Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
MACIEJ SZPUNAR
presentate il 28 settembre 2023 [1]

Causa C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
contro
Premier ministre,
Ministère de la Culture

[domanda di pronuncia pregiudiziale proposta dal Conseil d'État (Consiglio di Stato, Francia)]

«Rinvio pregiudiziale – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Articolo 15, paragrafo 1 – Facoltà per gli Stati membri di limitare la portata di taluni diritti ed obblighi – Obbligo di controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente con poteri vincolanti – Dati relativi all'identità civile corrispondenti ad un indirizzo IP»

I. Introduzione

1. Su richiesta della Grande Sezione, presentata in applicazione dell'articolo 60, paragrafo 3, del regolamento di procedura della Corte, quest'ultima ha deciso, il 7 marzo 2023, di rinviare la presente causa alla Seduta plenaria.

2. Con ordinanza del 23 marzo 2023, la Corte (Seduta plenaria) ha deciso di riaprire la fase orale del procedimento e ha invitato gli interessati di cui all'articolo 23 dello Statuto della Corte di giustizia dell'Unione europea nonché il Garante europeo della protezione dei dati (GEPD) e l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) a partecipare ad una nuova udienza.

3. Il 27 ottobre 2022 avevo presentato le mie prime conclusioni in tale causa, prima della chiusura della fase orale del procedimento. Queste nuove conclusioni mi offrono dunque l'opportunità di approfondire taluni elementi del ragionamento da me svolto in tale causa, che tocca aspetti essenziali concernenti la conservazione e l'accesso ai dati personali.

[1] Lingua originale: il francese.

II. Contesto normativo

A. Diritto dell'Unione

4. I considerando 2, 6, 7, 11, 22, 26 e 30 della direttiva 2002/58/CE [2] enunciano quanto segue:

«(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla [Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»)]. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta.

(...)

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(...)

(11) La presente direttiva, analogamente alla direttiva [95/46/CE [3]], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950], come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

[2] Direttiva 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) (GU 2002, L 201, pag. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11) (in prosieguo: la «direttiva 2002/58»).

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

(...)

(22) Il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione (...).

(...)

(26) I dati relativi agli abbonati sottoposti a trattamento nell'ambito di reti di comunicazione elettronica per stabilire i collegamenti e per trasmettere informazioni contengono informazioni sulla vita privata delle persone fisiche e riguardano il diritto al rispetto della loro corrispondenza o i legittimi interessi delle persone giuridiche. Tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, nonché per un periodo di tempo limitato. Qualsiasi ulteriore trattamento di tali dati (...) può essere autorizzato soltanto se l'abbonato abbia espresso il proprio consenso in base ad informazioni esaurienti ed accurate date dal fornitore dei servizi di comunicazione elettronica accessibili al pubblico circa la natura dei successivi trattamenti che egli intende effettuare e circa il diritto dell'abbonato di non dare o di revocare il proprio consenso a tale trattamento (...).

(...)

(30) I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari (...)».

5. L'articolo 2 di tale direttiva, intitolato «Definizioni», così recita:

«(...)

Si applicano inoltre le seguenti definizioni:

a) "utente": qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

b) "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

c) "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

d) "comunicazione": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato;

(...)».

6. L'articolo 3 di detta direttiva, intitolato «Servizi interessati», dispone quanto segue:

«La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati».

7. L'articolo 5 della stessa direttiva, intitolato «Riservatezza delle comunicazioni», prevede quanto segue:

«1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.

(...)

3. Gli Stati membri assicurano che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva [95/46], tra l'altro sugli scopi del trattamento. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio».

8. L'articolo 6 della direttiva 2002/58, intitolato «Dati sul traffico», così recita:

«1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.

(...)».

9. L'articolo 15, paragrafo 1, di tale direttiva 2002/58, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», enuncia quanto segue:

«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 [dell'Unione], compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [TUE]».

B. Normativa francese

1. Codice della proprietà intellettuale

10. L'articolo L. 331-12 del codice della proprietà intellettuale, nella sua versione applicabile alla controversia di cui al procedimento principale (in prosieguo: il «CPI»), dispone quanto segue:

«La Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet [Alta Autorità per la diffusione delle opere e la protezione dei diritti su Internet; in prosieguo: la "Hadopi"] è un'autorità pubblica indipendente».

11. L'articolo L. 331-13 del CPI prevede quanto segue:

«La [Hadopi] espleta:

(...)

2° Una funzione di protezione [delle opere e degli oggetti ai quali è correlato un diritto d'autore o un diritto connesso sulle reti di comunicazione elettronica] nei confronti delle violazioni di tali diritti commesse sulle reti di comunicazione elettronica utilizzate per la fornitura di servizi di comunicazione al pubblico online; (...)».

12. L'articolo L. 331-15 di tale codice così recita:

«La [Hadopi] è composta da un collegio e da una commissione per la protezione dei diritti (…)

(...)

Nell'esercizio dei loro poteri, i membri del collegio e della commissione per la protezione dei diritti non ricevono istruzioni da nessuna autorità».

13. L'articolo L. 331-17 di detto codice dispone quanto segue:

«La commissione per la protezione dei diritti è incaricata di adottare le misure previste all'articolo L. 331-25».

14. L'articolo L. 331-21 dello stesso codice così recita:

«Per l'esercizio dei suoi poteri da parte della commissione per la protezione dei diritti, la [Hadopi] si avvale di agenti pubblici giurati, autorizzati dal [suo] presidente alle condizioni stabilite per decreto adottato previo parere del Conseil d'État [Consiglio di Stato] (...).

I membri della commissione per la protezione dei diritti e gli agenti menzionati al primo comma ricevono i ricorsi indirizzati alla suddetta commissione alle condizioni previste dall'articolo L. 331-24 e svolgono l'esame dei fatti.

Essi possono ottenere, ai fini del procedimento, tutti i documenti, qualunque ne sia il supporto, compresi i dati conservati e trattati dagli operatori di comunicazioni elettroniche ai sensi dell'articolo L. 34-1 del code des postes et des communications électroniques [codice delle poste e delle comunicazioni elettroniche] e dai fornitori di servizi di cui all'articolo 6, I, paragrafi 1 e 2, della loi n. 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [legge n. 2004-575 del 21 giugno 2004 per la fiducia nell'economia digitale].

Essi possono, inoltre, ottenere copia dei documenti menzionati al comma precedente.

Essi possono, in particolare, ottenere dagli operatori di comunicazioni elettroniche l'identità, l'indirizzo postale, l'indirizzo di posta elettronica e i recapiti telefonici dell'abbonato il cui accesso a servizi di comunicazione al pubblico online è stato utilizzato al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere o oggetti protetti senza l'autorizzazione dei titolari dei diritti (…), laddove questa sia richiesta».

15. L'articolo L. 331-24 del CPI dispone quanto segue:

«La commissione per la protezione dei diritti agisce su ricorso di agenti giurati e autorizzati (...) designati:

– dagli organismi di difesa professionale regolarmente costituiti;

– dagli organismi di gestione collettiva;

– dal Centre national du cinéma et de l'image animée (Centro nazionale della cinematografia e dell'immagine animata).

La commissione per la protezione dei diritti può parimenti agire sulla base di informazioni che le vengono trasmesse dal procuratore della Repubblica.

Essa non può essere investita di fatti risalenti a più di sei mesi».

16. L'articolo L. 331-25 di tale codice, disposizione che disciplina la procedura cosiddetta di «risposta graduata», così recita:

«Qualora essa sia investita di fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3 [del CPI], la commissione per la protezione dei diritti può inviare all'abbonato (...) una raccomandazione contenente richiamo alle disposizioni di cui all'articolo L. 336-3, con l'intimazione di rispettare l'obbligo da esse definito, e lo avverte in merito alle sanzioni previste ai sensi degli articoli L. 335-7 e L. 335-7-1. Tale raccomandazione contiene parimenti un'informazione dell'abbonato sull'offerta legale di contenuti culturali online, sull'esistenza di strumenti di messa in sicurezza che consentono di prevenire gli inadempimenti all'obbligo definito all'articolo L. 336-3 nonché sui pericoli per il rinnovamento della creazione artistica e per l'economia del settore culturale generati dalle pratiche che non rispettano il diritto d'autore e i diritti connessi.

In caso di reiterazione, entro sei mesi a decorrere dall'invio della raccomandazione di cui al primo comma, di fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3, la commissione può inviare una nuova raccomandazione contenente le stesse informazioni della precedente per via elettronica (…). Essa deve allegare a tale raccomandazione una lettera consegnata contro firma o qualsiasi altro mezzo atto a provare la data di notifica di tale raccomandazione.

Le raccomandazioni inviate sulla base del presente articolo indicano la data e l'ora in cui i fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3 sono stati constatati. Per contro, esse non divulgano il contenuto delle opere o degli oggetti protetti interessati da tale violazione. Esse indicano i recapiti telefonici, postali ed elettronici ai quali il loro destinatario può inviare, se lo desidera, osservazioni alla commissione per la protezione dei diritti ed ottenere, qualora formuli una richiesta espressa in tal senso, precisazioni sul contenuto delle opere o degli oggetti protetti interessati dalla violazione addebitatagli».

17. L'articolo L. 331-29 di detto codice dispone quanto segue:

«La [Hadopi] è autorizzata a creare un trattamento automatizzato dei dati personali per le persone che sono oggetto di un procedimento ai sensi della presente sottosezione.

Tale trattamento è diretto all'attuazione, da parte della commissione per la protezione dei diritti, delle misure previste dalla presente sottosezione, di tutti gli atti procedimentali connessi e delle modalità di informazione, nei confronti degli organismi di difesa professionale e degli organismi di gestione collettiva, degli eventuali ricorsi all'autorità giudiziaria e delle notifiche previste al quinto comma dell'articolo L. 335-7.

Un decreto (...) stabilisce le modalità di applicazione del presente articolo. Esso specifica in particolare:

– le categorie di dati registrati e il loro periodo di conservazione;

– i destinatari autorizzati a ricevere la comunicazione di tali dati, in particolare le persone la cui attività consiste nell'offrire accesso a servizi di comunicazione al pubblico online;

– le condizioni alle quali le persone interessate possono esercitare il loro diritto di accesso ai dati che li riguardano presso la [Hadopi] (...)».

18. L'articolo R. 331-37 del medesimo codice prevede quanto segue:

«Gli operatori di comunicazioni elettroniche (…) e i fornitori di servizi (…) sono tenuti a comunicare, mediante interconnessione al trattamento automatizzato dei dati personali di cui all'articolo L. 331-29 o mediante un supporto di registrazione che garantisca la loro integrità e sicurezza, i dati personali e le informazioni di cui al punto 2 dell'allegato al [décret n. 2010 236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du [CPI] dénommé «Système de gestion des mesures pour la protection des œuvres sur Internet» (decreto n. 2010 236 del 5 marzo 2010 relativo al trattamento automatizzato dei dati personali autorizzato dall'articolo L. 331-29 del [CPI] denominato «Sistema di gestione delle misure per la protezione delle opere su Internet»)[4]] (in prosieguo: il "decreto del 5 marzo 2010") (…) entro un termine di otto giorni dalla trasmissione, da parte della commissione per la protezione dei diritti, dei dati tecnici necessari all'identificazione dell'abbonato il cui accesso a servizi di comunicazione al pubblico online è stato utilizzato al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere o oggetti protetti senza l'autorizzazione dei titolari dei diritti (…) laddove questa sia richiesta.

(...)».

19. L'articolo R. 335-5 del CPI dispone quanto segue:

«I.- Costituisce una negligenza grave, punita con l'ammenda prevista per le contravvenzioni della quinta classe, il fatto, senza motivo legittimo, per la persona titolare di un accesso a servizi di comunicazione al pubblico online, qualora ricorrano le condizioni previste sub II:

1° o di non avere predisposto uno strumento di messa in sicurezza di tale accesso;

2° o di avere mancato di diligenza nell'attuazione di tale strumento.

II.- Le disposizioni sub I si applicano solo qualora ricorrano le due condizioni seguenti:

1° In applicazione dell'articolo L. 331-25 e nelle forme previste da tale articolo, la commissione per la protezione dei diritti abbia raccomandato al titolare dell'accesso l'attuazione di uno strumento di messa in sicurezza del suo accesso che consenta di prevenire la reiterazione di un uso del medesimo al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere od oggetti protetti dal diritto d'autore o da un diritto connesso senza l'autorizzazione dei titolari dei diritti (...) laddove questa sia richiesta;

2° Nell'anno successivo alla presentazione di tale raccomandazione, siffatto accesso venga nuovamente utilizzato ai fini menzionati al punto 1 del presente paragrafo II».

20. L'articolo L. 336-3 di tale codice enuncia quanto segue:

«Il titolare dell'accesso a servizi di comunicazione al pubblico online è tenuto ad assicurare che tale accesso non sia utilizzato al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere od oggetti protetti dal diritto d'autore o da un diritto connesso senza l'autorizzazione dei titolari (…) laddove questa sia richiesta.

[4] JORF del 7 marzo 2010, testo n. 19.

La violazione da parte del titolare dell'accesso dell'obbligo definito al primo comma non comporta il sorgere della responsabilità penale dell'interessato (...)».

2. Decreto del 5 marzo 2010

21. Il decreto del 5 marzo 2010, nella sua versione applicabile ai fatti della controversia di cui al procedimento principale, prevede quanto segue al suo articolo 1:

«Il trattamento di dati personali denominato "Sistema di gestione delle misure per la protezione delle opere su Internet" ha per finalità l'attuazione, da parte della commissione per la protezione dei diritti della [Hadopi]:

1° delle misure previste dal libro III della parte legislativa del [CPI] (titolo III, capo 1, sezione 3, sottosezione 3) e dal libro III della parte regolamentare dello stesso codice (titolo III, capo I, sezione 2, sottosezione 2);

2° dei ricorsi al procuratore della Repubblica relativi a fatti idonei a costituire reati previsti agli articoli L. 335-2, L. 335-3, L. 335-4 e R. 335-5 dello stesso codice, nonché dell'informazione degli organismi di difesa professionali e degli organismi di gestione collettiva di tali ricorsi;

(...)».

22. L'articolo 4 di tale decreto dispone quanto segue:

«I.- Hanno accesso diretto ai dati personali e alle informazioni menzionate all'allegato al presente decreto gli agenti pubblici giurati autorizzati dal presidente della [Hadopi] in applicazione dell'articolo L. 331-21 del [CPI] e i membri della commissione per la protezione dei diritti menzionata all'articolo 1.

II.- Gli operatori di comunicazioni elettroniche e i fornitori di servizi menzionati al punto 2 dell'allegato al presente decreto sono destinatari:

– dei dati tecnici necessari all'identificazione dell'abbonato;

– delle raccomandazioni previste all'articolo L. 331-25 del [CPI] ai fini del loro invio per via elettronica ai loro abbonati;

– degli elementi necessari all'attuazione delle pene complementari della sospensione dell'accesso ad un servizio di comunicazione al pubblico online portate a conoscenza della commissione per la protezione dei diritti da parte del procuratore della Repubblica.

III.- Gli organismi di difesa professionale e gli organismi di gestione collettiva sono informati dell'adizione del procuratore della Repubblica.

IV.- Le autorità giudiziarie sono destinatarie dei verbali di accertamento di fatti idonei a costituire reati previsti agli articoli L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 e R. 335-5 del [CPI].

Il casellario giudiziale automatizzato è informato dell'esecuzione della pena della sospensione».

23. L'allegato al decreto del 5 marzo 2010 prevede quanto segue:

«I dati personali e le informazioni registrate nel trattamento denominato "Sistema di gestione delle misure per la protezione delle opere su Internet" sono i seguenti:

1° Dati personali e informazioni provenienti dagli organismi di difesa professionale regolarmente costituiti, dagli organismi di gestione collettiva, dal Centro nazionale della cinematografia e dell'immagine animata, nonché quelli provenienti dal procuratore della Repubblica:

Quanto ai fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3 del [CPI]:

Data e ora dei fatti;

Indirizzo IP degli abbonati interessati;

Protocollo peer-to-peer utilizzato;

Pseudonimo utilizzato dall'abbonato;

Informazioni relative alle opere o agli oggetti protetti interessati dai fatti;

Nome del file come presente sulla stazione dell'abbonato (se del caso);

Fornitore di accesso ad Internet presso il quale l'accesso è stato sottoscritto o che ha fornito la risorsa tecnica IP.

(...)

2° Dati personali ed informazioni relative all'abbonato raccolte presso operatori di comunicazioni elettroniche (...) e fornitori di servizi (...):

Cognome, nomi;

Indirizzo postale e indirizzi di posta elettronica;

Recapiti telefonici;

Indirizzo dell'impianto telefonico dell'abbonato;

Fornitore di accesso ad Internet, che utilizza le risorse tecniche del fornitore di accesso menzionato al punto 1°, presso il quale l'abbonato ha sottoscritto il suo contratto; numero di pratica;

data di inizio della sospensione dell'accesso ad un servizio di comunicazione al pubblico online.

(...)».

3. Codice delle poste e delle comunicazioni elettroniche

24. L'articolo L. 34-1 del codice delle poste e delle comunicazioni elettroniche, come modificato dall'articolo 17 della legge n. 2021-998 del 30 luglio 2021 [5], dispone al suo paragrafo II bis che «gli operatori di comunicazioni elettroniche sono tenuti a conservare:

1° Ai fini dei procedimenti penali, della prevenzione delle minacce alla pubblica sicurezza e della salvaguardia della sicurezza nazionale, le informazioni relative all'identità anagrafica dell'utente, fino alla scadenza del termine di cinque anni dalla fine della validità del suo contratto;

2° Per gli stessi scopi di cui al punto 1° del presente paragrafo II bis, le altre informazioni fornite dall'utente al momento della sottoscrizione di un contratto o della creazione di un conto nonché le informazioni relative al pagamento, fino alla scadenza del termine di un anno a decorrere dalla fine della validità del suo contratto o dalla chiusura del suo conto;

3° Ai fini della lotta alla criminalità e ai reati gravi, della prevenzione delle minacce gravi alla pubblica sicurezza e della salvaguardia della sicurezza nazionale, i dati tecnici che consentano di identificare l'origine della connessione o quelli relativi alle apparecchiature terminali impiegate, fino alla scadenza del termine di un anno dalla connessione o dall'impiego delle apparecchiature terminali».

III. Procedimento dinanzi alla Corte

25. In risposta all'invito rivolto agli interessati di cui all'articolo 23 dello Statuto della Corte di giustizia dell'Unione europea, i ricorrenti nel procedimento principale, i governi francese, danese, estone, irlandese, dei Paesi Bassi, finlandese, svedese nonché la Commissione europea hanno risposto ai quesiti scritti posti dalla Corte.

26. Queste stesse parti, ad eccezione del governo finlandese, i governi ceco, spagnolo, cipriota, lettone e norvegese, nonché il GEPD e l'ENISA, hanno partecipato all'udienza tenutasi il 15 maggio 2023.

IV. Analisi

27. La mia analisi delle questioni pregiudiziali nelle mie prime conclusioni mi aveva indotto a proporre alla Corte di dichiarare che l'articolo 15, paragrafo 1, della direttiva 2002/58 deve essere interpretato nel senso che esso non osta ad una normativa nazionale che consente la conservazione, da parte dei fornitori di servizi di comunicazioni elettroniche, e l'accesso, da parte

[5] JORF del 31 luglio 2021, testo n. 1. Questa versione dell'articolo L. 34-1 di tale codice, in vigore dal 31 luglio 2021, è stata adottata a seguito della decisione del Conseil d'État (Consiglio di Stato, Francia) del 21 aprile 2021, n. 393099 (JORF del 25 aprile 2021) che aveva respinto la versione precedente di tale disposizione, la quale includeva un obbligo di conservazione di dati personali «ai fini della ricerca, dell'accertamento e del perseguimento dei reati o di una violazione dell'obbligo stabilito all'articolo L. 336-3 [del CPI]» al solo scopo di consentire, ove necessario, la messa a disposizione, segnatamente, della Hadopi. Con decisione n. 2021-976-977 QPC, del 25 febbraio 2022 (M. Habib A. et autre), il Conseil constitutionnel (Corte costituzionale, Francia) ha dichiarato la contrarietà alla Costituzione francese di tale precedente versione dell'articolo L. 34-1 di detto codice essenzialmente in quanto, «autorizzando la conservazione generale e indifferenziata dei dati di connessione, le disposizioni contestate arrecano un pregiudizio sproporzionato al diritto al rispetto della vita privata» (punto 13). Tale organo giurisdizionale ha infatti ritenuto che i dati di connessione che devono essere conservati in forza di tali disposizioni vertano non solo sull'identificazione degli utenti dei servizi di comunicazione elettronica bensì anche su altri dati che, «alla luce della loro natura, della loro diversità e dei trattamenti di cui possono essere oggetto (…), forniscono su tali utenti nonché, se del caso, su terzi, informazioni numerose e precise, particolarmente lesive della loro vita privata» (punto 11).

di un'autorità amministrativa come la Hadopi [6], limitatamente ai dati relativi all'identità civile corrispondenti ad indirizzi IP, affinché tale autorità possa identificare i titolari di tali indirizzi sospettati di essere responsabili di violazioni del diritto d'autore e dei diritti connessi e possa adottare, se del caso, misure nei loro confronti, senza che tale accesso sia subordinato ad un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente, qualora tali dati costituiscano l'unico strumento di indagine che permetta di identificare la persona alla quale tale indirizzo era attribuito al momento della commissione del reato.

28. Nelle presenti conclusioni, mi dedicherò ad approfondire taluni elementi della mia precedente analisi e i punti dibattuti all'udienza tenutasi il 15 maggio 2023, al fine di illustrare le ragioni per cui insisto nella mia proposta di risposta alle questioni pregiudiziali e confermo il ragionamento che vi ha portato [7].

29. Più specificamente, dimostrerò che il fatto di consentire la conservazione e l'accesso a dati relativi all'identità civile corrispondenti ad indirizzi IP, senza controllo preventivo, al fine di identificare gli autori di reati qualora tali dati costituiscano l'unico strumento di identificazione di questi ultimi, soddisfa i requisiti elaborati dalla Corte in relazione all'esame delle misure adottate ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 (sezione B).

30. Nel farlo, metterò in evidenza che una simile soluzione costituisce non un ribaltamento della giurisprudenza rigorosa e protettrice dei diritti fondamentali elaborata dalla Corte a partire dalle sentenze Tele2 Sverige e Watson e a. [8] e La Quadrature du Net e a. [9], bensì uno sviluppo necessario della stessa che si colloca, a mio avviso, nella scia dei principi enunciati dalla Corte. Tale distinzione non è unicamente semantica. Infatti, la soluzione che propongo non è intesa a rimettere in discussione la giurisprudenza esistente, bensì a consentire, in nome di un certo pragmatismo, il suo adattamento a circostanze particolari ed estremamente circoscritte (sezione C).

31. Per ragioni di chiarezza, e nella misura in cui dalle discussioni svoltesi in udienza è emersa un'esigenza di precisazioni al riguardo, inizierò la mia analisi richiamando il funzionamento del meccanismo di risposta graduata applicato dalla Hadopi (sezione A).

A. Meccanismo di risposta graduata applicato dalla Hadopi

32. La Hadopi è un'autorità amministrativa indipendente incaricata di proteggere il diritto d'autore e i diritti connessi contro le violazioni di tali diritti commesse su Internet. A tal fine, è stato istituito il meccanismo cosiddetto di «risposta graduata», la cui attuazione è affidata alla commissione per la protezione dei diritti della Hadopi.

6 Il 1º gennaio 2022, il Conseil supérieur de l'audiovisuel (Consiglio superiore dell'audiovisivo, CSA) et la Hadopi sono divenuti l'Autorité de régulation de la communication audiovisuelle et numérique (Autorità di regolamentazione della comunicazione audiovisiva e digitale, Arcom). Considerato il periodo durante il quale si sono svolti i fatti della controversia di cui al procedimento principale, mi riferirò tuttavia, nelle presenti conclusioni, alla Hadopi.

7 A tal riguardo, insisto parimenti nella mia proposta di riformulazione delle questioni pregiudiziali, nonché nella mia comprensione del loro oggetto. Infatti, pur se viene unicamente menzionato, nel testo delle questioni pregiudiziali, l'accesso ai dati relativi all'identità civile corrispondenti ad indirizzi IP, la questione dell'accesso a tali dati è tuttavia inscindibile da quella della loro conservazione da parte dei fornitori di servizi di comunicazione elettronica, cosicché l'analisi della compatibilità della conservazione con il diritto dell'Unione è necessariamente preliminare a quella della compatibilità dell'accesso. Su tale aspetto, v. paragrafo 45 e segg. delle mie prime conclusioni. Analogamente, benché le questioni pregiudiziali riguardino «i dati relativi all'identità civile corrispondenti a un indirizzo IP», esse devono essere intese nel senso che riguardano anche l'accesso agli indirizzi IP che consentono di individuare l'origine di una connessione. Su tale aspetto, v. paragrafo 41 e segg. delle mie prime conclusioni.

8 Sentenza del 21 dicembre 2016 (C-203/15 e C-698/15; in prosieguo: la «sentenza Tele2», EU:C:2016:970).

9 Sentenza del 6 ottobre 2020 (C-511/18, C-512/18 e C-520/18; in prosieguo: la «sentenza La Quadrature du Net e a.», EU:C:2020:791).

33. Tale commissione viene adita da organismi di aventi diritto, all'interno dei quali taluni agenti giurati e autorizzati dal ministro della Cultura raccolgono, sulle reti peer-to-peer, gli indirizzi IP degli utenti di Internet che mettono a disposizione del pubblico opere senza l'autorizzazione dei loro titolari. Vengono quindi redatti dei verbali. Essi contengono, segnatamente, l'indirizzo IP dell'accesso ad Internet utilizzato per commettere tali violazioni del diritto d'autore, la data e l'ora della violazione accertata nonché il titolo dell'opera in questione, e vengono trasmessi alla commissione per la protezione dei diritti della Hadopi. Occorre sottolineare, al riguardo e come rilevato dal GEPD, che il trattamento dei dati personali da parte degli agenti all'interno degli organismi di aventi diritto è oggetto di un'autorizzazione da parte della Commission nationale de l'informatique et des libertés (Commissione nazionale per l'informatica e le libertà; in prosieguo: la «CNIL»), l'autorità francese di controllo in materia di protezione dei dati [10].

34. Ricevuti i verbali, e a seguito di un controllo automatizzato inteso a garantire che essi contengano tutti i dati richiesti, la commissione per la protezione dei diritti della Hadopi può ottenere dai fornitori di servizi di comunicazioni elettroniche l'identità, l'indirizzo postale, l'indirizzo di posta elettronica e i recapiti telefonici del titolare dell'abbonamento che è stato utilizzato al fine di commettere una violazione del diritto d'autore.

35. La Hadopi può in tal caso inviare a siffatta persona una «raccomandazione» che informi quest'ultima del fatto che il suo accesso ad Internet è stato oggetto di un'utilizzazione contraria al diritto d'autore e che ingiunge alla persona sospettata di essere venuta meno al suo obbligo di sorveglianza quanto al rispetto su Internet delle opere protette dal diritto d'autore o da un diritto connesso di ottemperare a tale obbligo. In altre parole, la raccomandazione è rivolta al titolare dell'accesso ad Internet, il quale può essere, di fatto, una persona diversa da quella che ha proceduto alla messa a disposizione dell'opera in violazione del diritto d'autore. Una seconda raccomandazione può essere emessa nel caso di una seconda constatazione di contraffazione tramite il medesimo accesso ad Internet. In caso di nuove reiterazioni, la commissione per la protezione dei diritti della Hadopi può decidere di adire il procuratore della Repubblica ai fini dell'esercizio dell'azione penale. A tal riguardo, come precisato dal governo francese nelle sue prime osservazioni, gli agenti della Hadopi incaricati del meccanismo di risposta graduata sono agenti giurati e autorizzati dal presidente della Hadopi, sono vincolati al segreto professionale e sono i soli, all'interno della Hadopi, autorizzati ad accedere ai dati personali trattati nell'ambito di tale meccanismo.

36. Devo precisare, al riguardo, che vengono raccolti e trasmessi alla Hadopi non i dati di tutti gli utenti delle reti peer-to-peer qualora questi ultimi si limitino a scaricare siffatti contenuti [11], bensì unicamente quelli delle persone che hanno proceduto alla messa a disposizione di contenuti contraffatti, ossia che hanno *caricato* siffatti contenuti.

37. A titolo esemplificativo, per il 2021, la Hadopi ha in tal senso ricevuto dagli organismi di aventi diritto quasi quattro milioni di verbali, ha proceduto all'invio di 210 595 prime raccomandazioni e di 53 564 seconde raccomandazioni, e ha adito il procuratore della Repubblica in 1 484 casi.

[10] V., al riguardo, delibera n. 2010-225 della CNIL, del 10 giugno 2010, che modifica l'autorizzazione di attuazione, da parte della Société des auteurs, compositeurs et éditeurs de musique (società francese di gestione dei diritti d'autore, SACEM) di un trattamento di dati personali inteso alla ricerca e all'accertamento dei reati di contraffazione commessi tramite le reti di scambio di file denominate «peer to peer» (autorizzazione n. 1425421).

[11] Sul funzionamento delle reti peer-to-peer e sui diversi profili di utenti di Internet su tali reti, v. le mie conclusioni nella causa M.I.C.M. (C-597/19, EU:C:2020:1063, paragrafo 37 e segg.).

38. Fatti tali rilievi, dimostrerò in che modo un siffatto meccanismo, il quale presuppone la conservazione e l'accesso a dati relativi all'identità civile corrispondenti ad indirizzi IP, soddisfa, a mio avviso, i requisiti della giurisprudenza relativa alle misure nazionali adottate ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58.

B. Rispetto dei requisiti risultanti dalla giurisprudenza della Corte relativa all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58

39. Avendo già proceduto, nelle mie prime conclusioni, a richiamare la giurisprudenza della Corte relativa alla conservazione e all'accesso agli indirizzi IP attribuiti all'origine di una connessione [12], mi concentrerò, nelle presenti conclusioni, su ciò che costituisce, a mio avviso, il nucleo di tale giurisprudenza, ossia, da un lato, il requisito di proporzionalità e, dall'altro, per quanto riguarda l'accesso a tali dati, l'eventuale necessità di un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente.

1. Sulla proporzionalità della misura in questione

40. Al fine di determinare la compatibilità con il diritto dell'Unione di una misura di conservazione o di accesso a dati relativi all'identità civile corrispondenti ad un indirizzo IP, occorre procedere, come sottolineato a più riprese dalla Corte, ad un contemperamento dei diversi interessi legittimi e dei diritti in gioco, i quali sono, da un lato, i diritti alla tutela della vita privata nonché alla protezione dei dati personali [13] garantiti dagli articoli 7 e 8 della Carta, e, dall'altro, la protezione dei diritti e delle libertà altrui e dei diritti sanciti agli articoli 3, 4, 6 e 7 della Carta [14]. Aggiungerò che, nella causa in esame, i diritti alla tutela della vita privata e alla protezione dei dati personali devono parimenti essere contemperati con il diritto di proprietà sancito all'articolo 17 della Carta, nella misura in cui il meccanismo di risposta graduata è inteso, in definitiva, alla protezione del diritto d'autore e dei diritti connessi.

41. La Corte precisa, al riguardo, che tale contemperamento effettuato ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 consente agli Stati membri di adottare una misura che deroghi al principio di riservatezza qualora una tale misura sia «*necessaria, opportuna e proporzionata* all'interno di una società democratica» (il corsivo è mio). Il considerando 11 di tale direttiva precisa che una simile misura deve essere «strettamente» *proporzionata* allo scopo perseguito [15].

42. La Corte richiama peraltro il principio di proporzionalità in tutto il suo ragionamento relativo all'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 e fa dunque di quest'ultimo la chiave di volta dell'esame di una misura nazionale di conservazione o di accesso a dati personali adottata ai sensi di tale disposizione.

[12] Paragrafo 53 e segg. delle mie prime conclusioni.

[13] I diritti alla tutela della vita privata e alla protezione dei dati personali si traducono, nel contesto della direttiva 2002/58, nei principi della riservatezza delle comunicazioni e del divieto di memorizzazione dei dati ad esse correlati che essa sancisce.

[14] Sentenze La Quadrature du Net e a. (punti da 120 a 122 nonché 127 e 128); del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20; in prosieguo: la «sentenza Commissioner of An Garda Síochána e a.», EU:C:2022:258, punti 48 e 50), nonché del 20 settembre 2022, SpaceNet e Telekom Deutschland (C-793/19 e C-794/19; in prosieguo: la «sentenza SpaceNet e Telekom Deutschland», EU:C:2022:702, punti 63 e 65).

[15] Sentenze La Quadrature du Net e a. (punto 129), Commissioner of An Garda Síochána e a. (punto 51), e SpaceNet e Telekom Deutschland (punto 66).

43. Da una lettura più approfondita di tale ragionamento emerge che il principio di proporzionalità consta, nel contesto dell'articolo 15, paragrafo 1, della direttiva 2002/58, di diversi elementi, concernenti, da un lato, la gravità dell'ingerenza nei diritti fondamentali che la conservazione o l'accesso ai dati relativi al traffico implica e, dall'altro, la necessità della misura in questione.

44. Per quanto riguarda la conservazione e l'accesso alle identità civili corrispondenti ad indirizzi IP da parte della Hadopi, ritengo che sia la gravità dell'ingerenza sia il carattere indispensabile di tali dati dovrebbero indurre la Corte a modulare il suo esame della proporzionalità di una misura nazionale adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58.

a) Gravità relativa dell'ingerenza nei diritti fondamentali

45. Dalla giurisprudenza costante della Corte si evince chiaramente che, secondo il principio di proporzionalità, l'importanza dell'obiettivo perseguito da una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2022/58 deve essere rapportata alla gravità dell'ingerenza che ne risulta [16].

46. Più specificamente, la Corte ha dichiarato, come ho sottolineato nelle mie prime conclusioni, che un'ingerenza grave può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di violazioni penali, soltanto da un obiettivo di lotta contro una criminalità che sia sua volta da qualificarsi come «grave» [17].

47. Per quanto riguarda gli indirizzi IP, la Corte rileva che pur se essi presentano un grado di sensibilità inferiore rispetto agli altri dati relativi al traffico, la loro conservazione e la loro analisi costituiscono comunque ingerenze gravi nei diritti fondamentali, poiché essi possono essere utilizzati per effettuare un tracciamento completo del percorso di navigazione di un utente di Internet e, di conseguenza, per stabilire il profilo dettagliato di quest'ultimo e trarre conclusioni precise sulla sua vita privata [18].

48. Nel procedimento principale, la conservazione e l'accesso a dati relativi all'identità civile corrispondenti ad indirizzi IP mirano a combattere le violazioni del diritto d'autore e dei diritti connessi. Orbene, è chiaro, a mio avviso, che tale lotta non può rientrare nell'ambito della lotta alle forme gravi di criminalità [19], sebbene il volume di tali violazioni sia massiccio. Esisterebbe dunque un divario tra la gravità dell'ingerenza nei diritti fondamentali che la misura in questione comporta e l'obiettivo da essa perseguito.

16 Sentenze Commissioner of An Garda Síochána e a. (punto 56) e SpaceNet e Telekom Deutschland (punto 71).

17 Sentenze Tele2 (punto 115); del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punto 56), e del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18; in prosieguo: la «sentenza Prokuratuur», EU:C:2021:152, punto 33). V. parimenti paragrafo 92 delle mie prime conclusioni.

18 V. sentenze La Quadrature du Net e a. (punti 152 e 153); Commissioner of An Garda Síochána e a. (punto 73), e SpaceNet e Telekom Deutschland (punto 103). V. parimenti paragrafi 63, 64 e 93 delle mie prime conclusioni.

19 Ho sostenuto, nelle mie prime conclusioni, che la nozione di «forme gravi di criminalità» dovrebbe essere interpretata autonomamente, al fine di impedire un'elusione, da parte degli Stati membri, dei requisiti sanciti all'articolo 15, paragrafo 1, della direttiva 2002/58. Mantengo questa posizione. Devo tuttavia sottolineare che, anche se la Corte dovesse dichiarare che la definizione della nozione di «forme gravi di criminalità» è lasciata agli Stati membri, essa dovrebbe in ogni caso essere stabilita nei limiti del diritto dell'Unione e non potrebbe essere estesa fino al punto di privare tale disposizione della sua sostanza.

49. Nelle mie prime conclusioni, ho ritenuto, in conformità alla giurisprudenza della Corte, che l'accesso da parte della Hadopi ai dati relativi all'identità civile corrispondenti ad un indirizzo IP costituisca effettivamente un'ingerenza grave nei diritti fondamentali. Anche se ho parimenti ritenuto che la conservazione e l'accesso a tali dati dovessero cionondimeno essere consentiti nella specie, devo, a seguito dell'udienza, apportare ancora alcune precisazioni.

50. Il meccanismo di risposta graduata consente alla Hadopi di collegare l'indirizzo IP, comunicato dagli organismi di aventi diritto, di persone sospettate di avere utilizzato il loro accesso ad Internet per commettere una violazione del diritto d'autore su una rete peer-to-peer all'identità civile di tale persona, nonché ad un estratto del file caricato in violazione del diritto d'autore. Come rilevato dalla Commissione e dal GEPD in udienza, siffatti elementi, pur se consentono di ottenere sicuramente più informazioni rispetto alla mera identità del presunto autore di una violazione, non portano tuttavia a trarre conclusioni molto precise sulla vita privata di tale persona. Infatti, come indicato nelle mie prime conclusioni[20], siamo unicamente in presenza della rivelazione di una consultazione puntuale di un contenuto che, considerato isolatamente, non può consentire di stabilire il profilo dettagliato della persona che vi ha proceduto.

51. Ciò vale a maggior ragione in quanto, anzitutto, la maggior parte degli indirizzi IP comunicati alla Hadopi sono indirizzi IP cosiddetti «dinamici», i quali sono, per loro natura, mutevoli e corrispondono ad un'identità precisa solo in un unico momento, il quale coincide con la messa a disposizione del contenuto in questione. Essi escludono pertanto qualsivoglia tracciamento completo.

52. Inoltre, devo sottolineare che la protezione dei diritti fondamentali su Internet non mi sembra poter giustificare il diniego di accesso ai soli dati relativi all'indirizzo IP, al contenuto di un'opera e all'identità della persona che ha proceduto alla sua messa a disposizione in violazione del diritto d'autore, bensì unicamente la previsione di garanzie che accompagnino la conservazione e l'accesso a questi ultimi. Un'analogia con il modo reale mi sembra al riguardo eloquente: una persona sospettata di avere commesso un furto non può invocare il proprio diritto alla tutela della vita privata affinché le persone incaricate di perseguire tale reato non possano venire a conoscenza del contenuto rubato. Per contro, tale persona può invocare, a ragione, i propri diritti fondamentali al fine di impedire, nel corso del procedimento, l'accesso a un insieme di dati più ampio rispetto ai soli dati necessari alla qualificazione del presunto reato.

53. Infine, rilevo che, contrariamente a quanto fatto valere dalle ricorrenti, il meccanismo di risposta graduata non sembra comportare una sorveglianza generalizzata degli utenti delle reti peer-to-peer. Infatti, non si tratta di verificare la totalità della loro attività su una determinata rete al fine di stabilire se essi abbiano proceduto ad una messa a disposizione di un'opera in violazione del diritto d'autore, bensì piuttosto, a partire da un file identificato come contraffazione, di determinare il detentore dell'accesso ad Internet a partire dal quale l'utente di Internet ha proceduto alla messa a disposizione. Analogamente, come sottolineato dal GEPD in udienza, non si tratta di sorvegliare l'attività di tutti gli utenti delle reti peer-to-peer, bensì unicamente quella delle persone che procedono a caricare file contraffatti, fermo restando che il caricamento di tali file è tanto meno rivelatore di elementi relativi alla vita privata della persona in quanto esso può essere effettuato unicamente per consentire a tali utenti di Internet di procedere successivamente allo scaricamento di altri file.

[20] Paragrafo 101 delle mie prime conclusioni.

54. In tali circostanze, le ragioni che hanno indotto la Corte a considerare la conservazione e l'accesso agli indirizzi IP un'ingerenza grave nei diritti fondamentali non mi sembrano applicabili nel caso di un meccanismo di risposta graduata come quello operato dalla Hadopi. Ne consegue che la gravità dell'ingerenza che tale conservazione e tale accesso comportano dovrebbe, in sede di esame della proporzionalità, essere modulata.

55. In altri termini, ritengo che occorra interpretare la giurisprudenza della Corte relativa alla gravità dell'ingerenza nei diritti fondamentali causata dalla conservazione e dall'accesso ad indirizzi IP nel senso non che essa implica che tale ingerenza è sempre un'ingerenza grave, bensì che essa lo è soltanto qualora gli indirizzi IP possano dare luogo ad un tracciamento completo del percorso di navigazione dell'utente di Internet e a trarre conclusioni molto precise sulla sua vita privata.

56. Poiché ciò non è quanto avviene in una situazione come quella di cui al procedimento principale, ne consegue che l'ingerenza che la conservazione e l'accesso alle identità civili corrispondenti ad un indirizzo IP utilizzato per la messa a disposizione di un contenuto in violazione del diritto d'autore comportano dovrebbe poter essere giustificata da un obiettivo di lotta alla criminalità più ampio della lotta alle sole forme gravi di criminalità.

57. Preciso inoltre che l'ingerenza nei diritti fondamentali che la conservazione e l'accesso a dati relativi all'identità civile corrispondenti ad un indirizzo IP comportano in una situazione come quella di cui al procedimento principale non è aggravata dalla circostanza che il titolare dell'accesso ad Internet utilizzato per la messa a disposizione di un contenuto contraffatto non sia necessariamente all'origine di tale messa a disposizione, cosicché la raccomandazione inviata dalla Hadopi potrebbe portare a rivelare a tale titolare detto contenuto al quale un terzo ha potuto accedere. Da un lato, ricordo che il reato oggetto di indagine da parte della Hadopi consiste in un inadempimento all'obbligo di assicurare che l'accesso non sia utilizzato a fini di messa a disposizione di un contenuto in violazione del diritto d'autore. È dunque necessario che le informazioni che ne consentono la qualificazione vengano trasmesse al suo presunto autore. Dall'altro, come ho già osservato, ritengo che le informazioni relative all'opera in questione non consentano di trarre conclusioni precise sulla vita privata della persona all'origine della messa a disposizione. L'eventuale trasmissione di tali informazioni al titolare della connessione Internet non eccede dunque quanto necessario per permettere il perseguimento della violazione del diritto d'autore in questione.

b) Carattere indispensabile dei dati in questione per l'accertamento e il perseguimento di un reato

58. Al fine di assicurare la proporzionalità di una misura di conservazione e di accesso a dati relativi al traffico come i dati relativi all'identità civile corrispondenti ad un indirizzo IP adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, occorre, secondo la giurisprudenza della Corte, che l'ingerenza che essa comporta sia limitata allo stretto necessario per consentire la realizzazione dell'obiettivo perseguito [21]. È appunto quanto mi sembra avvenire nel caso della misura di cui al procedimento principale.

[21] Sentenze La Quadrature du Net e a. (punti da 120 a 122 e 132), Commissioner of An Garda Síochána e a. (punti 48 e 54), nonché SpaceNet e Telekom Deutschland (punti 63 e 69).

59. Come ho sottolineato nelle mie prime conclusioni [22], dalla giurisprudenza stessa della Corte emerge che, nel caso di un reato commesso esclusivamente online, come una violazione del diritto d'autore su una rete peer-to-peer, l'indirizzo 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 tale reato [23]. Ne consegue, a mio avviso, che la conservazione e l'accesso ai dati relativi all'identità civile corrispondenti ad indirizzi IP al fine di accertare e perseguire le violazioni del diritto d'autore commesse online sono, in conformità alla giurisprudenza, strettamente necessari alla realizzazione dell'obiettivo perseguito.

60. È vero che qualsiasi esigenza di protezione dei dati personali implica una limitazione dei poteri d'indagine. Ciò risulta dal principio stesso del contemperamento di interessi contrari, e una siffatta conclusione non può, in quanto tale, essere contestata. Tuttavia, nell'ipotesi in cui l'indirizzo IP costituisca l'unico strumento di identificazione della persona sospettata di avere commesso una violazione online di un diritto di proprietà intellettuale, una situazione del genere si distingue dalla maggior parte delle azioni penali, in relazione alle quali la Corte rileva che «l'efficacia (…) dipende in genere non da un solo strumento di indagine, bensì da tutti gli strumenti di indagine di cui dispongono le autorità nazionali competenti a tal fine» [24]. Ammettere che i dati relativi all'identità civile corrispondenti ad indirizzi IP non dovrebbero essere oggetto di una conservazione e di un accesso in una situazione come quella di cui al procedimento principale non condurrebbe, al pari di ogni misura che assicura la protezione dei dati relativi al traffico, ad una mera limitazione dei poteri d'indagine, bensì a privare le autorità nazionali dell'unico strumento di accertamento e di perseguimento di determinati reati.

61. In altre parole, non si tratta, secondo l'interpretazione da me proposta dell'articolo 15, paragrafo 1, della direttiva 2002/58, di consentire, tramite l'esame della necessità di una siffatta misura, la conservazione e l'accesso a dati che semplicemente *agevolano* l'accertamento e il perseguimento di reati, qualora tali reati possano parimenti essere accertati e perseguiti con strumenti concorrenti, anche se meno efficaci. Si tratta, per contro, di consentire la conservazione e l'accesso a tali dati qualora essi siano *indispensabili* all'identificazione della persona sospettata di avere commesso un reato, che non potrebbe essere perseguito senza siffatti strumenti, dal momento che i dati in questione costituiscono l'unico strumento di identificazione dell'utente di Internet nella misura in cui il reato è commesso esclusivamente online.

62. Una siffatta interpretazione, a mio avviso, si impone, salvo ammettere che tutta una serie di reati non possa mai essere perseguita [25].

63. Da tutto quanto suesposto risulta che, a mio avviso, una normativa nazionale che consente la conservazione da parte dei fornitori di servizi di comunicazione elettronica e l'accesso da parte di un'autorità amministrativa limitatamente ai dati relativi all'identità civile corrispondenti ad indirizzi IP è pienamente proporzionata all'obiettivo perseguito, ossia il perseguimento di violazioni commesse via Internet del diritto d'autore e dei diritti connessi, nella misura in cui l'ingerenza nei diritti fondamentali che essi comportano abbia una gravità limitata e tali dati costituiscano l'unico strumento di indagine che permetta di identificare la persona alla quale tale indirizzo era attribuito al momento della commissione del reato.

[22] Paragrafo 78 delle mie prime conclusioni.

[23] Sentenze La Quadrature du Net e a. (punto 154), Commissioner of An Garda Síochána e a. (punto 73) e SpaceNet e Telekom Deutschland (punto 100).

[24] Sentenza Commissioner of An Garda Síochána e a. (punto 69).

[25] Paragrafo 81 delle mie prime conclusioni. V. parimenti, su tale aspetto, paragrafo 79 e segg. delle presenti conclusioni.

64. Pertanto, ritengo che l'articolo 15, paragrafo 1, della direttiva 2002/58 debba essere interpretato nel senso che esso non osta ad una siffatta normativa

2. Sull'esistenza di garanzie sostanziali e procedurali adeguate

65. Per quanto riguarda specificamente l'accesso a dati relativi all'identità civile corrispondenti ad indirizzi IP, dalla giurisprudenza della Corte si evince che la mera proporzionalità rigorosa della misura non è sufficiente a renderla compatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58.

66. Infatti, al fine di assicurare che l'accesso a dati relativi al traffico e all'ubicazione sia limitato allo stretto necessario, la Corte ha dichiarato che è essenziale che tale accesso sia subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente che disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie per assicurare un contemperamento dei vari interessi legittimi e diritti in gioco [26].

67. Una lettura restrittiva della giurisprudenza porterebbe pertanto a ritenere che l'accesso da parte della Hadopi ai dati relativi all'identità civile corrispondenti agli indirizzi IP delle persone sospettate di avere commesso una violazione del diritto d'autore su Internet dovrebbe essere subordinato ad un siffatto controllo preventivo, che è invece assente nel meccanismo di risposta graduata attualmente vigente.

68. Tuttavia, come fatto valere dal governo irlandese in udienza e come ho sostenuto nelle mie prime conclusioni, ritengo che il requisito di un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente non sia un requisito sistematico, ma che dipenda da un'analisi più globale della misura in questione, la quale tenga conto sia della gravità dell'ingerenza che essa comporta sia delle garanzie che la stessa prevede.

69. Infatti, sottolineo che tutte le sentenze che hanno enunciato siffatto requisito di un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente vertevano su normative nazionali che consentivano l'accesso alla totalità dei dati relativi al traffico e all'ubicazione degli utenti concernenti tutti i mezzi di comunicazione elettronica degli utenti [27] o, quantomeno, la telefonia fissa e mobile [28] di utenti identificati.

70. Ne desumo che il requisito di un siffatto controllo preventivo è guidato dalla gravità dell'ingerenza di cui alle cause in questione. Come sottolineato dalla Corte, si trattava di dati che potevano «effettivamente consentire di trarre conclusioni precise, o addirittura molto precise, sulla vita privata delle persone (…) 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» [29]. Inoltre, venivano presi in considerazione i dati di persone già identificate e sospettate di avere commesso un reato sulla base di altri indizi, cosicché i dati in questione consentivano di corroborare gli elementi a carico contro l'utente in questione estendendo l'ambito dei dati che lo riguardavano.

[26] Sentenze Tele2 (punto 120); Prokuratuur (punti 51 e 52), nonché Commissioner of An Garda Síochána e a. (punti 106 e 107).

[27] Sentenze Tele2 e Commissioner of An Garda Síochána e a.

[28] Sentenza Prokuratuur.

[29] Sentenza Prokuratuur (punto 36).

71. Orbene, per quanto riguarda la normativa di cui al procedimento principale, e come ho sottolineato, la gravità dell'ingerenza che il collegamento ad un indirizzo IP di un dato relativo all'identità civile comporta è ben inferiore a quella risultante dall'accesso alla totalità dei dati relativi al traffico e all'ubicazione di una persona, nella misura in cui siffatto collegamento non fornisce alcun elemento che permetta di trarre conclusioni precise sulla vita privata della persona interessata.

72. Inoltre, come ho rilevato nelle mie prime conclusioni [30], tali dati riguardano unicamente le persone che, a seguito di una constatazione oggettiva di utilizzazione dell'indirizzo IP in violazione di un diritto d'autore effettuata dagli organismi di aventi diritto, hanno posto in essere fatti idonei a costituire una violazione dell'obbligo di sorveglianza previsto all'articolo L. 336-3 del CPI. Essi non sono previamente identificati tramite altri strumenti, e il collegamento dell'indirizzo IP ai dati relativi all'identità civile costituisce l'unico strumento di identificazione della persona interessata. L'accesso a tali dati non consente dunque, come avveniva nelle cause sulle quali la Corte è stata chiamata in precedenza a statuire, di ottenere informazioni supplementari e precise sull'attività di persone già sospettate sulla base di altri elementi, ma soltanto di rendere sfruttabile l'indirizzo IP, altrimenti privo di interesse. In tali circostanze, i dati ai quali la Hadopi ha accesso sono de facto limitati.

73. Esiste, a mio avviso, una differenza fondamentale tra il fatto di accedere a dati personali relativi ad una persona sospettata di avere commesso un reato al fine di dimostrare la sua colpevolezza e quello di consentire di svelare l'identità dell'autore di un reato già constatato.

74. Ciò vale a maggior ragione, a mio avviso, in quanto la raccolta degli indirizzi IP sulle reti peer-to-peer è oggetto di un'autorizzazione preliminare limitata a questi soli dati, cosicché la Hadopi non è mai in possesso di un insieme illimitato di dati nel caso degli utenti di Internet sospettati di avere commesso una violazione del diritto d'autore su Internet [31].

75. Pertanto, la logica sottesa al requisito di un controllo preventivo effettuato da un giudice o da un'entità amministrativa indipendente non si applica nel caso del meccanismo di risposta graduata come quello di cui al procedimento principale, cosicché un siffatto requisito non mi sembra necessario al fine di assicurare che l'ingerenza nei diritti fondamentali che tale meccanismo comporta sia limitata allo stretto necessario.

76. Risulta da tutte le considerazioni che precedono che una normativa nazionale che permette la conservazione e l'accesso, da parte di un'autorità amministrativa indipendente come la Hadopi, a dati relativi all'identità civile corrispondenti ad indirizzi IP al fine di identificare i titolari di tali indirizzi sospettati di essere responsabili di violazioni del diritto d'autore, senza che tale accesso sia subordinato ad un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente rispetta, in definitiva, i principi sanciti dalla giurisprudenza della Corte, qualora tali dati costituiscano l'unico strumento di identificazione della persona alla quale l'indirizzo IP era attribuito al momento della commissione del reato, cosicché l'articolo 15, paragrafo 1, della direttiva 2002/58 dovrebbe essere interpretato nel senso che esso non osta ad una siffatta normativa.

77. Al di là di tali considerazioni specifiche del procedimento principale, devo ancora formulare alcune osservazioni più generali sulla necessità di procedere a tale sviluppo della giurisprudenza della Corte.

[30] Paragrafo 102 delle mie prime conclusioni.

[31] Paragrafo 33 delle presenti conclusioni.

C. Uno sviluppo della giurisprudenza necessario e limitato

78. Diversi argomenti depongono a favore di un perfezionamento della giurisprudenza della Corte relativa alla conservazione e all'accesso a dati come gli indirizzi IP abbinati a dati relativi all'identità civile.

79. In primo luogo, e come ho già sottolineato [32], nella situazione di cui al procedimento principale, l'ottenimento dei dati relativi all'identità civile corrispondenti ad un indirizzo IP è l'unico strumento di indagine che permetta di identificare la persona alla quale tale indirizzo era attribuito al momento della commissione del reato in questione.

80. Ne consegue necessariamente che, se la Corte dovesse ritenere che l'articolo 15, paragrafo 1, della direttiva 2002/58 osti comunque alla loro conservazione e al loro accesso, le autorità nazionali sarebbero de facto private di questo unico strumento di identificazione e, pertanto, gli autori del reato in questione non potrebbero mai essere perseguiti [33]. Ciò mi ha indotto ad evocare, nelle mie prime conclusioni, la possibilità di un'impunità sistemica per tale reato [34].

81. Il rischio di un'impunità sistemica non è limitato alle violazioni del diritto d'autore commesse sulle reti peer-to-peer, ma si estende, come fatto valere dal governo ceco in udienza, a tutti i reati commessi esclusivamente online.

82. Infatti, i reati il cui autore può essere identificato unicamente mediante il suo indirizzo IP non potrebbero mai essere perseguiti e le disposizioni che li sanzionano non potrebbero mai essere applicate qualora dovesse essere statuito che sia la conservazione dei dati sia l'accesso ad essi sono contrari al diritto dell'Unione.

83. A tal riguardo, rilevo che è vero, come affermato dalle ricorrenti nel procedimento principale, che altri strumenti potrebbero consentire, in teoria, di identificare gli autori di taluni reati commessi esclusivamente online. In tal senso, esse si riferiscono segnatamente all'identificativo utilizzato sui social network e ai dati associati al conto dell'utente, al suo indirizzo di posta elettronica, al suo numero di telefono oppure ad un elemento della sua vita privata che la persona abbia rivelato. Tuttavia, siffatti dati, per poter essere collegati all'identità della persona, esigono indagini approfondite, nel corso delle quali viene esaminata l'attività online dell'utente di Internet. Il ricorso a siffatti strumenti di indagine mi sembra pertanto idoneo, a differenza del solo indirizzo IP, a trarre conclusioni molto precise sulla vita privata delle persone, cosicché la conservazione e l'accesso a tali dati sarebbero, in tal senso, contrari all'articolo 15, paragrafo 1, della direttiva 2002/58.

84. In tali circostanze, l'accesso a dati relativi all'identità civile corrispondenti all'indirizzo IP di un utente di Internet non è sicuramente l'unico strumento teorico di indagine che permetta di identificare la persona titolare di tale indirizzo al momento della commissione del reato, ma è quello che consente il suo perseguimento comportando al contempo un'ingerenza minima nei diritti fondamentali della stessa e, pertanto, di evitare un'impunità generale.

[32] Paragrafo 59 delle presenti conclusioni.

[33] Paragrafo 62 delle presenti conclusioni.

[34] Paragrafo 78 e segg. delle mie prime conclusioni.

85. In secondo luogo, sottolineo nuovamente che una simile soluzione consentirebbe, a mio avviso, di conciliare due linee giurisprudenziali della Corte, fonti di una certa tensione che avevo evidenziato nelle mie prime conclusioni [35] e in quelle relative alla causa M.I.C.M. [36], ossia, da un lato, la giurisprudenza relativa alla conservazione e all'accesso ai dati e, dall'altro, quella relativa alla comunicazione degli indirizzi IP attribuiti all'origine di una connessione nell'ambito dei ricorsi intesi alla tutela dei diritti di proprietà intellettuale, avviati da soggetti privati.

86. In terzo luogo, pur se la giurisprudenza della Corte a partire dalle sentenze Tele2 e La Quadrature du Net e a. deve essere accolta con favore, nella misura in cui ha consentito la predisposizione di un contesto che tutela i diritti fondamentali degli utenti di servizi di comunicazione elettronica, essa è cionondimeno caratterizzata da un'impostazione piuttosto casistica. Infatti, nella successione delle cause di cui è stata investita, la Corte ha proceduto ad un progressivo perfezionamento della sua giurisprudenza che le ha consentito di esaminare diverse normative nazionali alla luce dell'articolo 15, paragrafo 1, della direttiva 2002/58. È tuttavia impossibile per la Corte anticipare virtualmente tutte le misure che potrebbero essere oggetto di un'analisi alla luce di tale disposizione. Lo testimonia peraltro il numero di rinvii pregiudiziali [37] di cui quest'ultima è oggetto a partire dalla sentenza Tele2, il quale è indice, a mio avviso, della difficoltà che possono provare i giudici nazionali nell'applicare i principi enunciati nella giurisprudenza della Corte a situazioni diverse da quelle che hanno dato luogo alle sentenze in questione [38].

87. Ne consegue pertanto che una certa flessibilità mi sembra necessaria allorché vengano sottoposte all'esame della Corte misure che non potevano essere prese in considerazione in occasione di sentenze precedenti, come normative concernenti reati che possono essere perseguiti solo nella misura in cui i dati relativi all'identità civile corrispondenti ad indirizzi IP siano conservati ed accessibili, reati dei quali la Corte non è stata finora mai chiamata a conoscere.

88. Non si tratta pertanto, come sostenuto dal governo danese, di riconsiderare la giurisprudenza della Corte, bensì di ammettere che, sulla base dei principi ad essa sottesi, possa essere elaborata una soluzione più modulata, in circostanze molto limitate.

89. Infatti, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 da me proposta consente la conservazione e l'accesso a dati relativi all'identità civile corrispondenti ad indirizzi IP solo per quanto attiene al perseguimento di reati i cui autori, in assenza di siffatti dati, non potrebbero essere identificati. Essa riguarda pertanto unicamente i reati commessi

35 Paragrafo 69 e segg. delle mie prime conclusioni.

36 C-597/19, EU:C:2020:1063.

37 Sentenze del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); La Quadrature du Net e a.; Prokuratuur; Commissioner of An Garda Síochána e a., nonché SpaceNet e Telekom Deutschland.

38 Al riguardo, la moltiplicazione delle domande di pronuncia pregiudiziale aventi ad oggetto l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 può anche essere indice di una certa forma di reticenza dei giudici nazionali ad applicare i principi elaborati dalla Corte a situazioni leggermente diverse, a causa delle specificità degli ordinamenti giuridici nazionali. Su tale aspetto, v., segnatamente, Cameron, I., «Metadata retention and national security : *Privacy international* and *La Quadrature du Net*», *Common Market Law Review*, 2021, vol. 58, n.° 5, pag. da 1433 a 1471, o ancora Bertrand, B., «L'audace sans le tact : jusqu'où la Cour de justice peut-elle aller trop loin ?», *Dalloz IP/IT*, 2021, n. 9, pag. da 468 a 472. Mi sembra pertanto a maggior ragione essenziale, nell'ottica di mantenere un dialogo proficuo tra la Corte e i giudici degli Stati membri, che la Corte possa dare prova di adeguamento quando le circostanze lo impongono. Come rilevato dagli autori della dottrina, l'elevato standard di protezione istituito dalla giurisprudenza della Corte non può essere realmente efficace senza adesione da parte dei giudici nazionali, principali responsabili della sua attuazione. Su tale punto v., segnatamente, Teyssedre, J., «Strictly regulated retention and access regimes for metadata : *Commissioner of An Garda Siochana*», *Common Market Law Review*, vol. 60(2), 2023, pag. da 569 a 588, e Sirinelli, J., «La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite», *Revue trimestrielle de droit européen*, vol. 57, n.° 2, 2021, pag. da 313 a 329.

esclusivamente su Internet e non rimette in discussione le soluzioni enunciate nella giurisprudenza relative alla conservazione e all'accesso a dati più ampi, e che perseguono altri obiettivi.

V. Conclusione

90. Alla luce dell'insieme delle considerazioni che precedono, propongo alla Corte di rispondere nei seguenti termini alle questioni pregiudiziali sottoposte dal Conseil d'État (Consiglio di Stato, Francia):

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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea,

deve essere interpretato nel senso che:

esso non osta ad una normativa nazionale che consente la conservazione, da parte dei fornitori di servizi di comunicazioni elettroniche, e l'accesso, da parte di un'autorità amministrativa incaricata di proteggere il diritto d'autore e i diritti connessi contro le violazioni di tali diritti commesse su Internet, limitatamente ai dati relativi all'identità civile corrispondenti ad indirizzi IP, affinché tale autorità possa identificare i titolari di tali indirizzi sospettati di essere responsabili di siffatte violazioni e possa adottare, se del caso, misure nei loro confronti, senza che tale accesso sia subordinato ad un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente, qualora tali dati costituiscano l'unico strumento di indagine che permetta di identificare le persone alle quali tali indirizzi erano attribuiti al momento della commissione del reato.