LA NUOVA DISCIPLINA DEI TABULATI: IL COMMENTO "A CALDO" DEL PROF. FILIPPI

Leonardo Filippi

D.L. 30 settembre 2021, n. 132

IL DECRETO-LEGGE SUI TABULATI

Il decreto-legge.

Il Governo ha scelto la linea garantista. Dopo la sentenza di marzo della Corte di giustizia del Lussemburgo[1], che, seguendo analoghe pronunce precedenti, aveva affermato il contrasto rispetto al diritto dell'Unione europea della disciplina estone, che, come quella italiana, consentiva una conservazione generalizzata e indifferenziata dei dati relativi al traffico telefonico/informatico e dei dati relativi all'ubicazione, riservando al pubblico ministero il potere di acquisizione, era ormai indifferibile un intervento legislativo.

I principi espressi dalla Grande Camera.

La Grande Camera aveva precisato che l'art. 15 § 1 della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico telefonico/informatico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.

La Grande Camera aggiunse che lo stesso art. 15, § 1, deve essere interpretato nel senso che esso osta ad una normativa nazionale che renda il pubblico ministero competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale, dato che il compito del pubblico ministero è quello di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento[2].

La sentenza della Grande Camera del 2 marzo 2021 ribadì, peraltro, principi già perentoriamente affermati in passato in diverse sue pronunce. Infatti, la Grande Camera della Corte giust. U.E. affermò, anzitutto, il principio per cui l'obiettivo della prevenzione, della ricerca, dell'accertamento e del perseguimento dei reati è ammesso, conformemente al principio di proporzionalità, soltanto per la lotta contro "le forme gravi di criminalità e la prevenzione di gravi minacce alla sicurezza pubblica", le quali solamente sono idonee a

giustificare ingerenze gravi nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta, come quelle che comporta la conservazione dei dati relativi al traffico e all'ubicazione. Infatti, come già rilevato in passato, l'accesso a un insieme di dati relativi al traffico o all'ubicazione "può effettivamente consentire di trarre conclusioni precise, o addirittura molto precise, sulla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati". Pertanto, è vietata una conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione e "soltanto gli obiettivi della lotta contro le forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica sono atti a giustificare l'accesso delle autorità pubbliche ad un insieme di dati relativi al traffico o all'ubicazione, i quali sono suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali utilizzate da quest'ultimo e tali da permettere di "trarre precise conclusioni sulla vita privata delle persone interessate".

La Corte aggiunse che altri fattori attinenti alla proporzionalità di una domanda di accesso, come la durata del periodo per il quale viene richiesto l'accesso a tali dati, non possono avere come effetto quello di giustificare l'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale. Essa osservò che, indubbiamente, maggiore è la durata del periodo per il quale viene richiesto l'accesso o le categorie di dati richiesti, più grande è, in linea di principio, la quantità di dati che possono essere conservati dai fornitori di servizi di comunicazioni elettroniche, relativi alle comunicazioni elettroniche effettuate, ai luoghi di soggiorno frequentati, nonché agli spostamenti compiuti dall'utente di un mezzo di comunicazione elettronica, consentendo in tal modo di ricavare, a partire dai dati consultati, un maggior numero di conclusioni sulla vita privata di tale utente. Pertanto, il principio di proporzionalità, che consente le deroghe alla protezione dei dati personali e le limitazioni di quest'ultima, impone che tanto la categoria o le categorie di dati interessati, quanto la durata per la quale è richiesto l'accesso a questi ultimi, siano, in funzione delle circostanze del caso di specie, limitate a "quanto è strettamente necessario" ai fini dell'indagine in questione.

La Corte chiarì che l'autorizzazione all'accesso concessa dal giudice o dall'autorità indipendente competente deve intervenire necessariamente prima che i dati e le informazioni che ne derivano possano essere consultati. Pertanto, "la valutazione della gravità dell'ingerenza costituita dall'accesso si effettua necessariamente in funzione del rischio generalmente afferente alla categoria di dati richiesti per la vita privata delle persone interessate, senza che rilevi, peraltro, sapere se le informazioni relative alla vita privata che ne derivano abbiano o meno, concretamente, un carattere sensibile".

Come già affermato in passato, la Corte riconobbe che è vero che spetta al diritto nazionale stabilire le condizioni alle quali i fornitori di servizi di comunicazioni elettroniche devono accordare alle autorità

nazionali competenti l'accesso ai dati di cui essi dispongono. Tuttavia, per soddisfare il requisito di proporzionalità, tale normativa deve prevedere "regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissino dei requisiti minimi, di modo che le persone i cui dati personali vengono in discussione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abusi". Tale normativa deve inoltre essere "legalmente vincolante nell'ordinamento interno e precisare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di dati del genere, in modo da garantire che l'ingerenza sia limitata allo stretto necessario"[3].

In particolare, una normativa nazionale che disciplini l'accesso delle autorità competenti a dati conservati e relativi al traffico e all'ubicazione, adottata ai sensi dell'art. 15, § 1, della Direttiva 2002/58, non può limitarsi a esigere che l'accesso delle autorità ai dati risponda alla finalità perseguita da tale normativa, ma deve altresì prevedere "le condizioni sostanziali e procedurali che disciplinano tale utilizzo"[4].

Pertanto, poiché un accesso generalizzato a tutti i dati conservati, indipendentemente da un qualche collegamento, almeno indiretto, con la finalità perseguita, non può considerarsi "limitato allo stretto necessario", ogni normativa nazionale "deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati in questione".

La Corte precisò, inoltre, che "un accesso siffatto può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere".

Soltanto eccezionalmente, "in situazioni particolari, come quelle in cui interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica siano minacciati da attività di terrorismo, l'accesso ai dati di altre persone potrebbe essere parimenti concesso qualora sussistano elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo"[5].

Un altro cardinale principio, già affermato in passato dalla Corte[6], e poi ribadito dalla Grande Camera, nega al pubblico ministero la competenza, ai fini di un'indagine penale, ad autorizzare l'accesso di un'autorità pubblica sia ai dati di traffico, sia ai dati sulla posizione. Invero, la Grande Camera precisò che il controllo preventivo richiede, tra l'altro, che il giudice o l'entità incaricata di effettuare il controllo medesimo disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie per garantire un contemperamento dei diversi valori e diritti in gioco. Per quanto riguarda, più in particolare, un'indagine penale, "tale controllo preventivo

richiede che detto giudice o detta entità sia in grado di garantire un giusto equilibrio, da un lato, tra gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso"; qualora tale controllo venga effettuato non da un giudice bensì da un'entità amministrativa indipendente, quest'ultima deve godere di uno *status* che le permetta di agire nell'assolvimento dei propri compiti in modo obiettivo e imparziale, e deve a tale scopo essere al riparo da qualsiasi influenza esterna.

La Corte ribadì perciò che il requisito di indipendenza che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare impone che tale autorità abbia la "qualità di terzo rispetto a quella che chiede l'accesso ai dati", di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, "il requisito di indipendenza implica che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale". Tali caratteri non sono riscontrabili nel pubblico ministero che dirige il procedimento di indagine ed esercita, se del caso, l'azione penale, giacché "il pubblico ministero non ha il compito di dirimere in piena indipendenza una controversia, bensì quello di sottoporla, se del caso, al giudice competente, in quanto parte nel processo che esercita l'azione penale".

D'altra parte, la circostanza che il pubblico ministero sia tenuto, conformemente alle norme che disciplinano le sue competenze e il suo *status*, a verificare gli elementi a carico e quelli a discarico, a garantire la legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento "non può essere sufficiente per conferirgli lo *status* di terzo rispetto agli interessi in gioco", nel senso che non dispone di tutte le attribuzioni e non presenta tutte le garanzie necessarie per garantire una armonizzazione dei diversi valori e diritti contrapposti. Pertanto, la Corte concluse categoricamente che il pubblico ministero non è in grado di effettuare tale controllo preventivo sulla richiesta delle autorità nazionali competenti di accesso ai dati conservati.

Secondo la Corte, il pieno rispetto delle condizioni per l'accesso delle autorità nazionali competenti ai dati conservati può essere assicurato soltanto se sia subordinato ad "un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente".

La Grande Camera ritenne che il controllo indipendente debba essere, di regola, preventivo, cioè debba intervenire prima di qualsiasi accesso. Solo in via di eccezione, individuata in "situazioni di urgenza debitamente giustificate", il controllo può essere successivo all'accesso, ma "deve avvenire entro termini brevi" [7], tenendo presente che un controllo successivo è sempre inadeguato perché non consente di impedire un accesso ai dati in questione eccedente i limiti dello "stretto necessario".

La Corte inoltre escluse autorizzazioni d'ufficio e richiese che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette, presentata, in particolare, nell'ambito di procedure di prevenzione o di accertamento di reati ovvero nel contesto di azioni penali esercitate.

Per tutte tali considerazioni la Corte concluse dichiarando che l'art. 15, § 1, della Direttiva 2002/58, letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, § 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.

La disciplina italiana sui tabulati.

In Italia, com'è noto, le disposizioni legislative sulla conservazione dei dati personali si incentrano sull'art. 132 d.lgs. 30.6.2003, n. 196, Codice in materia di protezione dei dati personali (cd. Codice della *privacy)*, che, in nome dell'*habeas data* tutelato dall'art. 15 Cost., contiene la disciplina ordinaria. Essa prevede che, fermo restando quanto previsto dall'art. 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione (comma 1). I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni (comma 1-*bis*). La stessa disposizione stabilisce che, entro tali termini, i dati siano "acquisiti presso il fornitore con decreto motivato del pubblico ministero" (comma 2).

Inoltre, una disciplina speciale è dettata dall'art. 24 l. 20.11.2017, n. 167, che, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli artt. 51, comma 3-*quater*, e 407, comma 2, lettera a), c.p.p., ha innalzato a 72 mesi (6 anni) il periodo di conservazione dei dati di traffico telefonico e telematico, in deroga a quanto previsto dall'art. 132 commi 1 e 1-*bis* del Codice *Privacy*.

Il quadro complessivo della disciplina della *data retention*, pertanto, si articola secondo **una sorta di "quadruplice binario" a seconda del tipo di reato perseguito**. I tempi di conservazione sono di regola scanditi nei ventiquattro mesi, dodici mesi e trenta giorni previsti dall'art. 132 d.lgs. n. 196 del 2003; nei casi in cui vengono in rilievo reati a matrice terroristica o previsti dall'art. 407, comma 2, lett. *a*), i tempi di

conservazione sono dettati dall'art. 24 l. n. 1677/2017. Ma **il fornitore dei servizi, non potendo prevedere le richieste che gli perverranno in futuro, per adempiere ai suoi obblighi di conservazione, deve custodire in ogni caso tutti i dati di traffico per il termine massimo di settantadue mesi**. Naturalmente il soggetto titolare del rapporto contrattuale con l'ente gestore della telefonia è legittimato ad ottenere la documentazione dei dati memorizzati, che riguardano le proprie comunicazioni con i suoi interlocutori, senza la necessità di un provvedimento dell'autorità giudiziaria.

Su questa disciplina legislativa la Corte costituzionale non ha mai avuto il coraggio di incidere. Essa infatti dichiarò inammissibile, la questione di costituzionalità, sollevata con riferimento all'art.267 c.p.p., nella parte in cui non prescrive l'adozione di un provvedimento autorizzativo del giudice per l'acquisizione dei tabulati telefonici. Secondo questa decisione, **è ragionevole la previsione di diversi gradi di tutela**, in quanto per le intercettazioni, riguardando queste il contenuto del flusso delle comunicazioni, vi è la necessità dell'autorizzazione del giudice, mentre **per l'acquisizione dei tabulati, concernente i soli dati esterni delle comunicazioni, si è ritenuto sufficiente l'adozione di un provvedimento motivato dell'autorità giudiziaria**, e quindi anche del pubblico ministero[8].

E tale affermazione è rimasta immutata nel tempo, anche se successivamente la Consulta ebbe occasione di sottolineare "la notevole capacità intrusiva" di un'attività investigativa che coinvolga i tabulati[9], confermando che per ogni cittadino il ricorso a tale strumento di indagine deve necessariamente essere soggetto alle garanzie previste dall'art. 15 Cost.[10]

L'indirizzo giurisprudenziale italiano.

In Italia, un indirizzo giurisprudenziale consolidato ha sempre **ritenuto rispettosa del diritto U.E. la disciplina nazionale che legittima il pubblico ministero, anzichè il giudice, all'acquisizione dei dati**[11]**.** Si è argomentato, al riguardo, che le sentenze europee, nelle versioni in francese e in inglese, fanno riferimento al necessario intervento di un'autorità giudiziaria, non prescrivendo esclusivamente l'intervento del giudice. Nella traduzione italiana delle sentenze in esame, invece, si richiede "*un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente*". Pertanto, la giurisprudenza italiana ritiene che il termine "giudice" non vada inteso in senso stretto, ma possa essere esteso sino al concetto di "autorità giudiziaria", che pacificamente ricomprende anche la figura del pubblico ministero, con una interpretazione che valorizza il principio di indipendenza istituzionale, che nel sistema italiano, a differenza di quanto accade in altri ordinamenti europei, caratterizza tutta la magistratura, anche quella requirente, e risulta avallata dall'accostamento del "giudice" alla "autorità amministrativa indipendente"[12].

Da parte loro, le Sezioni Unite della Corte di cassazione si sono adeguate all'interpretazione della Consulta,

affermando che l'intercettazione dei flussi di comunicazione telefonica, informatica o telematica, con la captazione dei contenuti del dialogo in corso all'insaputa di almeno uno degli interlocutori, debba avvenire con un controllo giurisdizionale preventivo o, in caso di urgenza, immediatamente successivo, come previsto dall'art. 267 c.p.p., mentre per quanto attiene ai tabulati telefonici, per acquisire i dati esterni concernenti i soli contatti, possa essere sufficiente il decreto motivato del pubblico ministero[13].

Ovviamente il decreto di acquisizione del G.I.P. deve essere motivato *ex* artt. 253 c.p.p. e 132, comma 3, d.lgs. 30.6.2003, n. 196 e la motivazione deve indicare la necessità investigativa che impone di compiere l'atto. Ma, secondo l'orientamento giurisprudenziale consolidato, **poiché si ritiene modesto il livello di intrusione nella sfera di riservatezza delle persone,** ai fini dell'acquisizione dei tabulati relativi al traffico telefonico, telematico o di ubicazione, **l'obbligo di motivazione del decreto acquisitivo sarebbe soddisfatto anche con espressioni sintetiche**, nelle quali si sottolinei la necessità dell'investigazione, in relazione al proseguimento delle indagini ovvero all'individuazione dei soggetti coinvolti nel reato, o si richiamino, con espressione indicativa della loro condivisione da parte dell'autorità giudiziaria, le ragioni esposte da quella di polizia[14].

Inoltre, come conseguenza dell'inquadramento dell'acquisizione dei tabulati come mezzo di ricerca della prova diverso dall'intercettazione di comunicazioni o conversazioni, la giurisprudenza ritiene che, ai fini dell'acquisizione di tabulati relativi al traffico telefonico da altro procedimento, non è necessaria la procedura richiesta per le intercettazioni dall'art. 270 c.p.p.[15]

Tuttavia, la Corte di cassazione si è spinta ad affermare che il rispetto dei termini di conservazione dei dati rileva ai fini della loro utilizzabilità e, di conseguenza, s**ono stati ritenuti inutilizzabili i dati contenuti nei tabulati telefonici acquisiti dall'autorità giudiziaria senza rispettare i termini di cui all'art. 132 d.lgs. n. 196/2003**[16]**.** Si soggiunge che l'art. 132, comma 1, Codice della *privacy*, contiene un divieto di conservazione dei dati da parte del gestore oltre il periodo normativamente predeterminato[17], per cui i dati conservati oltre i termini indicati, se acquisiti agli atti, costituiscono una prova vietata dalla legge e la cui utilizzazione è dunque esclusa in maniera assoluta.

Secondo la Corte di cassazione, **la normativa nazionale rispetterebbe gli *standard* di tutela dei dati personali richiesti dalla normativa europea**. Essa, infatti, enuncia la finalità di repressione dei reati; delimita sul piano temporale l'attività di conservazione; prevede l'intervento preventivo dell'autorità giudiziaria, funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati nonché al rispetto del principio di proporzionalità in concreto.

In realtà, la disciplina ordinaria italiana non limitava l'accesso ai dati "strettamente necessari" ai fini dell'indagine nella lotta contro le "forme gravi di criminalità o della prevenzione di gravi minacce per la

sicurezza pubblica", non distingueva tra reati più o meno gravi, né tra i soggetti sospettati di reato o meno, come esige la Corte di giustizia U.E.

Inoltre, il Codice *privacy* attribuiva al P.M. la legittimazione esclusiva ad acquisire i dati telefonici o telematici - competenza censurata dalla Corte di giustizia U.E. - mentre in precedenza la legge italiana stabiliva che i dati erano acquisiti presso il fornitore con decreto motivato del giudice, su istanza delle parti. In altre parole, in Italia la conservazione dei dati era ordinariamente generalizzata e indifferenziata ed inoltre era attribuito al P.M. il "monopolio a disporre l'acquisizione dei dati", anche nel caso di istanza del difensore dell'imputato, dell'indagato, della persona offesa e delle altre parti private. La normativa riesumava la previgente prassi processuale, per cui il P.M. acquisiva il tabulato telefonico con proprio decreto *ex* art. 256 c.p.p., ma segnava un pericoloso *revirement* in rotta di collisione con il sistema accusatorio, come ripetutamente affermato dalla Grande Camera della Corte di giustizia U.E., dal momento che si riconoscono al P.M. poteri incidenti sulla vita privata e sull' "inviolabile" libertà di comunicazione che il diritto U.E. e l'art. 15 Cost. affidano al giudice.

La disciplina appariva ancora più negativa se si pensa che, a norma dell'art. 132, comma 3, Codice *privacy*, il difensore dell'imputato o della persona sottoposta alle indagini poteva richiedere, direttamente al fornitore, soltanto i dati relativi alle utenze intestate al proprio assistito (e non di terze persone) con le modalità indicate dall'art. 391-*quater* c.p.p., ferme restando inoltre per il traffico entrante le condizioni di cui all'art. 8, comma 2 lett. f), dello stesso d.lgs. La richiesta di accesso diretto alle comunicazioni telefoniche in entrata poteva essere effettuata "solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397; diversamente i diritti di cui agli articoli da 12 a 22 del Regolamento generale sulla protezione dei dati (Regolamento U.E. G.D.P.R. n. 2016/679) potevano essere esercitati "con le modalità di cui all'articolo 2-*undecies*, comma 3, terzo, quarto e quinto periodo", cioè tramite il Garante con le modalità di cui all'art. 160 dello stesso codice della *privacy*.

Nonostante l'evidente contrasto con le Direttive europee, la Corte di cassazione ha sempre escluso che l'art. 132 Codice *privacy* confliggesse con il diritto dell'Unione[18].

Si discuteva sugli effetti della pronuncia della Corte giust. U.E. negli ordinamenti interni. In Italia, la Corte di cassazione ha affermato che i principi enunciati dalle sentenze della Corte di giustizia U.E. non avrebbero effetto sulla disciplina italiana della conservazione e dell'acquisizione dei tabulati del traffico telefonico, perchè esse riguarderebbero Stati privi di una disciplina legislativa sulla conservazione e sull'accesso ai dati**, mentre l'Italia** dispone di una specifica disciplina[19].

A nostro parere, in una materia come quella riguardante la segretezza delle comunicazioni, presidiata dalla riserva di legge, la caducazione della Direttiva 2002/58/CE, nelle parti dichiarate contrastanti con il diritto U.E., toglie alla disciplina interna la "base legale".

Inoltre, anche se le sentenze della Corte di giustizia U.E. non sono immediatamente operanti nell'ordinamento interno, giacché esse incidono soltanto sugli atti dell'Unione, a norma dell'art. 267 T.F.U.E., tuttavia, una serie di pronunce, tutte dello stesso tenore, che evidenziano un così eclatante contrasto della legislazione italiana con il diritto U.E., non possono essere più ignorate.

E' vero che le disposizioni dei Trattati non specificano gli effetti delle pronunce pregiudiziali, ma è ovvio che il rinvio pregiudiziale comporti anzitutto un effetto endoprocessuale, nel senso che la decisione della Corte di giustizia U.E. è certamente vincolante sul giudice del rinvio, che è tenuto a conformarsi all'interpretazione resa dalla Corte per la risoluzione della controversia *sub iudice*, anche se la vincolatività della sentenza interpretativa non può impedire comunque al giudice nazionale di sollevare un nuovo rinvio alla Corte, anche al fine di provocarne un mutamento interpretativo. Tuttavia, non può negarsi alle sentenze interpretative della Corte giust. U.E. anche effetto extraprocessuale, cioè al di fuori del giudizio principale. Tali pronunce, infatti, pur originando da una specifica controversia, hanno carattere astratto, essendo volte a chiarire l'interpretazione e la portata delle disposizioni del diritto U.E. Anzi, la finalità del rinvio pregiudiziale è proprio quello di assicurare l'uniforme applicazione del diritto U.E. e tale finalità sarebbe frustrata se le sentenze interpretative della Corte dispiegassero i propri effetti soltanto nella causa *a qua*[20].

In conclusione, l'interpretazione dell'art. 15, § 1, della direttiva 2002/58 data dalla Corte di giustizia U.E. nel caso estone, assumeva rilievo anche per valutare la conformità della normativa italiana alla disciplina dell'Unione europea[21].

Dopo la sentenza della Corte giust. U.E., la giurisprudenza procedeva in ordine sparso, raramente disapplicando la normativa interna[22], più spesso negando la diretta applicabilità della sentenza della Corte giust. U.E.[23], altre volte richiedendo una pronuncia pregiudiziale della Corte giust. U.E.[24]

Il decreto-legge.

Il legislatore italiano è stato quindi costretto ad adeguarsi al diritto dell'Unione e introdurre finalmente una duplice riserva (di legge e di giurisdizione), prevedendo, con "regole chiare e precise", il divieto di una conservazione "generalizzata e indifferenziata" dei dati relativi al traffico e all'ubicazione[25], le "garanzie minime", cioè "i casi e i modi" per l'accesso ai dati.

E' rimasto inalterato, e darà luogo a difficoltà di coordinamento, l'art. 254-*bis* c.p.p. che, adeguandosi alla Convenzione di Budapest, disciplina le sequenze procedimentali del sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni[26], stabilendo che l'autorità giudiziaria (e quindi anche il P.M. ma non i difensori), quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può

stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità (la *bit stream image*). In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali. Tale sequestro ha ad oggetto i dati detenuti da fornitori di servizi telematici e non riguarda un flusso di comunicazioni in atto (quale è quello che si realizza con le *chat*, anche se non contestuali, le *mail* e i *social network*), che invece danno luogo ad un flusso di comunicazioni relativo a sistemi telematici, per la cui intercettazione opera il disposto dell'art. 266-*bis* c.p.p.[27]

È rimasto purtroppo inalterato anche l'irragionevole termine di conservazione prescritto dall'art. 132 d.lgs. 30.6.2003, n. 196, Codice in materia di protezione dei dati personali (cd. Codice della *privacy)*, che, in nome dell'*habeas data* tutelato dall'art. 15 Cost., contiene la disciplina ordinaria. Essa prevede che, fermo restando quanto previsto dall'art. 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione (comma 1). I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni (comma 1-*bis*). La stessa disposizione stabilisce che, entro tali termini, i dati siano "acquisiti presso il fornitore con decreto motivato del pubblico ministero" (comma 2).

Inoltre, una disciplina speciale è dettata dall'art. 24 l. 20.11.2017, n. 167, che, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli artt. 51, comma 3-*quater*, e 407, comma 2, lettera a), c.p.p., ha innalzato a 72 mesi (6 anni) il periodo di conservazione dei dati di traffico telefonico e telematico, in deroga a quanto previsto dall'art. 132 commi 1 e 1-*bis* del Codice *Privacy*.

Il quadro complessivo della disciplina della *data retention*, pertanto è rimasto inalterato, cioè sempre articolato sui tempi di conservazione scanditi nei ventiquattro mesi, dodici mesi e trenta giorni previsti dall'art. 132 d.lgs. n. 196 del 2003; nei casi in cui vengono in rilievo reati a matrice terroristica o previsti dall'art. 407, comma 2, lett. *a*), i tempi di conservazione sono di 72 mesi, cioè 6 anni (art. 24 l. n. 1677/2017).

Il legislatore nazionale ha invece finalmente individuato i "casi" nei quali è consentito l'accesso ai dati, ed essi, dovendo riguardare esclusivamente la lotta contro "forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica", il decreto-legge li indica nei casi in cui sussistono "sufficienti indizi" di un reato (*fumus delicti*) per il quale la legge stabilisce la pena dell'ergastolo o della reclusione non inferire

nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e dei reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove "rilevanti ai fini della prosecuzione delle indagini" (principio di pertinenza della prova). L'acquisizione dei dati può dunque avvenire anche in riferimento a persona non raggiunta da indizi di reato.

Ovviamente il decreto di acquisizione del G.I.P. deve essere motivato *ex* artt. 253 c.p.p. e 132, comma 3, d.lgs. 30.6.2003, n. 196 e la motivazione deve indicare la necessità investigativa che impone di acquisire i dati, precisando se quelli telefonici, telematici o le chiamate senza risposta, di un determinato soggetto, in riferimento ad un preciso arco temporale.

Anche se l'acquisizione dei dati deve essere rilevante "ai fini della prosecuzione delle indagini", non si può escludere una autorizzazione anche in momenti processuali successivi alla conclusione delle indagini preliminari, sia perché potrebbero esserci indagini suppletive e integrative del P.M., sia perché, a norma dell'art. 327-*bis* c.p.p., potrebbero essere svolte investigazioni difensive in ogni stato e grado del procedimento, nell'esecuzione penale e per promuovere il giudizio di revisione. Pertanto, l'autorizzazione compete al G.I.P. nella fase delle indagini preliminari e successivamente al giudice che procede. In ogni caso l'acquisizione dei dati non può mai costituire il primo atto di indagine, ma deve essere rilevante per la prosecuzione.

In realtà, si sarebbero dovuti legislativamente individuare anche i "soggetti" perché, di regola, l'accesso è ammesso soltanto ai dati di chi è sospettato di reato e solo eccezionalmente in "situazioni particolari" (come ad esempio quelle in cui gli interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica siano minacciati da attività di terrorismo), può ammettersi l'accesso ai dati di persone non sospettate, ma a condizione che esistano "elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo". Invece nulla al riguardo è stato precisato nel decreto-legge. Pertanto, sul punto, sarà inevitabile sollevare questione di legittimità costituzionale in rapporto all'art. 117 Cost., che vincola la potestà legislativa dello Stato al rispetto, tra l'altro, dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali.

Infine, come si è detto, la Grande Camera aveva imposto il previo controllo effettuato da "un giudice o da un'entità amministrativa indipendente", e che, in ossequio al principio della domanda, la decisione di tale giudice o di tale entità intervenisse a seguito di una richiesta motivata delle autorità competenti presentata, in particolare, nell'ambito di procedure di prevenzione o di accertamento di reati ovvero nel contesto di azioni penali esercitate. Solo eccezionalmente, in "caso di urgenza, debitamente giustificata", il controllo può essere successivo all'accesso ai dati, ma deve intervenire "entro termini brevi". E sul punto, il legislatore italiano è stato più diligente perché il decreto-legge, che modifica l'art. 132 d. lgs. 30 giugno 2003, n. 196, c.d.

Codice della *privacy*, stabilisce che "i dati sono acquisiti presso il fornitore con decreto motivato del giudice su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private" (art. 132, comma 3).

In questo modo si è finalmente riconosciuto il diritto alla prova in capo anche al difensore, che finora era impossibilitato a richiedere i tabulati direttamente al fornitore. Inoltre la novità consiste nel fatto che è legittimato alla richiesta di tabulati non solo il difensore della persona sottoposta alle indagini, ma in successivi momenti processuali anche quello di qualsiasi altra parte privata (e quindi non solo l'imputato, ma anche la parte civile, il responsabile civile e il civilmente obbligato per la pena pecuniaria).

Il decreto-legge stabilisce pure che "quando ricorrono ragioni d'urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati. (art. 132, comma 3-*bis*)

Il "nuovo" comma 3-*ter* dell'art. 132 del citato d. lgs. n. 196/2003 chiarisce che rispetto ai dati conservati per le finalità di accertamento e repressione di reati "i diritti di cui agli articoli da 12 a 22" del Regolamento generale sulla protezione dei dati (Regolamento U.E. G.D.P.R. n. 2016/679) del Parlamento europeo e del Consiglio del 27 aprile 2016, "possono essere esercitati con le modalità di cui all'articolo 2-*undecies*, comma 3, terzo, quarto e quinto periodo". In altre parole, i "diritti dell'interessato" al trattamento dei dati[28] possono essere esercitati tramite il Garante per la protezione dei dati personali con le modalità di cui all'art. 160[29].

In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facoltà che gli sono riconosciute nello stesso comma 3 dell'art. 2-*undecies*.

A parte l'ipotesi della mancata convalida del decreto d'urgenza del P.M., non è esplicitamente prevista alcuna previsione di inutilizzabilità dei dati acquisiti senza il rispetto delle prescrizioni dettate per la acquisizione dei dati. Tuttavia, l'inutilizzabilità deriva dal sistema, essendo irragionevole che, per i dati acquisiti sotto la previgente disciplina in assenza dei presupposti di legge, ne era prevista l'inutilizzabilità[30], che invece non è espressamente dettata per l'identica fattispecie che si realizzi nei procedimenti iscritti dopo l'entrata in vigore del decreto. Si può dunque plausibilmente sostenere l'esistenza di un divieto probatorio implicito all'utilizzazione di dati acquisiti senza i requisiti di legge.

La disciplina transitoria.

Il testo originario del decreto-legge sottoposto al Consiglio dei ministri, prevedeva all'art. 2 che "i dati relativi al traffico telefonico, al traffico telematico, esclusi comunque i contenuti delle comunicazioni, e alle chiamate senza risposta, acquisiti nei procedimenti pendenti alla data di entrata in vigore del presente decreto possono essere utilizzati, quando l'acquisizione è stata disposta dall'autorità giudiziaria, se ricorrono i presupposti previsti dall'articolo 132, comma 3, del decreto legislativo 30 giugno 2003, n. 196, così come modificato dall'articolo 1 del presente decreto" (art. 2, comma 1).

Pertanto, era imposta al giudice, in ogni stato e grado del procedimento, una valutazione "ora per allora" sia sul rispetto dei termini di conservazione dei dati, sia sull'esistenza dei "sufficienti indizi" di un reato per il quale la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 c.p.p. o dei reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia o il disturbo sono gravi, sia sulla "rilevanza" dell'acquisizione "ai fini della prosecuzione delle indagini".

Ai fini della valutazione di utilizzabilità dei dati, era previsto che "nella prima udienza successiva alla data di entrata in vigore del presente decreto, il giudice, sentite le parti, provvede con ordinanza alla convalida del provvedimento di acquisizione dei dati. Nei procedimenti in cui l'azione penale non è stata esercitata, alla verifica procede, anche d'ufficio, il giudice per le indagini preliminari all'atto dell'adozione del primo provvedimento successivo alla data di entrata in vigore del presente decreto che presupponga la valutazione dei dati di cui al comma 1" (art. 2, comma 2).

Ma nel testo definitivo del decreto-legge, approvato dal Consiglio dei ministri, è inopinatamente scomparsa la disposizione transitoria. Ciò comporta che le nuove disposizioni sull'acquisizione dei dati, in forza del principio del *tempus regit actum*, si applicheranno soltanto ai procedimenti penali iscritti dopo la data di entrata in vigore del decreto. Si tratta di una gravissima mutilazione alla riservatezza della vita privata dei cittadini, che lascia i provvedimenti di acquisizione dei dati personali, emessi in passato per decenni dal P.M., in contrasto con le direttive europee. Si auspica, pertanto, che in sede di conversione sia reinserita la disposizione transitoria.

Conclusioni.

L'intervento legislativo è certamente positivo, anche se sarebbe stato preferibile realizzare una "riserva di codice" e inserire le nuove disposizioni subito dopo gli artt. 266-271 c.p.p.

Biasimevole è anche l'aver lasciato inalterati i tempi di conservazione dei dati, così come non aver prescritto una motivazione "rafforzata" sui presupposti dell'acquisizione, in modo da evitare le consuete formule di stile ma vuote di contenuto che finora la giurisprudenza ha ammesso.

Sarebbe stato necessario pure un coordinamento tra le nuove disposizioni e l'art. 254-*bis* c.p.p., che disciplina il procedimento di sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni

Soprattutto, sarebbe stata auspicabile anche un'esplicita previsione di inutilizzabilità dei dati acquisiti in difetto di una autorizzazione del giudice e di una esauriente motivazione sulla qualificazione giuridica del fatto, sulla sufficienza indiziaria e sulla rilevanza dell'acquisizione dei dati ai fini della prosecuzione delle indagini.

[1] Corte giust. U.E. (Grande Camera) 2.3.2021, *H. K.* c. /*Prokuratuur*, C□746/18.

[2] Corte giust. U.E. (Grande Camera) 2.3.2021, *H. K.* c. /*Prokuratuur*, C□746/18.

[3] Come già avevano precisato Corte giust. U.E., Grande Camera, 21.12.2016, *Tele2 Sverige e Watson e al*., C□203/15 e C□698/15, cit.; Corte giust. U.E., Grande Camera, 6.10.2020, *Privacy International*, C□623/17, cit., nonché Corte giust. U.E., Grande Camera, 6.10.2020, *La Quadrature du Net e al*., C□511/18, C□512/18 e C□520/18 e la giurisprudenza ivi citata.

[4] Il principio era stato già enunciato da Corte giust. U.E., Grande Camera, 6.10.2020, *Privacy International*, C□623/17, cit. nonché Corte giust. U.E., Grande Camera, 6.10.2020, *La Quadrature du Net e al*., C□511/18, C□512/18, e C□520/18, e la giurisprudenza ivi citata.

[5] In tal senso, Corte giust. U.E., Grande Camera, 21.12.2016, *Tele2 Sverige e Watson e al*., C□203/15 e C□698/15, cit., nonché Corte giust. U.E., Grande Camera, 6.10.2020, *La Quadrature du Net e al*., C□511/18, C□512/18 e C□520/18.

[6] Come già affermato da Corte giust. U.E. , Grande Camera, 9.3. 2010, *Commissione/Germania*, C□518/07.

[7] In tal senso, si era già pronunciata Corte giust. U.E., Grande Camera, 6.10.2020, *La Quadrature du Net e al*., C□511/18, C□512/18 e C□520/18 e la giurisprudenza ivi citata.

[8] Corte cost. 7.7.1998, n. 281.

[9] Corte cost. 26.5.2010, n. 188.

[10] Corte cost. 23.1.2019, n.38.

[11] Nel senso della compatibilità della disciplina italiana con le disposizioni europee (v. Cass., sez. II, n. 5741/20202, *CED* 278568; Cass., sez. III, n. 48737/2019, *CED* 277353; Cass., sez. V, n. 33851/2018, *CED* 273892). In particolare, poi, per la S.C., i principi enunciati dalle sentenze della CGUE non avrebbero effetto sulla disciplina italiana della conservazione e dell'acquisizione dei tabulati del traffico telefonico, perché esse

riguarderebbero Stati privi di una disciplina legislativa sulla conservazione e sull'accesso ai dati, mentre l'Italia dispone di una specifica disciplina. (v. Cass., sez. V, n. 3385172018, *CED* 273892; Cass., sez. III, 36380/2019). Cass., sez. II, 15.4.2021 (dep. 22.7.2021), Lordi, n. 28523, in *Guida dir.*, 2021, n.34, p. 68, ritiene che la sentenza 2.3. 2021, emessa nella causa C 746/18m, della Corte di Giustizia U.E., in tema di tabulati telefonici "sembra incapace di produrre effetti applicativi immediati e diretti a causa dell'indeterminatezza delle espressioni ivi utilizzate al fine di legittimare l'ingerenza dell'autorità pubblica nella vita privata dei cittadini". Secondo la S.C., gli unici dati patologicamente inutilizzabili sarebbero quelli relativi al traffico telefonico contenuti nei tabulati acquisiti dall'autorità giudiziaria dopo i termini previsti dall'art. 132 d. lgs. n. 196/2003, atteso il divieto di conservazione degli stessi da parte del gestore al fine di consentire l'accertamento dei reati oltre il periodo normativamente predeterminato (Cass., sez. V, n. 7265/2016, *CED* 267144).

[12] Cass., sez. V, 24.4.2018 (dep. 19.7.2018), M., n. 33851, Rv. 273892, cit.; Cass., sez. III, 19.4.2019 (dep. 23.8.2019), D'Addiego e altro, n. 36380, cit.

[13] Cass., Sez. un., 23.2.2000, n. 6, D'Amuri, Rv. 215841.

[14] È stato ritenuto sufficientemente motivato il provvedimento acquisitivo che si limita a richiamare l'assoluta necessità dell'acquisizione ai fini del proseguimento delle indagini (Cass., sez. I, 28.4.2014, n. 37212, Rv. 260589; Cass., sez. I, 26.9.2007, n. 46086, Rv. 238170).

[15] Cass., sez. II, 18.10.2007 (dep. 22.11.2007), n. 43329 , Rv. 238834.

[16] **Cass., sez, V 5.12.2014 (dep. 15.4.2015), n. 15613**, in CED Cass., Rv. 263805.

[17] Cass. sez. V, 25.1.2016 (dep.24.2.2016), n. 7265, in CED Cass. Rv. 267144.

[18] Cass., sez. II, 10.12.2019, Dedej e altri, n. 5741/2020; Cass., sez. III, 19.4.2019, n. 36380/2019; Cass., sez. V, 24.4.2018, n.33851, Rv. 273892.

[19] Cass., sez. V, 24.4.2018 (dep. 19.7.2018), n. 33851; Cass., sez. III, 19.4.2019 (dep. 23.8.2019), n. 36380.

[20] In questo senso cfr. R. MASTROIANNI, *Pregiudiziale comunitaria*, in *Digesto discipline penalistiche*, 2010.

[21] V. in generale Corte giust. U.E., che ha stabilito che l'art. 288 T.F.U.E. dev'essere interpretato nel senso che osta a che un giudice nazionale il quale, nell'ambito di un procedimento previsto a tal fine dal diritto interno, constati che lo Stato membro al quale appartiene non ha adempiuto il proprio obbligo di recepire correttamente la direttiva 2001/82/CE del Parlamento europeo e del Consiglio, del 6 novembre 2001, recante un codice comunitario relativo ai medicinali veterinari, come modificata dalla direttiva 2004/28/CE del Parlamento europeo e del Consiglio, del 31 marzo 2004, rifiuti di adottare, per il motivo che la normativa

nazionale gli sembra conforme al regolamento (UE) 2019/6 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, relativo ai medicinali veterinari e che abroga la direttiva 2001/82 – regolamento che abroga tale direttiva e che sarà applicabile a decorrere dal 28 gennaio 2022 – una dichiarazione giurisdizionale secondo la quale tale Stato membro non ha correttamente recepito detta direttiva ed è tenuto a rimediarvi (Corte giust. U.E. , sez. I, 17.3.2021, *Uh Ic/ An Taire Talmhaíochta, Bia Agus Mara, Éire,An Tard-Aighne*, C-64/2).

[22] In questo senso Trib.Roma, GIP (decreto) 25.4.2021, che, applicando direttamente la prevalente normativa sovranazionale, ha autorizzato la richiesta acquisizione dei dati, dopo aver ritenuto sussistenti i presupposti delineati dalla normativa U.E. e cioè gli indizi di uno dei reati di cui agli artt. 266 e 266-*bis* c.p.p., nonché l'indispensabilità per la prosecuzione delle indagini. Nel senso della disapplicazione è anche Trib. Bari, GIP (decreto) 1.5.2021, che ritiene il giudice organo legittimato ad autorizzare l'acquisizione dei tabulati, dopo un vaglio giurisdizionale che decida sulla necessità di limitazioni di diritti fondamentali e ritenendo applicabile analogicamente l'art. 271 c.p.p. in caso di acquisizione dei tabulati da parte del P.M. (in *Guida dir.*, 2021, n. 20, p. 42). Si è affermata la diretta applicabilità della sentenza della Grande Sezione della Corte di Giustizia U.E. 2.3. 2021, H.K., C-746/18, in tema di tabulati telefonici, traendone conclusioni in termini di inutilizzabilità degli esiti di prova, con un provvedimento che - per gli effetti che ne conseguono sulle intercettazioni richieste sulla scorta di dati di traffico acquisiti in assenza del decreto autorizzativo del giudice - apre a considerazioni di ulteriori criticità (G.I.P. Trib. Bari (decreto) 1.5.2021, ne *Il Penalista*, 25.5.2021).

[23] Trib. Milano (ord.) 22.4.2021, e Trib. Roma, GIP (decreto) 28.4.2021 e (decreto)29.4.2021 (in *Guida dir.*, 2021, n. 20, p. 42).

[24] Trib. Rieti (ord.) 4.5.2021, in *Guida dir.*, 2021, n. 20, p. 36.

[25] La nozione di "dato di ubicazione" è offerta dall'art. 1, comma 1 lett. c) d. lgs. n. 109/2008 che considera tale "ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico".

[26] L'art. 254-*bis* è stato introdotto nel codice di rito penale dall'art. 8 l. 18.3.2008, n. 48, Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

[27] Secondo la giurisprudenza, l'estrazione dei dati archiviati in un *computer* non dà luogo ad accertamento tecnico irripetibile, trattandosi di operazione meramente meccanica, riproducibile per un numero indefinito di volte, come si desume, del resto, dalla disciplina introdotta dalla l. 18.3.2008, n. 48 (Cass., sez. II, 1.7.2015, n. 29061, p.c. in proc. Artergiani e altro, in *Guida dir.*, 2015, n. 32, p. 91).

[28] Si tratta di informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato : art. 12; informazioni da fornire qualora i dati personali siano raccolti presso l'interessato: art. 13; informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato: art. 14; diritto di

accesso dell'interessato : art. 15; diritto di rettifica : art. 16; diritto alla cancellazione (diritto all'oblio):art. 17; diritto di limitazione di trattamento: art. 18; obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento: art. 19; diritto alla portabilità dei dati: art. 20; diritto all'opposizione: art. 21; processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione: art. 22).

[29] In altre parole, gli accertamenti sono effettuati per il tramite di un componente designato dal Garante. Se il trattamento non risulta conforme alle norme del Regolamento ovvero alle disposizioni di legge o di Regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, se ciò non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto su ciò di cui sono venuti a conoscenza in ordine a notizie che devono rimanere segrete. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal Regolamento di cui all'articolo 156, comma 3, lettera a). Per gli accertamenti di cui al comma 3 relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

[30] L'art. 2 comma 1 del d.-l. , nel suo testo originario, stabiliva che "i dati relativi al traffico telefonico, al traffico telematico, esclusi comunque i contenuti delle comunicazioni, e alle chiamate senza risposta, acquisiti nei procedimenti pendenti alla data di entrata in vigore del presente decreto possono essere utilizzati, quando l'acquisizione è stata disposta dall'autorità giudiziaria, se ricorrono i presupposti previsti dall'articolo 132, comma 3, del decreto legislativo 30 giugno 2003, n. 196, così come modificato dall'articolo 1 del presente decreto". Tale disposizione transitoria è scomparsa nel testo del d.-l. approvato dal Consiglio dei ministri.