**TRIBUNALE DI BARI**
**Sezione del Giudice per le Indagini Preliminari**
**DECRETO DI NON CONVALIDA E DI NON AUTORIZZAZIONE DI INTERCETTAZIONE**
**(artt. 266, 267, comma 2, c. p. p.)**

Il Giudice, dott. Francesco Agnino,
esaminato il decreto emesso dal pm il 30 aprile 2021, alle ore 13.30, e depositato in cancelleria il 30 aprile 2021, con il quale sono state disposte in via d'urgenza le operazioni di intercettazione delle conversazioni o comunicazioni d'urgenza mediante ascolto telefonico e relativa localizzazione in tempo reale (positioning) per la durata di giorni 40 (quaranta) a carico della seguente utenza telefonica:

OSSERVA

I. L'individuazione della utenza oggetto del decreto di urgenza adottato dal PM è avvenuta in forza dei tabulati telefonici dell'utenza in uso a , acquisiti dal Pm.

Orbene, a parte l'insussistenza del requisito dell'urgenza legittimante il decreto del PM, tenuto conto che tale utenza telefonica è stata identificata a seguito di un messaggio in entrata registrato nella mattinata del 26 aprile 2021, di modo che la PG era già da oltre quattro giorni era conoscenza di tale numero, si pone un problema di disporre l'intercettazione su un numero telefonico, la cui valenza probatoria è stata determinata dall'acquisizione dei dati di traffico conservati presso il gestore dei servizi telefonici, in assenza di decreto autorizzativo del giudice,.

In altri termini occorre stabilire se l'acquisizione dei c.d. tabulati del traffico telefonico disposta dal PM e non dal Giudice possa dare luogo alla applicazione dell'art. 271 c.p.p.

La risposta deve ritenersi affermativa, sulla scorta della sentenza adottata dalla Grande Sezione della Corte di giustizia UE, nella sentenza del 2 marzo 2021, *H.K*., C-746/18, in tema di tabulati telefonici e telematici.

Com'è noto, nel menzionato arresto, i giudici europei, rispondendo a un rinvio pregiudiziale sollevato dalla Corte suprema estone, hanno precisato la loro già articolata giurisprudenza in materia di *data retention* (basti pensare solo alle celebri sentenze Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland* e Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*).

Essi hanno, infatti, stabilito che il diritto UE (e in particolare l'art. 15 della direttiva 2002/58/UE, letto alla luce degli artt. 7, 8, 11 e 52 della Carta di Nizza) osta a una disciplina nazionale che: 1) non circoscriva l'accesso di autorità pubbliche a dati idonei a fornire informazioni su comunicazioni effettuate da un utente «a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica»; 2) affidi nel corso di un rito penale al pubblico ministero e non a un soggetto terzo (come un giudice) la competenza ad autorizzare l'accesso a tali dati.

La Grande Camera ribadisce alcuni chiari principi di diritto, peraltro già affermati in passato nella sua giurisprudenza, a tutela della riservatezza, della protezione dei dati di carattere personale, della libertà di espressione e d'informazione, nonché del principio di proporzionalità delle limitazioni a tali diritti e libertà.
Infatti, con sentenza del 2 marzo 2021 la Grande Camera della Corte giust. U.E. ha precisato che l'art. 15, § 1, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni (Direttiva sulla vita privata e le comunicazioni elettroniche), letta alla luce degli artt. 7 (tutela della riservatezza), 8 (protezione dei dati di carattere personale) e 11 (libertà di espressione e d'informazione) nonché dell'art. 52, § 1 (principio di proporzionalità delle limitazioni ai diritti e alle libertà), della Carta dei diritti fondamentali dell'Unione europea, 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 ha aggiunto 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 .
II. La pronuncia della Grande Camera non giunge inaspettata. Infatti, già una prima volta, la Corte di giustizia U.E. (Grande Camera), con sentenza 8 aprile 2014, dichiarò invalida la Direttiva 2006/24/CE sulla conservazione dei dati, in rapporto agli stessi valori del rispetto della vita privata e della vita familiare, della protezione dei dati di carattere personale e per violazione del principio di proporzionalità.
Anche allora la Corte affermò che la direttiva 2006/24/CE comportava un'ingerenza di vasta portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, non limitata allo "stretto necessario". A tale riguardo, la Corte osservò che, in considerazione, da un lato, dell'importante ruolo svolto dalla protezione dei dati personali nei confronti del diritto fondamentale al rispetto della vita privata e, dall'altro, della portata e della gravità dell'ingerenza in tale diritto che la direttiva comporta, il potere discrezionale del legislatore risulta ridotto e che occorre quindi procedere a un controllo rigoroso.
Anche se la conservazione dei dati imposta dalla Direttiva può essere considerata idonea a raggiungere l'obiettivo perseguito dalla medesima, l'ingerenza vasta e particolarmente grave di tale direttiva nei menzionati diritti fondamentali non fu ritenuta sufficientemente regolamentata in modo da essere effettivamente limitata allo "stretto necessario".

In primo luogo, infatti, la Direttiva trovava applicazione generalizzata all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venisse operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi.
In secondo luogo, la Direttiva non prevedeva alcun criterio oggettivo che consentisse di garantire che le autorità nazionali competenti avessero accesso ai dati e potessero utilizzarli solamente per prevenire, accertare e perseguire penalmente reati che possano essere considerati, tenuto conto della portata e della gravità dell'ingerenza nei diritti fondamentali summenzionati, sufficientemente gravi da giustificare una simile ingerenza. Al contrario, la Direttiva si limitava a fare generico rinvio ai «reati gravi» definiti da ciascuno Stato membro nella propria legislazione nazionale. Inoltre, la Direttiva non stabiliva i presupposti materiali e procedurali che consentivano alle autorità nazionali competenti di avere accesso ai dati e di farne successivo uso. L'accesso ai dati, in particolare, non era subordinato al previo controllo di un giudice o di un ente amministrativo indipendente.
In terzo luogo, quanto alla durata della conservazione dei dati, la Direttiva imponeva che essa non fosse inferiore a sei mesi, senza operare distinzioni tra le categorie di dati a seconda delle persone interessate o dell'eventuale utilità dei dati rispetto all'obiettivo perseguito. Inoltre, tale durata era compresa tra un minimo di sei ed un massimo di ventiquattro mesi, senza che la direttiva precisasse i criteri oggettivi in base ai quali la durata della conservazione doveva essere determinata, in modo da garantire la sua limitazione allo stretto necessario.
La Corte constatò peraltro che la Direttiva non prevedeva garanzie sufficienti ad assicurare una protezione efficace dei dati contro i rischi di abusi e contro qualsiasi accesso e utilizzo illeciti dei dati. Essa rilevò, tra l'altro, che la Direttiva autorizzava i fornitori di servizi a tenere conto di considerazioni economiche in sede di determinazione del livello di sicurezza da applicare (in particolare per quanto riguarda i costi di attuazione delle misure di sicurezza) e non garantiva la distruzione irreversibile dei dati al termine della loro durata di conservazione. La Corte censurò, infine, il fatto che la Direttiva non imponeva che i dati fossero conservati sul territorio dell'Unione. In definitiva, la Direttiva non garantiva il pieno controllo da parte di un'autorità indipendente del rispetto delle esigenze di protezione e di sicurezza, come è invece espressamente richiesto dalla Carta; concludendo che siffatto controllo, compiuto sulla base del diritto dell'Unione, costituisce un elemento essenziale del rispetto della protezione delle persone con riferimento al trattamento dei dati personali .
In una seconda occasione la Grande Camera 21 dicembre 2016 ribadì che l'art. 15, § 1, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche), letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, § 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica.
L'art. 15, § 1, della Direttiva 2002/58, letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, § 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e

la sicurezza dei dati relativi al traffico e 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 . Infine, la Corte di giustizia U.E., Grande Camera, con sentenza 6.10.2020, confermò che il diritto dell'Unione si oppone ad una normativa nazionale che impone a un fornitore di servizi di comunicazione elettronica, a fini di lotta contro le infrazioni in generale o di salvaguardia della sicurezza nazionale, "la trasmissione o la conservazione generalizzata e indifferenziata di dati relativi al traffico e alla localizzazione". Si tratta di "metadati", ovvero informazioni di dettaglio su numero del chiamante, numero del ricevente, data e durata della conversazione, frequenza delle chiamate e altro, mentre quanto alla navigazione Internet viene registrato ogni elemento della navigazione (indirizzo IP, siti visitati, *device* usato, durata della consultazione, pagine visionate, traffico e-mail). Tuttavia, la Corte consentì molte deroghe, ma solo per periodi limitati. Infatti, secondo la Corte, nelle situazioni in cui uno Stato membro si trova ad affrontare una grave minaccia per la sicurezza nazionale che si rivela autentica, presente o prevedibile, lo Stato membro può derogare all'obbligo di garantire la riservatezza dei dati relativi alle comunicazioni elettroniche richiedendo, mediante misure legislative, la conservazione generale e indiscriminata di tali dati per un periodo limitato nel tempo a quanto strettamente necessario, ma che può essere esteso se la minaccia persiste. Per quanto riguarda la lotta contro la criminalità grave e la prevenzione di gravi minacce alla sicurezza pubblica, uno Stato membro può anche prevedere la conservazione mirata di tali dati nonché la loro conservazione accelerata. Tale interferenza con i diritti fondamentali, concluse la Corte di Giustizia U.E., deve essere accompagnata da garanzie efficaci ed essere esaminata da un tribunale o da un'autorità amministrativa indipendente. Allo stesso modo, uno Stato membro può effettuare una conservazione generale e indiscriminata sia degli indirizzi IP assegnati alla fonte di una comunicazione laddove il periodo di conservazione sia limitato a quanto strettamente necessario; sia anche per effettuare una conservazione generale e indiscriminata di dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica, e in quest'ultimo caso la conservazione non è soggetta ad uno specifico termine. La sentenza concluse che l'art. 1, § 3, l'art. 3 e l'art. 15, § 1, della Direttiva 2002/58 CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nelle comunicazioni elettroniche, devono essere interpretati nel senso che la legislazione nazionale che consente a un'autorità statale di richiedere ai fornitori di servizi di comunicazione elettronica di inoltrare dati sul traffico e dati sull'ubicazione alle agenzie di sicurezza e di intelligence allo scopo di salvaguardare la sicurezza nazionale rientra nell'ambito di applicazione di tale Direttiva. La stessa sentenza precisò inoltre che l'art. 15, § 1, della Direttiva 2002/58, come modificata dalla Direttiva 2009/136, letto alla luce dell'art. 4, § 2, TUE e degli artt. 7, 8 e 11 e dell'art. 52, § 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che preclude una legislazione nazionale che consente a un'autorità statale di richiedere ai fornitori di servizi di comunicazione elettronica di effettuare la trasmissione generale e

indiscriminata dei dati sul traffico e dei dati sull'ubicazione alle agenzie di sicurezza e di intelligence allo scopo di salvaguardare la sicurezza nazionale.
III. Con la sentenza 2 marzo 2021 la Grande Camera della Corte giust. U.E. afferma, 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.
In passato la Corte aveva già chiarito che l'accesso ai dati relativi al traffico e all'ubicazione può essere concesso soltanto se e in quanto tali dati siano stati conservati da detti fornitori in un modo conforme al citato art. 15, § 1, il quale, letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, § 1, della Carta, osta a misure legislative che prevedano, per finalità siffatte, a titolo preventivo, la "conservazione generalizzata e indifferenziata" dei dati relativi al traffico e all'ubicazione.
La necessità di "regole chiare e precise" per l'accesso ai dati, di regola soltanto del sospettato di reato, "strettamente necessari" ai fini della lotta contro le "forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica". Sulla scorta di tali precedenti, i giudici di Lussemburgo ribadiscono che "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 aggiunge 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 osserva 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.
Ma la Corte precisa che l'ingerenza nei diritti fondamentali del rispetto della vita privata e familiare e della protezione dei dati di carattere personale, sanciti dagli artt. 7 e 8 della Carta, provocata dall'accesso dell'autorità pubblica ad un insieme di dati relativi al traffico o all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da esso utilizzate, "presenta in ogni caso un carattere grave indipendentemente dalla durata del periodo per il quale è richiesto l'accesso a tali dati e dalla quantità o dalla natura dei dati disponibili per un periodo siffatto", qualora questo insieme di dati sia tale da permettere di trarre precise conclusioni sulla vita privata della persona o delle persone interessate. Sotto tale profilo, anche l'accesso a un quantitativo limitato di dati relativi al traffico o all'ubicazione, oppure l'accesso a dati per un breve periodo, possono essere idonei a fornire precise informazioni sulla vita privata di un utente di un mezzo di comunicazione elettronica. Inoltre non si può trascurare che sia la quantità dei dati disponibili, sia le informazioni concrete sulla vita privata della persona interessata che ne derivano sono entrambe circostanze che possono essere valutate solo dopo la consultazione dei dati suddetti.
La Corte chiarisce 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".
Alla luce delle considerazioni che precedono, la Corte chiarisce 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 consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o 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.
IV. Come già affermato in passato, la Corte riconosce 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".
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". .
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 precisa, però, 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".
Il secondo principio affermato dalla Corte è ancora più *tranchant*, perché 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. Infatti, la grande Camera precisa 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.
V. Da tali premesse la Corte ricava 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".
Né 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 conclude 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".
Essa esclude autorizzazioni d'ufficio ed esige 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.
Inoltre, la Corte ritiene 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" , 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".
Per tutte tali considerazioni la Corte conclude 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.
VI. Com'è noto, in Italia, l'art. 132 d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (cd. Codice della privacy), in nome dell'*habeas data* tutelato dall'art. 15 Cost., contiene la disciplina ordinaria, la quale 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). 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 novembre 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.
La disciplina ordinaria italiana quindi non limita 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 distingue 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 attribuisce 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 è ordinariamente generalizzata e indifferenziata ed inoltre è 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 riesuma la previgente prassi processuale, per cui il P.M. acquisiva il tabulato telefonico con proprio decreto ex art. 256 c.p.p., ma segna 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 appare 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 può 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 “può 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 possono 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.
VII. Nessun dubbio in merito alla diretta applicazione della pronuncia del 2 marzo 2021 della corte di giustizia, tenuto conto della circostanza che la Corte costituzionale, nell’applicare il diritto dell’Unione così come interpretato dalla Corte di giustizia, si è espressa in termini di «efficacia diretta» o di «immediata operatività» delle sentenze della Corte del Lussemburgo (Corte Cost. n. 284/2007 ove si afferma che “le statuizioni della Corte di giustizia delle Comunità europee hanno, al pari delle norme dell’Unione direttamente applicabili cui ineriscono, operatività immediata negli ordinamenti interni”; Corte Cost. n. 227/2010 ribadisce che: “le sentenze della Corte di giustizia vincolano il giudice nazionale

all’interpretazione da essa fornita, sia in sede di rinvio pregiudiziale, che in sede di procedura d’infrazione”.
Dal canto suo, la Corte di Cassazione a volte ha riconosciuto “valore normativo” alle sentenze della Corte di giustizia (Cass. 30 dicembre 2003, n. 19842).
E questo, se da un lato dimostra che i giudici italiani riconoscono ormai alla giurisprudenza della Corte di giustizia un valore particolarmente stringente e vincolante, dall’altro lato rivela anche che il diritto legislativo e quello (di fonte) giurisprudenziale vengono sostanzialmente equiparati.
VIII. L’intestato Tribunale non ignora che la Cassazione aveva finora escluso che il codice della privacy ponesse profili di frizione con il diritto eurounitario (Cass., sez. III, 23 agosto 2019, n. 36380); e ciò, tra l’altro, sulla base della convinzione per cui la figura del pubblico ministero, per come disciplinata nell’ordinamento italiano, rappresentasse un organo sufficientemente indipendente da soddisfare la normativa europea.
Tuttavia, se la scelta dell'individuazione dell'Autorità giudiziaria ricadesse sul pubblico ministero, ci troveremmo indubbiamente dinanzi ad una situazione affatto preoccupante se si considera che l'organo della pubblica accusa, cui è certamente devoluto l'obbligo (se non di “prevenire” quanto meno) di perseguire e “reprimere i reati”, verrebbe in maniera del tutto arbitraria ad accentrare in sé anche il potere di valutare se le esigenze investigative possano comportare, caso per caso, una violazione della libertà e della segretezza delle comunicazioni.
E nell'attuale sistema processuale, si può immaginare quale tipo di tutela della libertà e della segretezza delle comunicazioni possa garantire il pubblico ministero, vincolato, com'è, all'esercizio obbligatorio dell'azione penale.
In tale situazione, ad usare un'espressione eufemistica, ci troveremmo dinanzi ad un organo non completamente sereno per valutare le esigenze e l'interesse relativi alla segretezza delle conversazioni dell'indagato o dell'imputato.
Già questo giustificherebbe ampiamente la necessità che sull'acquisizione dei dati esteriori delle conversazioni telefoniche si esprimesse un giudice terzo che, al contrario dell'organo della pubblica accusa, si trovi in una situazione di equidistanza tra il principio della libertà e della segretezza delle comunicazioni da una parte e quello della persecuzione e repressione dei reati dall'altra.
In altri termini, l’autorità chiamata ad autorizzare l’acquisizione dei tabulati deve essere terza e neutrale (ovverosia caratteristiche intrinsecamente estranee alla parte pubblica).
Ed infatti, è pur vero che, facendo parte le intercettazioni telefoniche dei mezzi di ricerca della prova, la loro acquisizione dovrebbe pertenere esclusivamente all'organo della pubblica accusa, anche per preservare la naturale terzietà del giudice, tuttavia, allorquando nell'attività di ricerca della prova si debba necessariamente incorrere in limitazioni di diritti fondamentali sanciti dalla nostra Costituzione, l'intervento del giudice appare invero necessario, dovendosi contemperare la coesistenza di due contrastanti interessi di pari dignità.
Per lo stesso motivo, dunque, indipendentemente dal fatto che siano acquisiti semplicemente dati esteriori e non già contenutistici di conversazioni telefoniche, in ossequio ad una più rigorosa osservanza dei ruoli processuali, si ritiene necessario che anche l'acquisizione del tabulato telefonico sia acquisito solo dopo un vaglio giurisdizionale che decida sulla necessità del verificarsi di limitazioni di diritti fondamentali.

IX. Riconosciuta la diretta applicabilità della sentenza della Corte di giustizia UE, 2 marzo 2021, *H.K*., C-746/18, l'ulteriore questione attiene all'eventuale utilizzabilità del materiale probatorio acquisito in violazione di divieti costituzionali.
La Grande Camera si occupa anche delle conseguenze processuali di un'acquisizione illegittima, rammentando che, allo stato attuale del diritto dell'Unione, spetta, in linea di principio, al solo diritto nazionale stabilire le regole relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti criminali, di informazioni e di elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati in questione, contraria al diritto dell'Unione od anche mediante un accesso delle autorità nazionali ai dati suddetti, contrario a tale diritto dell'Unione.
Infatti, una consolidata giurisprudenza europea riconosce il "principio dell'autonomia procedurale", per cui, in assenza di norme dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro, stabilire le regole di procedura applicabili ai ricorsi giurisdizionali destinati a garantire la tutela dei diritti riconosciuti ai singoli dal diritto dell'Unione. Tuttavia, secondo la medesima giurisprudenza, tale principio di autonomia procedurale dello Stato vige in presenza di una duplice condizione: che le regole processuali nazionali in tema di utilizzabilità della prova illegittima non siano meno favorevoli di quelle disciplinanti nel diritto interno situazioni analoghe (principio di equivalenza) e che le regole nazionali non rendano impossibile in pratica o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività).
La Corte sottolinea che la necessità di escludere informazioni ed elementi di prova ottenuti in violazione delle prescrizioni del diritto dell'Unione deve essere valutata alla luce, in particolare, del rischio che l'ammissibilità di informazioni ed elementi di prova siffatti comporta per il rispetto del principio del contraddittorio e, pertanto, del diritto ad un "processo equo".
La Grande Camera enuncia quindi un vero e proprio "divieto di utilizzazione" della prova illegittima, affermando che "un organo giurisdizionale, il quale consideri che una parte non è in grado di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova rientrante in una materia estranea alla conoscenza dei giudici e idoneo ad influire in modo preponderante sulla valutazione dei fatti, deve constatare una violazione del diritto ad un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione siffatta".
E' estremamente importante l'affermazione della Corte secondo cui il principio di effettività impone al giudice penale nazionale, a causa della mancanza di contraddittorio, di escludere informazioni ed elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione incompatibile con il diritto dell'Unione, od anche mediante un accesso dell'autorità competente a tali dati in violazione del diritto dell'Unione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti di criminalità, "qualora tali persone non siano in grado di svolgere efficacemente le proprie osservazioni in merito alle informazioni e agli elementi di prova suddetti, riconducibili ad una materia estranea alla conoscenza dei giudici e idonei ad influire in maniera preponderante sulla valutazione dei fatti" .
Ma, riguardo all'accesso illegittimo ai dati (vuoi perché vi sia stata una conservazione generalizzata e indifferenziata, vuoi perché acquisiti dal pubblico ministero) è difficile ravvisare la violazione del principio del contraddittorio, in

quanto i dati, sia pure illegittimamente acquisiti, sono successivamente posti a disposizione delle parti e su di essi può quindi liberamente svolgersi il contraddittorio, per cui, nel caso specifico, non sembra possa intaccarsi l'"equo processo".
Forse, può invece invocarsi il "principio di equivalenza", sul fronte interno, per individuare il rimedio da applicarsi all'acquisizione dei tabulati in violazione delle regole individuate dalla Corte di giustizia U.E.
Infatti, la mancanza di regole processuali nazionali in tema di utilizzabilità dei dati del traffico o di localizzazione acquisiti illegittimamente, potrebbe essere superata con l'applicazione delle norme disciplinanti l'analoga situazione di un'intercettazione avvenuta illegittimamente, cioè in violazione della riserva di legge e di giurisdizione. Ne risulterebbe, in applicazione del "principio di equivalenza", l'applicazione della sanzione dell'inutilizzabilità, che l'art. 271 c.p.p. riserva ai casi di esecuzione delle intercettazioni al di fuori dei casi previsti dalla legge o di mancata autorizzazione del giudice.
La *quaestio iuris* attiene al problema se l'acquisizione dei cd. dati esteriori delle conversazioni telefoniche (e, dunque, l'individuazione dell'utenza chiamante, di quella chiamata, della data, dell'ora e durata della conversazione telefonica nonché delle località dalle quali proviene o si riceve la comunicazione telefonica) possa, in qualche modo, godere delle stesse garanzie costituzionali - estrinsecate negli artt. 266 e ss. c.p.p. - che, secondo l'interpretazione più restrittiva, si ritengono appannaggio esclusivo delle intercettazioni del contenuto delle medesime conversazioni.
X. Strettamente connessa alla problematica *de qua*, risulta, poi, essere quella concernente l'utilizzabilità o meno di tali acquisizioni probatorie in violazione della normativa in questione.
La sentenza interpretativa di rigetto dell'11 marzo 1993 n. 81 - ha rappresentato il primo importante tentativo di definire la questione giuridica che, già allora, aveva determinato opinioni oscillanti tra il preminente interesse di tutelare il diritto fondamentale della libertà e della segretezza delle comunicazioni e il quotidiano, pressante interesse di acquisire utili elementi di prova attraverso una procedura più agevole, meno rigorosa nelle forme e maggiormente flessibile rispetto all'intercettazione del contenuto delle conversazioni.
Orbene, la Consulta, pur prendendo le mosse dall'ampiezza della portata dell'art. 15 Cost. che, apprestando una specifica tutela alla libertà e alla segretezza della comunicazione, certamente ricomprende fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica, conclude nel senso di limitare la portata della normativa codicistica (artt. 266 - 271 c.p.p.) alle sole intercettazioni del contenuto di conversazioni o comunicazioni.
Il Legislatore ordinario, cioè, pur potendosi muovere legittimamente nei margini fissati dalla Carta fondamentale, avrebbe adottato un'interpretazione restrittiva del dettato costituzionale, escludendo dalle cautele approntate dagli artt. 266 e ss. c.p.p. (almeno fino alla L. n. 547/1993), l'acquisizione dei dati esteriori delle conversazioni telefoniche.
Tali conclusioni trovavano, peraltro, le proprie giustificazioni anche nel necessario contemperamento di due contrastanti interessi: nell'art. 15 trovano protezione due distinti interessi: quello inerente alla libertà e alla segretezza delle comunicazioni, riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'art. 2 Cost., e quello connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad

un bene anch'esso oggetto di protezione costituzionale (Corte Cost., v. anche sentt. nn. 120 del 1975, 98 del 1976, 223 del 1987 e 366 del 1991).
La stessa giurisprudenza della Consulta ha, in più occasioni, sottolineato la notevole capacità intrusiva […] di un'attività investigativa che coinvolga i tabulati (Corte cost., 188/2010), confermando che, per ogni cittadino, il ricorso a tale strumento d'indagine deve necessariamente essere soggetto alle garanzie previste dall'art. 15 Cost. (Corte cost., 38/2019).
XI. Orbene, quanto alla sorte dei tabulati del traffico telefonico acquisiti direttamente senza autorizzazione del giudice, il giudice della nomifilachia ha ritenuto che non sia utilizzabile il tabulato contenente l'indicazione dei dati esteriori delle conversazioni telefoniche...tutte le volte che sia stato acquisito agli atti senza l'autorizzazione motivata dell'autorità giudiziaria, includendo in tale nozione anche il PM (Cass., sez. un., 13 luglio 1998, n. 21).
Si considera infatti che il livello minimo di garanzia previsto dall'art. 15 Cost. sia condizione necessaria anche per l'acquisizione dei tabulati del traffico telefonico.
Una volta riconosciuta la segretezza anche dei dati esteriori della comunicazione, l'art. 15 Cost. impone il rispetto della duplice riserva di legge e di giurisdizione.
Tirando le file delle argomentazioni che precedono in presenza del conflitto tra fonti prima ricordato, l'intestato Tribunale ritiene che la parte dell'art. 132, comma 3, del codice della privacy, che autorizza il pubblico ministero a disporre con decreto l'acquisizione dei tabulati, non è più operativa, essendo necessario, per contro, richiedere a tal fine da subito l'autorizzazione a un giudice.
La necessità di disporre la diretta applicazione della norma UE, in vece di quella italiana, non sarebbe ostacolata dal fatto che la Corte di giustizia non abbia (inevitabilmente) indicato nella propria giurisprudenza un catalogo di reati specifico per cui l'autorità potrebbe legittimamente acquisire i dati in questione. La dimostrazione di ciò viene data sulla base del rilievo per cui la categoria delle "forme gravi di criminalità e la prevenzione di gravi minacce per la sicurezza pubblicata" indicata dalla Corte di giustizia quale indispensabile condizione per rendere proporzionata […] l'acquisizione dei dati, [sarebbe] facilmente individuabile con il rinvio integrale ai reati previsti nel catalogo dettato dagli articoli 266 c.p.p. e 266 *bis* c.p.p.
In conclusione l'estensione della disciplina legale in tema di intercettazioni di conversazioni e comunicazioni telefoniche all'acquisizione dei dati di identificazione dei soggetti e delle connotazioni spazio-temporali della comunicazione nella giurisprudenza di legittimità comporta – in assenza del decreto dell'autorità giudiziaria intesto quale Tribunale - la radicale sanzione dell'inutilizzabilità degli esiti di prova, è, quindi l'impossibilità di disporre l'intercettazione telefonica avente ad oggetto un numero telefonico individuato sulla scorta di tabulati telefonici acquisiti dal PM, trattandosi di inutilizzabilità conseguente ad un divieto di acquisizione della prova, ovvero a violazione espressamente comminata dalla legge ex art. 271 c.p.p.
Peraltro, nella categoria delle prove sanzionate, *ex* art. 191 c.p.p., dall'inutilizzabilità rientrano non solo quelle "oggettivamente vietate", ma anche le prove formate o acquisite in violazione dei diritti soggettivi tutelati dalla legge, e, a maggior ragione, trattandosi di libertà assolute indipendenti dal fenomeno normativo ordinario, direttamente dalla Costituzione.

Nell'uno e nell'altro caso, deve trovare, infatti, secondo tale autorevole orientamento, immediata applicazione la norma generale dell'art. 191 c.p.p., potendo discendere l'antigiuridicità della prova direttamente dalla violazione di divieti probatori ricavabili in modo diretto dal dettato costituzionale.

**P. Q. M.**

**NON CONVALIDA il decreto di intercettazione in premessa indicato.**
**NON AUTORIZZA l'intercettazione in premessa indica.**
Manda alla cancelleria per l’immediata restituzione degli atti al pm.
**Bari, 1° maggio aprile 2021, ore 12.00**

**Il G.I.P.**
**Dott. Francesco Agnino**