterminazione informativa per l'ulteriore periodo di transizione appare ancora tollerabile (il termine posto all'intervento legislativo è il 30 giugno 2013).