TRIBUNALE DI CATANIA

SEZIONE DEL GIUDICE PER LE INDAGINI PRELIMINARI

Ordinanza di rinvio pregiudiziale alla Corte di Giustizia dell'Unione europea

(con richiesta di procedimento accelerato)

- artt. 267 Trattato sul Funzionamento dell'Unione europea –

Il giudice per le indagini preliminari, Simona Ragazzi,
investito di richiesta del Pubblico Ministero presso la Procura della Repubblica di Catania di archiviazione del procedimento contro Ignoti (**n. 1206/2025 Reg. Notizie di reato Ignoti e 5030/2025 Reg. GIP Ignoti)** per il reato di sostituzione di persona (art. 494 del codice penale italiano);
attivato il contraddittorio tra le parti (Pubblico Ministero e persona offesa) all'udienza del 3 giugno 2025 (con prosecuzione all'udienza del 16 giugno 2025), ai sensi dell'art. 409 del codice di procedura penale, a seguito del mancato accoglimento della richiesta di archiviazione;
ritiene di dovere promuovere domanda di pronuncia pregiudiziale alla Corte di Giustizia della Unione Europea, affinché voglia pronunciarsi su questioni necessaria ai fini della decisione del caso in esame per le ragioni di seguito esposte.

I. Il procedimento principale

1. Il 30/1/2025 il Pubblico Ministero chiedeva allo scrivente Giudice per le Indagini Preliminari di autorizzare l'acquisizione dei dati esterni delle comunicazioni telematiche di seguito specificati, in base all'art. 132, comma 3, del Decreto Legislativo 30/6/2003 n. 196 (c.d. Codice in materia di protezione dei dati personali o Codice della Privacy) in un procedimento relativo al reato di sostituzione di persona ai sensi dell'art. 494 del codice penale (qualificazione, questa, frutto della revisione di quella iniziale, errata, di molestie o disturbo alle persone con il mezzo del telefono ai sensi dell'art. 660 del codice penale). Questi i fatti a sostegno. A.B., di anni 19, denunciava di essersi accorto circa un mese addietro della presenza *online* di un profilo Facebook avente numero identificativo "ID 123…", il quale riportava una sua foto personale come foto del profilo, il suo effettivo prenome e poi il suo cognome alla nascita, cognome che anni addietro egli aveva dismesso a favore di quello dei genitori adottivi in virtù di una legale procedura di adozione. Tale profilo social, a distanza di oltre un mese dalla prima scoperta, era ancora attivo e con i dati falsi e ingannevoli a lui riconducibili e da lui certamente non autorizzati. Nel profilo vi erano ulteriori riferimenti alla sua famiglia d'origine (ovvero la foto della sua sorella naturale, peraltro ancora minorenne, la quale era stata a sua volta adottata da un'altra famiglia, famiglia della quale aveva preso un ulteriore cognome, ed altri dati propri personali). Il Pubblico Ministero, sulla base della denuncia e della relazione della Polizia Postale - Centro Operativo per la Sicurezza Cibernetica della Sicilia orientale, chiedeva, pertanto, l'acquisizione dei ***file di log*** **inerenti all'account del profilo apparentemente**

***fake*, comprensivi di indirizzo IP, data e orari degli accessi nel periodo compreso dal 24/11/2024 alla data di notifica del provvedimento autorizzativo del Giudice**, decreto poi da notificarsi alla società gerente il social media, META Platforms Ireland Limited. Il Pubblico Ministero sottolineava trattarsi dell'unico strumento attraverso il quale sarebbe stato possibile risalire all'autore della creazione di un profilo *fake* ai danni del denunciante, del quale venivano abusivamente utilizzati i dati identificativi personali (nome e foto), addirittura facendo riemergere profili di una identità giuridica frattanto dismessa (ovvero il cognome della nascita) a scapito della nuova identità acquisita legalmente tramite adozione.

2. Il Giudice, pur condividendo l'indicazione del Pubblico Ministero per cui i chiesti dati telematici erano l'unico mezzo investigativo idoneo a permettere di identificare l'ignoto autore dei fatti, rigettava la richiesta, poiché il reato previsto dall'art. 494 del codice penale non consente l'acquisizione di dati telematici (ove intesi come dati di traffico) ai sensi dell'art 132 del Decreto Legislativo 196/2003, e ciò in quanto punito con la pena massima di un anno di reclusione, inferiore alla soglia minima richiesta dalla normativa sui dati di traffico (v. *infra*), né potendosi qualificare i fatti sotto uno degli ulteriori tipi di reato per i quali è possibile acquisire i dati di traffico telematico.

3. A seguito di tale decisione il Pubblico Ministero chiedeva al giudice l'archiviazione del procedimento, ritenendo di non potere andare avanti nelle indagini senza l'acquisizione dei file di log originariamente richiesti. Il giudice ha, tuttavia, fissato udienza ai sensi dell'art. 409, comma 2, del codice di procedura penale, ritenendo di non accogliere la richiesta di archiviazione e di dovere instaurare il contraddittorio tra le parti (nell'ambito delle relative udienze è stata acquisita una nota di chiarimenti tecnici elaborata dalla Polizia Postale - Centro Operativo per la Sicurezza Cibernetica della Sicilia orientale, mentre la persona offesa del reato, intervenuta, ha segnalato che il profilo Facebook *fake* è ancora attivo e ha illustrato in una nota scritta i danni che sta subendo). La decisione di non accogliere la richiesta di archiviazione e attivare il contraddittorio si è basata su una più meditata analisi della vicenda, idonea a condurre a un esito diverso, derivante dalla preliminare necessità di verificare **se il diritto dell'Unione europea**, alla luce della pertinente giurisprudenza della Corte di Giustizia della UE, **osti** alla **esclusione dei file di log dal novero dei "dati di *traffico* telematico"** e, comunque, se esso osti alla possibilità di autorizzare **l'accesso ai medesimi dati telematici (file di log quali qui richiesti), laddove essi siano gli unici e indispensabili a identificare l'autore di un reato, anche al di fuori delle forme di criminalità grave.** Interpellate in udienza le parti, le quali hanno aderito a quanto prospettato dal giudice, ne è scaturita la decisione di formulare richiesta di interpretazione pregiudiziale alla Corte di Giustizia dell'UE sull'art. 15 Direttiva 2002/58/UE.

II. Le norme di diritto nazionale di riferimento.

4. I fatti emersi dalla denuncia e dai primi accertamenti, compatibilmente con la fase delle indagini preliminari, vanno effettivamente inquadrati nel delitto di **sostituzione di persona previsto art. 494 del codice penale.**

5. Giurisprudenza consolidata e dottrina interne riconducono, infatti, univocamente ogni condotta consistente nella manipolazione o usurpazione dell'altrui identità digitale

o virtuale, accompagnata dalla finalità di vantaggio o di danno e dalla induzione in errore nei terzi, nel delitto di sostituzione di persona previsto dall'art. 494 del codice penale, la cui norma così recita:
«Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno».

6. Invero, la crescente diffusione delle interazioni sulla rete e l'attitudine sempre più pervasiva a costruire e svolgere relazioni umane di qualsivoglia natura (affettiva, sociale, economica, politica, etc.) negli spazi virtuali e nei domini digitali hanno portato al moltiplicarsi delle possibili identità di una persona fisica o giuridica, per cui oggi alla nozione di identità personale in senso naturalistico e anagrafico si affianca e si sostituisce sempre più l'identità digitale o virtuale, ovvero il complesso delle informazioni che servono a identificare un soggetto e ad accreditarlo come tale nel mondo virtuale. Allo stesso tempo, però, l'anonimato, la falsificabilità dei dati, la libertà e capillarità delle interazioni proprie del dominio cibernetico hanno altresì moltiplicato le forme di possibile utilizzo fraudolento dell'altrui identità digitale/virtuale.
All'esigenza di tutela tanto della identità digitale dei singoli utenti della rete quanto della fede pubblica dai potenziali abusi risponde, nel diritto interno, proprio la figura di reato, non di nuovo conio, prevista dall'art. 494 del codice penale.

7. A titolo di esempio, la Suprema Corte di Cassazione ha affermato che risponde del delitto previsto dall'art. 494 del codice penale chi sostituisce online alla propria identità quella di altri per la generalità degli utenti in connessione, indipendentemente dalla propalazione all'esterno delle diverse generalità utilizzate (Cassazione penale, Sez. V, sentenza n. 42572 del 22/06/2018, Rv. 274008-01); commette il reato anche chi crea un falso profilo Facebook con il quale contatta i conoscenti della vittima per rivelarne l'orientamento sessuale (Cassazione penale, sez. V, sentenza n. 38911 del 12/06/2018, dep. 24/8/2018). In termini simili, secondo Cassazione penale, sez. V, sentenza n. 33862 del 08/06/2018, dep. 19/7/2018, Rv. 273897 – 01, integra il delitto di sostituzione di persona la creazione ed utilizzazione di un profilo su social network, utilizzando abusivamente l'immagine di una persona del tutto inconsapevole, trattandosi di condotta idonea a rappresentare una identità digitale non corrispondente al soggetto che lo utilizza; nella specie, l'imputato aveva creato un profilo Facebook apponendovi la fotografia di una persona minorenne per ottenere contatti con persone minorenni e scambio di contenuti a sfondo erotico. Negli stessi termini si esprime la sentenza della Cassazione, Sez. V, n. 323/2022 del 14/10/2021, RV 282768–02, per cui integra il delitto di sostituzione di persona la condotta di colui che crea ed utilizza "profili social" e "account internet" servendosi dei dati anagrafici di altra persona, esplicitamente contraria, al fine di far ricadere su quest'ultima l'attribuzione delle connessioni eseguite in rete. La casistica è molto varia. Vi rientra anche la condotta di chi crea un account di posta elettronica o di home-banking mediante credenziali false, ossia ricorrendo ai dati identificativi di altra persona inconsapevole, al fine di procurarsi un ingiusto profitto con danno del titolare dell'identità abusivamente utilizzata, mediante operazioni di trasferimento di denaro (Cassazione, Sez. II, sentenza n. 23760 del 2/7/2020, Rv. 279585-01).

8. Il delitto di sostituzione di persona è, inoltre, considerato un reato "pluri-offensivo", tale cioè da offendere sia il bene della fede pubblica sia l'interesse del soggetto privato nella cui sfera giuridica l'atto di manipolazione sia destinato ad incidere concretamente (Cassazione, Sez. V, Sentenza n. 21574 del 27/3/2009, dep.25/5/2009, Rv. 243884-01).

9. I fatti per cui si procede integrano "sufficienti indizi" del reato di sostituzione di persona (tale è il parametro da soddisfare per acquisire i dati di traffico telefonico e telematico, nella fase delle indagini preliminari). Quanto prospettato dal denunciante, riscontrato dalla Polizia Giudiziaria, lascia, infatti, ipotizzare un tipico uso non autorizzato di elementi identificativi dell'altrui identità, quali le fotografie personali e il nome di battesimo, all'interno di un profilo social creato di proposito da terzi ignoti, con l'aggiunta di elementi ulteriori, in modo idoneo a trarre in inganno gli utenti della rete sulla reale identità del titolare di quell'account e in modo dannoso per il denunciante, del quale vengono rivelati un'identità anagrafica e l'originario contesto familiare, non più veritieri in ragione della adozione.

10. Come accennato, però, il reato previsto dall'art. 494 c.p., essendo punito con la pena massima di un anno di reclusione, non permette al giudice di autorizzare l'acquisizione di "dati del traffico telefonico e/o telematico", e ciò ove i file di log qui richiesti siano qualificati come dati di traffico.

11. La normativa italiana (articolo **132 del Decreto legislativo 30/6/2003 n. 196 – Codice in materia di protezione dei dati personali, c.d. Codice della Privacy)**, permette, infatti, l'acquisizione dei dati di traffico o di localizzazione delle comunicazioni elettroniche da parte dei fornitori di servizi di telecomunicazioni solo con riferimento a tipologie di reati, tra i quali non rientra quello in esame. Così dispone l'art. 132 citato:
«1. Fermo restando quanto previsto dall'articolo 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.
1-*bis*. 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.
2. [abrogato]
3. Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di 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 per l'accertamento dei fatti, i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, 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.
3-bis. Quando ricorrono ragioni di 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 48 successive, decide sulla convalida con decreto motivato.

[…]
3-*quater*.I dati acquisiti in violazione delle disposizioni dei commi 3 e 3-bis non possono essere utilizzati. […]».

12. In sintesi, il citato art. 132, comma 3, del Decreto legislativo 30/6/2003 n. 196 – Codice della privacy, incisivamente modificato con il decreto-legge 30 settembre 2021 n. 132, convertito nella Legge 23 novembre 2021 n. 178 al fine di conformare il quadro normativo interno ai principi enunciati dalla Corte di Giustizia dell'Unione europea nella sentenza del 02/03/2021 nella causa C-746/2018, EU:C:2021:152, permette l'accesso ai dati di traffico nell'ambito di indagini penali con decreto autorizzativo del Giudice per le Indagini preliminari, per due tipologie di reati: a) reati connotati da gravità, come definita sulla base della cornice edittale di pena (pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 c.p.p., tenendo conto della pena base e considerando le sole circostanze speciali o ad effetto speciale); b) reati di minaccia, molestia o disturbo alle persone con il mezzo del telefono – purché la minaccia, la molestia e il disturbo siano ritenute in concreto gravi. Circa questa seconda categoria – come si legge nella Relazione illustrativa del disegno di legge (v. Dossier di Senato della Repubblica n. 462/1 e Camera dei Deputati n. 483/1) – occorre tenere conto «che vi sono specifici reati, la cui pena edittale è inferiore, per i quali, però, la principale, se non unica, modalità di accertamento è da rinvenire esattamente nei dati del traffico telefonico (oltre che, quando la condotta è in atto, nelle intercettazioni telefoniche), reati cioè, che, al di là del dato sanzionatorio, possono in concreto manifestarsi come particolarmente gravi per beni primari della persona, soprattutto allorché prodromici a condotte estremamente più serie (di aggressione fisica), che spesso ne costituiscono lo sviluppo concreto, prevenibili solo a mezzo di mirati e tempestivi accertamenti; l'ulteriore limite della gravità in concreto delle condotte di minaccia, molestia o disturbo vale a ribadire l'esigenza di un rapporto di proporzionalità tra l'atto di indagine e i diritti compressi con esso».

13. La normativa del 2021 non considera, invece, l'eventuale ipotesi di reati, i quali, seppur non integranti forme di criminalità grave in astratto, siano commessi con mezzi telematici o informatici (come quello in esame) e possano parimenti essere accertati *soltanto* con dati di traffico telematico, similmente a quelli che possono essere commessi con il mezzo del telefono e suscettibili di essere accertati esclusivamente con dati di relativo traffico e geolocalizzazione, ai quali si è opportunamente riservata specifica considerazione.

14. Inoltre, la normativa italiana di settore appena richiamata non contiene uno specifico ed esplicito riferimento alle tipologie di dati di traffico telematico, né richiama espressamente i "*file di log*" quali dati di traffico telematico. Gli unici riferimenti utili sono costituiti dallo stesso art. 132 del Decreto legislativo n. 196/2003 e altresì dall'art. 121 dello stesso Decreto legislativo, che richiamano la categoria unica e unitaria dei "dati di traffico telematico", senza ulteriori specificazioni. L'art. 121, lett. h) citato definisce "dati relativi al traffico" come « *qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione* ».

15. La mancanza di una definizione esplicita dei dati di traffico telematico ha indotto la dottrina specialistica a evidenziare la coesistenza di una duplice possibile interpretazione degli articoli 121 e 132 del Decreto legislativo n. 196/2003 rispetto al tema della **riconducibilità o meno dei file di log alla nozione normativa di dati di traffico telematico**.

16. Secondo un primo orientamento i file di log andrebbero nettamente distinti dai dati di traffico [telematico] ai sensi dell'art. 132 D. Lgs. 196/2003. I *file di log* sarebbero, infatti, soltanto i dati sulla connessione assegnata ad un'utenza, cioè indirizzo IP di destinazione, che consente di identificare siti web visitati dall'utente, slegati da una qualsiasi comunicazione telematica tra due o più dispositivi connessi alla rete. Ne discende che, se i *file di log* non sono dati di traffico, perché non implicanti una "comunicazione" su una rete elettronica, essi non ricadono nell'ambito dell'articolo 132 D. Lgs. 196/2003 e possono essere acquisiti autonomamente con provvedimento, pur sempre motivato, del Pubblico Ministero sulla base di altre disposizioni di legge (quali gli artt. 234-bis e 256 del codice di procura penale) e a prescindere dall'aggancio a reati gravi.

17. Secondo un'altra linea interpretativa, vi sarebbe una perfetta coincidenza tra il concetto di *file di log* e quello di dati di traffico telematico previsti dall'art. 132 D. Lgs. 196/2003; anzi, soltanto i file di log conterrebbero dati di traffico telematico, indicando gli accessi alla rete effettuati, i siti web visitati, la durata della connessione, tutti dati, cioè, che comportano informazioni sulla vita privata e le scelte degli utenti della rete.

18. La Suprema Corte di Cassazione italiana, ad oggi, ha avuto modo di richiamare i file di log soltanto in passaggi incidentali di pochissime sentenze, aventi un oggetto specifico diverso, e dunque senza doverne esaminare compiutamente la natura ai fini che qui interessano (così le sentenze della Sez. V, n. 45278 del 26/10/2021, punto 1, pag. 1; Sez. V, n. 8968 del 24/2/2022, punti 2 e 4.3.1.). In una recente pronuncia (Sez. III, sentenza n. 18464 del 26.2.2025, dep. 16.5.2025, punto 6, pag. 3), invece, la Corte ha più esplicitamente menzionato i file di log in relazione al distinto ambito delle intercettazioni tra presenti con captatore informatico nello smartphone, rispetto alle quali i *file di log* fornirebbero tutte le informazioni relative al momento preciso della programmata captazione, della sua effettuazione e dell'ascolto, o della "smarcatura", dell'intercettazione così effettuata. La Corte ha premesso che «per file di log si intendono quei file in formato di testo, nei quali vengono indicate le operazioni compiute da un utente durante una sessione di lavoro del proprio dispositivo elettronico, quali, ad esempio, un personal computer, uno smartphone o un tablet. Come efficacemente sostenuto in dottrina, si tratta di vere e proprie "impronte digitali 2.0", particolarmente importanti in sede investigativa in quanto consentono di individuare molteplici profili relativi all'utilizzo dell'apparecchio, tra cui: a) gli orari e la durata della connessione ad Internet, con il relativo l'indirizzo IP (codice univoco che identifica un dispositivo su Internet o in una rete locale); b) le informazioni che questi ha inviato o ricevuto attraverso lo stesso indirizzo; c) l'anagrafica dell'intestatario di un contratto di utenza».

19. Pur in mancanza di un monitoraggio formale, si può affermare che nella prassi delle indagini penali prevale la tendenza a considerare i file di log, anche se rivolti solo a identificare l'autore del reato, "dati di traffico telematico" e, come tali, soggetti alle condizioni dell'art.132 del Decreto Legislativo 196/2003, con i limiti che ne derivano sull'accertamento di alcune figure di reato. La dottrina specialistica non manca di sottolineare

al riguardo che proprio il tenore non esplicito e chiaro delle norme richiamate può generare un certo "disorientamento definitorio" e quindi condurre a decisioni giudiziarie difformi.

20. Un ostacolo investigativo analogo a quello qui descritto e derivante dalla ricomprensione dei file di log nel novero dei dati di traffico si verifica, peraltro, anche in relazione ad **altre figure di reato,** ugualmente lesive di diritti personali. Si tratta, per esempio, di ulteriori delitti commessi sulla rete, dei quali si registra una crescente casistica giudiziaria, inquadrabili nella minaccia grave (prevista dall'art. 612 del codice penale con la reclusione fino a un anno) o nella tentata violenza privata, prevista dagli artt. 56 e 610 del codice penale con la pena massima di due anni e otto mesi di reclusione (è il caso, per esempio, estraneo a questo procedimento, ma realmente verificatosi, di chi, utente di piattaforma telematica che garantisce l'anonimato, minacci altro utente di un danno grave – la artificiosa creazione e divulgazione nella rete di immagini compromettenti di quest'ultimo – per costringerlo a una condotta non voluta, come inviargli immagini intime di sé).

21. In tali circostanze l'impossibilità di accedere ai file di log, costituenti l'unico strumento utile (e talvolta non sufficiente) a identificare l'autore del reato, rischia di creare **delle "zone franche di impunità" nell'universo digitale** e, quindi, di comportare la rinuncia in via pregiudiziale e generalizzata a porre le necessarie premesse per perseguire una intera gamma di reati, pur aventi un crescente impatto nella vita degli individui che sempre più frequentemente interagiscono in tale dimensione virtuale.

III. Il diritto dell'Unione europea di riferimento

22. Cardine e parametro essenziale di riferimento della disciplina interna dei Paesi della UE in materia di acquisizione dei dati esterni delle comunicazioni elettroniche, anche ai fini della prevenzione, dell'accertamento e della repressione dei reati, è costituito dalla Direttiva 2002/58/UE (soprattutto nel suo art. 15), disciplinante il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche, come interpretata nel tempo da plurime sentenze della Corte di Giustizia dell'Unione europea, alla luce dei diritti fondamentali stabiliti negli articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali della UE.

23. L'art. **15 dell**a **direttiva 2002/58/UE «Applicazione di alcune disposizioni della direttiva [95/46]»,** paragrafo 1, stabilisce: «Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.
A tal fine gli Stati membri possono tra l'altro adottare misure legislative, le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [TUE]».

24. La Corte di Giustizia dell'Unione europea ha chiarito che l'obbligo imposto da uno Stato membro ai fornitori di servizi di comunicazione elettronica, in forza di una normativa nazionale, di conservare i dati relativi al traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto degli **articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea**, relativi, rispettivamente, alla tutela della vita privata e alla protezione dei dati personali, ma anche dell'**articolo 11 della Carta**, relativo alla libertà di espressione. Inoltre, **l'articolo 52, paragrafo 1, della medesima Carta** ammette limitazioni all'esercizio dei menzionati diritti, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

25. Tra le pronunce della Corte di Giustizia pertinenti ai fini che qui interessano, si segnalano per estratto le seguenti.

26. Con la fondamentale **sentenza della Grande Sezione del 21 dicembre 2016 nelle cause riunite C-203/15 e C-698/15, Tele2 Sverige e Watson e a.,** ECLI:**EU:C:2016:970,** la Corte dichiarava che: 1) l'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, […..] 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; 2) l'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 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 dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione. […].

27. Nella successiva **sentenza** della **Grande Sezione del 2 ottobre 2018** nella **causa C-207/16, c.d. Ministerio Fiscal**, ECLI:EU:C:2018:788, sempre sul tema della soglia di gravità del reato che può giustificare l'accesso delle autorità nazionali ai dati di comunicazione elettronica, la Corte poneva un importante distinguo tra dati delle comunicazioni elettroniche che determinano una circoscritta intrusione nella sfera della vita privata, quali quelli meramente identificativi dei titolari di carte SIM attivate con un telefono cellulare, e dati comportanti una più elevata ingerenza nella vita privata e quindi suscettibili di fornire informazioni approfondite sulle abitudini di una persona. Rispetto alla prima categoria di dati la Corte riteneva possibile l'accesso ai dati per qualunque tipo di reato e non solo per le forme gravi di criminalità. «L'articolo 15, paragrafo 1, della direttiva 2002/58/CE …., letto alla luce degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un

telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta dei diritti fondamentali, che non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave».

28. La Corte ha, altresì, chiarito che l'accesso ai dati relativi al traffico e all'ubicazione conservati dai fornitori di servizi di comunicazione elettronica, a fini di prevenzione, ricerca, accertamento e perseguimento dei reati, può essere concesso ad autorità pubbliche, in applicazione di una misura legislativa adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, soltanto se e in quanto tali dati siano stati conservati da detti fornitori conformemente a direttiva [già in tal senso, La Quadrature du Net e a. C-470/21, punto 65 nonché giurisprudenza ivi citata].

29. Nella **sentenza della Grande Sezione del 2 marzo 2021 nella Causa C-746/18,** ECLI:EU:C:2021:152, la Corte ribadiva ancora che «….soltanto gli obiettivi di lotta contro le forme gravi di criminalità o di prevenzione di gravi minacce alla sicurezza pubblica sono atti a giustificare la grave ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta UE derivante dall'accesso delle autorità pubbliche a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, 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, senza 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, possano rendere l'obiettivo di prevenzione, ricerca, accertamento e generale perseguimento di reati idoneo a giustificare tale accesso [punto 35 e giurisprudenza ivi citata] ».

30. Nella **sentenza della Grande Sezione 30 aprile 2024 nella causa C-178/22,** ECLI: EU:C:2024:371, la Corte ha ribadito, in sintesi, che: a) la definizione dei reati, delle circostanze attenuanti e aggravanti e delle sanzioni riflette tanto le realtà sociali quanto le tradizioni giuridiche, che variano non solo tra gli Stati membri, ma anche nel tempo, e che tali realtà e tradizioni rivestono un'indubbia importanza nella determinazione dei reati considerati gravi; b) tenuto conto della ripartizione delle competenze tra l'Unione e gli Stati membri ai sensi del Trattato FUE e delle notevoli differenze esistenti tra gli ordinamenti giuridici degli Stati membri in materia penale, spetta agli Stati membri definire i «reati gravi» ai fini dell'applicazione dell'articolo 15, paragrafo 1, della direttiva 2002/58; c) la definizione dei «reati gravi» fornita dagli Stati membri deve rispettare i dettami di tale articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta; l'articolo 15, paragrafo 1, cit., nella misura in cui consente agli Stati membri di adottare misure legislative intese a «limitare» i diritti e gli obblighi previsti agli articoli 5, 6 e 9 della direttiva 2002/58 (derivanti dai principi di riservatezza delle comunicazioni e dal divieto di memorizzazione dei dati ad esse relativi), prevede un'eccezione alla regola generale dettata da detti articoli 5, 6 e 9 e deve, pertanto, secondo costante giurisprudenza, essere oggetto di un'interpretazione restrittiva. La deroga all'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati [non può diventare] la regola, salvo privare

l'articolo 5 di detta direttiva di gran parte della sua portata (v. sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 40).

31. La Corte ha poi chiarito nella medesima sentenza che l'articolo 15, paragrafo 1, terza frase, della direttiva 2002/58 impone che le misure adottate dagli Stati membri ai sensi di tale disposizione siano conformi ai principi generali dell'Unione, tra i quali il principio di proporzionalità, e devono assicurare il rispetto dei diritti fondamentali garantiti dagli articoli 7, 8 e 11 della Carta (v., in tal senso, sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 42). Pertanto, l'articolo 15, paragrafo 1, […] dev'essere interpretato nel senso che esso non osta a una disposizione nazionale che impone al giudice nazionale – in sede di controllo preventivo su richiesta motivata di accesso a dati relativi al traffico o all'ubicazione, idonei a permettere di trarre precise conclusioni sulla vita privata dell'utente di un mezzo di comunicazione elettronica, conservati dai fornitori di servizi di comunicazione elettronica, nell'ambito di un'indagine penale – di autorizzare tale accesso qualora sia richiesto ai fini dell'accertamento di reati puniti dal diritto nazionale con la pena della reclusione non inferiore nel massimo a tre anni, purché sussistano sufficienti indizi di tali reati e detti dati siano rilevanti per l'accertamento dei fatti, a condizione, tuttavia, che tale giudice abbia la possibilità di negare detto accesso se richiesto nell'ambito di un'indagine relativa a reato manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato.

32. Infine, nella **sentenza della Grande Sezione 30 aprile 2024 nella causa C-470/21** (c.d. ***Quadrature du Net 2***) la Corte ha stabilito a quali condizioni una normativa nazionale che autorizza l'autorità pubblica incaricata della protezione dei diritti d'autore e dei diritti connessi contro le violazioni di tali diritti commesse su Internet (costituenti reato) ad accedere ai dati, conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico, relativi all'identità civile corrispondenti a indirizzi IP precedentemente raccolti da organismi degli aventi diritto, affinché tale autorità possa identificare i titolari di tali indirizzi, utilizzati per attività che possono costituire violazioni del genere, e possa adottare, eventualmente, misure nei loro confronti, possa ritenersi rispettosa dell'art. 15, par. 1 Direttiva 2002/58/CE.

33. Nei par. 116 e 117 di tale sentenza la Corte significativamente afferma che: «occorre ricordare che, ai fini della necessaria conciliazione dei diritti e degli interessi in gioco imposta dal requisito di proporzionalità prescritto dall'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58, pur se la libertà di espressione e la riservatezza dei dati personali sono preoccupazioni primarie e gli utenti delle telecomunicazioni e dei servizi Internet devono avere la garanzia del fatto che la loro intimità e la loro libertà di espressione saranno rispettate, tali diritti fondamentali non sono assoluti. Infatti, al termine di un bilanciamento tra i diritti e gli interessi in gioco, talvolta questi ultimi devono cedere il passo dinanzi ad altri diritti fondamentali e ad imperativi di interesse generale quali la difesa dell'ordine pubblico e la prevenzione dei reati o la protezione dei diritti e delle libertà altrui. Ciò si verifica, in particolare, qualora la preponderanza accordata a dette preoccupazioni primarie sia atta a ostacolare l'efficacia di un'indagine penale, in particolare rendendo impossibile o eccessivamente difficile l'identificazione effettiva dell'autore di un reato e l'imposizione di una sanzione nei suoi confronti (v., per analogia, Corte EDU, 2 marzo 2009, K.U. c. Finlandia, CE:ECHR:2008:1202JUD000287202, § 49).

In tale contesto, si deve tenere debitamente conto del fatto che, come già dichiarato dalla Corte, **nel caso di reati commessi online, l'accesso agli indirizzi IP può costituire l'unico strumento di indagine che permetta di identificare la persona alla quale tale indirizzo era attribuito al momento della commissione di detto reato** (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 154) ».

IV. I motivi che rendono necessario il rinvio pregiudiziale.

34. Il presente rinvio pregiudiziale scaturisce dalla necessità di verificare, alla luce della evoluzione del diritto dell'Unione europea come interpretato dalla Corte di giustizia della stessa, anche in relazione alla crescita esponenziale delle forme di cybercriminalità e alla corrispondente e sottostante evoluzione tecnologica, se i file di log richiesti nel caso in esame e in tutta una classe di vicende simili, ove costituiscano imprescindibili elementi per identificare l'autore delle condotte di reato ipotizzate, possano non qualificarsi come "dati di traffico" ed essere, pertanto, acquisiti con diverse modalità, ovvero – in subordine –se, laddove ritenuti dati di traffico, possano comunque essere acquisiti anche a prescindere dalla qualificazione di "criminalità grave" dei reati ai quali si riferiscono.

35. In altri termini, l'impossibilità di autorizzare l'accesso ai dati telematici costituenti file di log nel caso in esame induce il giudice a interrogarsi sulla portata dell'articolo 15, paragrafo 1, della direttiva 2002/58/UE con riferimento alla possibilità di qualificare effettivamente i *file di log*, ove mirati esclusivamente a identificare l'autore di una condotta tenuta sulla rete, nell'alveo dei "dati di traffico" intesi come dati idonei a consentire di trarre conclusioni precise riguardo alla 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, […] dati idonei a fornire gli strumenti per stabilire il profilo delle persone interessate, informazione tanto sensibili, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni (sentenza C 203-15 e 698-15 Telesverige, EU:C:2016:970, punto 99; sentenza C 207-16 Ministerio Fiscal, EU:C:2018:788, punto 54; sentenza C-178-22, punto 39).

36. Come ricordato, la CGUE ha avuto modo di affermare che, quanto più grave è l'ingerenza nella vita privata e nella riservatezza delle comunicazioni elettroniche, tanto più la facoltà di chiedere l'acquisizione di dati ai fornitori a fini di indagine penale deve essere circoscritta alle gravi forme di criminalità. Pertanto, ingerenze di ampiezza assai minore, come la acquisizione di dati inerenti alla identità civile di un utente (elementi identificativi del titolare di una carta SIM attivata con un telefono cellulare rubato, come il cognome, il nome, l'indirizzo, oggetto del caso Ministerio Fiscal C-207/16, cit.) possono essere oggetto di accesso alle autorità, a fini di accertamento di qualsivoglia tipo di reato, e non solo di quelli gravi.

37. I file di log, almeno della tipologia di quelli richiesti nel caso in esame, invero non considerati espressamente in precedenti pronunce della Corte di Giustizia della UE, se è vero che da un lato non si risolvono in un insieme di dati informativi 'statici', come quelli anagrafici del caso c.d. Ministerio Fiscal C-207/16 (nome, cognome, indirizzo del titolare di una carta SIM o di un account) e come l'indirizzo IP del caso c.d. Quadrature du Net

2 C-470/21, rappresentando piuttosto una *sequenza* di dati temporali (accessi e uscite in una certa fascia temporale), dall'altro parrebbero non possedere quella caratteristica tipica riconosciuta ai "dati di traffico" nel significato del diritto euro-unitario, ovvero quella di consentire di trarre conclusioni precise sulla vita privata e le scelte di vita della persona 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 tenute, gli ambienti sociali frequentati.

38. Come si ricava, infatti, anche dalla **nota esplicativa elaborata dal dirigente della Polizia Postale - Centro Operativo per la Sicurezza Cibernetica della Sicilia orientale in data 10/6/2025, integrata il 16/6/2025,** prodotta dal Pubblico Ministero in udienza a seguito di chiarimenti chiesti dal giudice (fogli 29-34 del fascicolo del proc. allegato), tali dati, ancorché essenziali ai fini di indagine, hanno una valenza informativa assai più limitata dal punto di vista dell'ingerenza nella vita privata degli utenti della rete. In particolare, si chiarisce nella citata nota che nelle comunicazioni telematiche i file di log sono file di testo in cui si registrano in ordine cronologico e, pertanto, in sequenza le attività e le informazioni relative ad un sistema di comunicazioni; il file di log è, in altri termini, un registro dettagliato nel quale si può dare atto delle possibili seguenti vicende: a) accessi ed uscite (log-in e log-out) di un utente del sistema o applicazione con relativi indirizzi IP e marche temporali *timestamp*; b) operazioni compiute dall'utente, quali invio di messaggi, richiesta di un servizio o di una risorsa, eccetera); c) errori o malfunzionamento del sistema. **I file di log specificamente richiesti nelle indagini in esame forniscono esclusivamente: I) indirizzi IP di creazione del profilo social di un soggetto, non sempre associato a data e ora *timestamp*, con eventuale numero telefonico e/o indirizzo di posta elettronica verificati; II) indirizzi IP - con data e ora - degli accessi al profilo nel periodo richiesto (da una certa data e ora a un'altra data e ora) e per periodi temporali massimi comunque limitati**.

39. Se ne può, peraltro, concludere che i file richiesti, per la loro stessa natura, sono finalizzati esclusivamente a identificare l'autore di una condotta (quella tenuta sulla rete e per la quale si indaga) e non sono, invece, suscettibili di fornire informazioni più ampie e approfondite sulla vita privata le abitudini delle persone i cui dati sono stati conservati.

40. Tali dati, come si sottolinea sia nella citata nota della Polizia Postale sia nella richiesta di archiviazione del Pubblico Ministero, rappresentano un elemento necessario al prosieguo dell'indagine nelle sue fasi iniziali, e ciò sebbene possano, in ultima analisi, perfino non rivelarsi sufficienti per l'esatta identificazione dell'autore del reato. Inoltre, la società statunitense META Platforms Ireland Limited rientra tra i provider stranieri che collaborano con le forze di polizia da lungo tempo (anche prima della riforma normativa italiana di cui al Decreto Legge n. 132/2021, convertito nella Legge n. 178/2021) e ai fini dell'acquisizione dei file di log e in vicende che non rientrano in casi di urgente necessità per pericolo di vita, richiedono un provvedimento dell'autorità giudiziaria, ivi compreso un provvedimento del Pubblico Ministero e – nel vigore della precedente disciplina italiana – anche in relazione al delitto di sostituzione di persona previsto in Italia dall'art. 494 del codice penale (diverso è il caso di altre figure di reato, rispetto alle quali non sarebbe soddisfatto il principio della doppia incriminazione, come, per esempio la diffamazione online).

41. Ciò chiarito, un'interpretazione tendente a escludere i file di log dal novero dei dati di traffico nel significato proprio dell'articolo 15 della direttiva 2002/58/UE, si può ricavare dal testo del **Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio del 12 luglio 2023 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali** (parte del c.d. *E-Evidence Package* dell'Unione Europea).

42. Tale corpus normativo, che è già in vigore dal 20° giorno successivo alla pubblicazione sulla GU della UE del 28 luglio 2023, ma che sarà operativo dal 26 agosto 2026 (cfr. art. 34), definisce, secondo regole certe e uniformi, forme di cooperazione diretta e più agile tra autorità giudiziarie o autorità inquirenti autorizzate a raccogliere prove nei rispettivi sistemi nazionali dei Paesi UE e «fornitori di servizi di comunicazioni elettroniche», ai fini della produzione e della conservazione provvisoria di prove elettroniche, sulla base di decisioni giudiziarie veicolate da «certificati» dal contenuto definito (Certificato di ordine europeo di produzione - EPOC, e Certificato di ordine europeo di conservazione - EPOC-PR), obblighi di risposta da parte dei fornitori, motivi di eventuale rifiuto codificati, tempistiche certe, piattaforme di comunicazione interconnesse, sicure e definite.

43. Tale quadro giuridico, sebbene concerna non la generalità dei casi di acquisizione di dati esterni delle comunicazioni, ma solo quelli forniti da provider di *determinati* servizi e che siano stabiliti in *altro* Stato UE rispetto all'autorità giudiziaria che mira ad acquisirli e dunque in un ambito di cooperazione giudiziaria e diretta con i provider e le AG degli Stati di stabilimento, costituisce già parte integrante del diritto dell'Unione europea e cruciale base di rinnovata interpretazione della materia, anche perché adottato sulla scorta di una consapevole assimilazione della giurisprudenza della Corte di Giustizia della UE formatasi sul tema dei dati di traffico e di geolocalizzazione.

44. Ora, l'art. 3 del Regolamento ("Definizioni") distingue nettamente i "**dati richiesti al solo scopo di identificare l'utente**" (indicati come gli indirizzi IP e, se necessario, le porte sorgenti e le marche temporali pertinenti, vale a dire la data e l'ora, o gli equivalenti tecnici di tali identificativi e le informazioni connesse, se richiesto dalle autorità di contrasto o dalle autorità giudiziarie al solo scopo di identificare l'utente in una specifica indagine penale (**punto 10**), da un parte, e i "**dati sul traffico"** (indicati come i dati riguardanti la fornitura di un servizio offerto da un prestatore di servizi, che servono per fornire informazioni di contesto o supplementari sul servizio e che sono generati o trattati da un sistema di informazione del prestatore di servizi, come la fonte e il destinatario di un messaggio o altro tipo di interazione, sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, e altre comunicazioni elettroniche e i dati, diversi dai dati relativi agli abbonati, relativi all'inizio e alla fine di una sessione di accesso utente a un servizio, come la data e l'ora d'uso, la connessione al servizio (log-in) e la disconnessione (log-off) dal medesimo (**punto 11**), dall'altra parte.

45. L'art. 5 del Regolamento, nello stabilire le condizioni per emettere gli Ordini europei di produzione, in linea con l'art. 3, definisce il tipo di reati per i quali possono essere richiesti e ottenuti i *dati.* Per i dati relativi agli abbonati e i dati richiesti al solo scopo di

identificare l'utente (ritenuti dati meno sensibili), ivi compresi quelli di cui al punto 10) dell'art. 3, l'ordine di produzione può disporsi per qualsiasi tipo di reato; per i dati relativi al traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente ai sensi del presente Regolamento (cioè, ancora i dati del punto 10), e dati di contenuto, vi è il limite dei gravi reati. Di seguito il testo della norma:
<<Articolo 5. Condizioni di emissione dell'ordine europeo di produzione.
L'autorità di emissione può emettere un ordine europeo di produzione laddove siano soddisfatte le condizioni stabilite dal presente articolo.
L'ordine europeo di produzione è necessario e proporzionato ai fini del procedimento di cui all'articolo 2, paragrafo 3, tenuto conto dei diritti della persona oggetto di indagini o imputata, e può essere emesso solo se un ordine dello stesso tipo avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo.
L'ordine europeo di produzione per ottenere dati relativi agli abbonati o per ottenere dati richiesti al solo scopo di identificare l'utente, quali definiti all'articolo 3, punto 10), può essere emesso per qualsiasi reato e per l'esecuzione di una pena o di una misura di sicurezza detentiva di almeno quattro mesi, a seguito di un procedimento penale, irrogata con decisione non pronunciata in contumacia, nei casi in cui la persona condannata è latitante.
Un ordine europeo di produzione per ottenere dati sul traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente, quali definiti all'articolo 3, punto 10), del presente regolamento, o per ottenere dati relativi al contenuto è emesso solo:
a) per i reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno tre anni; oppure
b) per i seguenti reati, se commessi in tutto o in parte a mezzo di un sistema di informazione:
    i) i reati definiti agli articoli da 3 a 8 della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio;
    ii) i reati definiti agli articoli da 3 a 7 della direttiva 2011/93/UE;
    iii) i reati definiti agli articoli da 3 a 8 della direttiva 2013/40/UE;
c) per i reati definiti agli articoli da 3 a 12 e all'articolo 14 della direttiva (UE) 2017/541;
d) per l'esecuzione di una pena o di una misura di sicurezza detentiva di almeno quattro mesi, a seguito di un procedimento penale, irrogata con decisione non pronunciata in contumacia, nei casi in cui la persona condannata è latitante, per i reati di cui alle lettere a), b) e c) del presente paragrafo. […]>>.

46. Ora, i dati elencati nel punto 10) dell'articolo 3 del Regolamento paiono essere perfettamente sovrapponibili ai dati telematici del tipo file di log richiesti nel presente procedimento (accessi ed uscite, ovvero log-in e log-out, di un utente del sistema o applicazione con relativi indirizzi IP e marche temporali *timestamp*, ossia in un certo arco temporale) richiamati anche dai considerando 32, 33, 34 del medesimo Regolamento.

47. Così testualmente il considerando 32: <<Gli indirizzi IP, come pure i numeri di accesso e le relative informazioni, possono rappresentare un punto di partenza fondamentale per le indagini penali in cui l'identità di un indagato non è nota. Tipicamente essi costituiscono componenti di una registrazione di eventi, anche conosciuta come «log server», che indica l'inizio e la fine di una sessione di accesso utente a un servizio. Il più delle volte si tratta di un indirizzo IP, statico o dinamico, o di un altro identificatore che individua l'interfaccia di rete usata durante la sessione di accesso. Sono necessarie

informazioni correlate sull'inizio e la fine di una sessione di accesso utente a un servizio, quali porte sorgenti e marche temporali o equivalenti, in quanto gli indirizzi IP sono spesso condivisi tra utenti, ad esempio quando sono in essere servizi di traduzione degli indirizzi di rete di livello carrier (CGN) o equivalenti tecnici. Tuttavia, in conformità dell'*acquis* dell'Unione, gli indirizzi IP devono essere considerati quali dati personali e devono godere di piena protezione a norma dell'*acquis* dell'Unione sulla protezione dei dati. Inoltre, in determinate circostanze, gli indirizzi IP possono essere considerati dati relativi al traffico. In alcuni Stati membri anche i numeri di accesso e le relative informazioni sono considerati dati relativi al traffico. Tuttavia, ai fini di un'indagine penale specifica, le autorità di contrasto possono dover richiedere un indirizzo IP, nonché i numeri di accesso e le relative informazioni al solo fine di identificare l'utente prima che i dati relativi agli abbonati collegati a quell'identificativo possano essere richiesti al prestatore di servizi. In tali casi, è opportuno applicare lo stesso regime applicabile ai dati relativi agli abbonati, quali definiti nel presente Regolamento>>.
48. Il successivo considerando 34 sottolinea che <<l'intensità dell'impatto sui diritti fondamentali varia a seconda delle categorie, in particolare tra i dati relativi agli abbonati e i dati richiesti al solo scopo di identificare l'utente ai sensi del presente regolamento, da un lato, e i dati relativi al traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente ai sensi del presente regolamento, e i dati relativi al contenuto, dall'altro. Mentre i dati relativi agli abbonati nonché gli indirizzi IP, i numeri di accesso e le relative informazioni, se richiesti al solo scopo di identificare l'utente, potrebbero essere utili per ottenere i primi indizi in un'indagine sull'identità dell'indagato, i dati relativi al traffico, ad eccezione dei dati richiesti al solo scopo di identificare l'utente ai sensi del presente regolamento, e i dati relativi al contenuto sono spesso più pertinenti come materiale probatorio>>.

49. Nell'ipotesi in cui si potesse aderire con certezza interpretativa a tale criterio discretivo, si arriverebbe alla conclusione che nel presente caso l'accesso a tali file di log, non avendo a oggetto “dati di traffico [telematico]” può ricadere, anziché nell'articolo 132 del Codice della privacy (con il vincolo della natura dei reati per cui si procede e del decreto autorizzativo del giudice), in altre disposizioni del codice di procedura penale, quali, in particolare, l’articolo 234-bis del codice di procedura penale (in caso di dati acquisiti da provider stabilito all’estero) e 256 del codice di procedura penale (in caso di dati da acquisire da provider italiano, in quanto esercente pubblico servizio), che consentono al Pubblico Ministero di acquisire tali dati senza dover chiedere autorizzazione giudiziaria.

50. Così recita l’art. 234-bis c.p.p.: «Acquisizione di documenti e dati informatici- 1. È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare».
Così recita l’art. 256 c.p.p. - Dovere di esibizione e segreti: «1. Le persone indicate negli articoli 200 e 201 [norma questa del codice di proc. penale, che richiama anche le figure dei pubblici impiegati e degli incaricati di un pubblico servizio: n.d.r.] devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo

che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione».

51. In via subordinata, ove si accedesse, invece, alla conclusione per cui anche questo genere di file di log ricadono nell'area dei "dati di traffico", perché parimenti tali da consentire di ricavare informazioni precise e sensibili sulla vita privata e le abitudini delle persone coinvolte i cui dati sono conservati, ci si permette di chiedere se l'articolo 15 della Direttiva 2002/58/UE possa essere interpretato nel senso di ritenere proporzionato e conforme agli articoli 7, 8, 11 e 52 della Carta dei diritti fondamentali della Unione europea l'accesso a tali dati (file di log nei termini qui rappresentati), **per tutti i reati commessi attraverso strumenti informatici o telematici**, ancorché non definibili come "grave forma di criminalità", come definita dagli Stati membri della UE, **laddove tali dati siano indispensabili alla identificazione dell'autore del reato.**

52. È opportuno ribadire che senza i dati telematici qui descritti non si possono porre le condizioni basilari per l'identificazione degli autori dei reati, con conseguente frustrazione della tutela delle vittime dei reati. Appare, altresì, opportuno ricordare che l'ordinamento dell'Unione europea accorda particolare rilievo alla tutela delle vittime dei reati, come attesta, tra l'altro, anche la **Direttiva 2012/29/UE del Parlamento europeo e del Consiglio del 25 ottobre 2012**, che (sia pure in specifici ambiti) istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato.

53. Ed invero, l'acquisizione dei dati conservati dai fornitori di servizi potrebbe ritenersi legittima e proporzionata (salva ogni valutazione del caso concreto, come da sentenza della Corte di Giustizia nella causa C-178-22, prima citata) per qualsiasi reato commesso mediante lo sfruttamento del computer o comunque della rete digitale, in ragione del fatto che i primi elementi essenziali identificativi dei potenziali autori di tali reati, per le intrinseche modalità esecutive di detti reati, non possono che provenire dall'accesso ai dati esterni delle comunicazioni elettroniche conservati dai gestori dei relativi servizi e rilevanti ai sensi dell'art. 15 della Direttiva 2002/58, ivi compresi i file di log.

54. Tale necessità emerge dal costante aggiornamento ed espansione delle *new technologies* e della parallela evoluzione dei costumi sociali, che vedono in maniera sempre più massiccia gli individui interagire fra loro stabilendo relazioni amicali, affettive, finanziarie, commerciali anche solo ed esclusivamente attraverso la rete con le sue peculiari caratteristiche di anonimato, diffusività, volatilità, a-territorialità, transnazionalità.

55. La preclusione all'accesso ai dati delle comunicazioni elettroniche in condotte apparentemente non gravi – come il furto di identità digitale, la tentata violenza privata, la minaccia tra due soggetti – può risultare ancora più irragionevole ove si osservi che le condotte tenute per via digitale e telematica, ad esempio tra utenti di app e/o piattaforme, sono solitamente visibili a una vasta platea di ulteriori fruitori di tali spazi virtuali e, quindi, espongono la persona offesa, bersaglio dell'altrui azione malevola (la quale, invece, si può fare scudo dell'anonimato della rete stessa), a un danno di immagine intrinseco e amplificato, che detta persona offesa non può controllare, se non attivando un procedimento penale (ove ne ricorrano gli ulteriori presupposti).

56. In definitiva, possono venire in rilievo quelle stesse **esigenze di rispetto della vita privata e della vita familiare e di protezione dei dati di carattere personale sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali della Unione europea**, evocate dalla giurisprudenza della Corte di Giustizia quale fondamentale parametro di proporzionalità nel bilanciamento tra esigenze di tutela dei privati ed esigenze di accertamento dei reati.

57. Ancora il Regolamento (UE) n.1543/2023 può fornire utili riferimenti al riguardo. Il considerando 41 precisa che "Esistono reati specifici per i quali le prove sono tipicamente disponibili esclusivamente in formato elettronico, per natura particolarmente effimero. Si tratta dei reati connessi all'informatica, anche quando non sono considerati gravi di per sé ma potrebbero causare un danno esteso o considerevole, in particolare i reati che comportano un effetto individuale scarso, ma un danno complessivo di elevato volume. Per la maggior parte dei reati commessi a mezzo di un sistema d'informazione, l'applicazione della stessa soglia fissata per gli altri tipi di reato comporterebbe l'impunità nella maggior parte dei casi. Questa considerazione giustifica l'applicazione del presente regolamento per tali reati anche qualora comportino una pena detentiva della durata massima inferiore a tre anni».

58. Quanto alla specifica rilevanza del furto di identità digitale, che nel diritto interno ricade nel reato di sostituzione di persona, previsto dall'art. 494 del codice penale, oggetto di questo procedimento, la crescente considerazione che esso è destinato a ricevere nel diritto della Unione europea si può ricavare dalla **Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione**, la quale, pur avendo a oggetto – nel suo articolato – una serie di gravi reati costituenti attacchi contro sistemi di informazione, nel considerando 14 sottolinea che «Altro elemento importante di un approccio integrato alla criminalità informatica è l'istituzione di efficaci misure contro il furto d'identità e altri reati connessi all'identità. L'eventuale bisogno di un'azione dell'Unione contro tale tipo di comportamento criminale potrebbe anche essere considerato nel contesto di una valutazione della necessità di uno strumento orizzontale e globale dell'Unione».
Il Parlamento e il Consiglio, dunque, già nel 2013 mettevano in guardia sulla necessità di assicurare misure efficaci contro tutte le forme di usurpazione di identità consumate attraverso la rete, rinviando a una futura azione di diritto euro-unitario. E se ciò costituiva un'esigenza già avvertita ed esplicitata nel 2013, lo è ancora di più oggi, a fronte della già ricordata crescita esponenziale e pervasiva dell'uso della rete telematica nelle relazioni umane, sociali, economiche e nel dibattito pubblico, e di un livello sempre più sofisticato di tecnologia a disposizione, l'una e l'altra generando occasioni crescenti di potenziale abuso e manipolazione dell'altrui identità digitale.

59. Un utile termine di paragone è, infine, costituito dalla **legislazione francese** su una figura di reato del tutto assimilabile al delitto italiano di sostituzione di persona in ambito digitale e sul relativo regime di acquisizione dei dati di traffico telematico.

60. Il delitto di usurpazione di identità ("usurpation d'identité"), previsto dall'Articolo 226-4-1 del Codice penale[1] punisce l'usurpazione dell'identità di un terzo o l'utilizzo

[1] **Article 226-4-1 du Code pénal (« usurpation d'identité")** : *« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa*

di uno o più dati di qualsiasi tipo che consentano di identificarlo al fine di turbare la sua tranquillità o quella altrui, o [al fine] di ledere il suo onore o la sua reputazione con la pena massima di un anno di reclusione e 15.000 € di ammenda. Il reato è punito con le stesse pene se commesso su una rete di comunicazione pubblica *online*.

61. Sul versante della acquisizione processuale dei dati di traffico e di localizzazione, l'articolo 60-1-2 del codice di procedura penale francese[2], introdotto con legge del 02/03/2022, prevede due condizioni: 1) la prima è che le esigenze del procedimento lo richiedano, donde la necessità di una argomentazione specifica nel processo verbale degli inquirenti per giustificare l'esigenza di acquisizione e permettere il controllo da parte del giudice; 2) la seconda inerisce al perimetro edittale di pena dei reati legittimanti l'acquisizione, per cui deve trattarsi di crimini o delitti (*crimes ou délits*) puniti con la pena massima pari ad almeno tre anni di reclusione (con ciò ottemperandosi alla interpretazione della Corte di Giustizia dell'Unione europea sulla necessaria *gravità* dei reati che possono giustificare l'intrusione nella vita privata derivante dall'acquisizione dei dati di traffico e geolocalizzazione), ovvero, per rispondere all'esigenza di non lasciare fuori reati aventi una intrinseca portata di cybercriminalità, delitti puniti con la pena massima di almeno un anno di reclusione, se commessi con l'utilizzazione di una rete di comunicazione elettroniche e l'acquisizione dei dati di traffico abbia come unico scopo identificare l'autore dell'infrazione penale. Ciò permette di includere, per esempio, proprio reati come la *usurpation d'identité* o furto di identità digitale.

62. Tutto ciò premesso, si sottopone all'attenzione della Corte l'opportunità di trattare la causa con il procedimento accelerato di cui all'art. 105 del Regolamento di procedura della Corte. Sebbene non vi siano indagati identificati, è noto che i dati esterni delle comunicazioni elettroniche sono conservati dai fornitori di servizi digitali per un arco limitato di tempo. Pertanto, il protrarsi del tempo potrebbe frustrare in modo definitivo la possibilità di acquisire tali dati ove ciò sia considerato legalmente possibile dalla Corte.

---

tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, ***est puni d'un an d'emprisonnement*** *et de 15 000 € d'amende.*
Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.
Lorsqu'ils sont commis par le conjoint ou le concubin de la victime ou par le partenaire lié à la victime par un pacte civil de solidarité, ces faits sont punis de deux ans d'emprisonnement et de 30 000 euros d'amende».

[2] **Article 60-1-2** (Version en vigueur depuis le 04 mars 2022) :
Création LOI n°2022-299 du 2 mars 2022 - art. 12
A peine de nullité, les réquisitions portant sur les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés mentionnées au 3° du II bis de l'article L. 34-1 du code des postes et des communications électroniques ou sur les données de trafic et de localisation mentionnées au III du même article L. 34-1 ne sont possibles, si les nécessités de la procédure l'exigent, que dans les cas suivants:
1° La procédure porte sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement ;
2° La procédure porte sur un délit puni d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques et ces réquisitions ont pour seul objet d'identifier l'auteur de l'infraction ;
3° Ces réquisitions concernent les équipements terminaux de la victime et interviennent à la demande de celle-ci en cas de délit puni d'une peine d'emprisonnement;
4° Ces réquisitions tendent à retrouver une personne disparue dans le cadre des procédures prévues aux articles 74-1 ou 80-4 du présent code ou sont effectuées dans le cadre de la procédure prévue à l'article 706-106-4.

Inoltre, la causa solleva questioni interpretative suscettibili di produrre conseguenze immediate rispetto ai procedimenti penali pendenti in fase di indagini preliminari simili a questa, tanto nell'ordinamento italiano quanto negli ordinamenti degli altri Stati Membri, procedimenti rispetto ai quali si manifestano le stesse esigenze di acquisizione tempestiva dei dati conservati dagli Internet service provider.

V. Questioni pregiudiziali sottoposte alla Corte di Giustizia

Per le ragioni sopra esposte,
il giudice
SOSPENDE il procedimento in corso;
RINVIA sulla base dell'art. 267 par. 1 lett. b) T.F.U.E. alla Corte di Giustizia dell'Unione Europea, affinché voglia pronunciarsi sulle seguenti **questioni pregiudiziali,** come da quesiti di seguito articolati:

1. se l'articolo 15, paragrafo 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, modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25/11/2009, letto alla luce degli articoli 7, 8, 11 e 52 della Carta dei diritti fondamentali dell'Unione europea e nel quadro della nuova disciplina della prova elettronica (artt. 3, 5 Regolamento 1543/2023), può essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati telematici definibili come *file di log*, consistenti in accessi ed uscite (log-in e log-out) di un utente del sistema o applicazione con relativi indirizzi IP e marche temporali (ossia relativi a un certo arco temporale) e ove questi mirino soltanto a identificare l'autore di un reato – in materia di prevenzione, ricerca, accertamento e perseguimento dei reati –, comporti un'ingerenza nei diritti fondamentali dei soggetti ai quali i dati si riferiscono, che – diversamente dai dati di traffico e geolocalizzazione – non presenti una gravità tale da dover limitare il suddetto accesso alla lotta contro la criminalità grave, potendo invece estendersi alla generalità dei reati;

2. in subordine, laddove la Corte ritenga che l'accesso ai file di log (consistenti in accessi ed uscite, ovvero log-in e log-out, di un utente del sistema o applicazione con relativi indirizzi IP e marche temporali), sebbene questi siano mirati al solo scopo di identificare l'autore di un reato, possa comportare un'ingerenza grave nei diritti fondamentali dei soggetti ai quali i dati si riferiscono, come sanciti dalla Carta dei diritti fondamentali, se l'articolo 15 della Direttiva 2002/58/UE possa essere interpretato nel senso che l'esigenza di accertare e perseguire i reati commessi attraverso la rete telematica – laddove l'autore possa essere identificato unicamente mediante l'acquisizione di dati telematici, quali i citati file di log, e tenuto conto della tipica anonimizzazione della rete – sia idonea a giustificare l'accesso ai dati personali trattati dai service providers (compresi i dati di traffico e localizzazione), a prescindere dalla "gravità" di detti reati, come definita dagli Stati, e dunque se una legislazione nazionale che ciò preveda possa ritenersi appropriata, proporzionata allo scopo perseguito e necessaria in una società democratica, anche avuto riguardo alla salvaguardia del diritto alla riservatezza e alla identità delle vittime di detti reati.

CHIEDE che la causa venga trattata con il procedimento accelerato di cui agli artt. 105 e ss. del Regolamento di procedura della Corte.
Onera la Cancelleria della trasmissione alla Corte di Giustizia dell'Unione Europea della presente ordinanza e degli atti del procedimento per via telematica.
Segue elenco degli atti allegati alla ordinanza

Catania, 26 giugno 2025

il Giudice per le Indagini Preliminari
Simona Ragazzi