Parere 23/2018 sulle proposte della Commissione relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (articolo 70, paragrafo 1, lettera b)

Adottato il 26 settembre 2018

Indice

Introduzione 3

1. Base legale della proposta di regolamento (articolo 82 TFUE) 4

2. Necessità di prove elettroniche rispetto a mutua assistenza giudiziaria e OEI 5

a) Necessità di prove elettroniche rispetto alle garanzie fornite dalla direttiva OEI e dal trattato di mutua assistenza giudiziaria 5

b) L'abbandono del principio di doppia punibilità 6

c) La conseguenza del contatto diretto con le società 7

3. Il nuovo fondamento della giurisdizione e la cosiddetta scomparsa del criterio di stabilimento .. 8

4. Come limitare o completare il concetto di «prestatori di servizi» con garanzie aggiuntive per i diritti dei soggetti interessati 9

5. I concetti di «stabilimento» e «rappresentante legale» nel contesto di queste proposte dovrebbero essere ben distinti dagli stessi concetti nel contesto del RGPD 11

a) Stabilimento 11

b) Rappresentante legale 11

6. Nuove categorie di dati 12

7. Analisi delle procedure per gli ordini europei di conservazione e produzione 13

a) Le soglie per l'emissione di ordini dovrebbero essere innalzate e gli ordini stessi dovrebbero essere emessi o autorizzati dal tribunale 14

b) Le scadenze per la trasmissione dei dati dovrebbero essere giustificate 16

c) Gli ordini europei di produzione e conservazione non devono essere usati per chiedere dati di un soggetto interessato di un altro Stato membro senza almeno informare le autorità competenti dello Stato in questione, in particolare per i dati relativi al contenuto 16

d) Gli ordini europei di conservazione non devono essere usati dai prestatori di servizi per aggirare gli obblighi sulla conservazione dei dati 17

e) Riservatezza e informazioni relative all'utente 17

f) Procedura per l'applicazione di un ordine quando il fornitore di servizi rifiuta di eseguirlo ... 17

g) Applicazione di ordini e obblighi confliggenti in base a leggi di paesi terzi (articoli 15 – 16) .. 18

h) Sicurezza dei trasferimenti di dati quando si risponde a un ordine 20

Conclusioni 20

Il Comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera b, del regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (RGPD),

HA ADOTTATO IL SEGUENTE PARERE:

Introduzione

Ad aprile 2018 la Commissione ha presentato una proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018) 225 final) e una proposta di direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018) 226 final). Le due proposte sono tra loro complementari. L'obbiettivo complessivo della Commissione è migliorare la cooperazione tra autorità negli Stati membri e prestatori di servizi, compresi quelli che hanno sede fuori dall'UE, e proporre soluzioni riguardo a come determinare e applicare la giurisdizione nello spazio cibernetico.

La proposta di regolamento prevede norme e procedure sull'emissione, la notifica e l'esecuzione di ordini di conservazione e produzione rivolti ai prestatori di servizi di comunicazione elettronica, mentre la proposta di direttiva stabilisce norme minime sulla nomina di rappresentanti legali di prestatori di servizi non stabiliti nel territorio dell'UE.

A novembre 2017[1], prima che la Commissione presentasse la proposta, il Gruppo di lavoro articolo 29 ("Gruppo di lavoro") ha richiamato la necessità che qualsiasi proposta legislativa rispettasse pienamente l'*acquis* comunitario sulla protezione dei dati, oltre che la legislazione e la giurisprudenza dell'UE.

In particolare, il Gruppo di lavoro ha messo in guardia contro possibili limitazioni dei diritti alla protezione dei dati e alla privacy in relazione ai dati trattati dai prestatori di servizi di telecomunicazione e della società dell'informazione, soprattutto quando trattati ulteriormente dalle autorità di contrasto, ha sottolineato quanto fosse importante che qualsiasi strumento dell'UE fosse coerente con la convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica e con la direttiva dell'UE sull'ordine europeo d'indagine (OEI), e ha raccomandato di chiarire le norme procedurali che disciplinano l'accesso alle prove elettroniche a livello nazionale e dell'UE per garantire che il nuovo strumento non conceda alle autorità nuovi poteri di cui non dispongono a livello nazionale. Oltre a tali osservazioni generali, il Gruppo di lavoro ha formulato osservazioni sulle opzioni legislative considerate all'epoca dalla Commissione riguardo le categorie di dati in questione e le corrispondenti garanzie per accedervi, sulla possibilità di obbligare mediante ordini/richieste di produzione i prestatori di servizi a fornire dati situati al di fuori dell'UE, e sulle condizioni sostanziali e procedurali e garanzie necessarie per l'accesso diretto ai dati.

Con la proposta concreta sulle prove elettroniche ora disponibile, il Comitato desidera fornire un'analisi più dettagliata degli strumenti giuridici proposti dal punto di vista della protezione dei dati.

[1] Cfr. dichiarazione del Gruppo di lavoro (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

1. Base giuridica della proposta di regolamento (articolo 82 TFUE)

La base giuridica suggerita nella proposta di regolamento sulle prove elettroniche è l'articolo 82, paragrafo 1 del TFUE, relativo alla cooperazione giudiziaria in materia penale, che dispone:

> *"1.* La cooperazione giudiziaria in materia penale nell'Unione è fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e include il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri nei settori di cui al paragrafo 2 e all'articolo 83.
>
> Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, adottano le misure intese a:
>
> a) definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza e di decisione giudiziaria;
>
> b) prevenire e risolvere i conflitti di giurisdizione tra gli Stati membri;
>
> c) sostenere la formazione dei magistrati e degli operatori giudiziari;
>
> d) facilitare la cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni."

Come sottolineato dalla Commissione nella valutazione d'impatto che accompagna le proposte, l'"articolo 82, paragrafo 1, specifica che la cooperazione giudiziaria in materia penale deve basarsi sul principio del riconoscimento reciproco. Tale base giuridica si applicherebbe all'eventuale legislazione in materia di cooperazione diretta con i prestatori di servizi, nell'ambito della quale l'autorità dello Stato membro di emissione si rivolgerebbe direttamente a un'entità (il prestatore di servizi) nello Stato di esecuzione imponendole di assolvere a determinati obblighi. Ciò introdurrebbe una nuova dimensione nel riconoscimento reciproco, che va oltre la cooperazione giudiziaria tradizionale nell'Unione, attualmente basata su procedure che coinvolgono due autorità giudiziarie, una nello Stato di emissione e l'altra nello Stato di esecuzione." (sottolineatura aggiunta)

Data la novità dell'uso di tale base giuridica nel contesto delle richieste dirette tra autorità pubbliche e privati, il Comitato lamenta che la Commissione non abbia fornito alcuna ulteriore analisi o valutazione al riguardo.

In effetti, come già sottolineato dal Gruppo di lavoro nella sua precedente dichiarazione, il Comitato continua a far presenti i propri dubbi sull'appropriatezza di tale base giuridica, dubbi che sono supportati anche dall'analisi della Corte di giustizia dell'Unione europea e dal suo avvocato generale nel parere 1/15. Tra gli sviluppi rilevati riguardo alla validità dell'articolo 82 come base giuridica per la proposta di accordo PNR tra UE e Canada, la Corte ha sottolineato che l'autorità competente canadese "*non costituisce né un'autorità giudiziaria né un ente equivalente*"[2]. Nel contesto delle proposte relative alle prove elettroniche, uno degli scopi principali dichiarati dalla Commissione pare essere quello di evitare l'eccessiva "onerosità" della cooperazione giudiziaria. Di conseguenza, la proposta si basa sul principio che la cooperazione dovrebbe avere luogo tra un'autorità e un prestatore di servizi piuttosto che tra due autorità. La procedura prevista pone in primo luogo gli enti privati nella posizione di essere la parte ricevente e di rispondere alle richieste provenienti dall'autorità giudiziaria.

Il Comitato fa notare che la procedura di esecuzione degli ordini di produzione e conservazione potrebbe comportare il coinvolgimento di un'autorità ricevente nel caso in cui il prestatore di servizi

[2] Cfr. punto 103 del parere 1/15 e punto 108 delle conclusioni dell'avvocato generale nella causa in oggetto.

destinatario non adempia ai propri obblighi, rendendo quindi necessaria un'esecuzione *ex-post* dell'ordine in questione. Tuttavia, dato che l'obiettivo principale della procedura è precisamente quello di non coinvolgere un'autorità ricevente, il Comitato dubita che una simile procedura ausiliaria possa giustificare il riferimento all'articolo 82 come sola base giuridica per questo strumento.

Pertanto, il Comitato ritiene che per usare l'articolo 82 come base giuridica i principali passi procedurali della cooperazione dovrebbero svolgersi tra due autorità giudiziarie e che sarebbe opportuno far riferimento a un'altra base giuridica per la cooperazione qui prevista.

2. Necessità di prove elettroniche rispetto agli accordi di assistenza giudiziaria e all'OEI

Il Comitato rileva che la Commissione è impegnata ad analizzare gli ostacoli alle indagini penali, soprattutto riguardo all'accesso alle prove elettroniche. Nella relazione, la Commissione delinea il contesto della proposta e sottolinea la natura volatile di tali prove, la loro dimensione internazionale e la necessità di adattare il meccanismo di cooperazione all'era digitale. Le proposte di regolamento e di direttiva per il trasferimento e l'accesso alle prove elettroniche non mirano a sostituire i precedenti strumenti di cooperazione in materia penale come la convenzione di Budapest, gli accordi di assistenza giudiziaria (MLAT) e l'ordine europeo di indagine (direttiva OEI). Secondo la Commissione, le proposte sulle prove elettroniche hanno lo scopo di migliorare la cooperazione giudiziaria in materia penale tra autorità e prestatori di servizi all'interno dell'Unione europea, oltre che con paesi terzi, in particolare gli Stati uniti d'America.

Dato che tali nuovi strumenti aggiuntivi saranno specificamente dedicati all'accesso e al trasferimento di prove elettroniche, il Comitato si occuperà di analizzare il loro valore aggiunto rispetto alla direttiva OEI e agli accordi di assistenza giudiziaria.

a) Necessità di prove elettroniche rispetto alle garanzie fornite dalla direttiva OEI e dagli accordi di assistenza giudiziaria

L'argomento principale della Commissione a favore delle proposte sulle prove elettroniche consiste nell'accelerazione della procedura per mettere in sicurezza e ottenere prove elettroniche che sono conservate e/o detenute da prestatori di servizi stabiliti in un'altra giurisdizione.

Il Comitato, tuttavia, lamenta che la necessità di un nuovo strumento per organizzare l'accesso alle prove elettroniche non è dimostrata nella valutazione d'impatto. In effetti, nelle proposte non si dimostra l'assenza di strumenti meno intrusivi eventualmente utilizzabili per raggiungere lo scopo della proposta sulle prove elettroniche, mentre si sarebbero potute valutare soluzioni alternative. Ad esempio, si sarebbe potuta esaminare l'opzione di modificare e migliorare la direttiva OEI, e ciò avrebbe anche risposto allo specifico requisito previsto dalla suddetta direttiva di valutare la necessità di una modifica del testo entro il 21 maggio 2019[3]. Un'altra opzione sarebbe potuta consistere nel prevedere l'utilizzo di ordini di conservazione per congelare i dati fino all'emissione di una richiesta formale secondo un accordo di assistenza giudiziaria. Tali opzioni avrebbero permesso di mantenere le garanzie fornite da questi strumenti, garantendo al contempo che i dati personali richiesti non siano cancellati.

[3] Cfr. articolo 37 della direttiva OEI.

Il Comitato rileva come i termini fissati nella direttiva OEI siano più lunghi di quelli previsti dalla proposta sulle prove elettroniche. In effetti, l'autorità di esecuzione ha 30 giorni per decidere sulla richiesta[4] e deve poi dare esecuzione all'ordine entro 90 giorni[5]. A parere del Comitato concedere 30 giorni di riflessione alle autorità di esecuzione nella direttiva OEI costituisce una garanzia fondamentale che permette loro di stabilire se la richiesta di esecuzione sia fondata e rispetti tutte le condizioni per l'emissione e la trasmissione di un OEI[6].

La preoccupazione del Comitato è che il termine di 10 giorni previsto nelle proposte sulle prove elettroniche per l'esecuzione del certificato di ordine europeo di produzione (EPOC), senza un periodo di riflessione, impedisca di valutare adeguatamente se l'EPOC rispetti tutti i relativi criteri e sia completato correttamente.

Pertanto la raccomandazione del Comitato è che al destinatario di un EPOC sia concesso più tempo per stabilire se si debba o meno dare esecuzione all'ordine.

Il Comitato rileva che, per l'ordine europeo di conservazione (EPOC-PR), non vi è alcuna garanzia che la conservazione dei dati sarà limitata a ciò che è necessario produrre. Infatti il periodo di conservazione potrebbe superare 60 giorni poiché non è previsto un termine entro cui l'autorità di emissione comunichi al destinatario di astenersi dall'emettere o di revocare un ordine di produzione. Il Comitato raccomanda quindi che sia fissato almeno un termine entro cui l'autorità di emissione debba comunicare di astenersi dall'emettere o di revocare l'ordine di produzione al fine di rispettare il principio della minimizzazione dei dati previsto dal RGPD[7].

Infine, il Comitato rileva che la direttiva OEI prevede la restituzione delle prove dallo Stato di emissione all'autorità di esecuzione[8]. Tuttavia, la proposta di regolamento sulle prove elettroniche non dice nulla su tale possibilità. Non è chiaro cosa accada alle prove elettroniche dopo la loro trasmissione all'autorità di emissione.

Pertanto, il Comitato raccomanda che la proposta di regolamento contenga maggiori informazioni sull'utilizzo delle prove elettroniche dopo il loro trasferimento all'autorità di emissione al fine di rispettare il RGPD e il principio di trasparenza[9] oltre che il principio di specificità previsto dagli accordi di assistenza giudiziaria.

b) L'abbandono del principio di doppia punibilità

Il Comitato è consapevole del fatto che il riconoscimento reciproco dipende dall'applicazione del principio di doppia punibilità, il quale è un modo per gli Stati membri di conservare la sovranità. Tuttavia, il principio della doppia punibilità è sempre più considerato un ostacolo alla cooperazione giudiziaria. Gli Stati membri dell'UE sono sempre più disponibili a cooperare, anche se le misure investigative si riferiscono ad azioni che non sono considerate reato dalle rispettive norme nazionali. Il Comitato sottolinea, tuttavia, che il principio di doppia punibilità mira a fornire un'ulteriore garanzia per assicurare che uno Stato non possa basarsi sull'assistenza di un altro Stato per imporre una sanzione penale che non esiste nella legge di un altro Stato. Tale principio, ad esempio, impedirebbe a uno Stato di chiedere l'aiuto di un altro Stato per imprigionare qualcuno a causa di opinioni politiche che non costituiscono reato nello Stato a cui è presentata la richiesta, oppure di perseguire una donna

[4] Articolo 12, paragrafo 3, della direttiva OEI.
[5] Articolo 12, paragrafo 4, della direttiva OEI.
[6] Articolo 12, paragrafo 6, della direttiva OEI.
[7] Articolo 5, paragrafo 1, lettera c), del regolamento generale sulla protezione dei dati.
[8] Articolo 13, paragrafi 3 e 4, della direttiva OEI.
[9] Articolo 5, paragrafo 1, lettera a), del regolamento generale sulla protezione dei dati.

per avere abortito se risiede in uno Stato dove l'aborto non è reato. Il principio di doppia punibilità è spesso accompagnato da limitazioni o garanzie aggiuntive riguardo alle sanzioni se queste differiscono troppo tra lo Stato richiedente e quello di esecuzione. L'esempio emblematico è l'impegno a non applicare la pena di morte previsto da alcuni accordi di assistenza giudiziaria quando essa non è contemplata dalla legislazione di una delle due parti.

Il Comitato fa notare che il principio di doppia punibilità è escluso nella proposta di regolamento sulle prove elettroniche. Ciò tuttavia comporta non solo l'eliminazione delle consuete formalità per il riconoscimento reciproco, ma anche il venir meno delle garanzie correlate al principio di doppia punibilità in quanto tale.

In effetti, il Comitato rileva che non c'è alcun riferimento alla legge del paese dove è situato il prestatore di servizi e che la conservazione dei dati, oltre che la produzione dei dati relativi agli abbonati o agli accessi, può riguardare qualsiasi reato[10] indipendentemente dal fatto che ve ne sia uno simile nell'ordinamento di altri Stati membri.

Allo stesso tempo gli ordini di produzione possono essere emessi ed eseguiti solo se una misura simile è a disposizione per lo stesso reato in una situazione nazionale paragonabile nello Stato di emissione[11]. Inoltre, come spiega la Commissione nella relazione figurante nella proposta di regolamento, si riconosce la specificità dei dati relativi alle operazioni e al contenuto, in quanto ritenuti più sensibili. In effetti, gli ordini riguardanti dati relativi alle operazioni o al contenuto si basano su una soglia pari a una pena detentiva della durata massima di almeno tre anni, in modo da rispettare la proporzionalità e i diritti delle persone coinvolte[12]. D'altro canto il Comitato sottolinea come non vi è stata tuttora all'interno dell'UE un'armonizzazione dei reati passibili di una pena detentiva della durata massima di almeno tre anni.

Il Comitato è contrario all'abbandono del principio di doppia punibilità, che mira a garantire che uno Stato non possa contare sull'aiuto esterno per far applicare il proprio diritto penale fuori dal territorio nazionale da parte di un altro Stato che non segue la stessa impostazione, specialmente considerando il venir meno di altre importanti garanzie tipiche del diritto penale (cfr. il punto 3 infra sul criterio di ubicazione e il punto 7, lettera g), su potenziali contrasti con il diritto di un paese terzo).

c) La conseguenza del contatto diretto con le società

Il Comitato è consapevole che le prove elettroniche sono disponibili sempre più su infrastrutture private e si possono trovare fuori dal territorio del paese che conduce l'indagine presso prestatori di servizi.

Il Comitato rileva che a seguito delle decisioni su *Yahoo*[13]! e *Skype*[14] in Belgio, e nel contesto di attentati terroristici, serve una collaborazione più fluida e veloce tra entità pubbliche e private. Nella valutazione d'impatto condotta dalla Commissione si fa riferimento a tre tipi di strumenti procedurali che coinvolgono sia autorità pubbliche sia prestatori di servizi: cooperazione giudiziaria, cooperazione diretta e accesso diretto. Mentre il primo strumento non pone la responsabilità per l'esecuzione dell'OEI in capo al prestatore di servizi bensì all'autorità di esecuzione[15], il secondo (cooperazione

[10] Articolo 5, paragrafo 3, e articolo 6, paragrafo 2, del proposto regolamento sulle prove elettroniche.
[11] Articolo 5, paragrafo 2, del proposto regolamento sulle prove elettroniche.
[12] Articolo 5, paragrafo 4, lettera a), del proposto regolamento sulle prove elettroniche.
[13] Hof van Cassatie of Belgium, YAHOO! Inc., n. P.13.2082.N del 1° dicembre 2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, n.. ME20.F1.105151-12 del 27 ottobre 2016. (Skype ha impugnato il provvedimento).
[15] Articoli 10 – 16.

diretta) si basa sulla cooperazione col prestatore di servizi. Il più intrusivo dal punto di vista del prestatore di servizi è l'accesso diretto, in quanto le autorità pubbliche possono avere accesso ai dati senza l'ausilio di intermediari.

Pertanto il Comitato teme che, se contattati direttamente, i prestatori di servizi non garantiscano la protezione dei dati personali con la stessa efficienza che le entità pubbliche possono e devono garantire, e sottolinea che ciò comporta anche l'inapplicabilità di talune garanzie procedurali previste nel contesto della cooperazione giudiziaria per le persone fisiche, oltre che per le società stesse[16]. Ad esempio, un prestatore di servizi cui sia stato richiesto di ottemperare a un ordine dovrebbe agire in giudizio in un altro Stato (membro) per opporsi all'ordine, mentre nel contesto della cooperazione giudiziaria potrebbe farlo nel suo paese. Il Comitato raccomanda di inserire nella proposta di regolamento motivazioni aggiuntive che assicurino che i prestatori di servizi tuteleranno i diritti fondamentali tra cui la protezione dei dati personali e il rispetto della vita privata e familiare, oltre a informare la competente autorità di protezione dati per garantire il controllo.

3. Il nuovo fondamento della giurisdizione e la cosiddetta scomparsa del criterio di ubicazione

Il Comitato prende atto di come la Commissione sottolinei che uno dei principali cambiamenti introdotti da queste proposte sia la scomparsa del criterio di ubicazione e la possibilità per le autorità competenti di richiedere la conservazione e la produzione dei dati indipendentemente dal luogo ove questi siano effettivamente conservati.

Dal punto di vista della protezione dei dati non è una novità che la legislazione UE in materia si applichi indipendentemente dal luogo ove sono conservati i dati degli interessati. In effetti, l'applicabilità del RGPD dipende o dal fatto che il titolare o il responsabile del trattamento è stabilito nell'UE, o dal fatto che sono trattati dati di interessati che si trovano nell'UE, anche se il titolare o il responsabile del trattamento non è stabilito nell'UE[17], nel qual caso si deve designare un rappresentante legale nell'UE[18]. Dal punto di vista della protezione dei dati è importante notare che l'estensione dell'ambito territoriale mira a garantire una protezione più completa agli interessati che si trovano nell'UE, indipendentemente da dove abbia sede la società che tratta i loro dati personali.

Pertanto sebbene la scomparsa del criterio di ubicazione possa essere una novità nell'ambito del diritto penale, non pare essere un cambiamento significativo dal punto di vista della protezione dei dati. Inoltre, il Comitato rileva che si mantiene comunque un collegamento col territorio dell'UE, in quanto solo i prestatori di servizi che offrono servizi all'interno dell'UE rientrano nell'ambito di applicazione delle proposte, e il fatto che le richieste possano essere formulate unicamente nel contesto di indagini penali implica un collegamento con l'UE (in quanto o il reato è stato commesso nel territorio di uno Stato membro, oppure la vittima o il reo erano cittadini di uno Stato membro).

Se la scomparsa del criterio di ubicazione deve ora essere applicata nel diritto penale, il Comitato ritiene che la questione principale sia garantire che tale sviluppo non leda la protezione dei dati e i

[16] Cfr. altresì, dal punto di vista della protezione dei dati internazionale «Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes» (in inglese), gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni, 63° incontro, 9-10 aprile 2018, Budapest (Ungheria).
[17] Cfr. articolo 3, in particolare il paragrafo 2.
[18] Cfr. articolo 27.

diritti nel procedimento penale degli interessati e dei prestatori di servizi cui è richiesto di ottemperare a un ordine. A tale riguardo, il Comitato riconosce che all'interno dell'UE le garanzie procedurali sono state almeno in parte armonizzate e devono essere attuate nel rispetto della Convenzione europea sui diritti dell'uomo. Si può quindi sostenere che la scomparsa del criterio di ubicazione avrebbe forse effetti più limitati nel caso in cui si cerchino prove all'interno dell'UE rispetto alla situazione opposta, ossia quando autorità di paesi terzi chiedono dati a società stabilite nell'UE alle stesse condizioni previste dalla proposta di regolamento sulle prove elettroniche. Effettivamente una preoccupazione particolare del Comitato è che ciò possa portare a situazioni più problematiche. In tale contesto, le autorità di un paese terzo, dove le garanzie procedurali sono diverse e potenzialmente minori, potrebbero avere accesso a dati protetti da garanzie aggiuntive all'interno dell'UE. A tale proposito il Comitato reitera le proprie preoccupazioni riguardo a un doppio standard e a un indebolimento dei diritti fondamentali quando i prestatori di servizi e gli interessati non beneficiano delle garanzie procedurali previste dal diritto dell'UE qualora la richiesta sia presentata da un'autorità di un paese terzo.

Inoltre, poiché questo nuovo fondamento della giurisdizione «indipendentemente dall'ubicazione dei dati» si associa a una procedura basata principalmente su richieste dirette rivolte da autorità competenti a prestatori di servizi, il Comitato esprime la preoccupazione che le garanzie per la protezione dei dati non siano applicate dalle società private che ricevono le richieste e che non sono vincolate da uno strumento giuridico come un accordo di assistenza giudiziaria, che tradizionalmente regola gli scambi di dati tra autorità giudiziarie e fornisce le necessarie garanzie. In particolare, nel contesto di accordi di assistenza giudiziaria, le garanzie minime per la protezione dei dati implicano, ad esempio, obblighi di riservatezza e il principio di specificità, secondo cui i dati non possono essere trattati per uno scopo diverso.

Il Comitato sottolinea che dovrebbero essere rese applicabili quanto meno le garanzie previste dalla direttiva (UE) 2016/680, anche in riferimento ai trasferimenti di dati, in particolare l'articolo 39 qualora il prestatore di servizi sia situato in un paese terzo che non sia oggetto di una decisione di adeguatezza in questo ambito. In particolare, il Comitato sottolinea che quest'ultima disposizione prevede segnatamente l'obbligo di informare l'autorità per la protezione dei dati dello Stato membro dell'autorità di emissione dell'ordine e la tenuta di documentazione relativa al trasferimento, anche per quanto riguarda la giustificazione dell'inefficacia o inadeguatezza di un trasferimento all'autorità competente del paese terzo.

4. Il concetto di "prestatori di servizi" dovrebbe essere limitato o integrato da garanzie aggiuntive per i diritti degli interessati

Per quanto concerne i prestatori di servizi, il Comitato è favorevole alla definizione ampia che consente di comprendere sia i servizi di comunicazione sia quelli Over-The-Top (OTT), poiché tutti questi servizi sono equivalenti dal punto di vista funzionale e, pertanto, le misure previste potrebbero avere un impatto simile sul diritto alla privacy e alla riservatezza delle comunicazioni, come evidenziato nella dichiarazione del Gruppo di lavoro e ancora prima nel parere 01/2017 sulla proposta di regolamento in materia di ePrivacy. In effetti, la proposta di regolamento sulle prove elettroniche si applica ai prestatori di servizi che forniscono servizi di comunicazione elettronica come definiti all'articolo 2, paragrafo 4, della direttiva che istituisce il Codice europeo delle comunicazioni elettroniche, ai servizi della società dell'informazione come definiti all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 "per i quali la conservazione dei dati è una componente propria del servizio fornito

all'utente, compresi i social network nella misura in cui non possono essere considerati servizi di comunicazione elettronica, i mercati online che agevolano le operazioni tra utenti (come consumatori o imprese) e altri prestatori di servizi di hosting" e ai servizi di nome di dominio e di numerazione IP "quali i prestatori di indirizzi IP, i registri di nomi di dominio, i registrar di nomi di dominio e i connessi servizi per la privacy o proxy"[19].

Tuttavia, ai sensi della proposta di regolamento, essendo un prestatore di servizi «qualsiasi persona fisica o giuridica che fornisca una o più delle seguenti categorie di servizi», il Comitato esprime la preoccupazione che lo strumento in questione riguardi sia i titolari sia i responsabili del trattamento ai sensi del RGPD. In effetti, poiché «che offre servizi» secondo l'articolo 2, paragrafo 4, della proposta di regolamento implica sia permettere alle persone fisiche o giuridiche in uno o più Stati membri di ricorrere ai servizi in questione, sia un collegamento sostanziale con gli Stati membri coinvolti, tali attività includono quelle svolte da un responsabile del trattamento per il titolare del trattamento, ad esempio la conservazione dei dati.

Il Comitato teme, dunque, che se non ci si limita ai prestatori di servizi che agiscono come titolari del trattamento ai sensi del RGPD, e se non si prevede alcun obbligo specifico in capo al responsabile di informare il titolare del trattamento qualora sia destinatario di un ordine di produzione o conservazione, si possano eludere i diritti degli interessati. Ciò vale specialmente nel caso di possibili obblighi contrastanti che impediscono al destinatario di notificare gli ordini ricevuti, poiché in tal caso le autorità giudiziarie sono invitate nella proposta di regolamento a rivolgersi al soggetto più adeguato indipendentemente dalle norme sulla protezione dei dati applicabili, soprattutto tenuto conto che è possibile richiedere qualsiasi dato, non solo dati personali coperti dal RGPD[20].

Conformemente al RGPD, il responsabile del trattamento agisce solo su istruzione del titolare del trattamento. Ne consegue che quest'ultimo ha la responsabilità di garantire il rispetto dei diritti degli interessati e di fornire loro le informazioni pertinenti, anche per quanto riguarda i destinatari dei loro dati, ad esempio nel contesto dell'esercizio del loro diritto di accesso. Il responsabile del trattamento non riceverà tali richieste dagli interessati e non è in grado di rispondervi, a meno che non glielo chieda espressamente il titolare del trattamento.

Di conseguenza, a meno che i loro diritti siano stati limitati in applicazione del RGPD, il Comitato sottolinea che gli interessati che beneficiano dell'applicazione del suddetto regolamento potrebbero non essere in grado di esercitare in modo efficace i propri diritti se il titolare non è in condizione di fornire loro informazioni complete. Il Comitato rileva inoltre che la probabilità di una tale carenza di informazioni è ancora più elevata in assenza di un obbligo specifico per il responsabile del trattamento di informare il titolare del trattamento quando i dati richiesti riguardano interessati che non beneficiano della protezione garantita dal RGPD. Infatti, in questo caso le autorità giudiziarie richiedenti non avranno necessariamente l'obbligo di informare gli interessati riguardo al successivo trattamento dei dati da esse svolto. Il Comitato pertanto chiede di limitare l'ambito di applicazione ai titolari del trattamento ai sensi del RGPD, ovvero di introdurre una disposizione al fine di chiarire che qualora il prestatore di servizi cui è rivolta la richiesta non sia il titolare del trattamento, ne informi il titolare.

[19] Articolo 2, paragrafo 3, lettera c), del proposto regolamento sulle prove elettroniche.
[20] Cfr. articolo 7, paragrafi 3 e 4.

5. Le nozioni di "stabilimento" e "rappresentante legale" nel contesto di queste proposte dovrebbero essere ben distinte dalle stesse nel contesto del RGPD

Data l'inapplicabilità del criterio di ubicazione dei dati, i destinatari degli ordini di produzione e di conservazione nell'ambito della proposta di regolamento sono limitati ai prestatori di servizi che offrono servizi all'interno dell'Unione europea, siano essi stabiliti o meno nell'UE, con l'obbligo di nominare un rappresentante legale secondo le norme proposte nella proposta di direttiva. Le nozioni di "stabilimento" e "rappresentante legale" sono pertanto definiti nelle proposte di strumento.

Il Comitato rileva che le nozioni in questione compaiono anche nel contesto di altri strumenti UE, in particolare il RGPD. Pertanto è opportuno che siano forniti chiarimenti sulla definizione e sulla descrizione di tali nozioni nel contesto delle proposte e nel contesto del RGPD.

a) Stabilimento

Il Comitato ricorda che la nozione di "stabilimento" nel contesto della proposta di regolamento non deve essere confusa con quella nel contesto del RGPD. Infatti, ai fini della proposta di regolamento la nozione di stabilimento come definito all'articolo 2, paragrafo 5, è più ampia di quella del RGPD poiché comprende "l'esercizio effettivo di un'attività economica a tempo indeterminato con un'infrastruttura stabile a partire dalla quale viene svolta l'attività di prestazione di servizi, o l'infrastruttura stabile a partire dalla quale l'attività è gestita", indipendentemente dal fatto che un trattamento di dati personali abbia luogo nel contesto delle attività svolte presso lo stabilimento. Pertanto, se è vero che lo «stabilimento» ai sensi del RGPD deve indubbiamente rientrare nella nozione di stabilimento definita dalla proposta di regolamento, potrebbe non valere il contrario.

Il Comitato segnala pertanto che gli stabilimenti di prestatori di servizi ai sensi della proposta di regolamento non implicano necessariamente il rispetto delle condizioni per l'applicazione del RGPD secondo l'articolo 3, paragrafo 1. A tale riguardo, il titolare del trattamento e il responsabile del trattamento sono invitati a verificare se l'applicabilità del RGPD non derivi dall'articolo 3, paragrafo 2, il che richiederebbe la nomina di un rappresentante legale all'interno dell'UE e l'assenza del meccanismo detto di sportello unico (One-Stop-Shop).

b) Rappresentante legale

Nella sua dichiarazione il Gruppo di lavoro afferma che è necessario evitare qualsiasi confusione tra l'obbligo di nominare un rappresentante legale in base all'articolo 27 del RGPD e il rappresentante legale previsto dalla proposta di regolamento in materia di prove elettroniche.

Il Comitato desidera ribadire le proprie raccomandazioni, sottolineando in particolare che, a suo avviso, il rappresentante legale di cui alla proposta di direttiva sulla nomina di un rappresentante legale nel contesto delle proposte sulle prove elettroniche deve essere designato in ogni caso, avere funzioni specifiche indipendentemente da un mandato attribuito dal prestatore di servizi, avere il potere di rispondere a richieste e di agire per conto del prestatore di servizi, oltre che una maggiore responsabilità rispetto al rappresentante legale di cui al RGPD.

Inoltre, il Comitato sottolinea che l'obbligo di designare in ogni caso un rappresentante legale a norma delle proposte sulle prove elettroniche, indipendentemente dal fatto che il prestatore di servizi sia stabilito o meno nell'UE, la possibilità di designare addirittura più rappresentanti legali per lo stesso prestatore di servizi in base alla proposta di direttiva sulle prove elettroniche e l'obbligo di comunicare

la designazione del rappresentante legale alle autorità degli Stati membri differiscono da quanto previsto dal RGPD, che non impone alcun obbligo di comunicazione della designazione del rappresentante legale, né esenzioni dall'obbligo di designazione o limitazioni alle responsabilità del rappresentante legale.

Considerando quindi le sostanziali differenze in termini di ruolo, responsabilità e rapporto con gli altri stabilimenti del prestatore di servizi in un caso e del titolare del trattamento e del responsabile del trattamento nell'altro, il Comitato raccomanda che, nel caso in cui un prestatore di servizi non sia situato nell'UE ma sia comunque soggetto sia al RGPD ai sensi dell'articolo 3, paragrafo 2 di quest'ultimo, sia al regolamento sulle prove elettroniche, si debbano designare due diversi rappresentanti legali, ciascuno con funzioni chiaramente distinte conformemente allo strumento in base al quale avviene tale designazione.

6. Nuove categorie di dati

La proposta di regolamento all'articolo 2 definisce diverse categorie di dati: i dati relativi agli abbonati, i dati relativi agli accessi, i dati relativi alle operazioni e i dati relativi al contenuto. Il considerando 20 della proposta della Commissione specifica inoltre che *"[l]e categorie di dati rientranti nell'ambito di applicazione del presente regolamento comprendono i dati relativi agli abbonati, i dati relativi agli accessi, i dati relativi alle operazioni (categorie congiuntamente denominate «dati non relativi al contenuto») e i dati relativi al contenuto. Questa distinzione, tranne per quanto riguarda i dati relativi agli accessi, esiste negli ordinamenti giuridici di molti Stati membri e nell'attuale quadro giuridico statunitense, che consente ai prestatori di servizi di condividere su base volontaria i dati non relativi al contenuto con le autorità di contrasto straniere."*

In tale contesto, il Comitato prima di tutto sottolinea che tutte e quattro le categorie di dati citate sopra sono da considerarsi dati personali ai sensi della legislazione dell'UE in materia di protezione dei dati personali poiché contengono informazioni relative a una persona fisica identificata o identificabile, indipendentemente dal fatto che l'interessato sia indicato come «abbonato» o «utente» nella proposta di regolamento. Analogamente va notato che le «prove elettroniche» come definite all'articolo 2, paragrafo 6, della proposta della Commissione riguardano tutte e quattro le categorie di dati e quindi si riferiscono a dati personali. Pertanto, piuttosto che stabilire le norme di accesso alle prove, definite e qualificate dal diritto nazionale e dalle procedure giudiziarie, la proposta di regolamento prevede nuove condizioni sostanziali e procedurali per l'accesso ai dati personali.

Mentre La proposta di regolamento crea nuove sottocategorie di dati personali ai quali si applicano diverse condizioni procedurali di accesso, il Comitato sottolinea che, secondo la giurisprudenza della Corte di giustizia UE, per stabilire se vi sia interferenza col diritto fondamentale alla privacy non importa se le informazioni sulle vite private siano sensibili o se le persone coinvolte abbiano subito un tipo di disagio.

Inoltre, il Comitato rileva che, in relazione ai "dati non relativi al contenuto" che comprendono dati relativi agli abbonati, agli accessi e alle operazioni ai sensi della proposta delle Commissione, la Corte di giustizia dell'Unione europea ha stabilito con la sentenza nelle cause riunite C-203/15 e C-698/15 Tele*2 Sverige AB* che i metadati (come i dati relativi al traffico e i dati relativi all'ubicazione) permettono

di definire il profilo dei soggetti coinvolti, informazioni che non sono meno sensibili, nel contesto del diritto alla privacy, dell'effettivo contenuto delle comunicazioni[21].

Come già indicato nella dichiarazione del Gruppo di lavoro riguardo alla protezione dei dati e ad aspetti relativi alla privacy nell'accesso transfrontaliero alle prove elettroniche del 29 novembre 2017, il Comitato ribadisce quindi i propri dubbi e preoccupazioni sull'attuale demarcazione tra dati "non relativi al contenuto" e dati relativi al contenuto, e sulle quattro categorie di dati personali previste dalla proposta di regolamento. In effetti, tali quattro gruppi non paiono ben delineati e la definizione di "dati relativi agli accessi" rimane ancora vaga rispetto alle altre categorie. Il Comitato lamenta pertanto come la valutazione di impatto e la proposta della Commissione abbiano omesso di fornire elementi più specifici a sostegno della creazione di queste nuove sottocategorie di dati personali, ed esprime preoccupazione riguardo al diverso livello di garanzie connesse alle condizioni sostanziali e procedurali per l'accesso alle categorie di dati personali, specialmente vista la difficoltà pratica, in qualche caso, nel valutare a quale categoria di dati appartengano le informazioni richieste. Ad esempio, gli indirizzi IP potrebbero essere sia dati relativi alle operazioni sia dati relativi agli abbonati.

In tale contesto, il Comitato ricorda come al considerando 14 della proposta di regolamento riguardante il rispetto della vita privata e la protezione dei dati personali nelle comunicazioni elettroniche (ePrivacy), la Commissione stabilisca che «[i] dati delle comunicazioni elettroniche dovrebbero essere definiti in modo sufficientemente ampio e tecnologicamente neutro da ricomprendere tutte le informazioni relative al contenuto trasmesso o scambiato (contenuto delle comunicazioni elettroniche) nonché le informazioni relative a un utente finale di servizi di comunicazione elettronica trattati al fine di trasmettere, distribuire o consentire lo scambio di contenuto delle comunicazioni elettroniche, compresi i dati atti a tracciare e identificare la fonte e la destinazione di una comunicazione, l'ubicazione geografica nonché la data, l'ora, la durata e il tipo di comunicazione». Dato che il quadro attuale e futuro in materia di ePrivacy, oltre che le relative limitazioni al diritto alla riservatezza, troveranno applicazione in materia di accesso alle prove elettroniche nelle attività di polizia e giudiziarie, il Comitato raccomanda di inserire una definizione più ampia di dati relativi alle comunicazioni elettroniche nella proposta di regolamento per garantire garanzie e condizioni adeguate in relazione all'accesso che comprendano in modo coerente sia i dati «non relativi al contenuto» sia quelli «relativi al contenuto».

7. Analisi delle procedure per gli ordini europei di conservazione e produzione di prove

A grandi linee, la procedura da seguire per un ordine di produzione o di conservazione si può riassumere come segue:

- L'autorità giudiziaria competente – l'autorità di emissione – a seconda del tipo di dati richiesti e del tipo di ordine, emette l'ordine sulla base delle (limitate) condizioni elencate agli articoli 5 e 6, e lo invia utilizzando un certificato standard al rappresentante legale del prestatore di servizi o a uno dei suoi stabilimenti nell'UE – il destinatario.
- Una volta ricevuto il certificato, il destinatario esegue l'ordine – vale a dire trasmette i dati entro 10 giorni oppure entro sei ore in caso di emergenza, o li conserva fino a 60 giorni –

[21] CGUE - Sentenza del 21 dicembre 2016, punto 99.

eccetto qualora ciò risulti impossibile in quanto il certificato è incompleto o a causa di forza maggiore o per impossibilità di fatto per il destinatario, o perché il destinatario rifiuta a causa di obblighi contrastanti relativamente a diritti fondamentali o interessi fondamentali di un paese terzo o per altri motivi.

- Nel caso in cui il destinatario non ottemperi all'ordine ricevuto e non fornisca motivazioni accettate dall'autorità di emissione, si applicano procedure per l'esecuzione dell'ordine da parte dell'autorità di esecuzione competente dello Stato membro in cui il prestatore di servizi è rappresentato o stabilito, a meno che sussistano motivi limitati per il rifiuto e l'autorità competente si opponga al riconoscimento o all'esecuzione dell'ordine.
- Nel caso in cui il destinatario presenti un'obiezione motivata all'ordine sulla base di obblighi contrastanti, l'autorità di emissione deferisce il caso all'organo giurisdizionale competente del proprio Stato membro, che valuterà il possibile conflitto e, se questo non sussiste, confermerà l'ordine. Qualora invece il conflitto sussista, l'organo giurisdizionale competente può rivolgersi alle autorità centrali del paese terzo, attraverso le proprie autorità centrali nazionali, con un termine di 15 giorni per la risposta (che può essere prorogato di 30 giorni su richiesta motivata in caso di obblighi contrastanti relativamente a diritti fondamentali o interessi fondamentali di un paese terzo), oppure decidere esso stesso se confermare o ritirare l'ordine per altri motivi di rifiuto invocati dal destinatario.
- Fatti salvi i rimedi disponibili ai sensi del RGPD e della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, le persone i cui dati sono stati ottenuti mediante ordine di produzione hanno anche diritto a un rimedio effettivo contro tale ordine.

Il Comitato, avendo valutato le procedure previste e le garanzie fornite nella proposta di regolamento quanto alle diverse fasi e su ciascuno degli aspetti presentati di seguito, raccomanda le garanzie e le modifiche illustrate qui di seguito.

a) Le soglie per l'emissione degli ordini dovrebbero essere innalzate e gli ordini dovrebbero essere emessi o autorizzati da organi giurisdizionali

Quanto alle condizioni per l'emissione degli ordini, il Comitato approva il principio di maggiori garanzie per l'accesso ai dati relativi alle operazioni o al contenuto. Tuttavia, esso rileva che, in assenza di armonizzazione completa delle sanzioni penali tra gli Stati membri, il riferimento a «reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni»[22] implica ancora soglie divergenti e discrepanze nella protezione dei dati nel caso di interessati che si trovano all'interno dell'UE.

Inoltre, il Comitato sottolinea che, soprattutto considerando l'ampiezza della definizione di dati relativi agli abbonati, la soglia prevista sembra piuttosto bassa per gli ordini di conservazione e di produzione riguardanti dati relativi agli abbonati o agli accessi, poiché tutti i reati in teoria ne giustificano l'emissione. Allo stesso modo, le autorità che possono emettere tali ordini sono più limitate nel contesto degli ordini di produzione riguardanti dati relativi alle operazioni o al contenuto rispetto agli ordini di conservazione o produzione di dati relativi agli abbonati o agli accessi, poiché i pubblici ministeri possono emettere o autorizzare solo questi ultimi, mentre i giudici, gli organi giurisdizionali o i magistrati inquirenti possono emettere o autorizzare ogni ordine.

[22] Cfr. articolo 5, paragrafo 3, lettera a).

In particolare, il Comitato lamenta che la soglia più bassa che permette alle autorità di contrasto di richiedere l'accesso ai dati relativi agli abbonati e agli accessi per qualsiasi reato si basa su una lettura "a contrario" della giurisprudenza della Corte (che si concentra sugli altri dati) per creare distinzioni sulle garanzie da concedere. In effetti, la Corte sottolinea espressamente che, per i dati relativi al traffico e all'ubicazione, l'accesso da parte delle autorità competenti va limitato unicamente alla lotta contro i reati gravi[23]. Il Comitato è consapevole che la proposta darebbe la possibilità di chiedere l'accesso a informazioni elementari che permetterebbero solo di identificare una persona senza rivelare alcun dato della comunicazione senza previa autorizzazione dell'organo giurisdizionale, tuttavia disapprova una simile lettura "a contrario" di questa giurisprudenza da parte della Commissione e chiede maggiori garanzie per limitare i motivi di accesso ad altri dati relativi agli abbonati e agli accessi. Il Comitato suggerisce di limitare l'accesso a tali dati a un elenco di reati stabilito nella proposta di regolamento o almeno ai "reati gravi", specialmente in considerazione del livello di autorizzazione più basso previsto per tali dati.

Inoltre, il Comitato sottolinea come tale lettura "a contrario" dia anche la possibilità ai pubblici ministeri di emettere o autorizzare l'emissione di ordini. Il Comitato ritiene che, eccetto in casi di richieste riguardanti informazioni elementari che permetterebbero semplicemente di identificare una persona senza rivelare dati relativi alle comunicazioni, ciò sarebbe un passo indietro rispetto alla giurisprudenza della Corte riguardo all'acceso ai suddetti dati. In effetti, nella giurisprudenza sull'accesso ai dati relativi alle comunicazioni, la Corte ha limitato la possibilità di concedere tale accesso, tra gli altri criteri, e "*salvo casi di urgenza debitamente giustificati*"[24], a "*un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente*", "*a seguito di una richiesta motivata delle autorità suddette presentata nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale*." [25]

Il Comitato fa notare che la nozione di "organo giurisdizionale" è una nozione autonoma del diritto UE e che la Corte ha sempre sottolineato e ribadito i criteri da soddisfare per tale qualifica, compreso quello di indipendenza,[26] che non sembra applicarsi ai pubblici ministeri come anche evidenziato dalla stessa nella sua giurisprudenza[27].

Di conseguenza, l'articolo 4, paragrafo 1, lettere a) e b), e l'articolo 3, lettere a) e b), portano a procedure dove si applicano garanzie molto minori nel caso di dati relativi agli abbonati e agli accessi, i quali potranno essere richiesti dal solo pubblico ministero, senza ulteriore controllo da parte dell'autorità dello Stato dove si trovano tali dati o dell'autorità dove si trova il rappresentante legale della società cui è presentata la richiesta, né alcun controllo da parte di un'autorità amministrativa indipendente.

Inoltre, il Comitato prende atto della cosiddetta garanzia addizionale prevista dall'articolo 5, paragrafo 2, che limita la possibilità di emettere un ordine di produzione ai casi in cui una misura simile sia disponibile per lo stesso reato in una situazione nazionale paragonabile. Tuttavia, il Comitato fa presente il possibile effetto controproducente di tale disposizione: invece di fornire garanzie addizionali, essa appare un incentivo affinché gli Stati membri amplino le previsioni nazionali che consentono di chiedere la produzione di dati relativi agli abbonati o agli accessi così da garantire la possibilità di emettere ordini di produzione ai sensi del regolamento in questione.

[23] Cfr. causa 203/15, punto 125.
[24] Cfr. causa 203/15, punto 120.
[25] Cfr. cause riunite C 293/12 e C 594/12, punto 62.
[26] Cfr. ad esempio, causa C-203/14.
[27] Cfr. ad esempio, causa Moulin/France del 23.11.2010.

b) I termini per la trasmissione dei dati dovrebbero essere giustificati

Il Comitato rileva che agli ordini europei di produzione si deve rispondere al massimo entro 10 giorni dalla ricezione del certificato, a meno che l'autorità di emissione indichi motivi per anticiparne la divulgazione, ed entro un massimo di sei ore nei casi di emergenza, come previsto dall'articolo 9, paragrafi 1 e 2.

Tuttavia, il Comitato non ha riscontrato nessun criterio che tratteggi l'obbligo per le autorità di dimostrare l'urgenza di produrre i dati, neanche ex post, permettendo così un possibile controllo dell'utilizzo di questa procedura estremamente accelerata, mentre il termine di sei ore probabilmente implicherà un controllo molto scarno prima di produrre i dati, se non addirittura l'assenza di controllo da parte del prestatore di servizi. La valutazione di impatto, in effetti, evidenzia la necessità che le autorità competenti abbiano accesso ai dati in modo tempestivo. D'altro canto gli esempi forniti nella suddetta valutazione riguardano sempre prove necessarie in caso di reati gravi (terrorismo con presa di ostaggi, situazioni di abusi contro minori in corso), ma la giustificazione basata sulla volatilità delle prove non sembra reggere quando non vi sia altra urgenza specifica se non la stessa potenziale volatilità in questione. Inoltre, tale volatilità non offre alcuna giustificazione ulteriore della proporzionalità dell'accesso ai dati in presenza di minori garanzie nei casi suddetti, dove non c'è altra urgenza se non la volatilità dei dati.

Inoltre, il Comitato esprime dubbi riguardo alla necessità di prevedere un termine di sei ore stabilendo al contempo che tale termine non si applichi fino a quando l'autorità di emissione abbia fornito ulteriori chiarimenti "entro cinque giorni" nel caso in cui il prestatore di servizi non possa adempiere a tale obbligo.

Il Comitato chiede dunque che siano aggiunti elementi nella valutazione di impatto per giustificare la necessità di tali termini nei casi in cui il reato commesso o perseguito non sia grave, e che, salva la messa a disposizione di tali elementi dettagliati, vi siano criteri espliciti per giustificare l'emergenza in caso di emissione dell'EPOC. Si potrebbe, ad esempio, prevedere lo stesso modello della direttiva OEI. Quest'ultima fissa un termine più breve quando ciò sia giustificato da " termini procedurali, gravità del reato o altre circostanze particolarmente urgenti" (cfr. articolo 12, paragrafo 2), o un termine di 24 ore per emanare provvedimenti provvisori (cfr. articolo 32, paragrafo 2). In effetti, la valutazione di impatto della proposta di regolamento non fornisce elementi dettagliati che giustifichino l'inefficienza di tali termini, essendo gli unici elementi evidenziati il sovraccarico di richieste pervenute che rende impossibile per le autorità giudiziarie riceventi rispettare i termini previsti.

c) Gli ordini europei di produzione e di conservazione non possono essere usati per chiedere dati di un interessato che si trova in un altro Stato membro senza almeno informare le autorità competenti di tale Stato, in particolare per i dati relativi al contenuto

Il Comitato fa notare che gli strumenti per la cooperazione esistenti prevedono garanzie aggiuntive, in particolare allo scopo di verificare la necessità e la proporzionalità delle richieste, e sottolinea che tali garanzie appaiono ancora più giustificate nei casi in cui i dati richiesti sono dati relativi al contenuto che implicano maggiori limitazioni al diritto degli interessati alla protezione dei dati personali e della privacy. A tale proposito, il Comitato sottolinea che la direttiva OEI contempla anche la possibilità di intercettare telecomunicazioni con l'assistenza tecnica di un altro Stato membro (cfr. articolo 30), oltre che l'obbligo di notifica dell'intercettazione dei dati all'autorità competente dello Stato membro in cui si trova o si troverà l'interessato qualora non serva l'assistenza di tale Stato membro (cfr. articolo 31).

Il Comitato non individua alcuna giustificazione per la procedura stabilita nella proposta di regolamento in materia di prove elettroniche che autorizza la produzione di dati relativi al contenuto senza coinvolgere almeno le autorità competenti dello Stato membro dove si trova l'interessato.

d) Gli ordini europei di conservazione non devono essere usati per aggirare gli obblighi sulla conservazione dei dati dei prestatori di servizi

Il Comitato rileva che lo scopo principale degli ordini europei di conservazione consiste nell'evitare che i dati siano cancellati.

Sebbene il Comitato riconosca che in alcuni casi ciò possa essere necessario e proporzionato, lamenta la mancanza di garanzie quanto all'emissione di tali ordini. Nello specifico, raccomanda che quando l'ordine di conservazione si riferisce solo a dati specifici, nei casi in cui la proposta sembra permettere richieste di portata ampia, e quando tale ordine è emesso per dati di cui è prevista la cancellazione in base al principio di conservazione limitata dei dati, l'ordine stesso non debba mai servire per legittimare il trattamento dei dati da parte del prestatore di servizi dopo la data inizialmente prevista per la cancellazione. In altre parole, i dati dovrebbero essere «congelati».

Inoltre, il collegamento tra l'ordine di conservazione e la successiva richiesta di produzione dei dati, sia essa presentata tramite un ordine europeo di produzione, un OEI o una richiesta di assistenza giudiziaria, dovrebbe essere rinforzato per garantire che l'ordine europeo di conservazione sia emesso solo quando vi è certezza della successiva richiesta (ossia che questa non è una mera possibilità) e che, qualora tale richiesta sia respinta, anche l'ordine di conservazione decada, senza dovere aspettare 60 giorni[28] se la richiesta successiva è respinta precedentemente allo scadere di tale termine.

e) Riservatezza e informazioni all'utente

Il Comitato rileva come nella proposta di regolamento sia stato introdotto uno specifico articolo[29] riguardante la riservatezza degli ordini emessi. Per evitare confusione e malintesi relativamente al diritto alla protezione dei dati, il Comitato sottolinea che, sebbene il RGPD stabilisca che si possano limitare i diritti degli interessati mediante misure legislative, e quindi conoscibili pubblicamente, , a fini di prevenzione, indagine, accertamento e perseguimento di reati[30] e che tali misure legislative devono prevedere disposizioni specifiche riguardo al diritto degli interessati a essere informati su tali limitazioni, a meno che ciò pregiudichi lo scopo della limitazione stessa[31], detto regolamento non prevede l'obbligo di informare i singoli interessati di ogni richiesta di accesso da parte delle autorità di contrasto.

Ciononostante, il Comitato fa presente, parallelamente, che la direttiva in materia di protezione dei dati garantisce a qualunque interessato tale diritto di informazione da parte delle autorità competenti, a meno che tale diritto sia stato limitato, senza riservarlo unicamente agli interessati residenti nel territorio dell'UE.

f) Procedura per l'esecuzione di un ordine quando il prestatore di servizi rifiuta di eseguirlo

[28] Cfr. articolo 10, paragrafo 1.
[29] Cfr. articolo 11.
[30] Cfr. articolo 23, paragrafo 1, lettera d).
[31] Cfr. articolo 23, paragrafo 2, lettera h).

Il Comitato rileva che l'articolo 14 della proposta di regolamento prevede una procedura per garantire l'esecuzione di un ordine quando il destinatario non vi ottempera, basata sulla cooperazione giudiziaria tra l'autorità di emissione e l'autorità competente dello Stato di esecuzione.

Sembra però che tale procedura non permetta all'autorità di esecuzione di rifiutare di eseguire l'ordine per motivi che non siano puramente procedurali (come avviene per il destinatario, essenzialmente la mancanza di informazioni oppure l'effettiva impossibilità di fornire i dati), perché le informazioni in questione sono coperte da immunità o privilegio in base al diritto nazionale, oppure perché la divulgazione potrebbe incidere su interessi fondamentali quali la sicurezza e la difesa nazionali[32].

Il Comitato ribadisce quindi le proprie preoccupazioni sulla rimozione di eventuali doppi controlli da parte dell'autorità competente destinataria dell'ordine trasmesso, rispetto agli altri strumenti. Anche la possibilità di rifiutare l'esecuzione di un ordine con la motivazione che esso violerebbe la Carta sembra postulare una soglia più alta di quella generalmente applicata, ossia la possibile violazione dei diritti fondamentali dell'interessato. Pertanto, seguendo l'esempio del mandato di arresto europeo, che prevede motivi obbligatori e motivi facoltativi per il rifiuto, o almeno della direttiva OEI, in base alla quale la presunzione secondo cui «la creazione di uno spazio di libertà, di sicurezza e di giustizia nell'Unione si fonda sulla fiducia reciproca e su una presunzione di conformità, da parte di tutti gli Stati membri, al diritto dell'Unione e, in particolare, ai diritti fondamentali» è confutabile [33], la proposta di regolamento dovrebbe almeno prevedere la deroga minima classica secondo cui, se vi sono motivi sostanziali per ritenere che l'esecuzione di un ordine comporti la violazione di un diritto fondamentale dell'interessato e che lo Stato di esecuzione venga meno ai propri obblighi in materia di protezione dei diritti fondamentali riconosciuti nella Carta, l'esecuzione dell'ordine dovrebbe essere respinta.

g) Esecuzione di ordini e obblighi contrastanti basati sul diritto di un paese terzo (articoli 15 – 16)

Il Comitato è favorevole alla possibilità prevista nella proposta di regolamento per i destinatari di rifiutare l'esecuzione di un ordine se ritengono che esso violi i diritti fondamentali, in quanto tale possibilità mira a fornire garanzie in caso di obblighi giuridici contrastanti. Il Comitato ritiene altresì essenziale che la proposta preveda la consultazione delle autorità dei paesi terzi, almeno in caso di contrasto, e l'obbligo di revocare l'ordine quando l'autorità del paese terzo si oppone.

Pertanto, la procedura prevista per rifiutare di eseguire un ordine a causa di obblighi contrastanti basati sul diritto di un paese terzo necessiterebbe di considerevole miglioramento.

Prima di tutto, il Comitato rileva che la proposta di regolamento lascia che sia una società privata, in quanto destinataria di un ordine di produzione, a stabilire se l'ordine sia o meno in contrasto con il diritto applicabile di un paese terzo che vieta la divulgazione dei dati richiesti. La società in questione deve presentare un'opposizione motivata, con tutti i dettagli rilevanti del diritto del paese terzo, la sua applicabilità al caso in oggetto e la natura degli obblighi contrastanti.

La preoccupazione del Comitato deriva soprattutto dal fatto che, quando è presentata un'opposizione di questo tipo, solo l'organo giurisdizionale competente dello Stato membro dell'autorità di emissione valuta se esista un contrasto, poiché le autorità del paese terzo vengono contattate soltanto quando tale organo giurisdizionale rileva l'esistenza di un tale contrasto. L'organo giurisdizionale competente dell'UE, in questo contesto, è dunque incaricato dell'interpretazione definitiva del diritto del paese terzo senza sostanzialmente essere uno specialista al riguardo. Il Comitato ritiene che l'obbligo di

[32] Cfr. articolo 14, paragrafo 2.
[33] Cfr. considerando 19 della direttiva OEI.

consultare le autorità competenti del paese terzo sia quindi troppo limitato nella proposta attuale. Nel settore della protezione dei dati, il Comitato desidera segnalare al legislatore che, qualora un organo giurisdizionale competente di un paese terzo dovesse interpretare il RGPD per valutare se esso contrasti con i requisiti del proprio paese, le autorità per la protezione dei dati dell'UE e gli organi giurisdizionali competenti manterrebbero comunque la propria competenza a valutare la liceità del trasferimento basato su una sentenza di un organo giurisdizionale o su una decisione di un'autorità amministrativa di un paese terzo che disponga il trasferimento o la divulgazione di dati personali che rientrano nell'ambito di applicazione del RGPD[34].

Inoltre, il Comitato sottolinea che la valutazione del diritto del paese terzo da parte dell'organo giurisdizionale competente dello Stato UE richiedente si deve basare su elementi oggettivi, e manifesta la propria preoccupazione rispetto ai criteri di cui tale organo deve tenere conto quando valuta il diritto del paese terzo a norma dell'articolo 15, paragrafo 4, e dell'articolo 16, paragrafo 5, lettera a), della proposta di regolamento. Infatti, l'organo giurisdizionale dovrebbe valutare se il diritto del paese terzo "anziché tutelare i diritti fondamentali o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, intenda manifestamente tutelare altri interessi o proteggere attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali" ovvero "l'interesse tutelato dal diritto del paese terzo, compreso l'interesse del paese terzo a impedire la divulgazione dei dati". Ad esempio, sebbene in linea di principio tale valutazione richieda una valutazione basata sull'evidenza in considerazione di tutte le informazioni disponibili dato il potenziale impatto di tale decisione, la formulazione in inglese ("is being aimed to") appare quantomeno poco chiara e dovrebbe essere rielaborata ("has the aim/objective to").

Il Comitato deplora che il solo caso in cui le autorità di un paese terzo possono essere consultate e opporsi all'esecuzione di un ordine di produzione sia quando l'organo giurisdizionale competente a livello UE ritiene che esista un contrasto rilevante, trasmette tutti gli elementi alle autorità centrali del paese terzo coinvolto e l'autorità centrale di tale paese terzo si oppone entro lo stretto termine di massimo 50 giorni (15 giorni, prorogabili eventualmente di 30 giorni, più un ultimo eventuale sollecito che concede altri 5 giorni). In tutti gli altri casi, l'organo giurisdizionale competente avrebbe la possibilità di confermare l'ordine di produzione e infliggere al prestatore di servizi che rifiuti di eseguirlo una sanzione pecuniaria. Di conseguenza, il Comitato è preoccupato del fatto che gli organi giurisdizionali competenti dell'UE non siano soggetti a un obbligo più ampio di consultare le autorità competenti dei paesi terzi in questione, al fine di garantire che la procedura assicuri in modo più sistematico che si tenga conto degli argomenti di entrambe le parti e rispetti in misura ancora maggiore il diritto dei paesi terzi.

Come sottolineato nella dichiarazione del Gruppo di lavoro e in precedenza, il Comitato ribadisce la necessità di prestare particolare attenzione all'adozione da parte di paesi terzi di strumenti simili che potenzialmente incidono sui diritti degli interessati e il loro diritto alla privacy nell'UE, con particolare riguardo al rischio che tali strumenti siano in diretto contrasto con il diritto dell'UE in materia di protezione dei dati.

Inoltre, il Comitato sottolinea che l'organo giurisdizionale competente dello Stato membro dell'autorità di emissione potrebbe anche non essere l'organo giurisdizionale competente per l'esecuzione dell'ordine previsto dall'articolo 14 della proposta di regolamento, e ciò aumenterebbe ancora il rischio di procedure contrastanti e la mancanza di controlli incrociati in caso di diritti divergenti. Ciò deriva dal fatto che, in alcuni casi, potrebbero esserci tre paesi coinvolti: quello dell'autorità che emette l'ordine, il paese terzo del prestatore di servizi, e lo Stato membro dove si

[34] Cfr. articolo 48 del regolamento generale sulla protezione dei dati.

trova il rappresentante legale del prestatore di servizi nell'UE e dove l'ordine dovrebbe essere eseguito. Di conseguenza, seguendo la procedura attualmente prevista, l'organo giurisdizionale dell'autorità richiedente nello Stato membro A potrebbe interpretare a proprio modo il diritto del paese terzo B del prestatore di servizi senza dover chiedere l'opinione delle autorità di tale paese terzo (che potrebbero invece avere riserve al riguardo), e chiedere all'organo giurisdizionale di un altro Stato membro C di eseguire la decisione senza possibilità di opporvisi.

A parte questo, il Comitato si compiace dell'introduzione di rimedi specifici contro gli ordini di produzione, in aggiunta a quelli previsti dal RGPD e dalla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. Il Gruppo di lavoro aveva già richiesto tali garanzie nella precedente dichiarazione. Tuttavia, il Comitato lamenta come tali rimedi non siano previsti anche rispetto agli ordini di conservazione, poiché anche tali ordini possono portare a limitazioni dei diritti fondamentali delle persone i cui dati sono conservati. Infatti, una delle conseguenze dell'ordine di conservazione può essere che i dati siano conservati più a lungo di quanto previsto dalle norme sulla protezione dei dati. Ne consegue che l'ordine di conservazione in sé porta a una limitazione dei diritti fondamentali dell'interessato, la cui giustificazione deve essere oggetto di revisione e rimedi specifici, soprattutto qualora l'ordine di conservazione sia accompagnato da un ordine di produzione per ottenere i dati. Come raccomanda il Gruppo di lavoro nella sua dichiarazione, è necessario prevedere rimedi giuridici almeno equivalenti a quelli disponibili a livello nazionale.

h) Sicurezza dei trasferimenti di dati quando si risponde a un ordine

Il Comitato fa notare che la proposta di regolamento prevede solo che gli ordini siano indirizzati a destinatari all'interno dell'Unione europea, quindi non include alcun canale specifico per il trasferimento di dati tra destinatari e prestatori di servizi situati fuori dall'Unione europea.

Sebbene il Comitato veda con favore l'assenza di ulteriori deroghe al quadro generale dell'UE per la protezione dei dati, ricorda che gli ordini indirizzati a un destinatario che implicano poi un trasferimento fuori dall'UE devono essere conformi al quadro giuridico previsto dal RGPD. Infatti, l'elusione del quadro giuridico della cooperazione giudiziaria, il quale prevede garanzie per la protezione dei dati, non dovrebbe anche portare ad aggirare i requisiti in materia di trasferimento dei dati da parte di destinatari di ordini di produzione o conservazione.

Inoltre, sebbene il Comitato sia favorevole all'assenza di una disposizione che impone l'obbligo di decriptare i dati criptati[35], esprime la propria preoccupazione per il fatto che le proposte non prevedano alcun obbligo specifico in capo ai destinatari di valutare l'autenticità dei dati prodotti e sottolinea come tale valutazione sia anche un valore aggiunto degli strumenti tradizionali che si basano sulla cooperazione giudiziaria; il Comitato mette in guardia dal rischio ulteriore cui possono essere esposti gli interessati in assenza di tale valutazione.

Conclusioni

Sulla base della presente valutazione il Comitato desidera rivolgere ai colegislatori le seguenti raccomandazioni:

1) La base giuridica del regolamento non dovrebbe essere l'articolo 82, paragrafo 1, del TFUE.
2) Dovrebbe essere dimostrata meglio la necessità di un nuovo strumento rispetto alla direttiva OEI o agli accordi di assistenza giudiziaria, anche con un'analisi dettagliata di strumenti meno

[35] Cfr. considerando 19 e pagina 240 della valutazione d'impatto.

invasivi dei diritti fondamentali, ad esempio apportando modifiche di tali strumenti già esistenti oppure limitando l'ambito di applicazione dello strumento proposto agli ordini di conservazione in combinazione con altre procedure esistenti per chiedere l'accesso ai dati.

3) Il regolamento dovrebbe prevedere un temine più lungo in modo da permettere al prestatore di servizi che deve eseguire l'ordine di garantire il rispetto delle garanzie per la protezione dei diritti fondamentali.
4) Dovrebbe essere mantenuto il principio di doppia punibilità, specialmente se si abbandona il criterio di ubicazione dei dati, al fine di conservare l'obbligo di valutare le garanzie previste in entrambi gli Stati coinvolti (quello dell'autorità richiedente e quello dove è situato il prestatore di servizi).
5) L'ambito di applicazione del regolamento dovrebbe essere limitato ai titolari del trattamento definiti dal RGPD, oppure comprendere una disposizione secondo cui il prestatore di servizi cui è rivolto l'ordine, se non è il titolare del trattamento ma il responsabile del trattamento, deve informare il titolare.
6) Il regolamento dovrebbe contenere garanzie sui trasferimenti dei dati quando il prestatore di servizi è situato in un paese terzo senza una decisione di adeguatezza in materia, oppure fare riferimento alla direttiva 2016/680 poiché le garanzie ivi previste saranno applicabili.
7) Poiché le disposizioni sulla nomina obbligatoria di un rappresentante legale differiscono da quelle dal RGPD, il regolamento sulle prove elettroniche dovrebbe precisare che il rappresentante legale ivi previsto è diverso da quello di cui all'articolo 3, paragrafo 2, del RGPD.
8) Il regolamento dovrebbe contenere una definizione più ampia di dati relativi alle comunicazioni elettroniche per assicurare che la necessaria definizione delle adeguate garanzie e condizioni di accesso copra sia i dati non relativi al contenuto che quelli relativi al contenuto.
9) Il regolamento dovrebbe elevare le soglie di emissione degli ordini, e questi ultimi devono essere emessi o autorizzati da organi giurisdizionali, eccetto per i dati relativi agli abbonati, sempre che la definizione di quest'ultima categoria sia limitata considerevolmente così da comprendere informazioni elementari che permettano solamente di identificare la persona senza implicare l'accesso ai dati relativi alle comunicazioni.
10) Il regolamento dovrebbe limitare l'accesso ai dati relativi agli abbonati e agli accessi a un elenco di reati rigorosamente stabilito, o quantomeno ai "reati gravi".
11) Il termine per trasmettere i dati, specialmente nei casi di emergenza, dovrebbe essere meglio giustificato nel regolamento, e la possibilità di ricorrere alla procedura rapida di sei ore dovrebbe prevedere l'obbligo per le autorità richiedenti di dimostrare l'emergenza che giustifica il ricorso a tale procedura, anche a posteriori, in modo da poter controllare l'uso di tali poteri eccezionali.
12) La procedura che consente la produzione di dati relativi al contenuto senza coinvolgere le autorità competenti dello Stato membro in cui è situato l'interessato dovrebbe essere abbandonata.
13) Nel regolamento dovrebbero essere migliorate le garanzie per l'emissione degli ordini europei di conservazione.
14) Il regolamento dovrebbe quanto meno prevedere la deroga classica minima secondo cui se vi sono motivi sostanziali per ritenere che l'esecuzione di un ordine comporti la violazione di un diritto fondamentale dell'interessato tale da comportare per lo Stato di esecuzione una violazione dei propri obblighi in materia di protezione dei diritti fondamentali riconosciuti nella Carta, l'esecuzione dell'ordine dovrebbe essere rifiutata.
15) Il regolamento dovrebbe prevedere un obbligo più ampio di consultare le autorità competenti del paese terzo in cui è situato il prestatore di servizi in caso di conflitto tra disposizioni

legislative, onde evitare interpretazioni soggettive da parte di un singolo organo giurisdizionale.

16) La validità e la durata degli ordini di conservazione dovrebbero essere maggiormente correlate agli ordini di produzione che li accompagnano.
17) Dovrebbe essere maggiormente garantita la sicurezza dei trasferimenti di dati.
18) Si dovrebbe prevedere la verifica dell'autenticità dei dati, in particolare quando sia possibile fornire dati criptati.

Per il Comitato europeo per la protezione dei dati

La Presidente

(Andrea Jelinek)