

DIRITTI COMPARATI

Comparare i diritti fondamentali in Europa

SÌ ALLA CONSERVAZIONE GENERALIZZATA E INDIFFERENZIATA DEI DATI DI CONNESSIONE: IL CONSEIL D'ÉTAT DIFENDE LA “SÉCURITÉ NATIONALE” EVITANDO (PER ORA) LO SCONTRO CON LUSSEMBURGO

Posted on Giugno 21, 2021 by [Sara Benvenuti](#)

In un contesto come quello francese, esposto a gravi e persistenti minacce alla sicurezza nazionale e al rischio di terrorismo, la conservazione generalizzata e indifferenziata dei dati di connessione, nonché l'accesso in tempo reale agli stessi, presentano “un'utilità dal punto di vista operativo senza equivalenti”. Aveva già messo le mani avanti, il Conseil d'État, in occasione del rinvio pregiudiziale del luglio 2018 [Quadrature du Net et a. et Igwan.net](#) quando, su ricorso di alcune associazioni attive nel campo della protezione dei dati personali, aveva interrogato la Corte di Giustizia circa la conformità del [regime francese](#) di accesso, trattamento e conservazione dei dati di connessione da parte dei servizi di informazione (integrato dalla [Legge n° 2004-575 per la fiducia nell'economia digitale](#) e dal [Decreto n° 2011-219](#)) alla [dir. 2002/58/CE](#) (relativa alla vita privata e alle comunicazioni elettroniche - art. 15, §1) e alla [dir. 2000/31/CE](#) (dir. sul

commercio elettronico - artt. da 12 a 15), lette alla luce della Carta dei diritti fondamentali UE (artt. 4, da 6 a 8, 11 e 52 §1) e dell'art. 4, §2, del TUE. E non indietreggia di un passo oggi, con la decisione [French Data Network et a.](#) del 21 aprile, nella quale il Conseil d'État interpreta la [risposta della Corte UE](#) in controtendenza rispetto ad altri Stati europei e a vantaggio del governo, facendo di fatto salva la legislazione francese, ma rimanendo formalmente in linea con quanto richiesto da Lussemburgo.

Procediamo con ordine. I dati di connessione oggetto del dibattere sono i c.d. "metadati", ovvero i dati concernenti identità, traffico e localizzazione. Questi non riguardano il contenuto della comunicazione, bensì informazioni relative, ad esempio, all'origine e alla destinazione di una chiamata, a data, ora, durata, frequenza, tipologia e strumento utilizzato, ubicazione delle apparecchiature terminali, nonché nome e indirizzo utente, numero di telefono del chiamante e del chiamato, indirizzo IP di accesso a Internet.

Stando alla normativa europea, il principio di riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico a queste correlati implica il divieto imposto, in linea di principio, a qualsiasi persona diversa dagli utenti di memorizzare senza il loro consenso i dati in questione. In particolare, il trattamento e la memorizzazione dei dati relativi al traffico da parte dei fornitori di servizi di comunicazione elettronica, così come di quelli di ubicazione, sono autorizzati soltanto in via temporanea, per talune specifiche finalità (ad es. per la commercializzazione dei servizi) e in presenza di determinate condizioni (ad es. dopo essere stati resi anonimi o con il consenso degli utenti - sentenza 21 dicembre 2016, [Tele2 e Watson](#)). Il perseguimento di obiettivi come la salvaguardia della sicurezza nazionale, della difesa e della sicurezza pubblica, inclusi la prevenzione, l'accertamento ed il perseguimento di gravi reati, possono giustificare eccezioni all'obbligo generale; tali misure derogatorie, tuttavia, devono risultare "necessarie", "opportune" e "proporzionate" (Corte di giustizia, [La Quadrature du Net et a.](#), punto 110). La *deroga* all'obbligo di garantire la riservatezza dei dati non

può diventare la *regola* (punto 111): non giustificerebbe, pertanto, misure legislative statali volte ad imporre ai fornitori di servizi di comunicazione elettronica l'obbligo generalizzato e indifferenziato di conservare i dati relativi al traffico e di renderli accessibili alle autorità nazionali competenti. Questo risulterebbe lesivo non solo del diritto alla vita privata (art. 7 Carta dei diritti fondamentali UE) e del diritto alla protezione dei dati personali (art. 8), ma anche del diritto alla libertà di espressione (art. 11) che - ribadisce la Corte UE - "costituisce uno dei fondamenti essenziali di una società democratica e pluralista" (punto 114 della sentenza).

Coup de tonnerre! Il sistema francese di conservazione generalizzata e indifferenziata dei dati di connessione, che impone per un anno un simile obbligo ai suoi fornitori, con la risposta europea [a tremblé sur ses bases](#). L'interpretazione della Corte UE non sembra lasciare alternative, se non quella, suggerita dal governo, di invocare la clausola di salvaguardia costituzionale e la difesa, dunque, di *objectifs de valeur constitutionnelle* necessari a realizzare interessi fondamentali dello Stato. E in effetti, ammessa l'esistenza di un ordinamento giuridico dell'UE integrato a quello interno, l'art. 88-1 della Costituzione francese conferma la posizione della Costituzione al vertice del sistema giuridico. Esso impone al giudice amministrativo, nel caso in cui l'applicazione del diritto UE, come interpretato dalla Corte di giustizia, abbia l'effetto di privare di garanzia effettiva un'esigenza costituzionale che non trova nel diritto europeo eguale protezione, di escluderla ("il doit l'écarter") nella misura in cui il rispetto della Costituzione lo esige (CE, [French Data Network et a.](#), cons. 5).

Vero è anche - aggiunge il Conseil d'État - che non spetta al giudice amministrativo il compito di assicurare il rispetto da parte del diritto derivato UE, o della stessa Corte UE, del riparto di competenze tra Unione europea e Stati membri. Il Conseil si rifiuta, in altre parole, di effettuare il c.d. [controllo "ultra vires"](#) e, più precisamente, di privare la decisione della Corte di giustizia della forza obbligatoria di cui è rivestita (ex art. 91 Regol. di proc.) per il motivo che questa avrebbe

ecceduto la propria competenza, attribuendo ad un principio o atto del diritto UE una portata più ampia rispetto a quanto stabilito nei Trattati (cons. 8).

Del resto, il Conseil d'État è ben consapevole che l'applicazione di un simile controllo avrebbe aperto le porte allo scontro diretto con Lussemburgo; una probabile "guerre des juges" invece evitabile in modo indolore per via interpretativa, portando (anzi, "tirando") a proprio favore quanto stabilito dalla Corte di giustizia. L'obiettivo di salvaguardia della sicurezza nazionale è ben più importante di quelli di lotta alla criminalità in generale e di tutela della sicurezza pubblica. Lo ha detto la Corte stessa: con riguardo al primo, la presenza di una minaccia "grave", "reale e attuale o prevedibile" può giustificare misure di conservazione preventiva dei dati. L'applicazione del diritto UE non compromette pertanto le esigenze costituzionali di sicurezza nazionale e lotta al terrorismo - ne ricava il Conseil d'État. Essa osta unicamente alla previsione di un obbligo di conservazione generalizzata dei dati sensibili per esigenze diverse (e minori) quali, ad esempio, il perseguimento di reati penali. E con riferimento a quest'ultime, il Conseil ritiene persino di adottare una posizione più stringente rispetto alla Corte UE: una conservazione "mirata" dei dati relativi al traffico e all'ubicazione, delimitata in funzione di specifiche categorie di persone interessate o secondo un criterio geografico, non sarebbe materialmente possibile, né efficace da un punto di vista operativo. In ogni caso - conclude il Conseil - la distinzione effettuata dalla Corte di giustizia in considerazione del grado di criminalità (grave o meno grave) trova esatto corrispondente nel principio di proporzionalità che, anche secondo la procedura penale francese, presiede alla corretta valutazione dello strumento di inchiesta impiegato rispetto alla gravità del reato perseguito.

Insomma, "Nous savions que la réponse de la Cour de Justice risquait de compromettre l'avenir de nos recours" - afferma il portavoce de [La Quadrature du Net](#), Bastien Le Querrec - "mais nous n'avions pas du tout anticipé a quel point le Conseil d'État allait

s'engouffrer dans cette brèche". Unica vittoria: l'indicazione al governo di modificare la normativa prevedendo, entro sei mesi, un parere vincolante (e non, come in precedenza, solo facoltativo) da parte della Commission nationale de contrôle des techniques de renseignement (CNCTR), da ottenersi ogni anno, circa la permanenza di una situazione di minaccia grave alla sicurezza nazionale. Un adempimento da ritenersi tuttavia meramente formale, se non "purement de façade", tenuto conto che lo stesso Conseil d'État ha confermato a chiare lettere (punti 44 e 50 della sentenza in esame) la sussistenza di una simile condizione e che la definizione di "menace grave", contenuta [art. L. 811-3](#) del Code de la sécurité intérieure (CSI), risulta assai ampia e lascia spazio a valutazioni del tutto discrezionali.

Il supremo giudice amministrativo in definitiva fa salva la normativa francese, convalida la linea politica dura avviata dal governo dopo gli attentati del 2015, [evitando almeno per ora](#) lo scontro diretto con la Corte di giustizia ma offrendo ai diritti fondamentali una lettura ben poco garantista. Un risultato che lascia forse interdetti nel confronto con l'opposta tendenza europea (v. anche le decisioni della Corte EDU del maggio scorso [Big Brother Watch](#) e [Centrum för Rättvisa](#)), ma che solo in parte stupisce: "[Le Conseil d'État](#) n'est pas le juge conçu pour protéger les droits et libertés fondamentales, mais bien pour protéger l'État".