Rivista di diritto amministrativo

Pubblicata in internet all'indirizzo www.amministrativamente.com

FASCICOLO N. 11-12/2018

estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

L'accesso alle autorità pubbliche a dati personali di natura meramente identificativa non costituisce un ingerenza grave nei diritti fondamentali degli interessati

di Donatella del Vescovo

(abilitata Professore Associato, Università degli Studi di Roma 3)

Sommario

Abstract

The European Court of Justice has decided on 2 October 2018 to extend the decision previously set out in Tele2 which allowed national authorities access to personal data held by electronic communications providers, in cases of serious crime, despite it being a breach of personal and fundamental freedoms enshrined in the Directive.

This case, from Spain (Case C-207/16 Ministerio Fiscal), was in some eyes regarding a small crime, though a prevalent one, of mobile phone theft.

Spanish police sought access to data identifying the users of telephone numbers activated with the stolen telephone during a period of 12 days as from the date of the robbery but were refused by the Magistrate as access to such data was only permitted for serious crimes. The appellate court sought guidance from the European Court of Justice which in considering the directive on privacy and electronic communications noted that it provides that Member States may restrict citizens' rights when such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society in order to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Whilst it recognised that for broader information the protection was necessary the European Court of Justice determined that given the data sought was limited, it was a proportionate interference with the subjects' personal data rights because it didn't give any information about their private lives but it did meet the objective of preventing, investigating, detecting and prosecuting "criminal offences" generally, without it being necessary that those offences be defined as "serious".

Articolo sottoposto a referaggio anonimo/*blind peer review*

1. Premesse.

Nella sentenza dell'ottobre 2018[1], la Corte di Giustizia dell'Unione Europea analizza nuovamente, dandole però una connotazione diversa dal passato, la legittimità dell'accesso ai dati personali conservati dai fornitori di servizi di telefonia, da parte delle autorità nazionali competenti ai fini dell'accertamento di reati.

La questione oggetto della sentenza si è posta nell'ambito delle indagini svolte dalla polizia giudiziaria spagnola relativamente a una rapina in cui erano stati sottratti un portafoglio e un telefono cellulare. In tale contesto, la polizia giudiziaria, per finalità investigative, aveva richiesto al giudice competente di accedere ai dati identificativi dei titolari di tutti i numeri attivati dal telefono rubato per un periodo di 12 giorni dalla data di consumazione del reato.

Il giudice istruttore respinse tale domanda con la motivazione che, in particolare, i fatti all'origine dell'indagine penale non avrebbero integrato gli estremi di un reato "grave" - vale a dire, secondo il diritto spagnolo, un reato punibile con pena detentiva superiore a cinque anni - posto che l'accesso ai dati di identificazione era in effetti possibile solamente per tale tipo di reati. Il Ministerio Fiscal (pubblico ministero spagnolo) interpose appello contro tale decisione dinanzi all'Audiencia Provincial de Tarragona (Corte d'appello di Tarragona, Spagna).

La Corte d'appello di Tarragona ritenne a sua volta che l'interesse dello Stato a reprimere i comportamenti penalmente illeciti non potesse giustificare ingerenze sproporzionate nei diritti previsti dalla Carta dei diritti fondamentali dell'Unione europea (in seguito Carta) e in virtù di tale presupposto interrogò la Corte di giustizia sul modo di fissare la soglia di gravità dei reati a partire dalla quale potesse essere giustificata, alla luce della giurisprudenza in essere, un'ingerenza nei diritti fondamentali da parte delle autorità nazionali competenti[2].

La direttiva 2002/58/CE[3], relativa alla vita privata e alle comunicazioni elettroniche è la normativa chiamata in causa in questa sentenza. Essa, all'articolo 15, paragrafo 1,

---

[1] Sentenza del 2 ottobre 2018, *Ministerio Fiscal*, causa C-207/16, EU:C:2018:788.

[2] L'Audiencia Provincial de Tarragona rilevava l'adozione di una ulteriore fonte normativa di riferimento, approvata in un momento successivo al provvedimento impugnato: la legge organica 13/2015 (Ley Organica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantias procesales y la regulación de las medidas de investigación tecnológica, 5 ottobre 2015). Tale normativa andava ad incidere sulle modalità di determinazione del concetto di "gravità" del reato, stabilendo due criteri alternativi: un criterio materiale (rilevanza criminosa della condotta e grave lesione dei beni giuridici) e uno normativo formale, meramente basato sulla durata della pena che, per determinare la gravità del reato, doveva essere non inferiore a tre anni. Ebbene, quest'ultimo criterio, che avrebbe potuto potenzialmente portare al di sopra della soglia di gravità la maggior parte dei reati, faceva sorgere in capo al giudice dell'appello un dubbio di conformità della normativa rispetto alla tutela dei diritti fondamentali sanciti dalla Carta e dai principi enucleati della Corte di Giustizia nella pronuncia *Digital Rights Ireland.*

[3] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (GUCE, L 201, del 31.7. 2002,

prevede che gli Stati membri possano limitare i diritti dei cittadini qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata, all'interno di una società democratica, per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica, e per la prevenzione, ricerca, accertamento e perseguimento dei reati ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.

In questo frangente la Corte rilevò che l'accesso ai dati che mirano all'identificazione dei titolari di SIM attivate con un cellulare rubato (quali cognome, nome e, se del caso, l'indirizzo degli stessi) comportava sicuramente un'ingerenza nel diritto fondamentale alla riservatezza sancito dalla Carta. Tuttavia, nel caso di specie, i dati oggetto della domanda di accesso da parte della polizia giudiziaria avrebbero permesso solamente di collegare una o più SIM all'identità del relativo titolare nel corso di un limitato arco temporale, non rendendo invece possibile conoscere i tabulati delle SIM, la relativa frequenza o localizzazione degli individui. Si trattava, dunque, di dati che non permettevano di trarre precise informazioni sulla vita privata degli interessati ed il cui esame non poteva qualificarsi quale ingerenza "grave" nei loro diritti fondamentali.

Tale ragionamento ha indotto la Corte ad affermare per la prima volta che, in conformità al principio di proporzionalità, l'accesso delle autorità pubbliche a dati di natura meramente identificativa non costituisce un'ingerenza grave nei diritti fondamentali degli interessati, poiché trova giustificazione nelle generali esigenze di repressione dei reati, a prescindere dalla loro gravità.

Questa sentenza se in apparenza sembra essere in contrasto con la precedente giurisprudenza in materia di protezione della privacy, in realtà come vedremo di seguito, porta la Corte di giustizia a seguire i suoi orientamenti di sempre, seppur sulla base di considerazioni differenti.

La Corte infatti in passato[4] aveva affermato che "soltanto" la lotta contro la criminalità "grave" era idonea a giustificare un accesso delle autorità pubbliche a dati personali conservati dai fornitori di servizi di comunicazione. Tale interpretazione era tuttavia motivata dal fatto che l'obiettivo perseguito da una normativa che disciplina tale accesso deve essere adeguato alla gravità dell'ingerenza nei diritti fondamentali che tale operazione determina. Infatti in conformità al principio di proporzionalità, una grave ingerenza può essere giustificata, in tale ambito, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come "grave".

---

pag. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GUUE, L 337, del 18.12. 2009, pag. 11).

[4] Sentenza del 21 dicembre 2016, *Tele2 Sverige e Watson e a.* (C-203/15 e C-698/15, v. comunicato stampa n. 145/16).

Ma qualora l'accesso a determinati tipi di dati, non possa essere qualificato come un'ingerenza "grave" nei diritti fondamentali delle persone, esso secondo la recente sentenza, può essere giustificato anche semplicemente dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale. Ciò viene supportato dalla considerazione da parte della Corte che la formulazione della direttiva 2002/58/CE non limita tale obiettivo alla lotta contro i soli reati "gravi", ma si riferisce ai reati in generale.

La Corte in sostanza sostiene che l'accesso ai dati personali deve essere in realtà adeguato alla gravità dell'ingerenza nei diritti fondamentali, per cui **anche i reati che non sono particolarmente gravi possono giustificare un accesso ai dati personali conservati dai fornitori di servizi di telefonia unicamente quando tale accesso non comporta una limitazione grave della vita privata**. Pertanto l'accesso delle autorità pubbliche a dati personali di natura meramente identificativa si può effettuare persino in mancanza di circostanze che permettano di qualificare tale ingerenza come grave senza che rilevi il fatto che le informazioni in questione relative alla vita privata siano o meno delicate.

2. La direttiva 2002/58/CE.

La sentenza in oggetto come abbiamo detto, si concentra principalmente sulla corretta interpretazione della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, come modificata dalla direttiva 2009/136/CE[5].

La direttiva 2002/58/CE enuncia, nel suo preambolo, quanto segue: "La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti dalla Carta. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta"[6].

[5] Direttiva del Parlamento europeo e del Consiglio, del 25 novembre 2009, in GUUE, L 337, del 18.13.2009, pag. 11.

[6] La Direttiva impone infatti ai fornitori di servizi di comunicazioni elettroniche di cancellare o rendere anonimi i dati raccolti e conservati, una volta che essi non siano più necessari per la fornitura o la fatturazione dei servizi stessi. La normativa europea fa riferimento in particolare a quelli che vengono definiti "dati relativi al traffico" (articolo 2, lettera b), nonché ai "dati relativi all'ubicazione" (articolo 2, lettera c): queste informazioni permettono di individuare fonte, destinatario, data, ora, durata, localizzazione e tipo di comunicazione. Pur non riguardando il contenuto delle comunicazioni, tali dati (cd. metadati) sono di estrema delicatezza e, come la costante giurisprudenza della Corte di Giustizia ha sempre affermato, "presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanenti o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati" (par. 27, pronuncia *Digital Rights Ireland*).

Tale direttiva è stata adottata in seguito all'entrata in vigore della direttiva 95/46/CE[7] con il precipuo obiettivo di adeguarne l'impianto rispetto all'ambito delle comunicazioni elettroniche[8]. Essa non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti doverosi per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato e l'applicazione della legge penale. Di conseguenza lascia liberi gli Stati di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali[9].

Al centro del rinvio pregiudiziale si colloca l'interpretazione dell'articolo 15 di tale direttiva. Tale disposizione consente agli Stati membri di derogare al principio di riservatezza, previsto nella direttiva, al fine di adottare misure necessarie, opportune e proporzionate per la salvaguardia di alcuni interessi fra cui la sicurezza dello Stato[10]. Sulla base di questa disposizione, ampiamente utilizzata dagli Stati Membri soprattutto a seguito del crescente numero di attacchi terroristici che hanno colpito l'Europa, si era venuto a creare un panorama normativo in materia di regolamentazione di dati estremamente frammentato e diversificato da Stato a Stato,

[7] Direttiva del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GUCE, L 281, del 23.9.1995, pag. 31.

[8] L'articolo 1 della direttiva 2002/58/CE, intitolato «Finalità e campo d'applicazione», così dispone: «1. La presente direttiva prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità. 2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva [95/46]. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.

[9] In particolare, conformemente all'articolo 8 della CEDU, a termini del quale: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

[10] L'articolo 15 prevede, al paragrafo 1, che «gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del Trattato sull'Unione europea».

capace di incidere anche sulla circolazione dei servizi[11]. Tale situazione aveva spinto il legislatore sovranazionale ad armonizzare la materia mediante l'approvazione della tristemente nota direttiva 2006/24/CE (direttiva *Frattini*)[12], riguardante la conservazione dei dati di traffico telefonico e telematico, la quale contiene specifiche indicazioni sia sui tempi di conservazione dei dati di traffico (da un minimo di sei mesi a un massimo di due anni), sia sulla uniforme individuazione delle categorie di dati da conservare, in relazione ad alcuni specifici servizi offerti dai fornitori (telefonia di rete fissa e telefonia mobile, accesso a Internet, posta elettronica in Internet e telefonia via Internet)[13].

Due in particolare sono i quesiti che, nell'ambito della causa, sono stati sottoposti all'attenzione della Corte. In primo luogo, viene richiesto alla Corte di giustizia di chiarire se l'articolo 15 della 2002/58/CE, letto alla luce della Carta (articoli 7 e 8 della Carta, nell'ambito della conservazione di dati personali e dell'accesso agli stessi), identificasse o meno i reati che abbiano una gravità sufficiente da giustificare un ingerenza nei diritti fondamentali.

In secondo luogo, si domandava in via accessoria alla Corte se la medesima disposizione aiutasse o meno gli Stati membri a individuare la soglia minima che la pena irrogabile dovrebbe raggiungere affinché un reato possa essere qualificato come "grave". E se una soglia di tre anni di reclusione, quale prevista dal codice di procedura penale spagnolo dopo la riforma intervenuta nel 2015[14], fosse conforme ai requisiti del diritto dell'Unione.

In sostanza pertanto il procedimento verteva proprio sull'interpretazione della nozione di "reati gravi"[15] quale criterio di valutazione della legittimità e della proporzionalità di un'ingerenza nei diritti sanciti dagli articoli 7 e 8 della Carta, vale a dire, rispettivamente, il diritto al rispetto della vita privata e della vita familiare nonché il diritto alla protezione dei dati di carattere personale.

---

[11] Si leggano più ampiamente sul punto le considerazioni espresse a livello europeo in European Commission, *Proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*, SEC (2005) 1131.

[12] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GUUE, L 105, del 13.4.2006, pag. 54).

[13] Quest' ultima direttiva era stata adottata, nel 2006, con lo scopo di uniformare l'atteggiamento degli Stati membri in merito alla deroga al diritto alla privacy prevista all'articolo 15 della direttiva 2002/58/CE. Evidente, infatti, era all'epoca la preoccupazione che, in carenza di indicazioni univoche, ciascun ordinamento potesse modellare in modo assai differente l'ambito di interferenza legittimato dalla norma ora richiamata.

[14] V. paragrafi 15 e segg. delle Conclusioni dell'Avvocato Generale Henrik Saugmandsgaard Øe, presentate il 3 maggio 2018, Causa C-207/16, *Ministerio fiscal*, EU:C:2018:300.

[15] L'espressione deve qui essere intesa come riferita alle sole infrazioni in materia penale.

3. La precedente giurisprudenza della Corte di giustizia e le sue questioni controverse.

La Corte di giustizia già in passato si era occupata della compatibilità con il diritto dell'Unione delle misure di conservazione dei dati di traffico telefonico.

Ciò avveniva nel caso *Digital Rights Ireland*[16], con l'annullamento della direttiva 2006/24/CE (direttiva *Frattini* anche detta "*data retention*") sulla conservazione dei dati personali da parte dei fornitori di servizi di comunicazione elettronica, e nelle cause riunite *Tele2 e Watson*[17] dove era chiamata a giudicare la compatibilità con il diritto dell'Unione di disposizioni di diritto interno che obbligavano i fornitori di servizi di comunicazioni elettronica alla conservazione, per un determinato periodo di tempo, di dati di traffico e di ubicazione degli utenti.

Entrambe le sentenze affrontavano la questione di quale sia il punto di equilibrio tra tutela della sicurezza pubblica, specie con riferimento all'esigenza di prevenire attacchi terroristici, per un verso, e protezione della privacy digitale, per altro[18].

Nella prima sentenza dell'8 aprile 2014 nella causa *Digital Rights Ireland*, la Corte di giustizia aveva dichiarato l'illegittimità della direttiva *Frattini,* in quanto il periodo di conservazione di dati previsto ai fini di protezione dell'ordine pubblico, da un minimo di sei mesi ad un massimo di due anni, veniva considerato eccessivo e non proporzionato, anche per la vaghezza delle condizioni cui detta conservazione era subordinata[19].

---

[16] Sentenza dell'8 aprile 2014 (C-293/12 e C-594/12, EU:C:2014:238), nella quale la Corte ha dichiarato invalida la direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GUUE, L 105, del 13.4.2006, pag. 54), con la motivazione che «adottando la direttiva 2006/24, il legislatore dell'Unione ha ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta» (punto 69).

[17] Sentenza del 21 dicembre 2016 (C-203/15 e C-698/15, EU:C:2016:970), nella quale la Corte ha dichiarato che il diritto dell'Unione, *da una parte*, «osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica» e, *dall'altra*, «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 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».

[18] Sia consentito segnalare le riflessioni già articolate, in proposito, da O. POLLICINO - M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo,* in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, pagg. 73 ss.

[19] Per un commento più approfondito si vedano i contributi di L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali,* in *Giur. it.*, 2014, 8-9, pagg. 1850 ss.; R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 2/2014, pagg. 178 ss.; F. FABBRINI, *The European Court of Justice Ruling in the Data*

All´attenzione della Corte erano, appunto, le disposizioni della direttiva volte a garantire la conservazione dei dati di traffico telefonico, i dati relativi all´ubicazione e quelli necessari all´identificazione dell´abbonato, per fini di accertamento e repressione dei reati[20]. Si tratta di dati che, pur non attingendo al contenuto della conversazione, fornivano comunque indicazioni importanti sulle comunicazioni intrattenute dai loro destinatari e sulla loro frequenza. In sostanza dati che svelavano la rete di tutti i rapporti interpersonali.

L´accesso a tali dati, da parte dell´autorità pubblica, comportava dunque - secondo la Corte - una forte ingerenza nella vita privata dei cittadini per cui la direttiva avrebbe ecceduto i limiti imposti dal principio di proporzionalità[21].

La violazione del principio di proporzionalità dunque sarebbe derivato, dall´avere la direttiva: 1) previsto le misure di conservazione dei dati come applicabili in via indifferenziata e generalizzata "all´insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell´obiettivo della lotta contro i reati gravi"; 2) omesso di prevedere alcun criterio oggettivo che limitasse l´accesso a tali dati per sole esigenze di accertamento di reati "sufficientemente gravi da giustificare una simile ingerenza", ben oltre - dunque - il generico rinvio ai reati gravi definiti da ciascuno Stato membro; 3) omesso di sancire i presupposti sostanziali e procedurali ai quali subordinare l´accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell´autorità giudiziaria o di un´autorità amministrativa indipendente; 4) omesso di prevedere criteri necessari a differenziare la durata della conservazione dei dati, limitandosi a stabilirne i soli termini minimi (6 mesi) e massimi (24); 5) omesso di imporre che i dati così acquisiti siano conservati nel (solo) territorio dell' Unione.

Si trattava, dunque, di una sentenza che valorizzava moltissimo la centralità del diritto alla protezione dei dati personali anche in un settore - quale quello del contrasto al crimine - in cui maggiori erano le limitazioni alle libertà, ammesse per esigenze di interesse generale.

Il punto cardine della pronuncia era indubbiamente il principio di stretta proporzionalità tra limitazioni dei diritti fondamentali ed esigenze di pubblica sicurezza. Proporzionalità che non andava delineata in astratto e in maniera indifferenziata rispetto a qualsiasi reato ma che, al contrario, esigeva una

---

Rentention Case and its Lessons for Privacy and Surveillance in the U.S., 28 *Harvard Human Rights Journal* (2015), pagg. 65 ss.

[20] Si v. gli articoli 3-13 della direttiva 2006/24/CE.

[21] Si v. D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* in *ERA Forum, Springer*, pubblicato online il 25 giugno 2018.

differenziazione attentamente modulata in base al tipo di delitto, alle esigenze investigative, al tipo di dato e di mezzo di comunicazione utilizzato. Ciò, fermo restando il rispetto di alcune garanzie essenziali, quali, in particolare, la subordinazione di tali limitazioni all´autorizzazione di un´autorità terza quale l´autorità giudiziaria (nel nostro ordinamento preferibilmente l´organo giudicante) o comunque un´autorità amministrativa indipendente[22].

Nella successiva sentenza *Tele2 e Watson* seppure oggetto diretto dell'interpretazione della Corte fosse una normativa diversa, adottata nel 2002 (direttiva 2002/58/CE), dunque ancor prima della direttiva *Frattini*, i giudici nazionali si sono chiesti se una legislazione nazionale che prevedesse una conservazione generalizzata e indifferenziata dei dati degli abbonati, utilizzando il margine di manovra fornito dalla direttiva, si ponesse o meno in contrasto, tra l'altro, con quanto affermato dalla Corte di giustizia nel 2014 nella sentenza *Digital Rights Ireland*[23]. All'epoca infatti era palpabile un atteggiamento di incertezza sulle effettive implicazioni della decisione *Digital Rights Ireland* e del conseguente annullamento della direttiva *Frattini*[24]. Il

---

[22] Per una completa ricostruzione e analisi critica della pronuncia *Digital Rights Ireland*, si vedano, tra la folta dottrina in merito: L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. It.*, 2014, 8-9, pagg. 1850 ss; F. FABBRINI, *The European Court of Justice ruling in the Data retention case and its lessons for privacy and surveillance in the US*, in *Harvard Human Rights Journal*, 28/2015, pagg. 65 ss.; R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. data retention contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. Cont.*, 2/2014, pagg. 178 ss.; A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Dir Pubb Comp ed Eur*, 3/2014; M. P. GRANGER, K. IRON, *The Court of Justice and the Data retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching lesson in privacy and data protection*, in *European Law Review*, 39 (6), 2014, pagg. 835 ss.; A. VEDASCHI, V. LUBELLO, *Data retention and its implications for the fundamental right to privacy: a European perspective*, in *Tilburg Law Review*, 14/2015; L. MARIN, *The fate of the Data retention Directive: about mass surveillance and fundamental rights in the EU legal order*, in V. MITSILEGAS e al. (a cura di), *Research Handbook on Eu Criminal Law*, Elgar Publishing, 2016; O. LYNSKEY, *The Data retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Common Market Law Review*, 51 (6), 2016, pagg. 1789 ss.

[23] Alcune normative nazionali infatti sono risultate in contrasto con il giudizio della corte in *Digital Rights Ireland* questa circostanza viene sottolineata per esempio, da P. SCHAAR, *New ECJ ruling on data retention: preservation of civil rights even in difficult times!*, in www.eaid-berlin.de, 22 dicembre 2016.

[24] Taluni Stati avevano modificato la normativa nazionale di recepimento della direttiva europea invalidata, direttamente mediante l'intervento del legislatore, in modo da adeguarla ai principi indicati dalla Corte di Giustizia; altri non erano invece intervenuti in alcun modo, mantenendo invariata la propria disciplina in materia (Italia, Portogallo); per altri ancora invece è stato decisivo l'intervento dei giudici, chiamati spesso a valutare la legittimità delle norme interne in materia di conservazione dei dati, giungendo all'annullamento o disapplicazione delle disposizioni nazionali (Belgio). Per un maggiore approfondimento: S. CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del Sistema UE di protezione dei dati*, in *Rivista italiana di Diritto Pubblico Comparato*, 3/2015, pagg. 819 ss.; A. ARENA, *La Corte di Giustizia sulla conservazione dei dati: quali conseguenza per le misure nazionali di recepimento?*, in *Quaderni Costituzionali*, 3/2014, pagg. 722 ss.; F. BOEHM, M. D. COLE, *Data retention after the judgement of the Court of Justice of the European Union Study, Study for the Greens/EFA Group in the European Parliament*, 30 giugno 2014. Merita rilevare, per completezza, che già prima della pronuncia *Digital Rights Ireland*, alcuni Stati membri avevano sollevato, all'interno del contesto nazionale, dubbi di conformità delle

vuoto normativo che si era venuto successivamente a creare in materia di conservazione dei dati per finalità di sicurezza infatti aveva portato ad una ri-espansione della disciplina dettata in materia dalla direttiva 2002/58/CE.
L'interrogativo centrale era dunque se una intromissione nel diritto alla privacy fosse ancora compatibile con il diritto europeo dopo la pronuncia che aveva annullato la direttiva *Frattini* o non configurasse piuttosto un elusione di quest'ultima decisione, fenomeno che sarebbe stato agevolato dalla diffusione di normative nazionali[25] in contrasto con il giudizio della Corte in *Digital Rights Ireland*[26]. Se da un lato, infatti, l'invalidità della *Digital Rights Ireland* non aveva toccato direttamente le legislazioni nazionali adottate in attuazione della direttiva 2006/24/CE, dall'altro, con riguardo a queste ultime, sono spesso sorti dubbi di legittimità costituzionale o di conformità della normativa interna rispetto ai parametri indicati dalla Corte di Giustizia.
I giudici europei infatti alla domanda se l'articolo 15 della direttiva 2002/58/CE impedisse agli Stati membri di prevedere misure di conservazione generalizzata e indifferenziata dei dati di traffico, risposero affermativamente, ribadendo che le misure legislative adottate dagli Stati membri ai sensi dell'articolo 15 rientravano senz'altro nell'ambito di applicazione della direttiva[27], in quanto avevano ad oggetto un trattamento di dati personali da parte dei fornitori di servizi di comunicazione elettronica. La Corte tuttavia sottolineava che tale articolo 15 andava interpretato restrittivamente[28]. Ossia **potevano essere adottate misure ai sensi di tale**

---

norme di recepimento della direttiva 2002/58/CE rispetto alla tutela costituzionale del diritto alla riservatezza. Così la Corte costituzionale tedesca, quella bulgara, rumena e cipriota, ben prima dell'intervento della Corte di Giustizia, avevano dichiarato incostituzionali le leggi di attuazione della direttiva europea in materia di conservazione dei dati. Per una ricostruzione del tema, si legga: N. VAINIO, S. MIETTENIN, *Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States,* in *International Journal of Law, Information and Technology*, 23/2015, pagg. 290 ss.; F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolta alle discipline nazionali*, in *DPCE on line*, 2/2017.

[25] Con riguardo allo scenario britannico e all'applicazione, anche a seguito dell'annullamento della direttiva *Frattini*, del Data Protection and Investigatory Powers Act 2014, si v. *Independent Reviewer of Terrorism Legislation, CJEU judgment in Watson,* in www.terrorismlegislationreviewer.independent.gov.uk, 21 dicembre 2016.

[26] La circostanza viene sottolineata per esempio, da P. SCHAAR, *New ECJ ruling on data retention: preservation of civil rights even in difficult times!,* in www.eaid-berlin.de, 22 dicembre 2016.

[27] È interessante osservare come nella sentenza in oggetto la Corte di giustizia sia tornata a sposare una concezione unitaria degli artt. 7 e 8 della Carta, senza esaminare separatamente i profili inerenti a ciascuno dei diritti interessati, adottando una prospettiva diametralmente opposta, invece, a quella fatta propria, per la prima volta, nella sentenza *Digital Rights Ireland.* Su questo punto sia consentito rinviare a O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale,* in *Federalismi.it,* 2014, pag. 3, spec. 8.

[28] È interessante osservare come nella sentenza in oggetto la Corte di giustizia sia tornata a sposare una concezione unitaria degli articoli 7 e 8 della Carta, senza esaminare separatamente i profili inerenti a ciascuno dei diritti interessati, adottando una prospettiva diametralmente opposta, invece, a quella fatta propria, per la prima volta, nella sentenza *Digital Rights Ireland.* Su questo punto sia consentito rinviare a O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale,* in *Federalismi.it,* 2014, pag. 3, spec. 8.

disposizione solo qualora avessero come obiettivo "la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica"[29].

Secondo la Corte pertanto l'elenco di limitazioni previsto dall'articolo 15 aveva carattere esaustivo. Ciò significava che gli Stati membri non potevano adottare misure che interferiscano con la riservatezza degli individui per perseguire finalità diverse da quelle espressamente menzionate dalla norma suddetta che costituisce l'unica eccezione al divieto di memorizzare dati di traffico senza il consenso degli utenti.

I giudici europei infatti ritennero che un'incisione così rilevante nei diritti fondamentali degli utenti poteva trovare ragion d'essere soltanto in un obiettivo altrettanto importante, come la lotta alla criminalità "grave".

Da ciò ne deriva che la **giustificazione di misure volte ad una conservazione mirata di dati di traffico telefonico venisse sottoposta a determinate condizioni** definite specificamente dalla Corte. Innanzitutto la **normativa nazionale doveva definire, 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. In secondo luogo la conservazione **doveva rispondere a criteri oggettivi**, in base a un rapporto tra dati da conservare e obiettivo perseguito. Infine per identificare i potenziali destinatari di tali misure ci dovevano essere dei criteri oggettivi che circoscrivessero le **situazioni idonee a rivelare la connessione con atti di criminalità grave o con un rischio grave per la sicurezza pubblica**[30]. Nessun altro obiettivo dunque può giustificare le misure di conservazione, se non la lotta alla criminalità "grave".

Inoltre secondo la Corte l'accesso delle autorità nazionali ai dati conservati doveva essere subordinato a un controllo preventivo effettuato da un organo giurisdizionale sulla base di una richiesta motivata dall'autorità procedente. Per cui ogni misura volta alla conservazione dei dati di traffico ordinata dalle autorità nazionali poteva trovare giustificazione nel diritto dell'Unione e non configurava una violazione dei diritti fondamentali di cui gli artt. 7, 8 e 11 della Carta, laddove rispettasse le

[29] La direttiva del 2002 dunque è rimasta, da allora, l'unica fonte legislativa europea in tema di conservazione dei dati relativi a comunicazioni elettroniche e che prevede la possibilità di deroghe per scopi securitari o investigativi, come stabilito all'articolo 15. Come si avrà modo di vedere più approfonditamente in seguito, è al momento al vaglio del Consiglio europeo la proposta di modifica della Direttiva e-privacy con un Regolamento (COM (2017) 10: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC), che andrebbe quindi a sostituire anche il controverso articolo 15.

[30] Particolarmente rilevante e al contempo delicato appare il passaggio in cui la Corte di giustizia, al punto 111, annovera, tra le condizioni che fondano l'esistenza di un collegamento oggettivo, anche l'appartenenza a una determinata area geografica in cui la commissione di attività criminali potrebbe presentare un elevato grado di rischio.

condizioni ora descritte che consentivano di circoscriverne entro i limiti di stretta necessità l'applicazione.
Dunque in questo caso la risposta della Corte alle barriere poste dal diritto alla privacy fu estremamente chiara in quanto restrinse alla sola lotta contro la criminalità "grave" il novero di fattispecie che giustificavano un intrusione grave alla protezione dei dati e alla libertà di espressione, laddove il disposto dell'articolo 15, invece, alludeva in termini generali e ampi alla prevenzione di attività criminali.

4. La particolarità della decisione della Corte.
Se dunque in precedenza la Corte ha affermato che soltanto la lotta alla criminalità "grave" era idonea a giustificare l'accesso delle autorità pubbliche ai dati personali conservati dai fornitori dei servizi di telefonia, con la sentenza in commento la Corte sembra a primo impatto cambiare orientamento, in quanto potrebbe portare il lettore a ritenere che non sia più necessario il criterio, tanto sottolineato in precedenza, della gravità del reato per giustificare l'accesso ai dati conservati.
Le decisioni antecedenti infatti, erano motivate dal fatto che l'obiettivo perseguito da una normativa che disciplina tale accesso deve essere adeguato alla gravità dell'ingerenza nei diritti fondamentali in questione che tale operazione determina. In questo frangente però la Corte fa di più chiarendo meglio la portata del principio di proporzionalità applicabile al diritto alla privacy.
L'accento posto dalla Corte sulla precedente giurisprudenza in questo caso deve essere visto come un tentativo di costruire un approccio coerente all'interno di questa giurisprudenza e anche di riaffermare i principi stabiliti nei casi precedentemente affrontati. Infatti, per stabilire quale tipo di criterio debba essere utilizzato per determinare la gravità di un reato, la Corte si trova a valutare se l'ingerenza nei diritti fondamentali sia tale da richiedere la presenza di un reato "grave" per poter essere legittimata. Per far questo essa analizza le notevoli peculiarità della controversia in esame che la distinguono nettamente dalle precedenti sentenze.
In questo frangente la richiesta delle autorità di polizia mirava a ottenere unicamente dati che consentissero di identificare i titolari o utenti dei numeri di telefono relativi alle carte SIM che erano state inserite nel telefono cellulare rubato. Inoltre, era pacifico che tale richiesta riguardasse un periodo chiaramente definito e limitato nel tempo, vale a dire una dozzina di giorni.
Altro dato interessante risultava essere secondo la Corte il fatto che il numero delle persone potenzialmente interessate dalla misura controversa non fosse illimitato, come negli altri casi, bensì ristretto. Inoltre, tali persone erano non già tutti i detentori di una carta SIM, bensì individui aventi un profilo molto particolare, ossia persone che avevano utilizzato il telefono rubato dopo la sua sottrazione e che potevano

essere quindi legittimamente sospettati di essere gli autori del reato o di essere in relazione con questi ultimi.

Per di più, secondo il parere dell'Avvocato generale[31], i dati oggetto della richiesta consistevano non già in qualsiasi tipo di dati personali[32] detenuti dai fornitori di servizi di comunicazione elettronica, bensì soltanto in quelli relativi all'identità civile degli individui summenzionati, vale a dire il loro nome, il loro cognome ed eventualmente il loro indirizzo, dati che potevano anche essere qualificati "di contatto", mentre le altre informazioni riguardanti tali individui, eventualmente presenti negli archivi di detti fornitori, erano escluse dal procedimento principale[33].

Pertanto sulla base di questi presupposti la Corte ha constatato anzitutto che una misura come quella chiesta dalla polizia giudiziaria nel caso di specie sicuramente costituiva un'ingerenza nel diritto al rispetto della vita privata e della vita familiare nonché nel diritto alla protezione dei dati di carattere personale.

Tuttavia, come abbiamo evidenziato, in base alla sua giurisprudenza (*Digital Rights Ireland e Tele2 e Watson*) **la Corte anche in questo caso ha stabilito un collegamento tra la gravità dell'ingerenza constatata e la gravità del motivo che consente di giustificare quest'ultima.** Quindi per accertare, nella fase della giustificazione di una siffatta ingerenza, che sussista un reato "grave", che consenta di derogare al principio della riservatezza delle comunicazioni elettroniche, occorre che l'ingerenza sia "grave".

Tale elemento essenziale tuttavia non ricorre nella fattispecie in esame. I giudici di Lussemburgo infatti sostengono che la natura dell'ingerenza di cui trattasi nel caso di specie è diversa da quelle ravvisate nelle due sentenze sopra citate. **Si tratta infatti di una misura mirata** e finalizzata ad una possibilità di accesso, da parte delle autorità competenti e per le esigenze di un'indagine penale, a dati detenuti a fini commerciali da fornitori di servizi. Questi dati riguardano unicamente l'identità (nome, cognome ed eventualmente indirizzo) di una categoria ristretta di abbonati, vale a dire quelli il cui numero di telefono è stato attivato dal telefono cellulare il cui

---

[31] Si v. punto 35 e ss. delle Conclusioni dell'Avvocato Generale Henrik Saugmandsgaard Øe, presentate il 3 maggio 2018, Causa C-207/16, *Ministerio Fiscal*, EU:C:2018:300.

[32] Conformemente alla definizione di cui all'articolo 2, lettera a), della direttiva 95/46/CE, al quale rinvia l'articolo 2 della direttiva 2002/58/CE, la nozione di «dati personali» comprende «qualsiasi informazione concernente una persona fisica identificata o identificabile», con la precisazione che «si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale». La Corte ha già dichiarato che «il rispetto del diritto alla vita privata alla luce del trattamento dei dati personali si riferisce ad ogni informazione» corrispondente a tale definizione (v., in particolare, sentenza del 17 ottobre 2013, *Schwarz*, C-291/12, EU:C:2013:670, punto 26) e che la portata di quest'ultima è molto ampia (v., in particolare, sentenza del 20 dicembre 2017, *Nowak*, C-434/16, EU:C:2017:994, punto 33).

[33] Informazioni, quali, ad esempio, la situazione matrimoniale di un individuo, il numero della sua carta nazionale d'identità, le sue coordinate bancarie o il suo eventuale abbonamento telefonico.

furto costituisce l'oggetto dell'indagine, e per un periodo limitato di una dozzina di giorni.

La differenza infatti rispetto al passato è che **gli effetti potenzialmente nocivi, per le persone interessate dalla richiesta di accesso in questione, sono nel contempo moderati e circoscritti**, in quanto i dati richiesti non sono destinati ad essere divulgati al pubblico e la facoltà di accesso offerta alle autorità di polizia è circondata da garanzie procedurali, poiché essa dà luogo ad un controllo giurisdizionale. Di conseguenza, l'ingerenza causata dalla comunicazione di tali dati di identità civile non riveste un carattere di particolare gravità, dal momento che, in tali circostanze, dati siffatti non pregiudicano direttamente e fortemente l'intimità della vita privata della persone interessate.

La Corte pertanto in virtù di questi presupposti arriva a sostenere che, secondo l'articolo15 della direttiva, non è necessario che i reati che legittimano la misura restrittiva in questione debbano essere qualificati come "gravi", ai sensi delle sentenze *Digital Rights Ireland* e *Tele2 e Watson*. Essa infatti senza disconoscere la sua precedente giurisprudenza osserva che **soltanto quando l'ingerenza subita presenta una particolare gravità i reati idonei a giustificare una siffatta ingerenza devono presentare essi stessi una particolare gravità. Per contro, nell'ipotesi di un'ingerenza non grave** (ossia quando i dati di cui è richiesta la comunicazione non pregiudicano gravemente il diritto al rispetto della vita privata), **anche i reati che non presentano una particolare gravità possono giustificare tale ingerenza** (ossia l'accesso ai dati richiesti).

Pertanto qualora l'ingerenza non sia "grave" non verrà richiesta ai fini della legittimità dell'accesso e dell'obbiettivo perseguito mediante esso, la presenza di un reato "grave".

Pertanto, alla luce della direttiva, la misura richiesta dalla polizia giudiziaria nel caso di specie comporta un'ingerenza nei diritti fondamentali che può essere giustificata dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale, senza che sia necessario che tali reati siano qualificati come "gravi".

5. Riflessioni conclusive.

Occorre a questo punto chiedersi se la Corte di giustizia abbia offerto, con la sentenza in commento, un'interpretazione radicalmente innovativa ovvero se, come sembra, si tratti in realtà di una sentenza che costituisce il naturale completamento dell'opera avviata dalla stessa.

La sentenza sembra infatti confermare un definitivo "scacco matto" alla prevalenza delle ragioni di sicurezza pubblica su quelle di protezione della privacy. Un risultato che i giudici europei ottengono in tre mosse distinte e quasi discordanti.

La prima si è concretizzata nella sentenza del 2014 in cui la Corte aveva annullato una direttiva che sacrificava la tutela dei dati personali sull'altare della lotta al terrorismo internazionale, frutto di un periodo di legislazione emergenziale (*Digital Rights Ireland*).
La seconda con l'obbligo di rispettare seriamente la tutela della privacy digitale che incombe pertanto non solo sulle istituzioni europee, ma vincola anche i legislatori degli Stati membri, stabilendo che l'accesso ai dati conservati è limitato ai casi di reati "gravi" (*Tele2 e Watson).*
La terza in cui la Corte specifica che l'obiettivo perseguito dall'accesso ai dati personali deve essere proporzionato alla gravità dell'interferenza con i diritti fondamentali che l'accesso comporta. Grave interferenza per reato grave e lieve interferenza per reato lieve (*Ministerio Fiscal*).
La domanda che viene subito in mente è se il caso in esame si discosta dalle severe condizioni per l'accesso ai dati conservati esposti nella sentenza *Tele2 e Watson*, consentendo così l'accesso da parte delle autorità nazionali in un numero maggiore di scenari.
Innanzitutto, è importante notare che la sovrapposizione tra le due sentenze è piuttosto ridotta in quanto riguardano questioni molto diverse.
Il caso *Tele2 e Watson* riguarda l'accesso a dati privati tali da consentire di trarre conclusioni molto precise sulla vita delle persone i cui dati sono conservati. Tale accesso costituisce una grave interferenza con i diritti fondamentali e può essere giustificato dunque solo dall'obiettivo di combattere i reati "gravi".
Al contrario, il caso in esame riguarda una situazione presumibilmente molto limitata in cui l'accesso ai dati non costituisce una grave interferenza proprio in quanto si limita ad ottenere unicamente l'identità degli abbonati. Pertanto esso può essere giustificato anche dall'obiettivo di combattere i reati in generale.
Vi è, tuttavia, uno scenario in cui la nuova sentenza potrebbe creare una certa confusione sull'interpretazione del giudizio *Tele2 e Watson*. Secondo i paragrafi 108-111 della sentenza *Tele2 e Watson* infatti, i requisiti di conservazione dei dati al fine di combattere i reati "gravi" sono compatibili con il diritto dell'Unione, a differenza della conservazione dei dati generale e indifferenziata che è illegale proprio ai sensi dello stesso diritto. Inoltre, il punto 115 della sentenza stessa limita l'accesso a tali dati conservati ai soli casi di reati "gravi" proprio perché il requisito di conservazione dei dati "mirato", costituisce di per sé una grave interferenza con i diritti fondamentali che può essere giustificata solo dall'obiettivo di combattere un crimine "grave". Consentire pertanto l'accesso ai dati conservati anche ai casi che non comportino reati "gravi" pregiudicherebbe verosimilmente il proposito della limitazione nella fase di conservazione.

Occorre anche evidenziare che la Corte, anche in questa sentenza, non ha voluto definire ciò che può costituire un "grave" crimine[34]. A tale riguardo, si ricorda come la nozione di reati "gravi" è stata utilizzata dalla Corte nella sentenza *Digital Rights Ireland*[35], talvolta in combinazione con la nozione di criminalità "grave"[36], quale criterio di verifica della finalità e della proporzionalità dell'ingerenza nei summenzionati diritti fondamentali che era causata da disposizioni del diritto dell'Unione riguardanti dati personali. Si precisa in aggiunta che tale nozione, che non figura nella direttiva 2002/58/CE[37], era utilizzata nella direttiva 2006/24/CE[38], la cui invalidità costituiva oggetto di detta sentenza. La Corte ha poi utilizzato entrambe le nozioni nella sentenza *Tele2 e Watson* [39], (senza mai tuttavia specificarne il contenuto) ma per quanto riguarda, questa volta, la conformità al diritto dell'Unione [40] di disposizioni adottate da Stati membri.

Si fa presente inoltre che, dato che sussistono grandi differenze tra le scale di sanzioni che sono tradizionalmente applicabili nei vari Stati membri[41], la gravità di un reato non dipende soltanto dall'entità della pena per esso prevista. Infatti, determinare se un reato sia grave è questione molto relativa, nel senso che dipende dalla scala delle sanzioni applicate in generale nello Stato membro interessato. Pertanto, il fatto che uno Stato membro preveda una pena detentiva poco elevata, o persino una pena alternativa alla reclusione, non incide di per sé sulla gravità intrinseca del tipo di reato in questione[42]. Occorre, a nostro avviso, rispettare le

[34] Secondo L. WOODS, *Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers*, in *EU Law Analysis*, 4 ottobre 2018, http://eulawanalysis.blogspot.com/2018/10/mobile-phone-theft-and-eu-eprivacy-law.html, la Corte ha appositamente evitato di prendere posizione sulla individuazione dei criteri che determinano la gravità del reato.

[35] V. punti 24, 41, 49 e da 57 a 61 della sentenza *Digital Rights Ireland*.

[36] V. punti 41, 42, 51 e 59 della sentenza *Digital Rights Ireland*.

[37] Si ricorda che nella direttiva 2002/58/CE figura soltanto l'espressione «reati», all'articolo 15, paragrafo 1, prima frase.

[38] In sostanza, al considerando 9 della direttiva 2006/24/CE, nonché, letteralmente, al considerando 21 e all'articolo 1, paragrafo 1, di quest'ultima.

[39] V. per quanto riguarda la nozione di «reati gravi», punti 105, 106 e 119 nonché, per quanto concerne la nozione di «criminalità grave», punti 102, 103, 108, 110, 111, 114, 115, 118, 125 e 134 della sentenza *Tele2 e Watson*.

[40] Vale a dire, l'articolo 15, paragrafo 1, della direttiva 2002/58/CE, in forza del quale gli Stati membri possono adottare una misura che deroga al principio di riservatezza delle comunicazioni e dei dati relativi al traffico ad esse correlati qualora tale misura sia necessaria, opportuna e proporzionata, all'interno di una società democratica, alla luce degli obiettivi enunciati da tale disposizione.

[41] A titolo di esempio, in materia di lotta contro la criminalità organizzata, una relazione della Commissione del 7 luglio 2016 indica che le pene previste dagli Stati membri variano tra loro in modo notevole (da 3 mesi a 17 anni di reclusione) per il reato grave costituito dalla partecipazione ad un'organizzazione criminale [v. relazione al Parlamento europeo e al Consiglio a norma dell'articolo 10 della decisione quadro 2008/841/GAI del Consiglio, del 24 ottobre 2008, relativa alla lotta alla criminalità organizzata, COM(2016) 448 final, pag. 7, punto 2.1.4.1].

[42] In Danimarca sono applicate sanzioni meno gravi, rispetto ad altri Stati membri, senza che ciò significhi che un determinato reato sia considerato privo di particolare gravità. Ad esempio, la sanzione prevista per il possesso di materiale pedopornografico è di un anno di reclusione, mentre essa potrebbe arrivare fino a dieci anni di

specificità dell'ordinamento giuridico penale di ciascuno degli Stati membri, purché il diritto dell'Unione non stabilisca obblighi che vincolano questi ultimi in maniera rigorosa, per analogia con quanto dichiarato dalla Corte per quanto riguarda la salvaguardia della sicurezza pubblica[43], nozione affine a quella di lotta contro la criminalità grave, in particolare alla luce del testo dell'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58/CE.

Pertanto, tramite la riformulazione di quanto chiesto dal giudice del rinvio, la Corte ha evitato il problema della determinazione non solo di reato "grave", ma del fatto che il reato "grave" sia un concetto autonomo dell'Unione. In tale contesto, la Corte ha seguito il parere dell'Avvocato generale che si è spinto fino a sostenere che la "legge penale" non dovrebbe essere un concetto autonomo del diritto dell'Unione[44]. Ciò che viene approfondito è infatti non la gravità del reato o i criteri utili per determinarla, quanto il suo rapporto con la gravità dell'ingerenza nei diritti fondamentali.

In sostanza la Corte attraverso il pretesto della proporzionalità ha suggerito anche l'accesso per reati meno gravi, creando così il rischio che si possa affermare che le leggi nazionali possano consentire l'accesso a questi dati, un'interpretazione che oltrepasserebbe i limiti della sua competenza. Così facendo essa ha evitato di occuparsi di quali fossero i criteri necessari per identificare un reato "grave", in quanto non risultava più necessario essendo la situazione caratterizzata da un ingerenza non grave.

Occorre domandarsi pertanto se la Corte potrà pronunciarsi su questo punto dinnanzi ad un nuovo rinvio pregiudiziale in un caso di ingerenza e lesione "grave" dei diritti fondamentali, richiedente pertanto la gravità del reato come elemento rafforzativo di legittimità. Merita comunque sottolineare come l'Avvocato generale, nelle sue Conclusioni, spinga la propria analisi a valutazioni attinenti anche ai criteri di determinazione della gravità del reato. Questo perché l'Avvocato propone le proprie considerazioni anche per il caso in cui la Corte avesse ritenuto necessario

---

reclusione, per gli stessi fatti, in altri Stati membri, ma ciò non toglie che tale reato sia, per sua natura, particolarmente grave.

[43] V. in particolare, sentenza del 22 maggio 2012, I (C-348/09, EU:C:2012:300, punti da 21 a 23), a termini della quale «il diritto dell'Unione non impone agli Stati membri una scala uniforme di valori per quanto riguarda la valutazione dei comportamenti che possono essere considerati contrari alla pubblica sicurezza» e «gli Stati membri restano sostanzialmente liberi di determinare, conformemente alle loro necessità nazionali – che possono variare da uno Stato membro all'altro e da un'epoca all'altra – le regole di ordine pubblico e di pubblica sicurezza, specie qualora autorizzino una deroga al principio fondamentale della libera circolazione delle persone», ma «tali regole devono tuttavia essere intese in senso restrittivo, di modo che la loro portata non può essere determinata unilateralmente da ciascuno Stato membro senza il controllo delle istituzioni dell'Unione europea».

[44] V. conclusioni dell'Avvocato Generale Henrik Saugmandsgaard Øe, presentate il 3 maggio 2018, EU:C:2018:300.

fornire una vera e propria definizione di reato "grave", cosa che invece non è avvenuta[45].

La Corte inoltre nella sentenza in commento non indica chiaramente il motivo per cui i dati sono stati conservati o se questo motivo possa o meno influenzare le condizioni per l'accesso a questi dati. Pertanto poiché non vi è alcuna connessione apparente al motivo per cui queste informazioni vengono conservate, la Corte di giustizia ha affermato nei paragrafi 54-61 della sentenza che se l'accesso riguarda solo piccole parti dei dati conservati, ad esempio al solo scopo di ottenere l'identità dell'abbonato, l'accesso a tali informazioni non costituisce una "grave" interferenza, anche se i dati in realtà sono disponibili a causa di una disposizione (mirata) di conservazione che può essere giustificata solo dall'obiettivo di combattere i reati "gravi".

Viene quindi lasciata in sospeso la questione del se e in quale misura sia possibile parlare di accesso mirato se prima alla base non vi è una conservazione generalizzata dei dati.

Lasciando da parte dunque il potenziale indebolimento delle rigide condizioni espresse in *Tele2 e Watson* in merito all'accesso ai dati conservati, andiamo ora ad evidenziare gli aspetti positivi del nuovo giudizio nella prospettiva dei diritti digitali.

[45] I punti cardine individuati dall'Avvocato sono: innanzitutto, alla luce della giurisprudenza *Digital Rights Ireland* e *Tele2 e Watson*, l'Avvocato è portato a considerare che la definizione di gravità non dovrebbe basarsi meramente sull'entità della pena e dunque su un criterio formale. Con una limitazione di fondo però: richiamando la necessità di una interpretazione restrittiva dell'articolo 15 stesso, anche la nozione di reato "grave" deve essere restrittiva e intesa in modo non eccessivamente ampio da parte degli Stati membri. Inoltre, se la Corte avesse ritenuto tale nozione come autonoma, la pronuncia dei giudici di Lussemburgo avrebbe dovuto spingersi a valutare anche i criteri che consentono di stabilire la gravità di un reato. In tal caso, l'Avvocato ha ritenuto necessario fondare la definizione di gravità su una pluralità di criteri di valutazione (par. 105). Inoltre, viene sottolineato come tale quesito avrebbe dovuto trovare risposta solo nel caso in cui la Corte avesse basato la nozione di gravità esclusivamente sul criterio formale e quindi sul *quantum* della pena. La seconda domanda pregiudiziale infatti ha ad oggetto l'individuazione della soglia minima di pena richiesta per attribuire la qualifica di gravità ad un reato e, in particolare, se la soglia individuata dal legislatore spagnolo in 3 anni di reclusione possa essere considerata conforme ai requisiti del diritto dell'Unione (par. 108). Se è vero che una tale soglia di pena non può essere determinata in modo uniforme su tutto il territorio europeo, viene ripreso quel principio, più volte affermato, secondo cui l'utilizzo della deroga prevista all'articolo 15 deve rimanere una eccezione. Partendo da questa considerazione di base, anche in questo caso, l'Avvocato è giunto ad affermare come non sia possibile fissare una soglia, che pur rimane prerogativa degli Stati membri, talmente bassa "da far diventare principio l'eccezione" (par. 114). L'Avvocato ammonisce comunque la Corte dai rischi derivanti dalla determinazione giurisprudenziale di una soglia: "poiché una (simile) determinazione richiede una valutazione complessa e potenzialmente soggetta a evoluzione, occorre a mio avviso restare prudenti a questo proposito e riservare tale operazione alla valutazione del legislatore dell'Unione, nella sfera delle competenze conferite a quest'ultima, o alla valutazione del legislatore di ciascuno Stato membro, entro i limiti dei requisiti derivanti dal diritto dell'Unione" (par. 117). Senza dunque arrivare a determinare un quantitativo specifico, si conclude che gli Stati membri sono liberi di fissare il livello minimo della pena, a condizione che siano rispettati i requisiti risultanti dal diritto dell'Unione e, in particolare, quello secondo cui le ingerenze nei diritti fondamentali devono restare eccezionali e rispettare il principio di proporzionalità (par. 121).

Innanzitutto viene chiarito che i dati sul traffico telefonico ai sensi della direttiva del 2002 includono i nomi degli abbonati di carte SIM attivate con il codice IMEI[46] del telefono cellulare rubato, con esclusione dei dati relativi alle comunicazioni effettuate con tali schede SIM e dei dati relativi all'ubicazione del telefono cellulare rubato[47]. Ciò implica che l'accesso a tali dati rientra nell'ambito e nelle garanzie della direttiva del 2002 e che la direttiva stessa non può essere aggirata dai tentativi di ampliare la definizione di "dati dell'abbonato" al fine di consentire l'accesso ad un maggior numeri di informazioni.

In secondo luogo, il giudizio della Corte sottolinea al punto 51 che, come rilevato dall'Avvocato generale ai paragrafi 76 e 77 delle sue Conclusioni, l'accesso delle autorità pubbliche a tali dati costituisce un'ingerenza nel diritto fondamentale al rispetto della vita privata, sancito all'articolo 7 della Carta, persino in mancanza di circostanze che permettano di qualificare tale ingerenza come "grave" e senza che rilevi il fatto che le informazioni in questione relative alla vita privata siano o meno delicate. Tale accesso costituisce anche un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta, poiché costituisce un trattamento di dati personali[48]. Proprio per questi motivi, la Corte ha richiesto che vi siano condizioni sostanziali e procedurali basate su criteri oggettivi per l'accesso ai dati conservati e che l'accesso debba essere soggetto a un controllo preventivo da parte di un tribunale o di un organo amministrativo indipendente.

Infine ai paragrafi 34-37 della sentenza, la Corte ribadisce quanto affermato nella sentenza *Tele2 e Watson* ossia che le legislazioni nazionali che consentono l'accesso delle autorità competenti ai dati personali conservati dai fornitori di servizi di comunicazione elettronica non possono essere considerate attività dello Stato che esulano dall'ambito di applicazione dell'articolo 15, paragrafo 1, della direttiva del 2002, in quanto l'accesso da parte delle autorità competenti presuppone necessariamente il trattamento dei dati personali da parte dei fornitori di servizi di comunicazione elettronica.

Tuttavia la Commissione europea ha recentemente presentato due proposte volte a consentire l'accesso ai dati degli abbonati per tutti i reati e senza alcun obbligo di revisione preventiva da parte di un tribunale (l'approvazione del pubblico ministero può essere sufficiente) o un organo amministrativo indipendente e questo creerà

---

[46] Il **codice IMEI** (acronimo di International Mobile Equipment Identity) è un codice composto da 15 cifre che consente di identificare in maniera univoca i telefoni cellulari. Nel caso in cui si smarrisca o si subisca il furto del proprio telefono l'IMEI può essere usato per denunciare il furto del dispositivo e in seguito richiedere al proprio operatore telefonico di bloccare l'accesso alla rete da parte di quest'ultimo.

[47] V. paragrafi 40-42 della sentenza della Corte.

[48] V. in tal senso, parere 1/15 (Accordo PNR (Passengers Name Records)UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 124 e 126 e giurisprudenza ivi citata.

notevoli problematiche in sede giurisdizionale[49]. Inoltre è ancora in fase di discussione una proposta di regolamento[50] volto a sostituire la direttiva del 2002[51].
La Corte di Giustizia Europea, pertanto, disimpegnandosi in una complessa attività di bilanciamento tra diritti primari che fanno capo alle persone fisiche e all'obbligatorietà dell'azione penale, ha fatto luce sulle ipotesi di compressione del diritto alla riservatezza a fronte della necessaria attività investigativa circa specifiche fattispecie di reato.
Tuttavia similari questioni pregiudiziali sono ancora pendenti dinanzi alla Corte. Come quella sollevata dal Tribunale inglese[52] che si è interrogato sulla conservazione generalizzata di dati da parte delle Agenzie di Intelligence. Nello specifico ci si interroga se i dettati della pronuncia *Tele2 e Watson* riguardanti l'accesso delle autorità pubbliche debbano riferirsi anche alle agenzie suddette. E come quella in cui la Corte Costituzionale belga[53], chiede se l'articolo 15 della 2002/58/CE possa impedire agli Stati membri di adottare normative nazionali che impongano un generico obbligo di conservazione indipendentemente dalla criminalità grave proprio perché riguardanti la sicurezza nazionale. Entrambe le questioni richiedono un chiarimento del campo di applicazione della direttiva proprio rispetto ad attività che appartengono all'esclusivo appannaggio degli Stati, come ad esempio la sicurezza nazionale.
Entrambi questi rinvii potrebbero essere l'occasione per i giudici europei di armonizzare finalmente le normative nazionali in materia di accesso ai dati relativi

[49] Il 17 aprile 2018, la Commissione europea ha presentato due proposte: una proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali (COM(2018) 225 final, del 17.4.2018.) e una proposta di direttiva che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018) 226 final, del 17.4.2018). Il regolamento e la direttiva proposti forniranno alle autorità di contrasto e alle autorità giudiziarie competenti nuovi strumenti per acquisire prove elettroniche ai fini dell'indagine e dell'azione penale, anche per i reati di terrorismo e criminalità informatica.
[50] Procedimento 2017/0003/COD, COM (2017) 10: *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC* (Regulation on Privacy and Electronic Communications).
[51] Si v. G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Medialaws*, 2/2018.
[52] Domanda di pronuncia pregiudiziale proposta dall'I*nvestigatory Powers Tribunal*, Londra (Regno Unito) il 31 ottobre 2017 – *Privacy International/Secretary of State for Foreign and Commonwealth Affairs e a.*, C-623/17. Nel rinvio pregiudiziale si legge infatti: "tenuto conto dell'esigenza fondamentale delle SIA di utilizzare tecniche di acquisizione in massa e di trattamento automatizzato per proteggere la sicurezza nazionale".
[53] Domanda di pronuncia pregiudiziale proposta dalla *Cour constitutionnelle* (Belgio) il 2 agosto 2018, Causa C-520/18. Il caso trae origine da alcuni ricorsi promossi, a seguito della decisione *Tele2 e Watson* , avverso la normativa nazionale "loi du 29 mai 2016 relative aux communications électroniques", del 18 luglio 2016, ritenuta non conforme ai principi individuati dalla Corte nella sua giurisprudenza. È interessante sottolineare come la Corte Costituzionale belga si fosse già in precedenza pronunciata, a seguito della decisione *Digital Rights Ireland*, sulla previa normativa nazionale in materia di conservazione di dati (Loi du 30 juillet 2013), annullandola con sentenza del 11 giugno 2015.

alle comunicazioni elettroniche da parte delle autorità pubbliche al fine di creare un deciso bilanciamento tra gli interessi dello Stato e la tutela dei diritti fondamentali.