

REGNO UNITO***Court of Appeal, Secretary of State for the Home Department v. Watson and Others*, [2018] EWCA Civ 70, del 30 gennaio 2018, in tema di sorveglianza ed utilizzo dei dati relativi alle comunicazioni**

01/02/2018

La *Court of Appeal* ha dichiarato l'incompatibilità con il diritto dell'Unione europea della normativa britannica sull'accesso dell'Esecutivo a dati sulle comunicazioni, in quanto tale normativa permetteva l'accesso a dati conservati anche per scopi diversi rispetto alla lotta alla criminalità grave e non assoggettava l'accesso ad alcuna forma di controllo preliminare da parte di un organo giurisdizionale od amministrativo indipendente.

La normativa nazionale impugnata era, principalmente, la *section 1* del *Data Retention and Investigatory Powers Act 2014*¹, che aveva di fatto posto in essere un "programma di sorveglianza massiva"; la previsione dava ai ministri competenti il potere di obbligare un operatore di telecomunicazioni pubbliche a conservare dati sulle comunicazioni qualora il ministro lo ritenesse necessario e proporzionato: nell'interesse della sicurezza nazionale; per prevenire o combattere il crimine; nell'interesse del benessere economico del Regno Unito; per motivi di sicurezza pubblica; per tutelare la salute pubblica; per valutare o riscuotere qualsiasi imposta o altra cifra dovuta ad un dipartimento governativo; per impedire la morte oppure per impedire o limitare i danni all'incolumità fisica delle persone; per qualsiasi altro motivo stabilito mediante ordinanza dello stesso ministro². La previsione era stata abolita il 30 dicembre 2016, ma la giurisdizione di appello ha comunque ritenuto opportuno pronunciarsi, probabilmente perché la normativa analoga attualmente in vigore (contenuta nella *Part IV* dell'*Investigatory Powers Act 2016*) è parimenti incisiva.

Nella specie, la sentenza ha mirato ad attuare la pronuncia emessa nel 2016 dalla Corte di giustizia su rinvio pregiudiziale dalla stessa *Court of Appeal*. In tale decisione, la corte sovranazionale ha stabilito che il diritto europeo deve "essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da

¹ La legge era stata approvata in tempi accelerati per far fronte alla lacuna creatasi a seguito dell'invalidità della Direttiva 2006/24/CE sulla conservazione dei dati, dichiarata dalla sentenza nelle cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger e a.*; la lacuna venutasi a creare aveva infatti posto in dubbio la validità della relativa legislazione britannica di attuazione.

² Le condizioni sono stabilite dal *Regulation of Investigatory Powers Act 2000, section 22*.

parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione"³.

La *Court of Appeal* ha dapprima sottolineato che erano intervenuti diversi avvenimenti tra la data di emissione della pronuncia della Corte di giustizia e l'avvio, inspiegabilmente ritardato, del procedimento per la sua attuazione. Tra tali avvenimenti figuravano, oltre all'abrogazione di cui *supra*, anche la proposizione di un ricorso contro la nuova normativa sulla sorveglianza, il sopra citato *Investigatory Powers Act 2016*, nonché una nuova richiesta di rinvio pregiudiziale alla Corte di giustizia volta ad accertare se le tre condizioni da essa stabilite dovessero essere osservate anche nel contesto della sicurezza nazionale.

Per questi motivi, rigettando le richieste delle parti convenute, la corte di appello britannica ha deciso di non pronunciarsi sulla questione dell'obbligo di assicurare che i dati in questione venissero conservati entro il territorio dell'Unione, né su quella dell'eventuale necessità di informare *ex post* le persone interessate dalla conservazione e dall'analisi dei dati, poiché tali problematiche sarebbero state affrontate in sede giudiziale a breve. La corte si è quindi limitata a valutare il diritto previgente con riferimento solo all'asserita eccessiva ampiezza, discendente dal richiamo alla lotta contro la criminalità, e non unicamente alla criminalità grave. A tal proposito, la *Court of Appeal* ha dichiarato che la *section 1* del *Data Retention and Investigatory Powers Act 2014* era incoerente rispetto al diritto euro-unitario, nella parte in cui permetteva l'accesso a dati conservati allorché l'obiettivo perseguito mediante tale accesso non era ristretto alla lotta contro la criminalità *grave*, nonché in quanto l'accesso non era assoggettabile ad un controllo preliminare da parte di un'autorità giudiziale od amministrativa indipendente.

La sentenza è stata accolta favorevolmente dall'opinione pubblica e dagli esperti in materia di diritti e libertà fondamentali, essendo percepita come un ulteriore elemento di "pressione" nei confronti dell'Esecutivo⁴.

Sarah Pasetto

³ C-203/15, *Tele2 Sverige AB c. Post-och telestyrelsen*, e C-698/15, *Secretary of State for the Home Department c. Tom Watson e a.*, del 21 dicembre 2016.

⁴ A. TRAVIS, *UK mass digital surveillance regime ruled unlawful*, in *The Guardian*, 30 gennaio 2018, <https://www.theguardian.com/uk-news/2018/jan/30/uk-mass-digital-surveillance-regime-ruled-unlawful-appeal-ruling-snoopers-charter>.