FOCUS

La Corte di giustizia ancora sulla *data retention*: incompatibili con il diritto dell'Unione le misure di conservazione indiscriminata e generalizzata dei dati di traffico e ubicazione degli utenti di servizi di comunicazione elettronica

Articolo redatto in collaborazione con Marco Bassini

Con la sentenza della Grande Sezione del 21 dicembre (*Tele2 Sverige* e *Watson,* cause riunite C-203/15 e C-698/15), la Corte di giustizia è tornata a occuparsi della conformità con il diritto dell'Unione delle misure di conservazione dei dati di traffico.

Già nel 2014 la Corte di giustizia aveva annullato, nel caso *Digital Rights Ireland,* la direttiva 2006/24/CE (c.d. direttiva "Frattini" o "*data retention*") sulla conservazione dei dati personali da parte dei fornitori di servizi di comunicazione elettronica, ritenendo che il contenuto di tale atto non fosse compatibile con le garanzie previste dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea a tutela del diritto alla privacy.

Ed è proprio a quest'ultima decisione che si ricollega la pronuncia dello scorso dicembre che invece ha riguardato le legislazioni di Regno Unito e Svezia, in cui erano consentite misure generalizzate di conservazione dei dati di traffico e ubicazione degli abbonati a servizi di comunicazione elettronica il cui fondamento era individuato però non nella direttiva oggetto di annullamento nel 2014, bensì nell'art. 15 della direttiva 2002/58/CE, che consente agli Stati membri di derogare al principio di riservatezza per adottare misure necessarie, opportune e proporzionate, in una società democratica, per la salvaguardia di alcuni rilevanti interessi, fra cui la sicurezza dello Stato.

I quesiti

Nell'ambito di alcune controversie aventi ad oggetto le misure e le prassi adottate in sede nazionale, in primo luogo, veniva richiesto alla Corte di giustizia di specificare se, interpretando l'art. 15 alla luce della disposizioni della Carta, la norma impedisse agli Stati membri di stabilire misure di conservazione generalizzata e indifferenziata dei dati di traffico e dei dati relativi all'ubicazione di abbonati che fruiscono di servizi di comunicazione elettronica.

In uno dei due procedimenti principali, infatti, veniva contestata la legittimità di un'ingiunzione rivolta dalle autorità svedesi ai fornitori di servizi di comunicazioni sulla base della disciplina nazionale, con cui era stato ordinato a Tele2 di conservare i dati di traffico e di ubicazione degli utenti.

Con la seconda questione pregiudiziale, si chiedeva alla Corte di pronunciarsi sulla compatibilità con l'art. 15 di una normativa che consentiva alle autorità di pubblica sicurezza di ottenere i dati personali degli utenti senza limitare tale accesso alle finalità di lotta alla criminalità e senza istituire un controllo da parte dell'autorità giudiziaria o amministrativa. Nel secondo procedimento in via principale, infatti, era contestato il potere del Ministero degli interni britannico di ordinare ai fornitori di servizi la conservazione dei dati per un periodo massimo di dodici mesi non accompagnato da alcuno scrutinio da parte delle autorità competenti.

La prima questione pregiudiziale

La Corte di giustizia precisa, preliminarmente, che l'art. 15 della direttiva 2002/58/CE integra una deroga al divieto generale di memorizzare dati di traffico senza il consenso degli utenti e deve pertanto essere oggetto di un'interpretazione restrittiva. La Corte osserva che le misure adottate ai sensi di tale disposizione possono avere quale obiettivo esclusivamente "la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica".

Questo elenco, secondo i giudici, ha carattere esaustivo, sicché gli Stati membri non possono adottare misure che interferiscano con la riservatezza degli individui per perseguire finalità diverse da quelle espressamente menzionate.

Inoltre, secondo la Corte, occorre conformare, come lo stesso art. 15 ricorda, le misure legislative ai principi generali del diritto dell'Unione europea, tra cui i diritti fondamentali.

Dunque, la sentenza esplora i criteri per giudicare la legittimità delle possibili interferenze con i diritti fondamentali tutelati dalla Carta.

La Corte ricorda, anzitutto, che l'art. 52 della Carta riconosce che ogni limitazione all'esercizio di diritti e libertà ivi contemplati deve essere prevista dalla legge e rispettare il loro contenuto essenziale. Le restrizioni necessarie ed effettivamente rispondenti a obiettivi di interesse generale o alla tutela dei diritti altrui, invece, possono essere giustificate nel rispetto del principio di proporzionalità.

La Corte, quindi, svolge un controllo accurato sul rispetto di queste condizioni da parte della legislazione svedese e rileva come alla luce della vastità e dell'eterogeneità dei dati oggetto di conservazione, la normativa statale determini un'ingerenza di vasta portata e grave nel diritto alla privacy.

Secondo la Corte, una interferenza così grave con i diritti fondamentali può trovare la sua giustificazione soltanto in un obiettivo altrettanto importante, e segnatamente nella lotta alla criminalità grave.

Tuttavia, nemmeno in tale caso vengono meno le altre tutele residue: si dovrebbe egualmente ritenere non necessaria una conservazione del tutto generalizzata e indifferenziata dei dati di traffico.

Da un lato, infatti, le misure che l'art. 15 autorizza a titolo di eccezione finirebbero per costituire la regola, rovesciando l'ordine di priorità indicato dal legislatore europeo.

Dall'altro lato, le misure previste dalla normativa nazionale non lasciano spazio ad alcuna differenziazione, limitazione o eccezione in relazione all'obiettivo perseguito, riguardando in modo indistinto tutti gli individui che intendono avvalersi di servizi di comunicazione elettronica. Dunque, nessuna specifica correlazione è richiesta tra i dati di cui si richiede la conservazione e l'esistenza di una minaccia per la sicurezza pubblica. Parimenti, nessuna limitazione viene indicata in relazione al periodo di tempo, all'ambito geografico o alla cerchia di individui cui sarebbe indistintamente applicabile la conservazione dei dati di traffico.

Queste circostanze permettono alla Corte di dichiarare che una simile normativa travalicherebbe i limiti dello stretto necessario e non potrebbe trovare giustificazione nell'art. 15.

Al contrario, questa norma può senz'altro fondare l'applicazione di misure volte a una conservazione mirata di dati di traffico e dati relativi all'ubicazione, per finalità di lotta alla criminalità, qualora la conservazione sia limitata entro il limite di necessità in relazione a categorie di dati, mezzi di comunicazione e individui interessati, nonché durata della conservazione.

Così la Corte individua le condizioni che legittimano l'applicazione di queste misure.

In primo luogo, occorre che la normativa nazionale definisca, mediante regole chiare e precise, la portata e l'applicazione delle misure di conservazione, fissandone i requisiti anche al fine di permettere agli interessati di averne contezza e di poter proteggere i propri dati.

In secondo luogo, rispetto alle condizioni sostanziali che la normativa nazionale deve soddisfare, la Corte afferma che, per quanto esse possano variare in funzione delle misure adottate, la conservazione deve rispondere a criteri oggettivi, in base a un rapporto tra dati da conservare e obiettivo perseguito.

Da ultimo, la Corte precisa che analoghe cautele devono trovare applicazione in merito alla determinazione dei destinatari potenziali delle misure e delle situazioni in cui esse ricevono applicazione: in base a criteri oggettivi, cioè, che circoscrivano le situazioni idonee a rivelare la connessione con atti di criminalità grave o con un rischio grave per la sicurezza pubblica.

La seconda questione pregiudiziale

Alla seconda questione sollevata dal giudice britannico la Corte dedica le sue residuali attenzioni, anche alla luce della soluzione offerta al primo quesito.

La Corte si ricollega, anzitutto, quanto agli obiettivi idonei a giustificare un'interferenza con la riservatezza delle comunicazioni elettroniche, agli argomenti svolti in tema di tassatività degli obiettivi indicati dall'art. 15. Nessun altro obiettivo può giustificare le misure di conservazione, e nella fattispecie, data la gravità dell'interferenza, solo la lotta alla criminalità grave appare idoneo.

In seconda battuta, la Corte si sofferma sul principio di proporzionalità, argomentando come l'accesso ai dati garantito alle autorità nazionali competenti debba darsi entro i limiti dello stretto necessario e in presenza di norme chiare e precise che ne identifichino circostanze e condizioni.

Inoltre, si esplicita l'ulteriore requisito per cui l'accesso da parte delle autorità nazionali ai dati conservati dovrebbe essere subordinato, salvo il ricorrere di casi d'urgenza, a un controllo preventivo effettuato da un organo giurisdizionale o amministrativo sulla base di una richiesta motivata dall'autorità procedente.

Parimenti, enfasi viene data alla necessità che le autorità informino gli interessati dell'adozione delle misure, a partire dal momento in cui la comunicazione non è suscettibile di compromettere le indagini.

Da ultimo, la conservazione da parte dei fornitori di servizi di comunicazione elettronica richiede l'utilizzo di misure tecniche e organizzative appropriate che consentano di prevenire abusi e alterazioni all'integrità e alla riservatezza dei dati.

Il tutto, ovviamente, entro la cornice dell'ordinamento nazionale in cui un'autorità indipendente dovrá esercitare i propri poteri di controllo, vigilando sul livello di protezione dei diritti delle persone fisiche.

In conclusione, per la Corte, ogni misura volta alla conservazione dei dati di traffico ordinata dalle autorità nazionali può trovare giustificazione nel diritto dell'Unione e non configura una violazione dei diritti fondamentali di cui gli artt. 7, 8 e 11 della Carta, laddove rispetti le condizioni che consentono di limitarne entro i limiti di stretta necessità l'applicazione.

L'antitrust UE approva l'acquisizione di LinkedIn da parte di Microsoft, ma impone condizioni per preservare la concorrenza tra social network professionali, con un occhio ai temi dei big data e della privacy

Il 6 dicembre 2016 la Commissione europea (o "**Commissione**") ha comunicato di avere approvato, in via condizionata, l'acquisizione di **LinkedIn** da parte di **Microsoft** ai sensi del Regolamento UE sul controllo delle concentrazioni (Regolamento 139/2004), che ha la funzione di assicurare che sui mercati europei sia preservata una concorrenza effettiva, in particolare vietando la creazione o il rafforzamento di posizioni

dominanti. Proprio per preservare un'effettiva concorrenza nel mercato dei social network professionali, la Commissione ha condizionato l'approvazione dell'operazione al rispetto da parte di Microsoft di alcuni impegni finalizzati a garantire ai concorrenti di LinkedIn l'accesso ai sistemi e l'interoperabilità con alcuni software di Microsoft.

Questa decisione segna un passo importante nella politica della Commissione di controllo delle concentrazioni nei mercati dei servizi digitali per due motivi: (i.) per la prima volta nell'ambito del controllo delle concentrazioni di dimensione europea, viene definito e scrutinato a fondo il mercato dei *social networks* professionali; e (ii.) per la prima volta nel medesimo ambito, la Commissione dà un'indicazione della misura e dei limiti entro cui le tematiche riguardanti il controllo e lo sfruttamento di un'ampia base di dati sul comportamento degli utenti (i c.d. "big data") e la tutela dei dati personali possono impattare sulla valutazione di compatibilità delle concentrazioni con le regole di concorrenza.

In realtà, la decisione sull'acquisizione di WhatsApp da parte di Facebook, risalente al 2014, e in qualche modo, più indirettamente, anche quella sull'acquisizione di Skype da parte della stessa Microsoft, del 2011, avevano già toccato questi temi, ma in modo poco chiaro e superficiale per via della mancanza di esperienza della Commissione nell'analisi di questi mercati e dell'ancora scarsa consapevolezza sulle modalità di sfruttamento dei big data.

Il testo della decisione della Commissione sull'acquisizione di LinkedIn non è ancora stato reso pubblico, perché la Commissione e Microsoft devono accordarsi su di una versione non confidenziale del testo che obliteri i dati e le informazioni sull'attività delle parti considerate sensibili e segrete, attività che potrebbe richiedere anche mesi. Tuttavia, il comunicato pubblico della Commissione che dà conto della decisione fornisce gli elementi utili a delineare i contorni fattuali e giuridici della stessa, nonché i criteri utilizzati nella valutazione di compatibilità con le condizioni di concorrenza minima che il Regolamento 139/04 mira a preservare. Proviamo a illustrarli di seguito, in attesa di un'analisi più approfondita, che potrà effettuarsi solo a seguito della pubblicazione.

Innanzitutto, è importante fissare l'ambito dei mercati su cui si concentra la valutazione della Commissione. La corretta definizione dei mercati rilevanti è infatti il presupposto preliminare per una corretta valutazione concorrenziale delle concentrazioni.

In proposito, la Commissione afferma che le attività delle parti dell'operazione sono per lo più complementari tra di esse e non coincidenti, in quanto Microsoft non opera nel mercato dei social network professionali: le parti si sovrappongono in maniera limitata solo nel mercato della raccolta pubblicitaria online, che tuttavia ha una struttura molto frammentata e concorrenziale. Inoltre, la concentrazione dei dati degli utenti delle parti, che può essere usata per scopi pubblicitari, non rappresenta un problema per la Commissione poiché, da una parte, vi è sicuramente una grande base di dati alternativa disponibile sul mercato e, dall'altra, l'operazione non avrebbe ridotto l'ammontare di dati disponibili a terzi poiché né Microsoft né LinkedIn attualmente cedono i propri dati per motivi pubblicitari. Ragione per cui la Commissione ha ritenuto che l'operazione non sollevi seri problemi concorrenziali su tale mercato.

Di contro, la Commissione ha sollevato preoccupazioni per la possibilità che il notevole potere di mercato detenuto da Microsoft nei mercati dei sistemi operativi per PC (con Windows) e dei software di produttività (con il pacchetto Office) potesse essere utilizzato come leva per rafforzare la posizione di LinkedIn nel mercato dei social network professionali. In particolare, la Commissione ha paventato il rischio che Microsoft decidesse (i) di fare pre-installare LinkedIn su tutti i PC Windows; e (ii) di integrare LinkedIn in Office, combinando al contempo i rispettivi database di utenti, seppure soltanto nella misura ammessa dalle regole sulla privacy. L'ampliamento della base di utenza di LinkedIn e i conseguenti "effetti di rete" che ne sarebbero derivati, secondo la Commissione, avrebbero probabilmente reso molto più difficile a nuovi entranti penetrare il mercato di LinkedIn negli Stati membri dello SEE in cui LinkedIn è l'unico operatore, o distorto "irreversibilmente" la concorrenza a favore di quest'ultimo negli Stati in cui altri operatori sono già attivi (come in Germania, Polonia e Austria), in una misura che non sarebbe stata possibile senza la concentrazione.

La Commissione ha analizzato anche i potenziali effetti dell'operazione sul mercato delle soluzioni software di gestione delle relazioni con gli utenti (*Customer Relationship Management*, o "CRM"), ma ha concluso che anche nel caso in cui Microsoft vendesse i propri software CRM congiuntamente (e inscindibilmente) ai servizi di *sales intelligence* di LinkedIn (la cui clientela in parte si sovrappone a quella dei servizi di CRM), oppure impedisse ai suoi concorrenti nel mercato dei software CRM di accedere al database di LinkedIn per impedire loro di sviluppare nuove funzionalità attraverso il *machine learning*, non ne risulterebbe un effetto di preclusione della concorrenza su tale mercato. Ciò in quanto, da un lato, i servizi di LinkedIn sul mercato CRM non rappresentano un "*must have*", esistendo un numero di concorrenti forti, tra cui in particolare Salesforce, con quote di mercato sicuramente superiori a quelli di Microsoft, ma anche Oracle e SAP; e, dall'altro, la base di dati di LinkedIn non sembra essenziale per competere in detto mercato.

Conseguentemente, per superare le suddette preoccupazioni della Commissione, Microsoft ha offerto i seguenti "impegni" della durata di cinque anni, applicabili nello SEE, che la Commissione ha accettato e reso vincolanti come condizione per l'autorizzazione della concentrazione:

- assicurare che i produttori e distributori di PC siano lasciati liberi di non installare LinkedIn su Windows e consentire agli utenti di rimuoverlo nel caso in cui i produttori e distributori di PC decidessero di pre-installarlo;

- consentire ai concorrenti di LinkedIn di mantenere gli attuali livelli di interoperabilità con i prodotti di Microsoft Office tramite il c.d. Office *add-in program* e *Office application programming interfaces*;

- garantire ai concorrenti di LinkedIn l'accesso a Microsoft Graph, un portale per sviluppatori di software, usato per sviluppare applicazioni e servizi che, con il consenso degli utenti, accedono ai loro dati immagazzinati sulla *cloud* di Microsoft, come ad esempio i contatti, le informazioni del calendario ed e-mail. Gli sviluppatori possono eventualmente utilizzare questi dati per spingere gli utenti ad abbonarsi ai propri social network professionali.

La Commissione, infine, ha specificato che le condizioni di privacy in quanto tali, pur non rientrando nell'ambito del diritto UE della concorrenza, possono essere prese in considerazione nella valutazione antitrust nella misura in cui i consumatori le percepiscono come un fattore di qualità del servizio e le imprese concorrano tra loro anche sulla base di questo fattore. In questo caso, la Commissione ha concluso che i termini di protezione della privacy costituiscono un fattore concorrenziale importante tra gli operatori di social networks, e che tale parametro di qualità avrebbe potuto subire un abbattimento in conseguenza della concentrazione, in assenza degli impegni adottati da Microsoft.

BREVI

L'Avvocato generale Szpunar ha presentato le proprie Conclusioni nella causa C-568/15, ritenendo che l'utilizzo, per l'assistenza post-vendita, di un numero speciale (non geografico) il cui costo eccede la "tariffa base" prevista per una telefonata standard diretta a un numero fisso (geografico) costituisca una pratica commerciale sleale contraria alla direttiva 2011/83/UE relativa ai diritti dei consumatori, in quanto l'addebito di costi supplementari è idoneo a dissuadere i consumatori dal contattare un professionista.

Con sentenza del 10 novembre, la Corte di giustizia ha dichiarato che il regime applicabile al prestito di libri in formato elettronico può essere equiparato a quello del prestito tradizionale. La Corte era stata adita nell'ambito di una controversia che vedeva un'associazione di biblioteche pubbliche opporsi al differente trattamento riservato alla messa a disposizione di e-book. Secondo la Corte di giustizia, anche il prestito di

libri in formato digitale afferisce all'ambito di applicazione della direttiva 2006/115/CE concernente il diritto di noleggio, il diritto di prestito e taluni diritti connessi al diritto di autore in materia di proprietà intellettuale. Così, il prestito di una copia digitale secondo il modello "*one user, one copy*", qualora presenti caratteristiche sostanzialmente analoghe a quelle dei volumi cartacei, soggiace alla medesima disciplina prevista per questi ultimi, in quanto la nozione di "prestito" comprende anche la messa a disposizione in tale formato.

Con provvedimento del 27 ottobre, l'Autorità garante per la protezione dei dati personali ha rilasciato, in base al c.d. Privacy Shield, l'autorizzazione al trasferimento di dati personali dall'Italia verso organizzazioni stabilite negli Stati Uniti che aderiscono al registro tenuto dal Dipartimento del Commercio statunitense.

Il Comitato diritti civili del Parlamento europeo ha approvato la raccomandazione sul c.d. "Umbrella Agreement", l'accordo siglato tra l'Unione europea e gli Stati Uniti sul trasferimento di dati personali per finalità di prevenzione, accertamento, indagine e perseguimento di reati, che mira a rafforzare le tutele degli interessati nello scambio di informazioni tra autorità di pubblica sicurezza.

Il Consiglio ha approvato la bozza di regolamento sul c.d. "geoblocking" nell'ambito dei servizi di e-commerce. La proposta mira a eliminare ogni forma di discriminazione da parte degli operatori nell'offerta di questi servizi che sia fondata sulla nazionalità dei consumatori, nonché sul rispettivo luogo di residenza o di stabilimento.

Lo scorso 24 novembre l'Autorità per le garanzie nelle comunicazioni ha avviato un'indagine conoscitiva sullo sviluppo dei sistemi mobili di quinta generazione (5G) e sull'utilizzo di nuove porzioni di spettro al di sopra dei 6 GHz. Lo studio si inserisce nell'ambito dell'Action Plan 5G dalla Commissione europea diretto alla formazione di una *roadmap* per il lancio del 5G secondo una tempistica uniforme.

L'Autorità garante per la protezione dei dati personali ha rigettato una domanda di rimozione di alcuni link visualizzati da un motore di ricerca attraverso l'utilizzo del nome e cognome dell'interessato come parola chiave. Tali risultati di ricerca rinviavano a notizie relative a una vicenda giudiziaria risalente di circa dieci anni e conclusasi nel 2012 con una sentenza di patteggiamento passata in giudicato. L'Autorità, appellandosi ai criteri definiti dal Gruppo di lavoro Articolo 29, ha stabilito, per un verso, che nonostante fosse decorso un certo lasso di tempo dagli accadimenti, la definizione della vicenda giudiziaria era intervenuta solo in un'epoca recente e, per altro verso, che la gravità dei fatti narrati fosse tale da rivelare la persistenza di un interesse da parte dell'opinione pubblica.

L'Autorità garante per la protezione dei dati personali ha pubblicato una scheda informativa sintetica che illustra i principali pericoli connessi alla pratica del "*phishing*" e indica alcuni consigli per difendersi dalle aggressioni ai propri dati personali.

Il Gruppo di lavoro Articolo 29 ha diffuso una nota stampa per comunicare le iniziative che saranno adottate all'inizio del 2017 per assicurare un'implementazione omogenea del nuovo Regolamento generale sulla protezione dei dati personali e del Privacy Shield.

Il 13 dicembre il Gruppo di lavoro Articolo 29 ha adottato le linee guida sul diritto alla portabilità dei dati personali nelle quali si esaminano le caratteristiche del nuovo diritto sancito dall'art. 20 del regolamento generale sulla protezione dei dati personali entrato in vigore nel maggio 2016.

Il 13 dicembre il Gruppo di lavoro Articolo 29 ha adottato le linee guida sulla figura del Data Protection Officer introdotta dal nuovo regolamento generale sulla protezione dei dati personali. Le linee guida si soffermano, in particolare, sulle modalità di designazione, sul ruolo e sui compiti del DPO.

Il 13 dicembre il Gruppo di lavoro Articolo 29 ha adottato le linee guida sulle modalità di definizione della autorità capofila (*lead authority*) nell'ambito del nuovo meccanismo del c.d. *one-stop shop* previsto dal nuovo regolamento generale sulla protezione dei dati personali.

La Corte costituzionale ha dichiarato illegittime le norme contenute in una legge regionale adottata dalla Regione Piemonte recante "Misure urgenti per il contrasto dell'abusivismo", finalizzate a limitare il numero di soggetti abilitati a operare servizi di taxi e noleggio con conducente. Secondo la Corte costituzionale, infatti, la legge regionale lede la competenza in materia esclusiva in materia di concorrenza facente capo allo Stato, prevista dall'art. 117, c. 2, lett. *e)* della Costituzione

---

Con sentenza del 21 dicembre, la Corte di giustizia dell'Unione europea ha dichiarato che il giudice dello Stato in cui un venditore asserisca di aver sofferto un pregiudizio alle proprie vendite è competente a giudicare l'eventuale azione di risarcimento promossa per la violazione del divieto di vendita al di fuori da una rete di distribuzione selettiva per effetto dell'offerta dei relativi prodotti mediante siti Internet aventi come target utenti che risiedono in Stati membri diversi.

La Commissione ha pubblicato il 10 gennaio una proposta di regolamento sulla tutela della privacy nelle comunicazioni elettroniche. La proposta mira a estendere il campo di applicazione delle regole vigenti a tutti i fornitori di servizi di comunicazione elettronica e ad adeguare il quadro normativo in questo settore alle novità introdotte dal nuovo Regolamento generale sulla protezione dei dati personali.

I numeri precedenti sono disponibili online sul sito.

Se desideri iscriverti al servizio clicca qui.