Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio

CORTE DI CASSAZIONE; sezione III penale; sentenza 23 agosto 2019, n. 36380; Pres. Andreazza; Rel. Semeraro; P.M. Molino.

In tema di acquisizione di dati contenuti in tabulati telefonici, la disciplina prevista dall'art. 132 d.lgs. n. 196 del 2003 è compatibile con il diritto sovranazionale in tema di tutela della privacy (direttive 2002/58/CE e 2006/24/CE), così come interpretato dalla giurisprudenza della Corte di Giustizia dell'Unione Europea.

La presenza del possessore di un cellulare in una data zona, più o meno ampia rispetto alla grandezza della cella telefonica, deve essere qualificata quale semplice indizio, anche se l'utenza è precisamente attribuita ad una determinata persona.

...Omissis...

Svolgimento del processo.

1. La Corte di appello di Bologna, con la sentenza del 21 dicembre 2017, in parziale riforma della sentenza del giudice dell'udienza preliminare del Tribunale di Ravenna del 9 giugno 2011, emessa all'esito del giudizio abbreviato, ha:

...Omissis...

- confermato la condanna inflitta a B.A. per il reato D.P.R. n. 309 del 1990, ex art. 73, comma 1, per la cessione a G.D. di 314 grammi di cocaina, con principio attivo del 98%, in (*omissis*), ed ha rideterminato la pena in anni 3 mesi 6 giorni 20 di reclusione ed Euro 20.000 di multa.

La Corte di appello ha confermato la pena base inflitta dal giudice di primo grado di anni 8 di reclusione e rideterminato la multa in Euro 50.000; ha quindi ridotto la pena per le circostanze attenuanti generiche a anni 5 mesi 4 di reclusione ed Euro 30.000 di multa, ed ha operato la riduzione per il rito.

I difensori di D.G. e B.A. hanno proposto il ricorso per cassazione avverso la sentenza della Corte di appello di Bologna del 21 dicembre 2017.

...Omissis...

3. Il difensore di B.A. ha premesso che l'impugnazione si riferisce al capo 4) ed ai punti relativi alla ritenuta della responsabilità del ricorrente ed all'utilizzabilità degli elementi di prova raccolti mediante l'acquisizione dei tabulati telefonici.

3.1. Con il primo motivo si deducono, ex art. 606 c.p.p., lett. c) ed e), i vizi di violazione di legge per l'erronea applicazione dell'art. 192 c.p.p., comma 2 e art. 533 c.p.p., e della manifesta illogicità della motivazione nel punto relativo alla ritenuta partecipazione del ricorrente alla cessione della sostanza stupefacente.

Dopo aver sintetizzato la motivazione della sentenza impugnata in risposta al motivo di appello, si rileva che l'unico indizio posto a fondamento della responsabilità dai giudici di merito sarebbe costituito dalla presenza dell'utilizzatore dell'utenza (*omissis*) sul luogo del delitto; l'attribuzione dell'uso dell'utenza al ricorrente sarebbe avvenuto con ragionamenti inferenziali di tipo abduttivo, inidonei ad integrare la certezza indiziaria richiesta dall'art. 192 c.p.p., comma 2.

3.1.1. Si assume, in ogni caso, che anche ove fosse ritenuta la presenza sul luogo del ricorrente, questa non potrebbe costituire elemento sufficiente a ritenere la responsabilità per la cessione, in una condotta contestata ex art. 110 c.p., in assenza di elementi dai quali individuare quale contributo materiale o morale avrebbe il ricorrente posto in essere.

3.1.2. Si contesta poi che la Corte di appello abbia adoperato quale indizio il fatto che il ricorrente sia stato indagato nel 2002 nell'ambito di un'operazione relativa al traffico di sostanza stupefacente, in violazione delle più elementari regole probatorie e dei principi della giurisprudenza sulla valutazione della condotta dell'imputato pregiudicato (rv 264198).

3.1.3. La valorizzazione del precedente di polizia sarebbe avvenuta per dare corpo alla pluralità di indizi che deve sussistere per affermare la responsabilità secondo l'art. 192 c.p.p., comma 2: l'unico indizio sarebbe costituito dalla ritenuta disponibilità in capo al ricorrente dell'utenza (*omissis*) che ha agganciato le cellule di (OMISSIS) nella zona e nell'ora in cui il (*omissis*) sarebbe stata ceduta la sostanza stupefacente a G.D..

Tale dato però non costituisce un fatto certo, oggetto di diretta verifica storica, ma a sua volta il frutto di un ragionamento induttivo, inidoneo a ritenere la gravità indiziaria secondo l'art. 192 c.p.p., comma 2.

3.1.4. Si rileva che i giudici di merito hanno ritenuto, in base ad un sillogismo probatorio, che l'usuario dell'utenza (OMISSIS) fosse nell'Audi a6 nel momento in cui l'acquirente acquistò la cocaina.
...Omissis...
3.1.5. Quanto alla presenza dell'utenza (*omissis*), nella sentenza è stata dedotta dal dato emergente dai tabulati telefonici, in quanto l'utenza aveva agganciato le celle di (*omissis*) in cui avvenne la cessione a G.D.; la gravità dell'indizio è stata alimentata dal rilievo che l'utenza (OMISSIS *omissis* era stata contattata da G.D. nei momenti coevi al suo ingresso nell'Audi A6, occupata da due ignoti uomini.
La sentenza di appello avrebbe sottolineato che G.D., con un'altra utenza a lui in uso, avrebbe cercato di chiamare un altro numero, da lui memorizzato nelle memorie sotto la voce H.; anche l'utenza (*omissis*) era stata registrata dall'acquirente sotto lo stesso nome.
L'attribuzione dell'utenza (OMISSIS) al ricorrente sarebbe stata effettuata dalla Corte di appello sempre in via indiziaria, in base ad un criterio di verosimiglianza, contrario al principio del ragionevole dubbio.
L'attribuzione dell'utenza al ricorrente sarebbe avvenuta in base ad una conversazione intercettata tra l'utenza in uso a G.D. e quella (OMISSIS) nel corso della quale G.D. informò l'interlocutore su una conversazione precedente con un agente immobiliare relativa ad un immobile dietro via (*omissis*) di "un amico di nome A.".
L'attribuzione dell'utenza è avvenuta perché è stata acquisita presso l'agenzia immobiliare la documentazione relativa ad un negozio di via (OMISSIS) strada che si trova alle spalle di via (*omissis*) – per il quale era stato indicato per i contatti il nome di B.A., e per il fatto che quest'ultimo era già stato indagato per il reato D.P.R. n. 309 del 1990, ex art. 73.
Si rileva però che l'associazione tra i contatti dell'agenzia relativi ad immobili nelle vicinanze di via (*omissis*) ed B.A. è avvenuta in maniera probabilistica, solo in base al fatto che quest'ultimo era stato indagato per il delitto D.P.R. n. 309 del 1990, ex art. 73, senza verificare l'esistenza di altri contatti, e senza collegamenti reali con il nome H. registrato nella rubrica dell'acquirente.
3.1.6. Il ricorrente rileva che all'agenzia immobiliare B.A. aveva lasciato un numero di telefono diverso ((*omissis*)): tale prova è stata tralasciata dalle sentenze di merito, ciò incidendo sulla apparente correttezza dell'attribuzione dell'utenza (*omissis*) al ricorrente, ritenuto il soggetto informato da G.D. sulla trattativa immobiliare.
La Corte di appello non ha poi tenuto conto che non è emerso che il ricorrente fosse in possesso di più utenze telefoniche e che l'utenza (*omissis*) non era dedicata alle trattative illecite, posto che su tale utenza era avvenuta la conversazione sulla trattativa immobiliare.
Né è stato valutato che l'utenza (*omissis*) non è risultata associata nella rubrica di G.D. al nome H.
Dunque, l'attribuzione dell'utenza (*omissis*) al ricorrente sarebbe avvenuta non su un fatto certo ma su un fatto verosimile, in violazione dell'art. 192 comma 2 c.p.p. e ciò mina la logicità del ragionamento del giudice, che sarebbe in contrasto anche con il principio del ragionevole dubbio.
Il ricorso prosegue poi con l'esposizione in diritto sulla prova indiziaria (pagine 14-17); si afferma quindi che in violazione di tali principi di diritto le sentenze di merito si fonderebbero su un paralogismo giuridico, per effetto del quale si è giunti alla dichiarazione di responsabilità del ricorrente.
3.2. Con il secondo motivo si deduce, ex art. 606 c.p.p., lett. c), l'inosservanza dell'art. 191 c.p.p.; si ritiene che il D.Lgs. n. 196 del 2003, art. 132 sarebbe in contrasto con gli artt. 7, 8 e 52 par. 1 della Carta dei diritti fondamentali UE, come interpretati dalla Corte di Giustizia dell'Unione Europea con la sentenza del 8 aprile 2014, il cui contenuto è sintetizzato nel ricorso, in relazione alla direttiva 2006/24/CE in materia di data retention, con conseguente inutilizzabilità dei dati emergenti dal tabulato telefonico relativo all'utenza (OMISSIS).
L'inutilizzabilità ex art. 191 c.p.p. deriverebbe dalla lesione dei diritti fondamentali della persona, arrecata dall'art. 132 citato, per la mancanza dell'indicazione dei reati al cui accertamento è volta l'acquisizione del dato e per la scelta di attribuire ad una parte del procedimento penale, il pubblico ministero, l'opportunità di acquisire i dati.
La direttiva 2006/24/CE agli art. 3, 4 e 6 prevederebbe la conservazione dei dati derivanti dalle comunicazioni telefoniche e telematiche solo per il perseguimento di gravi reati ed ai soli fini di indagine.
Si invocano in particolare i principi di proporzionalità e stretta necessità elaborati dalla Corte di Giustizia, ed il collegamento della compressione delle libertà con la gravità dei reati per cui si procede, perché la necessità che l'accesso ai dati avvenga dopo l'esame di un giudice o di un'autorità amministrativa indipendente; si invocano gli ulteriori profili di illegittimità derivanti dalla finestra temporale per l'acquisizione dei dati senza distinguere tra le categorie di dati, in mancanza di previsione di garanzie sufficienti contro il rischio di abusi.
L'art. 132 citato conterrebbe dunque tutti i vizi già individuati dalla Corte di Giustizia, con conseguente necessità di disapplicare la norma interna e di ritenere la prova acquisita vietata dalla legge e quindi non utilizzabile.
In subordine si chiede il rinvio pregiudiziale ex art. 267 TFUE alla Corte di Giustizia dell'Unione Europea affinchè accerti se gli artt. 7, 8 e 52 par. 1 della Carta dei diritti fondamentali UE ostino ad una normativa nazionale, quale quella D.Lgs. n. 196 del 2003, ex art.

132 che consente l'acquisizione e la conservazione del traffico telematico per qualsiasi tipo di reato e senza un previo controllo della richiesta da parte di un'autorità indipendente.
Quanto alla cd. prova di resistenza, si rileva che il dato emerso dal tabulato nella motivazione è stato adoperato per ritenere che il possessore dell'utenza si trovasse in (OMISSIS) nella zona quindi in cui era stata ceduta la sostanza stupefacente al G.; costituisce quindi l'unico elemento di prova per individuare uno dei due soggetti presenti sull'Audi A6 in cui sarebbe avvenuta la cessione.

Motivi della decisione

...Omissis...

2. Il primo motivo del ricorso di B.A. è fondato, sussistendo i vizi della motivazione dedotti con il ricorso quanto alla sussistenza della penale responsabilità del ricorrente.
2.1. La Corte di appello ha ritenuto che il ricorrente sia l'autore della cessione a G.D., avvenuta a bordo di un'Audi A6, perché sul telefono cellulare in uso a quest'ultimo erano stati trovati tentativi di telefonate in uscita al n. (*omissis*), associata al nome H., e "prima del suo arresto" il (*omissis*) G.D. aveva contattato l'utenza (*omissis*); dall'analisi dei tabulati telefonici tale utenza si trovava nella cella di (*omissis*), luogo in cui era avvenuta la cessione.
L'utenza (*omissis*) è stata ritenuta in uso al ricorrente in base al collegamento tra due conversazioni telefoniche, una con un agente immobiliare e l'altra con l'usuario dell'utenza (*omissis*), ed in base agli accertamenti eseguiti presso l'agenzia immobiliare.
...Omissis...
2.3. Sussiste il dedotto vizio della motivazione nella parte in cui ha attribuito l'uso dell'utenza (*omissis*) al ricorrente.
L'attribuzione è avvenuta sulla base di due elementi: perché su altra utenza in uso all'acquirente G.D. il n. (*omissis*) era registrato in rubrica con il nome H., laddove il nome del ricorrente è A.; per gli accertamenti effettuati presso una agenzia immobiliare, a seguito di due conversazioni telefoniche, la prima con un agente immobiliare, nel quale si faceva riferimento ad A. e ad un negozio di (*omissis*).
Il ricorrente ha però dimostrato, mediante la produzione dell'annotazione di servizio relativa all'accertamento eseguito presso l'agenzia immobiliare, che la Corte di appello è incorsa in un travisamento della prova per omissione: non ha infatti valutato che il numero di telefono (*omissis*) lasciato da B.A. presso l'agenzia immobiliare non è perché il n. (*omissis*) perché quello n. (*omissis*) contattato invano il giorno dell'arresto e sempre inserito in rubrica da G.D. con il nome di H..
Il dato probatorio non può considerarsi neutro perché può anche escludere che H. ed il ricorrente siano la stessa persona.
2.4. In ogni caso, la conclusione a cui è giunta la Corte di appello è contraddittoria.
2.4.1. In punto di diritto deve infatti affermarsi che l'elemento di prova costituito della presenza di un telefono in una determinata cella dimostra, solo ed esclusivamente, che l'utilizzatore di quel telefono si trova in un data zona: per altro anche piuttosto grande, perchè le celle telefoniche non identificano un luogo preciso ma una zona di copertura della rete telefonica di grandezza variabile; nel caso in esame, la grandezza delle celle prese in esame non è neanche indicata: pertanto l'utilizzatore del n. (*omissis*) e G.D. avrebbero potuto trovarsi anche in due luoghi differenti.
La presenza del possessore di un telefono cellulare in una data zona, più o meno ampia rispetto alla grandezza della cella, può essere qualificato quale indizio, ma di per sè non dimostra nulla, anche se l'utenza è precisamente attribuita ad una determinata persona: per avere una valenza probatoria, tale da poter portare ad una sentenza di condanna, occorrono altri indizi, ugualmente gravi e precisi, ed infine tutti concordanti, che possano consentire di affermare che il possessore dell'utenza ha commesso il reato.
2.4.2. Orbene, il procedimento logico seguito dalla Corte di appello è sia contraddittorio che manifestamente illogico.
Nella sentenza di appello si fa riferimento alle trattative che sarebbero state svolte nei giorni precedenti l'arresto di G.D.: di tali conversazioni non sono riportati i contenuti e gli estremi, ma deve ritenersi che siano avvenute con utenze non ricondotte, già secondo l'ipotesi accusatoria, a B.A.; perché che sia stato quest'ultimo ad avere le conversazioni ritenute dall'oggetto illecito e che preannunciavano la consegna.
Le telefonate dirette verso il numero (*omissis*), rubricato H., contattato il giorno dell'arresto, non si sono concretizzate in conversazioni, ed anzi sarebbero costituiti in meri tentativi di chiamata. Dunque, è escluso che attraverso esse G.D. possa aver preso l'appuntamento per la consegna.
La sentenza impugnata indica che prima dell'arresto G.D. contattò il n. (*omissis*); non essendo stata intercettata la telefonata, non se ne conosce il contenuto.
Tale utenza, all'atto del contatto, si trovava in (*omissis*), luogo in cui nello stesso tempo si recò anche G.D. per acquistare la sostanza stupefacente.
Orbene, come già osservato, questo contatto non dimostra in alcun modo che l'utilizzatore dell'utenza n. (OMISSIS) si trovasse all'interno dell'Audi A6 ma solo che si trovava nella zona di (*omissis*); collocarlo all'inter-

no dell'auto ed attribuirgli la condotta di cessione è un salto logico privo di elementi di prova a sostegno.
...Omissis...
2.6. Va altresì rilevata una ulteriore contraddittorietà della motivazione: nella sentenza si indica che non vi sono conversazioni registrate, collegate alle utenze che la sentenza attribuisce al ricorrente, aventi un contenuto illecito.
L'unica conversazione riportata, se attribuibile al ricorrente, avrebbe un oggetto lecito, essendo relativa al rapporto con l'agenzia ed all'immobile. Dunque, la stessa sentenza indica una causale alternativa lecita al contatto tra l'utenza attribuita al ricorrente e G.D.
Dunque, emerge dalla sentenza della Corte di appello la totale assenza di elementi di prova per ritenere che il ricorrente abbia ceduto la sostanza stupefacente a G.D.; si impone pertanto l'annullamento della sentenza impugnata senza rinvio nei confronti di B.A. per non aver commesso il fatto.
3. Quanto al secondo motivo, dal testo del ricorso risulta subordinato al rigetto del primo motivo. Perché in sede di discussione la difesa ha affermato che va ritenuto pregiudiziale, ritiene la corte di doverlo esaminare.
3.1. Il motivo è infondato.
...Omissis...
3.2. Va ribadito il principio espresso dalla Corte di Cassazione, Sez. 5, con la sentenza n. 33851 del 24/04/2018, M., Rv. 273892 - 01 per cui in tema di acquisizione di dati contenuti in tabulati telefonici, la disciplina prevista dal D.Lgs. n. 196 del 2003, art. 132 è compatibile con il diritto sovranazionale in tema di tutela della privacy (direttive 2002/58/CE e 2006/24/CE), come interpretate dalla giurisprudenza della Corte di Giustizia dell'Unione Europea.
In motivazione, la Corte ha fatto riferimento alle sentenze della CGUE: Grande Sezione, Digital Rights, 8 aprile 2014, C-293/12 e C-594/12; Grande Sezione, Tele 2, 21 dicembre 2016, C-203/15 e C-698/15.
3.3. Come ha correttamente rilevato la sentenza M., nella motivazione, che qui si sintetizza, la direttiva 2002/58/CE, avente ad oggetto i diritti alla riservatezza delle comunicazioni, dei dati sul traffico e di quelli sull'ubicazione, consente agli Stati membri di derogare, ai sensi dell'art. 15, par. 1, a prescrizioni, divieti ed obblighi fissati per la tutela di quei diritti, con l'adozione legislativa di misure restrittive, purchè la restrizione costituisca "una misura necessaria, opportuna e proporzionata all'interno di una società democratica per 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".
Quanto alla conservazione dei dati (cd. Data retention), la memorizzazione da parte di persone diverse dagli utenti o senza il loro consenso è ammessa solo ai fini e per il tempo strettamente necessario alla trasmissione della comunicazione, perché, a date condizioni, per l'attività di fatturazione; diversamente, ogni dato è destinato alla distruzione o "anonimizzazione".
La direttiva 2006/24/CE, di modifica della direttiva 2002/58/CE, ha avuto l'obiettivo di armonizzare le disposizioni degli Stati membri quanto all'obbligo per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, o di una rete di comunicazione, di raccogliere e conservare, per un periodo di tempo determinato, dati ivi generati o trattati, allo scopo di cui all'art. 1, par. 1, "di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di gravi reati, quali definiti da ciascuno Stato membro nella propria legislazione nazionale".
3.4. Due sentenze della Grande Sezione della Corte di Giustizia hanno affrontato il tema del bilanciamento tra i diritti fondamentali dell'individuo e l'esigenza di accertamento e repressione dei reati mediante acquisizione di dati e informazioni presso service providers: la prima, nelle cause riunite C-293/12 e C594/12, decisa in data 8 aprile 2014, Digital Rights Ireland Ldt contro Minister for Communications, Marine and Natural Resources e a. e Karntner Landesregierung e a., su domande di pronuncia pregiudiziale proposte dalla High Court irlandese e dalla Verfassungsgerichtshof austriaca; la seconda, cause riunite C-203/15 e C698/15, del 21 dicembre 2016, Tele2 Sverige AB contro Post-och telestyrelsen e Secretary of State for the Home Department contro Tom Watson e a., su domande di pronuncia pregiudiziale proposte dal Kammarratten i Stockholm svedese e dalla Court of Appeal britannica.
La sentenza del 8 aprile 2014 si è occupata della legittimità della direttiva 2006/24/CE sul presupposto che già solo la previsione di un obbligo, in capo al provider, di conservare i dati, perché della possibilità di accesso agli stessi da parte delle autorità nazionali, rappresentano un'interferenza nei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta, al rispetto della vita privata e familiare. Imprescindibile, quindi, il passaggio attraverso l'art. 52, par. 1, della Carta, ai sensi del quale eventuali limitazioni all'esercizio dei diritti e delle libertà da essa riconosciuti devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà; in altri termini, resistere al vaglio di proporzionalità e di stretta necessità con riguardo a finalità di interesse generale.
La Corte di Giustizia ha ritenuto che – nonostante l'oggettivo e meritevole interesse di "lotta alla criminalità grave", essenziale alla sicurezza pubblica e reso, certamente, efficace dal largo uso di moderne tecnologie – la direttiva non rispetta i canoni di proporzionalità nella

parte in cui non pone regole chiare e precise sull'applicazione della data retention, affidata ad un regime generalizzato ed indifferenziato, per utenti e mezzi di comunicazione.
Oggetto di censura, in particolare, è l'assenza nella direttiva, con conseguente assoluta libertà sul punto degli Stati membri, di limiti oggettivi, sostanziali o procedurali, all'accesso e al successivo utilizzo dei dati da parte delle competenti autorità nazionali: per un verso, è generico il riferimento a "gravi reati, quali definiti da ciascuno Stato membro nella propria legislazione nazionale"; per altro verso, affinchè proporzionalità e stretta necessità possano essere effettivamente assicurate, si sarebbe dovuto imporre agli Stati membri di subordinare l'accesso al previo esame di un giudice o di un'autorità amministrativa indipendente.
La Corte di Giustizia ha invalidato la direttiva 2006/24/CE per non aver prescritto standard minimi di garanzia legittimanti un obbligo di conservazione di dati finalizzato alla prevenzione e repressione di reati.
Con la sentenza del 21 dicembre 2016 C.d. Tele2 la Corte di Giustizia ha risposto al quesito se, dall'individuazione giurisprudenziale di tali standard, possa o meno dedursi l'imperatività degli stessi all'interno delle legislazioni nazionali, tenute comunque al rispetto dell'art. 15, par. 1, della direttiva 2002/58/CE, come modificata dalla direttiva 2009/136/CE. La Corte di Giustizia ha fornito risposta affermativa, mediante un'interpretazione dell'art. 15, par. 1, collegata agli artt. 7, 8, 11 e 52 della Carta dei diritti fondamentali dell'Unione Europea: l'art. 15, par. 1 osta da una parte "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 (...)"; dall'altra "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 alla 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".
3.5. Quanto all'impatto nel sistema normativo italiano dei principi enunciati con le sentenze della Corte di Giustizia, la Corte di Cassazione ha affermato che tali sentenze hanno riguardato Stati privi di una regolamentazione dell'accesso e della conservazione dei dati, mentre lo Stato italiano si è dotato di una specifica disciplina.
Il D.Lgs. n. 196 del 2003, art. 132, attuativo della direttiva 2002/58/CE, prescrive che i dati di traffico telefonico e telematico siano conservati dai fornitori dei relativi servizi, per finalità di accertamento e di repressione dei reati, entro scadenze predeterminate e diversificate; il pubblico ministero può acquisirli presso il fornitore con decreto motivato, d'ufficio o su istanza.
Nella disciplina italiana pertanto si rinvengono l'enunciazione della finalità di repressione dei reati; la delimitazione temporale dell'attività di memorizzazione; l'intervento preventivo dell'autorità giudiziaria, funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati, perché al rispetto del principio di proporzionalità in concreto.
...Omissis...
P.Q.M.
Annulla la sentenza impugnata senza rinvio nei confronti di B.A. per non aver commesso il fatto e con rinvio ad altra sezione della Corte di appello di Bologna nei confronti di D.G. quanto alla ravvisabilità dell'ipotesi di cui al D.P.R. n. 309 del 1990, art. 73, comma 5 in ordine al reato residuo sub 1).
Così deciso in Roma, il 19 aprile 2019.
Depositato in Cancelleria il 23 agosto 2019

IL COMMENTO

di Luca Lupária

Sommario: 1. Una premessa. – 2. La *data retention* tra Carta di Nizza, direttiva Frattini e Corte di giustizia. – 3. La cristallizzazione di una lettura restrittiva degli standard europei. – 4. Contro un approccio semplicistico rispetto ad un tema complesso e colmo di nodi irrisolti.

La giurisprudenza continua a fornire letture restrittive degli standard garantistici enunciati dalla Corte di Giustizia dell'Unione in materia di data retention. L'intento è quello di "salvare" la disciplina interna sulla conservazione dei dati ed evitare ipotesi di inutilizzabilità probatoria. Lo scritto propugna un forte cambio di passo e un maggior rispetto del quadro sovranazionale, enucleando i vari nodi problematici e le possibili soluzioni.

Italian Courts keep providing restrictive interpretations of the guaranteeing standards stated by the European Court of Justice on data retention. The aim is to "save" the national regulation, avoiding cases in which data cannot be used as evidences. The paper advocates for a strong step change and a stronger compliance with the supranational framework, by identifying the problematic issues and the possible solutions.

1. Una premessa

Ci siamo in qualche modo assuefatti all'atteggiamento di "resistenza" che legislatore e parte della magistratura mostrano nei confronti delle novità normative o giurisprudenziali provenienti dall'Unione europea in materia di garanzie della persona nel processo penale. Una forma di negativa resilienza testimoniata, ad esempio, dagli approcci riduttivi nella attuazione delle Direttive approvate dall'UE (1) o dagli orientamenti ermeneutici di chiusura rispetto alla pienezza dei diritti invocata dal quadro sovranazionale.

La sentenza in commento fornisce una precisa riprova di quanto tale *mood* restrittivo persista anche con riguardo alla tormentata tematica della *data retention*, ossia della conservazione - teleologicamente finalizzata alla repressione della criminalità - dei "dati esterni" delle conversazioni (numero di chiamante o di chiamato, ora della conversazione, durata, celle telefoniche agganciate, ecc.).

La disciplina è stata al centro, negli ultimi anni, di una complessa "parabola" eurounitaria (2), idonea a produrre un significativo impatto anche sul nostro ordinamento, che sembra opportuno ricostruire al fine di comprendere appieno la portata della pronuncia in epigrafe.

2. La *data retention* tra Carta di Nizza, direttiva Frattini e Corte di giustizia.

I diritti dell'individuo al rispetto della propria vita privata e alla tutela dei dati personali trovano nell'ambito dell'Unione europea un sistema di protezione particolarmente maturo e articolato.

Come noto, tali garanzie sono proclamate, in modo espresso e autonomo, agli artt. 7 e 8 della Carta di Nizza. Quest'ultima, compiendo un passo avanti rispetto alla CEDU (3), chiarisce testualmente che i singoli sono titolari, sia del classico diritto a non subire interferenze nella propria sfera – legato all'elaborazione originaria del *right to be let alone* (4) –, sia di una libertà positiva a esercitare un controllo penetrante sul flusso dei propri dati, ovvero sulle informazioni che identificano o rendono individuabile una persona e che possono fornire notizie su caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica e così via (5). I principi della Carta di Nizza, insomma, disegnano un solido scudo posto al vertice delle fonti del diritto europeo che protegge la "*privacy*" dei singoli da ingerenze indebite tanto dell'autorità quanto dei privati.

Occorre tuttavia ribadire fin da subito che le garanzie in questione, nonostante il loro rango primario, non sono da considerarsi assolute: possono all'evidenza essere compresse, purché ciò avvenga entro i limiti di quanto stabilito dall'art. 52 della Carta di Nizza. Eventuali restrizioni all'esercizio dei diritti di cui agli artt. 7 e 8 CDFUE devono, pertanto, essere previste dalla legge, rispettare il "contenuto essenziale" di dette garanzie, essere proporzionate e rispondere a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere diritti e libertà altrui.

Orbene, tra i vari istituti del processo penale, idonei a interferire con i diritti fondamentali alla vita privata e al *right to the protection of personal data,* vi è proprio la *data retention*. La conservazione dei dati di traffico telefonico e telematico appare in effetti in grado di rivelare plurime notizie sulla persona, consentendo persino di tracciarne un profilo del carattere o di mapparne gli spostamenti. Ben si comprende allora come lo strumento investigativo *de quo*, pur perseguendo lo scopo certamente degno di tutela di contrastare gravi forme di reato, per risultare legittimo, debba, dal punto di vista del diritto dell'Unione, rispettare lo *standard* di tutela cristallizzato nella Carta di Nizza.

Per la verità, è stato lo stesso legislatore eurounitario a sottovalutare, almeno in un primo periodo, l'importanza di un'adeguata ponderazione tra interesse generale alla sicurezza e alla lotta contro la criminalità e tutela della *privacy*. A tal proposito, è notorio che il Parlamento europeo e il Consiglio UE adottarono nel 2006 la direttiva n. 24 (riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di

(1) Un cenno sul punto in Caianiello, *Dal terzo pilastro ai nuovi strumenti: diritti fondamentali, "road map" e l'impatto delle nuove direttive*, in *Dir. pen. cont. – Riv. trim*, 2015/4, 78.

(2) Per una ricostruzione della materia, v., *ex plurimis*, Andolina, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018; Flor, Data retention *ed art. 132 Cod.* privacy: vexata quaestio (?), in *Dir. pen. cont.*, 29 marzo 2017; Iovene, Data retention *tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 2014, 4274 ss.; Marcolini, *L'istituto della* data rention *dopo la sentenza della Corte di giustizia del 2014*, in *Cybercrime*, diretto da Cadoppi - Canestrari - Manna - Papa, Torino, 2019, 1579 ss.; Pascali, *La* data retention *dopo la dichiarazione di invalidità della Direttiva 2006/24/CE*, in *Riv. elettronica dir. econ. Manegement*, 2015, 3, 87 ss.; Riccardi, *Dati esteriori delle comunicazioni e tabulati di traffico – il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Dir. pen. cont. – Riv. trim.*, 2016/3, 157 ss.; Ruggeri, Data retention *e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen.*, 2017, 2483 ss.

(3) È noto, del resto, che nel sistema CEDU, il diritto alla protezione dei dati personali, pur essendo stato in plurime pronunce valorizzato dalla Corte di Strasburgo nell'alveo dell'art. 8 CEDU, non trova un riconoscimento espresso: Pollicino - Bassini, *Commento all'art. 8 della Carta di Nizza*, in *Carta dei diritti fondamentali dell'Unione europea*, a cura di Mastroianni – Pollicino – Allegrezza. Pappalardo – Razzolini, Milano, 2017, 136 s.

(4) Il rinvio va ovviemente a Warren - Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, 193 ss.

(5) Per più ampie riflessioni, volendo, L. Lupária, *Privacy, diritti della persona e processo penale*, in *Riv. dir. proc.*, 2019, in corso di pubblicazione.

reti pubbliche di comunicazione e che modificava la direttiva 2002/58/CE), la quale – anche in ragione del clima politico in cui la stessa fu approvata – risultava assai sbilanciata in favore delle esigenze di tutela della collettività rispetto a quelle di protezione della riservatezza dei singoli (6).

Una prima reazione a tale approccio securitario del legislatore UE è stata offerta da alcune Corti costituzionali interne: i Giudici delle leggi bulgaro, tedesco e rumeno censurarono gli atti di recepimento di quella che nella *vulgata* è ricordata come direttiva Frattini (7).

Nel 2014 è intervenuta poi direttamente la Corte di giustizia UE, la quale, con la storica sentenza pronunciata nelle cause riunite *Digital Rights Ireland LTD* e *Kärntner Landesregierung (8)*, ha dichiarato l'invalidità dell'intera direttiva 2006/24/UE, per contrarietà con gli artt. 7, 8 e 52, par. 1 della Carta di Nizza. I giudici di Lussemburgo hanno compiuto un ragionamento assai «lineare e convincente» (9), la cui chiave di volta va individuata nella valutazione circa il mancato rispetto del principio di proporzionalità, declinato, in questo caso, come canone di minima interferenza dello Stato nella sfera di riservatezza del singolo.

Più precisamente, la Corte di giustizia, dopo aver riconosciuto che la direttiva Frattini non violava il contenuto essenziale degli artt. 7 e 8 della Carta e che l'istituto della *data retention* persegue un obiettivo effettivamente di interesse generale dell'Unione (ossia quello di combattere gravi forme di criminalità), ha compiuto un controllo approfondito circa il fatto che le norme UE determinassero o meno restrizioni alla tutela del rispetto della vita privata e dei dati personali limitate allo «stretto necessario» (10).

Ebbene, il quesito ha avuto una risposta marcatamente negativa per plurime ragioni. In prima battuta, le misure previste dalla direttiva riguardavano potenzialmente la totalità della popolazione europea «e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi» (11). In secondo luogo, il provvedimento non contemplava alcun criterio oggettivo che permettesse «di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che po[ssano] [...] essere considerati sufficientemente gravi da giustificare siffatta ingerenza» (12). In terzo luogo, risultava criticabile la scelta della fonte UE di non subordinare l'accesso ai dati conservati «ad un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente la cui decisione sia diretta a limitare l'accesso ai dati e il loro uso a quanto strettamente necessario per raggiungere l'obiettivo perseguito e intervenga a seguito di una richiesta motivata delle suddette autorità presentata nell'ambito di procedure di prevenzione, di accertamento o di indagini penali» (13).

Da ultimo, quanto alla durata di conservazione dei dati, si è osteggiata, per un verso, la fissazione di un termine minimo di sei mesi senza che fosse effettuata «alcuna distinzione tra le categorie di dati previste all'articolo 5 della direttiva a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate» e, per un altro verso, la mancata previsione da parte della fonte UE di criteri oggettivi, idonei a garantire che l'interferenza nella sfera del singolo fosse limitata allo stretto necessario.

Una lettura garantista questa, poi sviluppata nella giurisprudenza successiva della Corte. A tal proposito, assume un rilievo peculiare la sentenza *Tele 2 Sverige AB* (14), nella quale i giudici del Lussemburgo hanno stabilito che la direttiva 2002/58/CE (ossia l'atto europeo diventato applicabile alla *data retention* dopo la caducazione della direttiva Frattini), letta alla luce degli articoli 7, 8, 11 e 52, par. 1, della Carta di Nizza, va interpretata nel senso che essa 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'ubi-

(6) In proposito, v. *amplius*, Andolina, *L'acquisizione nel processo penale*, cit., 58 ss.

(7) Cfr., a riguardo, ancora Andolina, *L'acquisizione nel processo penale*, cit., 59.

(8) Il rinvio va a Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, per un commento della quale cfr. Colombo, "Data retention" *e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.*, 2014, 2705 ss.; Flor, *La Corte di Giustizia considera la direttiva europea 2006/34 sulla cd.* "data retention" *contraria ai diritti fondamentali. Una lunga storia e lieto fine*, in *Dir. pen. cont. – Riv. trim.*, 2014/2, 178 ss.

(9) Così, Marcolini, *L'istituto della* data rention, cit., 1587.

(10) Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland* § 52.

(11) Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland* § 57.

(12) Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland* § 60.

(13) Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland* § 62.

(14) Il rinvio va a Corte giust., Grande Sezione, 21 dicembre 2016, cause rinute C-203/15 e C-698/15, *Tele2 Sverige AB*, per un commento della quale, v. Pollicino – Bassini, *La Corte di giustizia e una trama oramai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. pen. cont.*, 9 gennaio 2017.

cazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica» (15).
La Corte ha anche affermato che il diritto UE osta pure «a 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» (16).
In estrema sintesi, come si è condivisibilmente affermato, la seconda decisione ha segnato un ulteriore significativo *step* in avanti: nella sentenza *Tele 2 Sverige* la Corte non si è limitata a censurare l'operato del legislatore eurounitario in materia di conservazione dei dati finalizzata alla repressione dei reati, ma ha chiaramente scolpito una serie di condizioni che pure gli ordinamenti nazionali devono oggi osservare per porsi in linea con «i principi enunciati dalla CDFUE e, prima ancora, dalla stessa CEDU» (17).
Alla luce di tale parabola evolutiva, non si può fare a meno di osservare come la proclamazione di uno *standard* tanto elevato di protezione del diritto alla *privacy* nelle pronunce *Digital Rights* e *Tele 2 Sverige AB* non sia stata – a oggi – sufficientemente valorizzata tanto da molti legislatori interni (18), quanto da quello europeo. Se, infatti, i primi hanno, in non pochi casi, omesso di adeguare la loro disciplina normativa in materia, il secondo, nonostante abbia intrapreso un articolato percorso consultivo preparatorio, è ancora ben lontano da pervenire a un nuovo atto *ad hoc*, volto a sostituire l'oramai invalida direttiva 2006/24/CE.
Pochi mesi fa il Consiglio UE ha tuttavia mostrato di collocare la *data retention* tra le proprie priorità politiche, adottando delle articolate Conclusioni «sulla conservazione dei dati per finalità di lotta contro la criminalità» (19). Con tale documento si è non solo ribadito che «le sentenze della Corte di giustizia dell'Unione europea [...] nelle cause *Digital Rights Ireland* e *Tele 2*, [...] rivestono un'importanza fondamentale» (20), ma si è invitata la Commissione europea – tra l'altro – a predisporre «uno studio approfondito [...] sulle possibili soluzioni per conservare i dati, compresa la valutazione di una futura iniziativa legislativa» (21).
Per contro, si può riscontrare una maggiore sensibilità verso gli stimoli lanciati dai giudici di Lussemburgo da parte di alcune supreme giurisdizioni europee: diverse Corti hanno, anche assai di recente, presentato nuove domande di rinvio pregiudiziale, idonee a determinare un ulteriore sviluppo pretorio della tematica della *data retention* (22).
Non stupisce che uno *step* successivo sia, ad esempio, già stato fissato dalla Grande Sezione della Corte di giustizia con la recente sentenza *Ministerio Fiscal* (23): come noto, in tale arresto i giudici hanno parzialmente riformulato uno dei criteri fissati nei loro precedenti, e, più in particolare, quello della "gravità dei reati". Se, infatti, dalle sentenze *Digital Rights* e *Tele 2* pareva desumersi che la *data retention* potesse essere ammessa solo per soglie di criminalità qualificate come "gravi", nel nuovo arresto tale conclusione è stata apertamente smentita. A detta della Corte, infatti, la conservazione dei dati esterni di una comunicazione telefonica e telematica è possibile anche per reati "comuni", a patto che, però, in tal caso l'autorità utilizzi le informazioni nei confronti dei singoli solo per compiere ingerenze non "gravi" nella sfera di riservatezza del singolo, quali, ad esempio, la mera richiesta di accedere ai numeri di telefono corrispondenti a una carta SIM di un cellulare e ai dati relativi all'identità civile di un titolare di detta carta. A tal proposito, se è pur vero che la distinzione di "grado" così inaugurata dalla Corte tra intrusioni nella *privacy* pare aver complicato ancor di più una materia già assai tormentata, merita comunque segnalare che da alcuni passaggi della pronuncia in questione si ricava che i giudici europei continuano a ricomprendere tra le limitazioni "gravi" della riservatezza di un individuo ogni utilizzo di dati esterni alle comunicazioni che consenta di produrre conclusioni precise sulla sua vita privata, tra

(15) Corte giust., Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*, conclusione n. 1.

(16) Corte giust., Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*, conclusione n. 2.

(17) Così, testualmente, Marcolini, *L'istituto della* data rention, cit., 1589.

(18) Cfr. in proposito, EDRi, *EU Member States willing to retain illegal data retention*, in <https://edri.org/eu-member-states-willing-to-retain-illegal-data-retention/, 16 gennaio 2019>.

(19) Cfr. Doc. Consiglio UE, 9663/19 del 27 maggio 2019.

(20) Doc. Consiglio UE, 9663/19, 2.

(21) Doc. Consiglio UE, 9663/19, 6.

(22) Per un elenco dei rinvii pregiudiziali in materia, sollevati, dall'*Investigatory Powers Tribunal* del Regno Unito, dalla Corte costituzionale del Belgio, dal Consiglio di stato francese e dalla Corte suprema estone, cfr. Doc. Consiglio UE, 9663/19, 4.

(23) Cfr. Corte giust., Grande Sezione, 2 ottobre 2018, C-207/16, *Ministerio Fiscal*, sulla quale v. IT.Pol – Edri, *CJEU introduces new criteria for law enforcement to access to data*, in <https://edri.org/cjeu-introduces-new-criteria-for-law-enforcement-to-access-to-data/, 24 ottobre 2018>.

cui, ad esempio, le richieste volte a stabilire l'ubicazione di un telefono cellulare (24).
A ogni modo, al di là di quanto la sentenza *Ministerio Fiscal* abbia acuito la complessità della materia in esame un dato è certo: la stessa fornisce la definitiva riprova di come la *data retention* rappresenti un istituto davvero magmatico e in perenne evoluzione, il quale abbisogna di un urgente intervento normativo da parte del legislatore UE. In ossequio alla riserva di legge di cui al combinato disposto degli artt. 7, 8 e 52 della CDFUE spetta al Parlamento e al Consiglio UE (e non all'attività suppletiva della giurisprudenza) il compito di fissare quel delicato bilanciamento tra esigenze di sicurezza della collettività e di protezione dei diritti fondamentali dei singoli, che inevitabilmente sta alla base del meccanismo *de quo*.

3. La cristallizzazione di una lettura restrittiva degli standard europei.

Una volta ricostruito il contesto europeo di riferimento, è ora possibile soffermarsi sulla pronuncia in epigrafe, la quale – è bene chiarirlo fin da subito – non si presenta come isolata, ma si inserisce in un quadro pretorio ben definito.
Se è vero, infatti, che, dopo le sentenze *Digital Rights* e *Tele 2*, nella dottrina italiana si è denunciata a più voci la radicale incompatibilità dell'art. 132 del d.lgs. 30 giugno 2003, n. 196 (cd. codice della *privacy*), ossia della principale previsione interna in tema di *data retention*, con gli *standard* garantisti proclamati dalla Corte di giustizia (25), la giurisprudenza non è stata dello stesso avviso.
I giudici interni – tanto di merito (26), quanto di legittimità (27) – hanno compiuto una valutazione di piena compatibilità della disciplina del codice della *privacy*, concernente la conservazione dei dati esterni delle comunicazioni, con il diritto UE, rifiutandosi persino di investire a loro volta la Corte di giustizia di nuove domande pregiudiziali, così come richiesto da vari difensori.
La decisione in commento ha definitivamente ribadito questo atteggiamento "rassicurante" della giurisprudenza italiana. Nel caso di specie, il legale di un prevenuto, condannato dalla Corte di appello di Bologna per la cessione di un certo quantitativo di stupefacente, censurava in cassazione non solo il fatto che i giudici di merito avessero condannato il suo assistito pur essendovi a suo carico un solo indizio, rappresentato dall'aggancio, in una determinata ora, di un telefono cellulare a lui riconducibile alla cella della zona in cui sarebbe stata ceduta la droga, ma anche del contrasto tra l'art. 132 del codice della *privacy* con gli artt. 7, 8 e 52, par. 1, della CDFUE, come interpretati dalla Corte di giustizia nelle sentenze *Digital Rights* e *Tele 2*.
Più in particolare, a detta della difesa, la normativa interna concernente la *data retention* non avrebbe superato il vaglio stringente di proporzionalità fissato dai giudici europei, sia perché l'art. 132 del cod. *privacy* consente l'acquisizione e la conservazione del traffico telematico per qualsiasi tipo di reato, senza distinguere tra forme di criminalità più o meno gravi, sia perché la stessa affida al pubblico ministero e non a un giudice o a un'altra autorità indipendente il compito di autorizzare l'acquisizione dei dati. Insomma, esattamente come era stato già denunciato a più voci in dottrina, l'art. 132 del cod. *privacy* conterrebbe in sé «tutti i vizi già individuati dalla Corte di giustizia, con conseguente necessità di disapplicare la norma interna e di ritenere la prova acquisita vietata dalla legge e quindi non utilizzabile». Va, peraltro, rilevato che, in subordine, la difesa ha, anche in questo caso, richiesto alla Corte di legittimità di presentare un rinvio pregiudiziale circa l'effettiva compatibilità con la Carta di Nizza delle previsioni nazionali.
Ebbene, la Cassazione, pur accogliendo il primo motivo, sulla base del rilievo, in realtà abbastanza pacifico alla luce della teoria generale del diritto probatorio, per cui «la presenza di un telefono cellulare in una data zona [...] può essere qualificato quale indizio, ma di per sé non dimostra nulla, anche se l'utenza è precisamente attribuita ad una determinata persona», essendo necessario per condannare un soggetto che vi siano «altri indizi, ugualmente gravi e precisi, ed infine tutti concordanti, che possano consentire di affermare che il possessore dell'utenza ha commesso il reato», ha, invece, rigettato *in toto* le censure "europee" del ricorrente, senza percorrere neppure la strada del rinvio pregiudiziale.
Per giungere a tale conclusione, il collegio si è limitato a riprendere e ribadire i principali temi che avevano già portato in precedenza la Corte ad affermare che il più volte citato art. 132 del cod. *privacy* «è compatibile con il diritto sovranazionale in tema di tutela della *privacy* (direttive 2002/58/CE e 2006/24/CE), come interpretate dalla Corte di Giustizia dell'Unione europea» (28).

(24) Corte giust., Grande Sezione, 2 ottobre 2018, C-207/16, *Ministerio Fiscal*, § 59.

(25) Tra i tanti, v. Andolina, *L'acquisizione nel processo penale*, cit., 97 ss.; Flor, Data retention *ed art. 132 Cod.* privacy, cit., Marcolini, *L'istituto della* data rention, cit., 1590 ss.

(26) Cfr. Trib. Padova, ord. 15 marzo 2017, Pres. Marassi, in *Dir. pen. cont.*, 29 marzo 2017, con nota critica di Flor, Data retention *ed art. 132 Cod.* privacy, cit.

(27) Cfr. Cass., sez. V, 24 aprile 2018, n. 33851, in *Cass. pen.*, 2019, 299.

(28) Il rinvio va proprio a Cass., sez. V, 24 aprile 2018, n. 33851, cit., 299.

Due i principali argomenti su cui ha fatto leva il giudice nomofilattico per rigettare le censure della difesa. In una prima prospettiva, il collegio ha affermato che il diritto interno non contrasterebbe con le sentenze *Digital Rights* e *Tele 2*, posto che quest'ultime avrebbero «riguardato Stati privi di una regolamentazione dell'accesso e della conservazione dei dati, mentre lo Stato italiano si è dotato di una specifica disciplina». In un secondo angolo visuale, la Corte ha affermato che, in ogni caso, la normativa italiana supererebbe comunque il test europeo di proporzionalità, posto che la stessa non solo delimita temporalmente l'attività di memorizzazione in modo adeguato, ma soprattutto affida il potere di acquisire i dati a un organo – ossia il pubblico ministero – che in realtà sarebbe dotato di un'indipendenza funzionale sufficiente ad assicurare il rispetto dello *standard* eurounitario di tutela del diritto alla *privacy*. A tal proposito, il collegio ha ribadito che la versione italiana delle sentenze *Digital Rights* e *Tele 2* – ove, come si è visto, si fa un riferimento testuale alla necessità di un'autorizzazione «di un giudice o di un'autorità amministrativa indipendente», affinché i dati esterni possano essere comunicati dal *service provider* alle autorità di *law enforcement* - sarebbe affetta da un "errore linguistico". A detta dei supremi giudici, infatti, la traduzione non sarebbe fedele al testo francese e inglese della sentenza della Corte di giustizia, i quali utilizzano – rispettivamente – la locuzione "*juridiction*" e "*court*", riferibili alla magistratura nel suo complesso e dunque anche ai pubblici ministeri. In definitiva, dunque, per la Cassazione italiana la Corte di giustizia nelle sue pronunce avrebbe inteso fare riferimento al concetto generico di "autorità giudiziaria", che pacificamente ricomprende anche la figura della pubblica accusa, con la conseguenza che nessuna critica si potrebbe muovere alla vigente versione dell'art. 132 del cod. *privacy*.

A tali considerazioni generali, il collegio ne ha aggiunta anche una più specifica: secondo la suprema Corte il fatto che ad autorizzare la trasmissione e l'utilizzo del dato sia il solo pubblico ministero garantirebbe comunque un livello adeguato di tutela, posto che la trasmissione di un dato esterno di una comunicazione determinerebbe una compromissione del diritto alla *privacy* decisamente inferiore rispetto alle intercettazioni la cui tutela è affidata, invece, al controllo di un giudice.

4. Contro un approccio semplicistico rispetto ad un tema complesso e colmo di nodi irrisolti.

La pronuncia in esame, così come l'orientamento consolidatosi nelle aule di giustizia italiane in tema di compatibilità con le fonti europee dell'art. 132 del cod. *privacy*, non pare affatto giungere a risultati condivisibili e, soprattutto, mostra la scarsa volontà di prendere "sul serio" la questione.

Privo di pregio risulta anzitutto l'argomento preliminare su cui si fonda la decisione, ossia quello secondo cui le sentenze della Corte di giustizia avrebbero riguardato Stati che, a differenza dell'Italia, risulterebbero sprovvisti di una regolamentazione in punto di accesso e conservazione dei dati. Tale rilievo non solo non risponde alla realtà (29), ma, soprattutto, denota un profondo (e, in qualche misura, preoccupante) vizio metodologico. Le sentenze *Digital Rights*, *Tele 2* e *Ministerio Fiscal* hanno infatti chiarito quali requisiti debba possedere non soltanto la disciplina europea ma altresì quella nazionale per poter rientrare nel perimetro garantistico cristallizzato dalla Carta di Nizza in materia di *data retention*. Anche se le pronunce europee avessero, in ipotesi, riguardato Paesi privi di disciplina, il ragionamento non dovrebbe allora mutare: i giudici di Lussemburgo non si sono limitati a compiere ragionamenti specifici, legati alla normativa di un singolo ordinamento giuridico, ma hanno stabilito una serie di principi di diritto universalmente validi per l'intero spazio di libertà, sicurezza e giustizia.

Neppure la seconda ragione su cui ruota la motivazione può essere accolta senza riserve: il presunto errore del traduttore italiano delle sentenze *Tele 2* e *Digital Rights* nell'impiegare il vocabolo "giudice", in luogo di quello, stimato più corretto, di "autorità giudiziaria". A ben vedere, infatti, tale interpretazione suscita più di una perplessità tenuto conto di quello che, pur in altri contesti, è il lessico utilizzato nell'ambito del diritto dell'Unione europea. Sono infatti riscontrabili precisi esempi (si pensi solo all'art. 6 della decisione quadro 2002/584/GAI in tema di MAE) di come, allorquando il legislatore UE abbia voluto riferirsi al concetto di "autorità giudiziaria" in lingua inglese e francese non abbia utilizzato affatto i vocaboli "*court*" e "*juridicion*", ma le locuzioni ben più ampie "*judicial authority*" o "*autorité judiciaire*". Orbene, pare francamente arduo ritenere che la Corte di giustizia, in quanto supremo giudice del diritto UE, non abbia tenuto conto di quello che è il lessico proprio utilizzato dal legislatore eurounitario, allorquando sono state redatte le sentenze in questione.

Per di più, a diminuire la persuasività della tesi sostenuta dalla Cassazione sta il fatto che la sentenza *Tele 2*, nel momento in cui ha sottolineato la necessità di un controllo preventivo di una "*court*" sull'interferenza nella sfera privata del singolo, ha richiamato quanto stabilito nella sentenza della Corte europea dei diritti dell'uomo

(29) Si veda, in proposito, solo per fare un esempio, i § 15 e ss. della sentenza Corte giust., Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*, in cui è descritta la disciplina svedese e poi del Regno Unito in tema di *data retention*.

Szabó e Vissy c. Ungheria (30). Orbene, in tale pronuncia i giudici di Strasburgo, pur considerando possibile che anche autorità (indipendenti) diverse da un decisore possano compiere, in alcuni casi, limitazioni del diritto alla riservatezza dell'individuo, hanno affermato che «*judicial control offering the best guarantees of independence, impartiality and a proper procedure*» (31), manifestando oltretutto, a nostro avviso, un espresso *favor* circa il fatto che, di norma, le restrizioni nella *privacy* del singolo debbano essere autorizzate da un *judge* (32). Anche alla luce di ciò, pare insomma difficile ritenere che con la locuzione "*court*" i giudici di Lussemburgo abbiano voluto in generale riferirsi pure alla figura dei pubblici ministeri.
Certo, dove la pronuncia in epigrafe pare cogliere nel segno è nel rilevare che la garanzia primaria che la Corte di giustizia ha voluto preservare, richiedendo l'autorizzazione di una "*court*", è quella dell'indipendenza dai governi dell'organo deputato a consentire l'ingerenza nei diritti fondamentali del singolo, così da evitare un controllo orwelliano di massa degli esecutivi sugli individui. Tenuto conto di ciò, si potrebbe pensare che i pubblici ministeri italiani, a differenza di quelli di altri Paesi (come Francia, Spagna e Germania) ben potrebbero istituzionalmente considerarsi soggetti che, proprio perché non gerarchicamente subordinati al ministro, siano in grado di preservare adeguatamente i diritti della persona. Se ciò è vero, non si può peraltro affermare con certezza che la Corte di giustizia nelle sue pronunce abbia voluto preservare solo il valore dell'indipendenza e non anche quello della terzietà e imparzialità: l'utilizzo del termine "*court*" in luogo di "*judicial authority*" potrebbe, invero, proprio spiegarsi con la finalità di individuare un soggetto equidistante dalla regiudicanda che possa dunque trovarsi nella condizione idonea per salvaguardare a sufficienza i diritti dei singoli di cui agli artt. 7 e 8 della Carta di Nizza.
Né per dare una risposta univoca a tale quesito pare sufficiente l'ulteriore argomento, abbozzato dalla pronuncia in commento, per cui l'autorizzazione a trasmettere il contenuto di "dati esterni" a una comunicazione tollererebbe un livello di garanzie inferiori rispetto alle intercettazioni, comportando sempre un'intrusione meno intensa nella riservatezza del singolo. Siffatto assunto non sembra, invero, *in toto* convincente, in particolare in ragione del fatto che i giudici di Lussemburgo nelle loro pronunce hanno espressamente fatto rientrare alcune possibili ingerenze nella *privacy* del singolo tramite l'istituto della *data retention* tra le restrizioni "gravi" dei diritti dell'individuo. Ed è proprio in ragione di tale valutazione sulla potenziale profonda lesività della *data retention* sulla sfera dell'individuo che è stato ipotizzato uno standard di garanzia così elevato. Diverso discorso si potrebbe forse effettuare in relazione a quelle intrusioni della *privacy* qualificate dalla Corte di giustizia come lievi (quale la mera attribuzione della paternità di una SIM a un soggetto): quest'ultime, data la loro minore "aggressività" nei confronti dell'individuo, potrebbero forse essere legittimamente autorizzate anche da un soggetto sì indipendente, ma non terzo e imparziale quale la pubblica accusa italiana.
In definitiva, in un quadro caratterizzato più da dubbi che certezze, la strada maestra che si sarebbe dovuta seguire, a fronte della denunciata incompatibilità dell'art. 132 del cod. *privacy* con il diritto UE, era quella, sollecitata, del rinvio pregiudiziale. A ben vedere, infatti, tenuto conto in particolare di come la suprema Corte nostrana rappresenti l'organo di ultima istanza, istituzionalmente deputato a chiamare in causa i giudici di Lussemburgo, pare che gli ermellini avrebbero dovuto effettivamente domandare se anche un organo formalmente indipendente quale il pubblico ministero italiano, ma non terzo e imparziale, possa soddisfare lo *standard* di garanzie richiesto dalla Carta di Nizza.
Per di più, tale occasione sarebbe stata propizia anche per interrogare la Corte di giustizia, mediante un ulteriore quesito subordinato, circa le sorti sul piano probatorio di un dato esterno a una comunicazione acquisito in violazione del diritto UE sulla *privacy*. A tal proposito, va, infatti, ricordato che, anche da siffatto punto di vista, la suprema Corte nostrana ha adottato un approccio restrittivo, non accogliendo i suggerimenti di quella parte della dottrina che ha proposto di ricavare direttamente dagli artt. 7 e 8 della Carta di Nizza due divieti probatori "eurounitari" (33). Dal canto suo, infatti, la Cassazione (34) ha, invece, negato che il mancato rispetto delle norme europee stabilite nelle sentenze *Digital Rights* e *Tele 2* determini un'inutilizzabilità patologica. Si tratta all'evidenza di una soluzione del tutto insoddisfacente, posto che essa depotenzia alla radice la portata dei parametri di tutela imposti dagli artt. 7 e 8. Anche ove avessi una prova raccolta in palese violazione della CDFUE ciò non produrrebbe alcuna ripercussione sul piano probatorio. Proprio per questo motivo il caso deciso nella pronuncia in epigrafe avrebbe potuto risolvere l'*impasse* interrogando direttamente in proposito i giudici del Lussemburgo, così da chiarire se una discipli-

(30) Il rinvio va a Corte edu, 12 gennaio 2016, sez. IV, *Szabó e Vissy c. Ungheria*.

(31) Corte edu, 12 gennaio 2016, sez. IV, *Szabó e Vissy c. Ungheria*, § 77.

(32) V. ancora Corte edu, 12 gennaio 2016, sez. IV, *Szabó e Vissy c. Ungheria*, § 77.

(33) V., in particolare, Marcolini, *L'istituto della* data rention, cit., 1594.

(34) La tesi è argomentata in Cass., sez. V, 24 aprile 2018, n. 33851, cit., 299, ma non è stata ripresa nella pronuncia in commento.

na interna, che – stando a quanto affermato dalla giurisprudenza domestica – non consentirebbe di sanzionare la violazione dello *standard* di garanzie in tema di *data retention* fissato in *Digital Rights* e *Tele 2*, osti o meno con l'articolo 47 della Carta di Nizza, il quale richiede, in generale, che siano predisposti rimedi effettivi in caso siano violate le norme del diritto dell'Unione.

I difetti della pronuncia in commento non si fermano però qui. Non sfuggirà, infatti, come quest'ultima, esattamente come la decisione precedente alla quale è ispirata, non ha in alcun modo fornito risposta ad altre censure sollevate dalla difesa (e in dottrina) nei confronti dell'art. 132 del cod. *privacy*, tra cui spicca in particolare quella concernente la mancata individuazione da parte del legislatore UE di un limite edittale idoneo a consentire che interferenze penetranti nei confronti del diritto alla riservatezza dei singoli siano consentite unicamente per le fattispecie di reato più gravi.

Il vuoto motivazionale che affligge in proposito la decisione *de qua* non può che essere apertamente stigmatizzato: pare, invero, inaccettabile che i supremi giudici nomofilattici, vista la sostanziale impossibilità di salvare da siffatto punto di vista la legittimità delle previsioni interne, abbiano del tutto omesso di argomentare questo profilo. In definitiva, proprio tale lacuna argomentativa pare fornire la decisiva riprova di come la decisione in epigrafe abbia inteso preservare a tutti i costi la possibilità per l'autorità di *law enforcement* di avvalersi di un meccanismo oramai essenziale per la lotta contro la criminalità, quale la *data retention*. Così facendo, però, i giudici sono arrivati al risultato di far pagare ai soggetti deboli – ossia ai prevenuti – le lacune organizzative sistematiche dell'ordinamento interno e di quello europeo, dovute al fatto che tanto il legislatore italiano, quanto quello UE non sono stati finora politicamente in grado di adeguare la normativa in materia agli stringenti *standard* di tutela imposti dalla Carta di Nizza, così come interpretata dalla Corte di giustizia.

Per l'ennesima volta, dunque, nonostante la proclamazione di un livello astratto di tutela di diritti particolarmente elevato, le garanzie europee si stanno dimostrando prive di effettività, risultando meramente teoriche ed illusorie. Non si può allora che auspicare un futuro cambio di passo, *in primis*, da parte delle istituzioni UE istituzionalmente deputate a controllare il rispetto da parte degli Stati membri (e dei loro organi) del diritto eurounitario. Ci si riferisce, in particolare, alla Commissione europea, la quale vedendosi affidato il compito di "guardiano del diritto dell'Unione" non dovrebbe più indugiare e avviare formali procedure di infrazione, volte a obbligare gli Stati membri ad ottemperare ai loro obblighi europei in tema di *data retenion*. Solo in questo modo il *new deal* inaugurato dalla Corte di giustizia in materia di tutela del diritto alla *privacy* cesserà di assumere i contorni di una enorme occasione perduta.