EDPB-GEPD

Parere congiunto n. 4/2022 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori

Adottato il 28 luglio 2022

INDICE

1. Informazioni generali 7

2. Ambito del parere 9

3. Osservazioni generali sui diritti alla riservatezza delle comunicazioni e alla protezione dei dati personali 9

4. Osservazioni specifiche 12

4.1 Relazione con la legislazione vigente 12

4.1.1 Relazione con il GDPR e con la direttiva relativa alla vita privata e alle comunicazioni elettroniche 12

4.1.2 Relazione con il regolamento (UE) 2021/1232 ed effetto sull'individuazione volontaria di abusi sessuali online sui minori 12

4.2 Fondamento giuridico ai sensi del GDPR 13

4.3 Valutazione e attenuazione del rischio 13

4.4 Condizioni per l'emissione di ordini di rilevazione 15

4.5 Analisi della necessità e della proporzionalità delle misure previste 17

4.5.1 Efficacia della rilevazione 18

4.5.2 Assenza di misure meno intrusive 19

4.5.3 Proporzionalità in senso stretto 19

4.5.4 Rilevazione di materiale pedopornografico noto 21

4.5.5 Rilevazione di materiale pedopornografico precedentemente sconosciuto 22

4.5.6 Rilevazione dell'adescamento di minori (*grooming*) 23

4.5.7 Conclusione sulla necessità e sulla proporzionalità delle misure previste 24

4.6 Obblighi di segnalazione 24

4.7 Obblighi di rimozione e blocco 24

4.8 Tecnologie e salvaguardie pertinenti 25

4.8.1 Protezione dei dati fin dalla progettazione e per impostazione predefinita 25

4.8.2 Affidabilità delle tecnologie 26

4.8.3 Scansione delle comunicazioni audio 27

4.8.4 Verifica dell'età 27

4.9 Conservazione delle informazioni 28

4.10 Impatto sulla cifratura 28

4.11 Vigilanza, attuazione e cooperazione 30

4.11.1 Ruolo delle autorità nazionali di controllo ai sensi del GDPR 30

4.11.2 Ruolo dell'EDPB 31
4.11.3 Ruolo del Centro dell'UE in materia di abuso sessuale su minori 32
4.11.4 Ruolo di Europol 34
5. Conclusioni 38

Sintesi

L'11 maggio 2022 la Commissione europea ha pubblicato una proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori.

La proposta imporrebbe ai prestatori di servizi di hosting, di servizi di comunicazione interpersonale e di altri servizi obblighi condizionati di rilevazione, segnalazione, rimozione e blocco di materiale pedopornografico online noto e nuovo e per l'adescamento di minori. La proposta prevede inoltre l'istituzione di una nuova agenzia decentrata dell'UE (il «Centro dell'UE») e di una rete di autorità nazionali coordinatrici per le questioni di abuso sessuale su minori, al fine di consentire l'attuazione del regolamento proposto. Come riconosciuto nella relazione che accompagna la proposta, le misure ivi contenute lederebbero l'esercizio dei diritti fondamentali degli utenti dei servizi in questione.

L'abuso sessuale su minori è un reato particolarmente grave ed efferato; pertanto, la finalità di consentire un'azione efficace per contrastarlo costituisce un obiettivo di interesse generale riconosciuto dall'Unione e mira a tutelare i diritti e le libertà delle vittime. Allo stesso tempo l'EDPB e il GEPD ricordano che eventuali limitazioni dei diritti fondamentali, come quelle previste dalla proposta, devono essere conformi alle prescrizioni di cui all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea.

L'EDPB e il GEPD sottolineano che la proposta solleva serie preoccupazioni in merito alla proporzionalità dell'ingerenza e delle limitazioni previste in materia di protezione dei diritti fondamentali per quanto riguarda il rispetto della vita privata e la protezione dei dati di carattere personale. A tale riguardo fanno notare che le garanzie procedurali non possono mai sostituire completamente le garanzie sostanziali. Un complesso sistema di escalation dalle misure di valutazione e di attenuazione del rischio a un ordine di rilevazione non può sostituire la necessaria chiarezza degli obblighi sostanziali.

L'EDPB e il GEPD ritengono che la proposta difetti di chiarezza sugli elementi chiave, come la nozione di «rischio significativo». Inoltre i soggetti incaricati di applicare tali garanzie, a cominciare dagli operatori privati per finire con le autorità amministrative e/o giudiziarie, godono di un margine di discrezionalità molto ampio, il che comporta incertezza del diritto con riguardo ai criteri per il bilanciamento dei diritti in gioco in ogni singolo caso. L'EDPB e il GEPD sottolineano che il legislatore, nel consentire ingerenze particolarmente gravi a livello di diritti fondamentali, deve garantire che sia giuridicamente chiaro quando e dove tali ingerenze sono consentite. Pur riconoscendo che la legislazione non può essere eccessivamente prescrittiva e deve lasciare una certa flessibilità nell'applicazione pratica, ritengono che la proposta lasci troppo spazio a potenziali abusi a causa dell'assenza di norme sostanziali chiare.

Per quanto riguarda la necessità e la proporzionalità delle misure di rilevazione previste, l'EDPB e il GEPD sono preoccupati soprattutto per quelle relative alla rilevazione di materiale pedopornografico sconosciuto e dell'adescamento di minori («*grooming*») nei servizi di comunicazione interpersonale. Essi ritengono che l'ingerenza creata da tali misure vada oltre quanto necessario e proporzionato, a causa della loro invasività, della loro natura probabilistica e dei tassi di errore associati a tali tecnologie. Inoltre le misure che consentono alle autorità pubbliche di accedere in modo generalizzato al contenuto di una comunicazione al fine di individuare l'adescamento di minori hanno maggiori probabilità di pregiudicare il contenuto essenziale dei diritti garantiti dagli articoli 7 e 8 della Carta. Pertanto le disposizioni pertinenti relative al *grooming* dovrebbero essere eliminate dalla proposta. A ciò si aggiunge che la proposta non esclude dal suo ambito di applicazione la scansione delle comunicazioni audio. L'EDPB e il GEPD ritengono che la scansione delle comunicazioni audio sia particolarmente intrusiva e che debba pertanto rimanere fuori dall'ambito di

applicazione degli obblighi di rilevazione stabiliti nel regolamento proposto per quanto riguarda sia i messaggi vocali sia le comunicazioni in diretta.

L'EDPB e il GEPD esprimono inoltre dubbi in merito all'efficacia delle misure di blocco e ritengono che imporre ai prestatori di servizi internet di decrittare le comunicazioni online al fine di bloccare quelle relative al materiale pedopornografico sarebbe sproporzionato.

L'EDPB e il GEPD sottolineano, inoltre, che le tecnologie di cifratura contribuiscono in modo fondamentale al rispetto della vita privata, alla riservatezza delle comunicazioni e alla libertà di espressione, nonché all'innovazione e alla crescita dell'economia digitale, che si basa sull'elevato livello di fiducia e sicurezza che tali tecnologie offrono. Il considerando 26 della proposta vincola non solo la scelta delle tecnologie di rilevazione, ma anche delle misure tecniche per tutelare la riservatezza delle comunicazioni, come la cifratura, alla condizione che tale scelta tecnologica soddisfi le prescrizioni del regolamento proposto, ossia consenta la rilevazione. Ciò conferma il concetto emergente dall'articolo 8, paragrafo 3, e dall'articolo 10, paragrafo 2, della proposta, secondo il quale un prestatore di servizi non può rifiutare l'esecuzione di un ordine di rilevazione sulla base di un'impossibilità tecnica. L'EDPB e il GEPD ritengono che dovrebbe esserci un migliore equilibrio tra l'esigenza sociale di disporre di canali di comunicazione sicuri e privati e quella di contrastarne l'abuso. Sarebbe opportuno indicare chiaramente nella proposta che nessun elemento del regolamento proposto dovrebbe essere interpretato come inteso a vietare o indebolire la cifratura.

Pur accogliendo con favore la dichiarazione contenuta nella proposta secondo cui essa non incide sui poteri e sulle competenze delle autorità di protezione dei dati a norma del regolamento generale sulla protezione dei dati («GDPR»), l'EDPB e il GEPD sono del parere che dovrebbe comunque essere meglio disciplinata la relazione tra i compiti delle autorità coordinatrici e quelli delle autorità di protezione dei dati. A tale riguardo esprimono apprezzamento per il ruolo assegnato all'EDPB attraverso la previsione di un suo coinvolgimento nell'attuazione pratica della proposta, in particolare con riguardo alla necessità che l'EDPB esprima un parere sulle tecnologie che il Centro dell'UE mette a disposizione per eseguire gli ordini di rilevazione. Dovrebbe tuttavia essere chiarito quale sarebbe lo scopo del parere nel processo e quali passi dovrebbe compiere il Centro dell'UE dopo aver ricevuto un parere dall'EDPB.

Infine, l'EDPB e il GEPD osservano che la proposta prevede una stretta cooperazione tra il Centro dell'UE ed Europol, i quali dovrebbero consentirsi reciprocamente «il più ampio accesso alle informazioni e ai sistemi di informazione pertinenti». Pur sostenendo in linea di principio la cooperazione delle due agenzie, dato che il Centro dell'UE non è un'autorità di contrasto, l'EDPB e il GEPD formulano comunque diverse raccomandazioni per il miglioramento delle disposizioni pertinenti, tra le quali la previsione che la trasmissione di dati personali tra il Centro dell'UE ed Europol avvenga solo caso per caso, a seguito di una richiesta debitamente valutata e tramite uno strumento di comunicazione sicuro, come la rete SIENA.

Il comitato europeo per la protezione dei dati e il garante europeo della protezione dei dati

visto l'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE («EUDPR») ([1]),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37 dello stesso, modificati dalla decisione del Comitato misto SEE n. 154/2018, del 6 luglio 2018 ([2]),

vista la richiesta della Commissione europea, del 12 maggio 2022, di un parere congiunto del comitato europeo per la protezione dei dati e del garante europeo della protezione dei dati sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori ([3]),

HANNO ADOTTATO IL SEGUENTE PARERE CONGIUNTO.

1. INFORMAZIONI GENERALI

1. L'11 maggio 2022 la Commissione europea («Commissione») ha pubblicato una proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori (la «proposta» o il «regolamento proposto») ([4]).

2. La proposta è stata presentata a seguito dell'adozione del regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori (il «regolamento provvisorio») [5]. Il regolamento provvisorio non impone ai fornitori di servizi interessati di adottare misure per rilevare il materiale pedopornografico (ad esempio immagini, video ecc.) o l'adescamento di minori (noto anche come «*grooming*») nei loro servizi, ma consente loro di farlo su base volontaria, conformemente alle condizioni stabilite in tale regolamento ([6]).

([1]) GU L 295 del 21.11.2018, pag. 39.
([2]) Nel presente documento, con «Stati membri» ci si riferisce agli «Stati membri del SEE».
([3]) Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori [COM(2022) 209 final].
([4]) Ibidem.
([5]) Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio, del 14 luglio 2021, relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori (GU L 274 del 30.7.2001, pag. 41).
([6]) Cfr. anche GEPD, Parere n. 7/2020 sulla proposta di deroghe temporanee alla direttiva 2002/58/CE ai fini della lotta contro gli abusi sessuali online sui minori (10 novembre 2020).

3. La proposta si compone di due elementi costitutivi principali. Anzitutto impone ai prestatori di servizi di hosting, di servizi di comunicazione interpersonale e di altri servizi obblighi condizionati di rilevazione, segnalazione, rimozione e blocco di materiale pedopornografico online noto e nuovo e per l'adescamento di minori. In secondo luogo prevede l'istituzione di una nuova agenzia decentrata dell'UE (il «Centro dell'UE sull'abuso sessuale su minori» o il «Centro dell'UE») e di una rete di autorità nazionali coordinatrici delle questioni di abuso sessuale su minori, al fine di consentire l'attuazione del regolamento proposto ([7]).

4. Come riconosciuto nella relazione che accompagna la proposta, le misure ivi contenute lederebbero l'esercizio dei diritti fondamentali degli utenti dei servizi in questione. Tali diritti comprendono in particolare i diritti fondamentali al rispetto della vita privata (compresa la riservatezza delle comunicazioni, nell'ambito del più ampio diritto al rispetto della vita privata e della vita familiare), alla protezione dei dati di carattere personale e alla libertà di espressione e d'informazione ([8]).

5. Inoltre le misure proposte sono intese a riprendere e, in una certa misura, integrare la legislazione vigente dell'UE in materia di protezione dei dati e di rispetto della vita privata. A questo proposito la relazione osserva quanto segue:

> «La proposta si basa sul regolamento generale sulla protezione dei dati. Nella pratica i prestatori tendono ad invocare vari motivi per il trattamento previsti da tale regolamento per effettuare il trattamento di dati personali inerenti alla rilevazione volontaria e alla segnalazione di casi di abuso sessuale online sui minori. La proposta stabilisce un sistema di ordini di rilevazione mirati e specifica le condizioni per la rilevazione, garantendo una maggiore certezza del diritto per tali attività. Per quanto concerne le attività di rilevazione obbligatorie che comportano il trattamento di dati personali, la proposta, in particolare gli ordini di rilevazione emessi sulla base della stessa, stabilisce la base per tale trattamento di cui all'articolo 6, paragrafo 1, lettera c), del regolamento generale sulla protezione dei dati, in virtù del quale è lecito il trattamento di dati personali che è necessario per adempiere un obbligo legale ai sensi del diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.
>
> La proposta riguarda tra l'altro i prestatori che offrono servizi di comunicazione elettronica interpersonale e sono quindi soggetti alle disposizioni nazionali di attuazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche e della sua proposta di revisione attualmente in fase di negoziazione. Le misure stabilite nella proposta limitano per alcuni aspetti la portata dei diritti e degli obblighi previsti dalle pertinenti disposizioni di tale direttiva, in particolare in relazione alle attività strettamente necessarie per eseguire gli ordini di rilevazione. Al riguardo la proposta comporta l'applicazione, per analogia, dell'articolo 15, paragrafo 1, di tale direttiva» ([9]).

6. Data la gravità delle ingerenze previste nei diritti fondamentali, la proposta riveste particolare importanza per la tutela dei diritti e delle libertà delle persone con riguardo al trattamento dei dati personali. Il 12 maggio 2022 la Commissione ha pertanto deciso di consultare il comitato europeo per la protezione dei dati (l'«EDPB») e il garante europeo della protezione dei dati (il «GEPD») conformemente all'articolo 42, paragrafo 2, del regolamento EUDPR.

([7]) COM(2022) 209 final, pag. 17.
([8]) COM(2022) 209 final, pag.13.
([9]) COM(2022) 209 final, pag. 5.

2. AMBITO DEL PARERE

7. Il presente parere congiunto illustra le opinioni comuni dell'EDPB e del GEPD sulla proposta, limitandosi agli aspetti della proposta relativi alla protezione della vita privata e dei dati di carattere personale. In particolare il parere congiunto sottolinea i settori in cui la proposta non garantisce una protezione sufficiente dei diritti fondamentali al rispetto vita privata e alla protezione dei dati, o necessita di un ulteriore allineamento con il quadro giuridico dell'UE in materia di protezione della vita privata e dei dati personali.

8. Come ulteriormente spiegato nel presente parere congiunto, la proposta solleva serie preoccupazioni in merito alla necessità e alla proporzionalità delle ingerenze e delle limitazioni previste in materia di protezione dei diritti fondamentali per quanto riguarda il rispetto della vita privata e la protezione dei dati personali. Tuttavia lo scopo del presente parere congiunto non è quello di fornire un elenco esaustivo di tutte le questioni relative alla vita privata e alla protezione dei dati sollevate dalla proposta, né di fornire suggerimenti specifici per migliorarne la formulazione. Il presente parere congiunto contiene piuttosto osservazioni di ambito generale sulle principali questioni sollevate dalla proposta così come individuate dall'EDPB e dal GEPD. Questi ultimi rimangono tuttavia a disposizione per fornire ai co-legislatori ulteriori osservazioni e raccomandazioni in merito durante il processo legislativo.

3. OSSERVAZIONI GENERALI SUI DIRITTI ALLA RISERVATEZZA DELLE COMUNICAZIONI E ALLA PROTEZIONE DEI DATI PERSONALI

9. La riservatezza delle comunicazioni è un elemento essenziale del diritto fondamentale al rispetto della vita privata e della vita familiare, sancito dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea (la «Carta») ([10]). Inoltre l'articolo 8 della Carta riconosce un diritto fondamentale alla protezione dei dati personali. Il diritto alla riservatezza delle comunicazioni e il diritto al rispetto della vita privata e familiare sono garantiti anche dall'articolo 8 della Convenzione europea dei diritti dell'uomo (la «CEDU») e fanno parte delle tradizioni costituzionali comuni agli Stati membri ([11]).

10. L'EDPB e il GEPD ricordano che i diritti sanciti dagli articoli 7 e 8 della Carta non appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale ([12]). L'abuso sessuale su minori è un reato particolarmente grave ed efferato e predisporre un'azione efficace per contrastarlo costituisce un obiettivo di interesse generale riconosciuto dall'Unione che mira a tutelare i diritti e le libertà delle vittime. Per quanto riguarda la lotta effettiva contro i reati di cui sono vittime i minori e le altre persone vulnerabili, la Corte di giustizia dell'Unione europea («CGUE») ha sottolineato che obblighi positivi possono risultare dall'articolo 7 della Carta, ai fini dell'adozione da parte dei pubblici poteri di misure giuridiche dirette a tutelare la vita privata e familiare, il domicilio e

([10]) Cfr. ad esempio la dichiarazione del comitato europeo per la protezione dei dati sulla revisione del regolamento relativo alla vita privata e alle comunicazioni elettroniche (regolamento e-privacy) e sul suo impatto sulla tutela delle persone fisiche in relazione alla privacy e alla riservatezza delle loro comunicazioni (25 maggio 2018).

([11]) Quasi tutte le costituzioni europee prevedono un diritto che tutela la riservatezza delle comunicazioni. Cfr. ad esempio l'articolo 15 della Costituzione della Repubblica italiana, l'articolo 10 della Legge fondamentale della Repubblica federale di Germania, l'articolo 22 della Costituzione belga e l'articolo 13 della Costituzione del Regno dei Paesi Bassi.

([12]) Cfr. tra l'altro la sentenza della Corte di giustizia del 16 luglio 2020, *Facebook Ireland/Schrems*, C-311/18, ECLI:EU:C:2020:559, punto 172 e giurisprudenza ivi citata. Cfr. anche il considerando 4, GDPR.

le comunicazioni. Obblighi siffatti possono parimenti derivare dagli articoli 3 e 4 della Carta relativamente alla tutela dell'integrità fisica e psichica delle persone e al divieto di tortura e di trattamenti inumani e degradanti ([13]).

11. Allo stesso tempo, eventuali limitazioni dei diritti garantiti dalla Carta, come quelle previste dalla proposta ([14]), devono essere conformi alle prescrizioni di cui all'articolo 52, paragrafo 1, della Carta stessa. Eventuali misure che interferiscano con il diritto alla riservatezza delle comunicazioni e con il diritto al rispetto della vita privata e della vita familiare devono innanzitutto rispettare il contenuto essenziale dei diritti in questione ([15]). Il contenuto essenziale di un diritto è pregiudicato se il diritto è svuotato del suo contenuto di base e l'individuo non può esercitarlo. ([16]) L'ingerenza non può costituire, rispetto allo scopo prefissato, un intervento sproporzionato e inaccettabile, tale da ledere la sostanza stessa del diritto così garantito ([17]). Ciò significa che anche un diritto fondamentale di natura non assoluta, come il diritto alla riservatezza delle comunicazioni e il diritto alla protezione dei dati personali, presenta alcuni elementi centrali che non possono essere limitati.

12. La CGUE ha più volte applicato il criterio del «contenuto essenziale di un diritto» nel settore della riservatezza delle comunicazioni elettroniche. Nelle cause riunite *Tele2 Sverige e Watson* la Corte ha statuito che una normativa che non autorizzi la conservazione del contenuto di una comunicazione non è idonea a pregiudicare il contenuto essenziale dei diritti al rispetto vita privata e alla protezione dei dati personali ([18]). Nella causa *Schrems* la Corte ha sentenziato che si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta ([19]). Nelle cause riunite *Digital Rights Ireland e Seitlinger e a.*, la Corte ha statuito che, sebbene la conservazione dei dati imposta dalla direttiva 2006/24 costituisse un'ingerenza particolarmente grave nel diritto fondamentale al rispetto della vita privata e negli altri diritti sanciti all'articolo 7 della Carta, essa non era tale da pregiudicare il contenuto essenziale di tali diritti poiché la direttiva non permetteva di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale ([20]). Da tale giurisprudenza si può desumere che le misure che consentono alle autorità pubbliche di accedere in modo generalizzato al contenuto di una comunicazione hanno maggiori probabilità di pregiudicare il contenuto essenziale dei diritti garantiti dagli articoli 7 e 8 della Carta. Tali considerazioni sono altrettanto pertinenti anche per

([13]) Sentenza della Corte di giustizia del 6 ottobre 2020, *La Quadrature du Net e a.*, cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, punti da 126 a 128. Cfr. anche GEPD, Parere n. 7/2020 sulla proposta di deroghe temporanee alla direttiva 2002/58/CE ai fini della lotta contro gli abusi sessuali online sui minori (10 novembre 2020), punto 12.
([14]) COM(2022) 209 final, pag. 13-14.
([15]) Articolo 52, paragrafo 1, della Carta.
([16]) Cfr. «Orientamenti del GEPD sulla valutazione della proporzionalità di misure che limitano il diritto fondamentale alla vita privata e alla protezione dei dati personali» (19 dicembre 2019), pag. 8, disponibile all'indirizzo https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.
([17]) Sentenza della Corte di giustizia del 14 gennaio 2021, *OM*, C-393/19, ECLI:EU:C:2021:8, punto 53.
([18]) Sentenza della Corte di giustizia del 21 dicembre 2016, *Tele2 Sverige e Watson*, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970, punto 101.
([19]) Sentenza della Corte di giustizia del 6 ottobre 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, punto 94.
([20]) Sentenza della Corte di giustizia dell'8 aprile 2014, *Digital Rights Ireland e Seitlinger e a.*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238, punto 39.

quanto riguarda le misure per la rilevazione di materiale pedopornografico e dell'adescamento di minori come previste dalla proposta.

13. La CGUE ha inoltre statuito che le misure finalizzate alla sicurezza dei dati svolgono un ruolo fondamentale nel garantire che non sia pregiudicato il contenuto essenziale del diritto fondamentale alla protezione dei dati personali di cui all'articolo 8 della Carta ([21]). Nell'era digitale, le soluzioni tecniche per garantire e tutelare la riservatezza delle comunicazioni elettroniche, comprese le misure di cifratura, sono fondamentali per assicurare il godimento di tutti i diritti fondamentali ([22]). Ciò dovrebbe essere tenuto in debita considerazione quando si valutano misure per la rilevazione obbligatoria di materiale pedopornografico o dell'adescamento di minori, in particolare se esse comportano un indebolimento o una compromissione della cifratura ([23]).

14. L'articolo 52, paragrafo 1, della Carta prevede altresì che eventuali limitazioni all'esercizio di un diritto fondamentale garantito dalla Carta debbano essere previste dalla legge. Nel rispetto del principio di proporzionalità, possono essere imposte limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione, o all'esigenza di proteggere i diritti e le libertà altrui ([24]). Per soddisfare il requisito di proporzionalità, una normativa deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione delle misure considerate e fissino un minimo di requisiti, di modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente i loro dati contro i rischi di abuso ([25]). Detta normativa deve indicare in quali circostanze e a quali condizioni una misura che prevede il trattamento di siffatti dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario ([26]). Come chiarito dalla CGUE, la necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatizzato e quando è in gioco la protezione di quella categoria particolare di dati personali che sono i dati sensibili ([27]).

15. La proposta limiterebbe l'esercizio dei diritti e degli obblighi di cui all'articolo 5, paragrafi 1 e 3, e all'articolo 6, paragrafo 1, della direttiva 2002/58/CE («direttiva relativa alla vita privata e alle comunicazioni elettroniche») ([28]) nella misura necessaria all'esecuzione degli ordini di rilevazione emessi conformemente al capo 1, sezione 2, della proposta. L'EDPB e il GEPD ritengono pertanto necessario valutare la proposta non solo alla luce della Carta e del GDPR, ma anche alla luce degli articoli 5 e 6 e dell'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

([21]) Ibidem, punto 40.
([22]) Cfr. UNHRC, Resolution 47/16 on the promotion, protection and enjoyment of human rights on the Internet, documento ONU A/HRC/RES/47/16 (26 luglio 2021).
([23]) Cfr. anche il considerando 25 del regolamento provvisorio.
([24]) Cfr. «Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali: un kit di strumenti», 11 aprile 2017, disponibile all'indirizzo https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
([25]) Sentenza della Corte di giustizia del 6 ottobre 2020, *La Quadrature du Net e a.*, cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, punto 132.
([26]) Ibidem.
([27]) Ibidem.
([28]) 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), modificata dalla direttiva 2006/24/CE e dalla direttiva 2009/136/CE.

4. OSSERVAZIONI SPECIFICHE

4.1 Relazione con la legislazione vigente

4.1.1 Relazione con il GDPR e con la direttiva relativa alla vita privata e alle comunicazioni elettroniche

16. La proposta afferma che essa lascia impregiudicate le norme derivanti da altri atti dell'Unione, in particolare il GDPR ([29]) e la direttiva relativa alla vita privata e alle comunicazioni elettroniche. Contrariamente al regolamento provvisorio, la proposta non prevede una deroga temporanea esplicita, bensì una limitazione all'esercizio dei diritti e degli obblighi di cui all'articolo 5, paragrafi 1 e 3, e all'articolo 6, paragrafo 1 della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Va inoltre osservato che il regolamento provvisorio prevede una deroga esclusivamente alle disposizioni dell'articolo 5, paragrafo 1, e dell'articolo 6, paragrafo 1, ma non all'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

17. La proposta fa inoltre riferimento all'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche, che consente agli Stati membri di adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6 di tale direttiva, qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica, tra l'altro per prevenire, ricercare, accertare e perseguire reati. Secondo la proposta, l'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche si applica per analogia quando la proposta limita l'esercizio dei diritti e degli obblighi di cui all'articolo 5, paragrafi 1 e 3, e all'articolo 6, paragrafo 1, della suddetta direttiva.

18. L'EDPB e il GEPD ricordano come la CGUE abbia chiarito che l'articolo 15, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche deve essere interpretato in maniera restrittiva, nel senso che la deroga al principio della riservatezza delle comunicazioni consentita dall'articolo 15, paragrafo 1, deve rimanere un'eccezione e non deve diventare la regola ([30]). Come illustrato ulteriormente nel presente parere congiunto, l'EDPB e il GEPD ritengono che la proposta non soddisfi i requisiti di (stretta) necessità, efficacia e proporzionalità. Inoltre l'EDPB e il GEPD concludono che la proposta comporterebbe la conseguenza che l'ingerenza nella riservatezza delle comunicazioni possa di fatto diventare la regola anziché rimanere l'eccezione.

4.1.2 Relazione con il regolamento (UE) 2021/1232 ed effetto sull'individuazione volontaria di abusi sessuali online sui minori

19. A norma dell'articolo 88 della proposta, quest'ultima abrogherebbe il regolamento provvisorio, che prevede una deroga temporanea a talune disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche per consentire l'uso volontario di tecnologie per l'individuazione di materiale pedopornografico e dell'adescamento di minori da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero. Pertanto, a decorrere dalla data di

([29]) Regolamento (UE) 2016/679 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 (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).
([30]) Sentenza della Corte di giustizia del 21 dicembre 2016, *Tele2 Sverige e Watson*, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970, punto 89.

applicazione del regolamento proposto, non vi sarebbe alcuna deroga alla direttiva relativa alla vita privata e alle comunicazioni elettroniche che consenta l'individuazione volontaria di abusi sessuali online sui minori da parte di tali fornitori.

20. Dato che gli obblighi di rilevazione introdotti dalla proposta si applicherebbero solo ai destinatari degli ordini di rilevazione, sarebbe importante chiarire nel testo del regolamento proposto che l'uso volontario di tecnologie per la rilevazione di materiale pedopornografico e dell'adescamento di minori rimane consentito solo nella misura in cui sia ammesso dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche e dal GDPR. Ciò comporterebbe, ad esempio, che ai fornitori di servizi di comunicazione interpersonale indipendenti dal numero sia impedito di utilizzare tali tecnologie su base volontaria, a meno che ciò non sia consentito dalle leggi nazionali che recepiscono la direttiva relativa alla vita privata e alle comunicazioni elettroniche, conformemente all'articolo 15, paragrafo 1, della direttiva e-privacy e alla Carta.

21. Più in generale, il regolamento proposto trarrebbe vantaggio da una maggiore chiarezza riguardo allo status della rilevazione volontaria degli abusi sessuali online sui minori dopo la data di applicazione del regolamento proposto, nonché riguardo alla transizione dal regime di individuazione volontaria previsto dal regolamento provvisorio agli obblighi di rilevazione stabiliti nel regolamento proposto. Ad esempio, l'EDPB e il GEPD raccomandano di chiarire che il regolamento proposto non legittimerebbe il trattamento dei dati personali al solo scopo di individuare abusi sessuali online sui minori su base volontaria.

4.2 Fondamento giuridico ai sensi del GDPR

22. La proposta mira a stabilire un fondamento giuridico, ai sensi del GDPR, per il trattamento dei dati personali ai fini della rilevazione di materiale pedopornografico e del *grooming*. Nella relazione si osserva pertanto quanto segue: «Per quanto concerne le attività di rilevazione obbligatorie che comportano il trattamento di dati personali, la proposta, in particolare gli ordini di rilevazione emessi sulla base della stessa, stabilisce la base per tale trattamento di cui all'articolo 6, paragrafo 1, lettera c), del regolamento generale sulla protezione dei dati, in virtù del quale è lecito il trattamento di dati personali che è necessario per adempiere un obbligo legale ai sensi del diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento». ([31])

23. L'EDPB e il GEPD accolgono con favore la decisione della Commissione di eliminare l'incertezza sulla base giuridica del trattamento dei dati personali sorta nell'ambito del regolamento provvisorio. Concordano inoltre con la conclusione della Commissione secondo cui le conseguenze dell'introduzione di misure di rilevazione sono troppo ampie e gravi per lasciare ai prestatori di servizi la decisione in merito all'eventuale attuazione di tali misure ([32]). Allo stesso tempo osservano che qualsiasi base giuridica che obblighi i prestatori di servizi a interferire con i diritti fondamentali alla protezione dei dati e al rispetto della vita privata sarà valida solo nella misura in cui rispetti le condizioni di cui all'articolo 52, paragrafo 1, della Carta, come meglio esposto nelle seguenti sezioni.

4.3 Valutazione e attenuazione del rischio

24. Ai sensi del capo II, sezione 1, della proposta, i prestatori di servizi di hosting e i prestatori di servizi di comunicazione interpersonale sono tenuti a individuare, esaminare e valutare, per ciascun servizio che offrono, il rischio di ricorso agli stessi a fini di abuso sessuale su minori online e a tentare poi di

([31]) Ibidem, pag. 5.
([32]) COM(2022) 209 final, pag. 15.

ridurre al minimo il rischio individuato applicando «misure di attenuazione ragionevoli e adeguate al rischio individuato».

25. L'EDPB e il GEPD osservano che, nello svolgimento di una valutazione del rischio, il prestatore dovrebbe tenere conto in particolare degli elementi elencati all'articolo 3, paragrafo 2, lettere da a) a e), della proposta, tra cui: divieti e restrizioni disposti nelle condizioni generali del prestatore; il modo in cui gli utenti fruiscono del servizio e relativo impatto sul rischio; il modo in cui il prestatore ha ideato e gestisce il servizio, ivi compreso il business model, la governance e i pertinenti sistemi e processi, e relativo impatto sul rischio. Per quanto riguarda il rischio di adescamento di minori, gli elementi proposti da prendere in considerazione sono i seguenti: quanto il servizio sia usato o possa essere usato da minori; le fasce di età e il rischio di adescamento per fascia di età; la disponibilità di funzionalità che permettono di cercare altri utenti, di funzionalità che permettono all'utente di entrare in contatto con altri utenti, specie tramite comunicazioni private, e di funzionalità che permettono all'utente di condividere immagini o video con altri utenti.

26. Pur riconoscendo l'apparente pertinenza di tali criteri, l'EDPB e il GEPD temono tuttavia che essi lascino un margine piuttosto ampio di interpretazione e valutazione. Diversi criteri sono descritti in termini altamente generici (ad esempio «il modo in cui gli utenti usano il servizio e il relativo impatto sul rischio») o riguardano funzionalità di base comuni a molti servizi online (ad esempio «permettendo all'utente di condividere immagini o video con altri utenti») e, in quanto tali, sembrano prestarsi a una valutazione soggettiva (piuttosto che oggettiva).

27. Secondo l'EDPB e il GEPD, lo stesso vale per le misure di attenuazione del rischio da adottare a norma dell'articolo 4 della proposta. Provvedimenti come quello di adeguare, mediante opportune misure tecniche e operative e di personale, i propri sistemi di moderazione dei contenuti o di raccomandazione sembrano pertinenti per ridurre il rischio individuato. Tuttavia tali criteri, se applicati nell'ambito di un complesso processo di valutazione del rischio e combinati con termini astratti e vaghi per descrivere il livello di rischio accettabile (ad esempio «misura sensibile»), non soddisfano i criteri di certezza del diritto e di prevedibilità necessari per giustificare un'ingerenza nella riservatezza delle comunicazioni tra privati che costituisce una chiara ingerenza nei diritti fondamentali al rispetto della vita privata e alla libertà di espressione.

28. Sebbene i prestatori di servizi non siano autorizzati a interferire con la riservatezza delle comunicazioni nell'ambito delle loro strategie di valutazione e attenuazione del rischio prima di ricevere un ordine di rilevazione, esiste un collegamento diretto tra gli obblighi di valutazione e attenuazione del rischio e i conseguenti obblighi di rilevazione. L'articolo 7, paragrafo 4, della proposta subordina l'emissione di un ordine di rilevazione all'esistenza di prove di un rischio significativo che il servizio in questione possa essere usato a fini di abuso sessuale su minori online. Prima di emettere un ordine di rilevazione deve essere seguito un processo complesso che coinvolga i prestatori, l'autorità coordinatrice e l'autorità giudiziaria o altra autorità amministrativa indipendente responsabile dell'emissione dell'ordine. In primo luogo, i prestatori devono valutare il rischio di uso dei loro servizi a fini di abuso sessuale su minori online (articolo 3 della proposta) e valutare possibili misure di attenuazione del rischio (articolo 4 della proposta) per contenere tale rischio. Gli esiti di tale esercizio devono quindi essere comunicati all'autorità coordinatrice competente (articolo 5 della proposta). Se la valutazione del rischio dimostra che permane un rischio significativo nonostante gli sforzi compiuti per attenuarlo, l'autorità coordinatrice ascolta il prestatore in merito a un progetto di richiesta di emissione di un ordine di rilevazione e gli dà la possibilità di presentare osservazioni. Il prestatore è inoltre tenuto a presentare un piano di attuazione, compreso un parere dell'autorità di protezione dei dati competente in caso di rilevazione del *grooming*. Se prosegue la trattazione del caso, l'autorità coordinatrice richiede un ordine di rilevazione a un organo giurisdizionale o a un'altra autorità

amministrativa che provvede infine a emetterlo. Pertanto, la valutazione iniziale del rischio e le misure scelte per ridurre il rischio individuato costituiscono un fondamento determinante ai fini della valutazione, da parte dell'autorità coordinatrice e dell'autorità giudiziaria o amministrativa competente, della necessità di un ordine di rilevazione.

29. L'EDPB e il GEPD prendono atto delle fasi complesse che portano all'emissione di un ordine di rilevazione, che comprendono una valutazione iniziale del rischio da parte del prestatore e la proposta, da parte di quest'ultimo, di misure di attenuazione dello stesso, nonché la sua ulteriore interazione con l'autorità coordinatrice competente. Essi ritengono che vi sia una sostanziale possibilità per il prestatore di influenzare l'esito della procedura. A tale riguardo, osservano che il considerando 17 della proposta stabilisce che i prestatori dovrebbero essere in grado di indicare, nel rendere conto dei rischi, «la disponibilità e preparazione» a ricevere in ultima analisi un ordine di rilevazione. Pertanto non si può presumere che ciascun prestatore cercherà di evitare l'emissione di un ordine di rilevazione al fine di preservare la riservatezza delle comunicazioni dei suoi utenti applicando le misure di attenuazione più efficaci ma meno intrusive, in particolare qualora tali misure di attenuazione interferiscano con la libertà d'impresa del prestatore ai sensi dell'articolo 16 della Carta.

30. Il GEPD e l'EDPB desiderano sottolineare che le garanzie procedurali non possono mai sostituire completamente le garanzie sostanziali. Pertanto, il complesso processo che porta all'eventuale emissione di un ordine di rilevazione di cui sopra dovrebbe essere accompagnato da chiari obblighi sostanziali. L'EDPB e il GEPD ritengono che la proposta difetti di chiarezza su diversi elementi chiave (ad esempio le nozioni di «rischio significativo», «misura sensibile» ecc.), che non possono essere compensati dalla presenza di molteplici livelli di garanzie procedurali. Quanto sopra è tanto più pertinente alla luce del fatto che i soggetti incaricati di applicare tali garanzie (ad esempio prestatori di servizi, autorità giudiziarie ecc.) godono di un ampio margine di discrezionalità rispetto ai meccanismi di bilanciamento dei diritti in questione in ogni singolo caso. In considerazione delle ampie ingerenze nei diritti fondamentali che deriverebbero dall'adozione della proposta, il legislatore dovrebbe garantire che questa preveda con maggiore chiarezza quando e dove tali ingerenze sono consentite. Pur riconoscendo che le misure legislative non possono essere eccessivamente prescrittive e devono lasciare una certa flessibilità nell'applicazione pratica, l'EDPB e il GEPD ritengono che il testo attuale della proposta lasci troppo spazio a potenziali abusi a causa dell'assenza di norme sostanziali chiare.

31. Dato il potenziale impatto significativo su un numero molto elevato di interessati (vale a dire, potenzialmente, tutti gli utenti dei servizi di comunicazione interpersonale), l'EDPB e il GEPD sottolineano la necessità di un elevato livello di certezza del diritto, chiarezza e prevedibilità della legislazione al fine di garantire che le misure proposte siano realmente efficaci nel conseguire l'obiettivo perseguito e al tempo stesso pregiudichino il meno possibile i diritti fondamentali in questione.

4.4 Condizioni per l'emissione di ordini di rilevazione

32. L'articolo 7 della proposta prevede che l'autorità coordinatrice del luogo di stabilimento abbia facoltà di chiedere all'autorità giudiziaria competente o ad altra autorità amministrativa indipendente dello Stato membro di emettere un ordine di rilevazione che impone a un prestatore di servizi di hosting o a un prestatore di servizi di comunicazione interpersonale di prendere le misure di cui all'articolo 10 per rilevare casi di abuso sessuale su minori online in un servizio specifico.

33. L'EDPB e il GEPD tengono debitamente conto dei seguenti elementi che devono essere soddisfatti prima dell'emissione di un ordine di rilevazione:

a. è comprovata l'esistenza di un rischio significativo che il servizio sia usato a fini di abuso sessuale su minori online ai sensi dell'articolo 7, paragrafi 5, 6 o 7, a seconda dei casi;

b. i motivi per emettere l'ordine di rilevazione prevalgono sulle conseguenze negative per i diritti e gli interessi legittimi di tutte le parti interessate, vista in particolare l'esigenza di garantire un giusto equilibrio tra i diritti fondamentali di queste parti.

34. Il concetto di rischio significativo è specificato all'articolo 7, paragrafi 5 e seguenti, in rapporto alla tipologia dell'ordine di rilevazione in esame. In caso di ordini relativi alla rilevazione di materiale pedopornografico noto, si presume un rischio significativo se:

a. è probabile che, nonostante le misure di attenuazione che il prestatore può aver disposto o disporrà, il servizio sia usato in misura sensibile per la diffusione di materiale pedopornografico noto;

b. è comprovato che il servizio, o altro servizio comparabile se quello non è ancora offerto nell'Unione alla data della richiesta di emissione di un ordine di rilevazione, è stato usato negli ultimi 12 mesi e in misura sensibile per la diffusione di materiale pedopornografico noto.

35. Per emettere un ordine di rilevazione di materiale pedopornografico nuovo, la probabilità e le prove fattuali devono fare riferimento al materiale pedopornografico nuovo e in precedenza deve essere stato emesso un ordine di rilevazione per materiale pedopornografico noto che deve aver portato a un numero rilevante di segnalazioni di materiale pedopornografico da parte del prestatore (articolo 7, paragrafo 6, della proposta). Nel caso di un ordine di rilevazione del *grooming*, si considera sussistere un rischio significativo se il prestatore è un prestatore di servizi di comunicazione interpersonale, se è probabile che il servizio sia usato in misura sensibile per adescamento di minori e se è comprovato che il servizio è stato usato in misura sensibile per adescamento di minori (articolo 7, paragrafo 7, della proposta).

36. L'EDPB e il GEPD osservano che, anche con le precisazioni di cui all'articolo 7, paragrafi da 5 a 7, della proposta, le condizioni per l'emissione di un ordine di rilevazione contengono prevalentemente termini giuridici vaghi, quali «misura sensibile» e «numero significativo», e sono in parte ripetitive, in quanto le prove di precedenti abusi contribuiranno spesso a stabilire la probabilità di abusi futuri.

37. La proposta prevede un sistema in base al quale, nel decidere se un ordine di rilevazione sia necessario, deve essere presa una decisione previsionale sull'uso futuro di un servizio a fini di abuso sessuale su minori online. È pertanto comprensibile che gli elementi di cui all'articolo 7 abbiano carattere prognostico. Tuttavia il ricorso della proposta a nozioni vaghe rende difficile per i prestatori, nonché per l'autorità giudiziaria o altra autorità amministrativa indipendente competente abilitata, applicare le prescrizioni giuridiche introdotte dalla proposta in modo prevedibile e non arbitrario. L'EDPB e il GEPD temono che queste nozioni ampie e vaghe porteranno a una mancanza di certezza del diritto e determineranno anche notevoli divergenze nell'attuazione concreta della proposta in tutta l'Unione, a seconda delle interpretazioni che le autorità giudiziarie o altre autorità amministrative indipendenti degli Stati membri daranno a nozioni quali «probabilità» e «misura sensibile». Un tale esito non sarebbe accettabile alla luce del fatto che le disposizioni sugli ordini di rilevazione per i prestatori di servizi di comunicazione interpersonale costituiranno «limitazioni» al principio della riservatezza delle comunicazioni di cui all'articolo 5 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, cosicché la loro chiarezza e prevedibilità rivestono la massima importanza per garantire che tali limitazioni siano applicate in modo uniforme in tutta l'Unione.

4.5 Analisi della necessità e della proporzionalità delle misure previste ([33])

38. Come indicato in precedenza, possono essere emessi tre tipi di ordini di rilevazione: ordini di rilevazione per diffusione di materiale pedopornografico noto (articolo 7, paragrafo 5, della proposta), ordini di rilevazione per diffusione di materiale pedopornografico nuovo (articolo 7, paragrafo 6, della proposta) e ordini di rilevazione per adescamento di minori (articolo 7, paragrafo 7, della proposta). Ogni ordine di rilevazione richiederà di norma una tecnologia diversa per la sua attuazione pratica e avrà pertanto un diverso livello di invasività e, quindi, un impatto diverso sui diritti al rispetto della vita privata e alla protezione dei dati personali.

39. Le tecnologie per rilevare materiale pedopornografico noto sono generalmente tecnologie di abbinamento, nel senso che si basano su una banca dati esistente di materiale pedopornografico noto con cui possono confrontare immagini (compresi i fermo immagine di video). Per consentire l'abbinamento, le immagini che il prestatore sta elaborando e le immagini contenute nella banca dati devono essere state digitalizzate, in genere attraverso la conversione in valori di hash. Questo tipo di tecnologia di hashing ha un tasso stimato di falsi positivi non superiore a 1 su 50 miliardi (pari quindi a 0,000000002 %). [34]

40. Per la rilevazione di materiale pedopornografico nuovo è generalmente utilizzato un tipo diverso di tecnologia, tra cui classificatori e intelligenza artificiale (IA) ([35]). Tuttavia i tassi di errore sono in genere notevolmente più elevati. Ad esempio, la relazione sulla valutazione d'impatto indica che esistono tecnologie per la rilevazione di materiale pedopornografico nuovo il cui tasso di precisione può essere fissato al 99,9 % (corrispondente a un tasso di falsi positivi dello 0,1 %), ma con tale tasso di precisione sono in grado di identificare solo l'80 % del materiale pedopornografico totale nel pertinente insieme di dati ([36]).

41. Per quanto riguarda la rilevazione dell'adescamento di minori nelle comunicazioni sotto forma di testo, la relazione sulla valutazione d'impatto spiega che essa si basa tipicamente sulla rilevazione di schemi ricorrenti e osserva che alcune delle tecnologie esistenti per la rilevazione del *grooming* hanno un «tasso di accuratezza» dell'88 % ([37]). Secondo la Commissione ciò significa che «su 100 conversazioni segnalate come possibile adescamento di minori penalmente rilevante, è possibile che 12 siano escluse al momento della verifica [secondo la proposta, da parte del Centro dell'UE] e non vengano quindi segnalate alle autorità di contrasto» ([38]). Tuttavia, benché (contrariamente al regolamento provvisorio) la proposta si applichi anche alle comunicazioni in forma di audio, la relazione sulla valutazione d'impatto non illustra le soluzioni tecnologiche che potrebbero essere utilizzate per rilevare il *grooming* in tale contesto.

([33]) Cfr. anche «La guida rapida del GEPD sulla necessità e la proporzionalità», disponibile all'indirizzo: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.
([34]) Cfr. Commissione europea, documento di lavoro dei servizi della Commissione, Relazione sulla valutazione d'impatto che accompagna il documento Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori (SWD(2022) 209 final) (di seguito «relazione sulla valutazione d'impatto» o «SWD(2022) 209 final»), pag. 281, nota 511.
([35]) Relazione sulla valutazione d'impatto, pag. 281.
([36]) Ibidem, pag. 282.
([37]) Ibidem, pag. 283.
([38]) COM(2022)209 final, pag. 15, nota 32.

4.5.1 Efficacia della rilevazione

42. La valutazione della necessità comporta un'analisi fattuale dell'efficacia delle misure previste nel conseguire l'obiettivo perseguito e della loro minore intrusività rispetto ad altre opzioni disponibili al fine di conseguire lo stesso obiettivo ([39]). Un altro fattore da prendere in considerazione nella valutazione della proporzionalità di una misura proposta è l'efficacia delle misure esistenti rispetto a e a prescindere da quella proposta ([40]). Se già esistono misure che perseguono la stessa o un'analoga finalità, se ne dovrebbe valutare l'efficacia nell'ambito della valutazione della proporzionalità. In assenza di una siffatta valutazione dell'efficacia delle misure esistenti che perseguono la stessa o un'analoga finalità, non si può ritenere che sia stata debitamente verificata la proporzionalità di una nuova misura.

43. La rilevazione di materiale pedopornografico o del *grooming* da parte dei prestatori di servizi di hosting e dei prestatori di servizi di comunicazione interpersonale è in grado di contribuire all'obiettivo generale di prevenire e contrastare gli abusi sessuali su minori e la diffusione online di materiale pedopornografico. Allo stesso tempo, la necessità di valutare l'efficacia delle misure previste nella proposta solleva tre questioni fondamentali:

- Le misure per rilevare gli abusi sessuali su minori online possono essere eluse facilmente?
- Quale effetto avranno le attività di rilevazione sulle misure prese dalle autorità di contrasto ([41])?
- In che modo la proposta ridurrebbe l'incertezza del diritto?

44. Non spetta all'EDPB e al GEPD rispondere dettagliatamente a tali quesiti. Tuttavia, essi osservano che né la relazione sulla valutazione d'impatto né la proposta affrontano pienamente tali questioni.

45. Per quanto riguarda la possibilità di eludere la rilevazione del materiale pedopornografico, va osservato che al momento non sembra sussistere alcuna soluzione tecnologica in grado di rilevare il materiale pedopornografico condiviso in forma cifrata. Pertanto, qualsiasi attività di rilevazione, anche la scansione lato client per aggirare la cifratura da punto a punto (*end-to-end)* offerta dal prestatore ([42]), può essere facilmente elusa attraverso la cifratura del contenuto con l'ausilio di un'applicazione separata prima dell'invio o del caricamento. Le misure di rilevazione previste dalla proposta potrebbero quindi avere un impatto inferiore a quello auspicato sulla diffusione di materiale pedopornografico su internet.

46. Con l'adozione degli obblighi di rilevazione introdotti dalla proposta, la Commissione prevede inoltre un aumento del numero di segnalazioni di abusi sessuali su minori alle autorità di contrasto ([43]). Tuttavia, né la proposta né la relazione sulla valutazione d'impatto spiegano in che modo ciò consentirebbe di affrontare le carenze della situazione attuale. Date le risorse limitate delle autorità

([39]) GEPD, «Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali: un kit di strumenti» (11 aprile 2017), pag. 5; GEPD, «Orientamenti del GEPD sulla valutazione della proporzionalità di misure che limitano il diritto fondamentale alla vita privata e alla protezione dei dati personali» (19 dicembre 2019), pag. 8.
([40]) GEPD, «Orientamenti del GEPD sulla valutazione della proporzionalità di misure che limitano il diritto fondamentale alla vita privata e alla protezione dei dati personali» (19 dicembre 2019), pag. 11.
([41]) Secondo la relazione sulla valutazione d'impatto, allegato 2, pag. 132, l'85,71 % dei partecipanti all'indagine sull'attività di contrasto ha espresso preoccupazioni in merito all'aumento della quantità di materiale pedopornografico nell'ultimo decennio e alla mancanza di risorse (umane, tecniche).
([42]) Cfr. anche la sezione 4.10.
([43]) Cfr. tra l'altro la relazione sulla valutazione d'impatto, allegato 3 (SWD(2022) 209 final, pag. 176).

di contrasto, appare necessario capire meglio se l'aumento del numero di segnalazioni avrebbe un impatto significativo sulle attività di contrasto nei confronti degli abusi sessuali sui minori. L'EDPB e il GEPD desiderano comunque sottolineare che tali segnalazioni dovrebbero essere valutate tempestivamente per garantire che sia presa quanto prima una decisione sulla rilevanza penale del materiale segnalato e per limitare il più possibile la conservazione di dati non pertinenti.

4.5.2 Assenza di misure meno intrusive

47. Supponendo che si materializzino gli effetti positivi della rilevazione di materiale pedopornografico e del *grooming* previsti dalla Commissione, la rilevazione deve essere la meno intrusiva tra le misure di pari efficacia. L'articolo 4 della proposta stabilisce che, come primo passo, i prestatori dovrebbero prendere in considerazione l'adozione di misure di attenuazione per ridurre il rischio di uso dei loro servizi a fini di abuso sessuale su minori online al di sotto della soglia che giustifica l'emissione di un ordine di rilevazione. Se esistono misure di attenuazione che potrebbero portare a una riduzione sostanziale della mole di casi di *grooming* o di materiale pedopornografico scambiato nell'ambito di un determinato servizio, tali misure saranno spesso quelle meno intrusive rispetto a un ordine di rilevazione ([44]). Pertanto, qualora il prestatore interessato non le adotti su base volontaria, l'autorità amministrativa indipendente o l'autorità giudiziaria competente dovrebbero poter rendere obbligatoria ed esecutiva l'attuazione delle misure di attenuazione anziché emettere un ordine di rilevazione. Secondo l'EDPB e il GEPD, il fatto che, a norma dell'articolo 5, paragrafo 4, della proposta, l'autorità coordinatrice abbia il potere di «esigere» dal prestatore che introduca, riesamini, sospenda o ampli le misure di attenuazione non è sufficiente, in quanto tale prescrizione non sarebbe esecutiva in modo indipendente e la sua inosservanza sarebbe «sanzionata» solo disponendo un ordine di rilevazione.

48. L'EDPB e il GEPD ritengono pertanto che all'autorità coordinatrice o all'autorità amministrativa o giudiziaria indipendente competente dovrebbe essere esplicitamente conferito il potere di imporre misure di attenuazione meno intrusive prima o in luogo dell'emissione di un ordine di rilevazione.

4.5.3 Proporzionalità in senso stretto

49. Affinché una misura rispetti il principio di proporzionalità sancito dall'articolo 52, paragrafo 1, della Carta, i benefici da essa derivanti non dovrebbero essere superati dagli inconvenienti che la misura comporta per quanto riguarda l'esercizio dei diritti fondamentali. Pertanto il principio di proporzionalità "limita le autorità nell'esercizio delle loro competenze imponendo un bilanciamento tra i mezzi utilizzati e lo scopo perseguito (o il risultato conseguito)" ([45]).

([44]) Ad esempio potrebbero essere prese in considerazione misure quali bloccare lato client la trasmissione di materiale pedopornografico impedendo il caricamento e l'invio di contenuti di comunicazioni elettroniche, in quanto in alcuni contesti queste misure potrebbero contribuire a prevenire la circolazione di materiale pedopornografico noto.

([45]) Cfr. le sentenze della Corte di giustizia dell'8 luglio 2010, *Afton Chemical*, C-343/09, ECLI:EU:C:2010:419, punto 45; del 9 novembre 2010, *Volker und Markus Schecke e Hartmut Eifert*, cause riunite C-92/09 e C-93/09, ECLI:EU:C:2010:662, punto 74; del 23 ottobre 2012, *Nelson e a.*, cause riunite C-581/10 e C-629/10, ECLI:EU:C:2012:657, punto 71; del 22 gennaio 2013, *Sky Österreich*, C-283/11, ECLI:EU:C:2013:28, punto 50; e del 17 ottobre 2013, *Schaible*, C-101/12, ECLI:EU:C:2013:661, punto 29. Cfr. inoltre GEPD, «Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali: un kit di strumenti» (11 aprile 2017).

50. Per poter valutare l'impatto di una misura sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, è particolarmente importante individuare con precisione: [46]

- l'**ambito di applicazione** della misura, compreso il numero di persone interessate e se essa comporti «intrusioni collaterali» (ossia un'ingerenza nella vita privata di persone diverse dai soggetti interessati dalla misura);
- la **portata della misura**, anche per quanto riguarda la quantità di informazioni raccolte, per quanto tempo, se la misura in esame richiede la raccolta e il trattamento di categorie particolari di dati;
- il **livello di invasività**, tenendo conto di quanto segue: la natura dell'attività oggetto della misura (se incide o meno su attività soggette all'obbligo di riservatezza, sul rapporto tra avvocato e cliente, sull'attività medica); il contesto; se equivale o meno alla profilazione delle persone interessate; se il trattamento comporta l'uso di un sistema decisionale (parzialmente o totalmente) automatizzato con un «margine di errore»;
- se riguarda o meno **persone vulnerabili**;
- se incide anche su **altri diritti fondamentali** (ad esempio il diritto alla libertà di espressione, come nelle cause *Digital Rights Ireland e Seitlinger e a.* e *Tele2 Sverige e Watson*)[47].

51. In tale contesto è altresì importante osservare che l'impatto può essere minore per quanto riguarda la persona interessata, ma comunque significativo o molto significativo collettivamente/per la società nel suo insieme ([48]).

52. In tutti e tre i tipi di ordini di rilevazione (rilevazione di materiale pedopornografico noto, di materiale pedopornografico nuovo e del *grooming*), le tecnologie attualmente disponibili si basano sul trattamento automatizzato dei dati relativi ai contenuti di tutti gli utenti interessati. Le tecnologie utilizzate per analizzare i contenuti sono spesso complesse e di solito comportano l'uso dell'IA. Di conseguenza l'operatività di tali tecnologie potrebbe non essere del tutto comprensibile per l'utente del servizio. Inoltre è noto che le tecnologie attualmente disponibili, in particolare quelle per la rilevazione di materiale pedopornografico nuovo o del *grooming*, presentano tassi di errore relativamente elevati ([49]). Vi è poi il rischio di essere segnalati al Centro dell'UE a norma dell'articolo 12, paragrafo 1, e dell'articolo 48, paragrafo 1, della proposta, sulla base della rilevazione di «potenziale» materiale pedopornografico.

53. Inoltre le condizioni generali per l'emissione di un ordine di rilevazione ai sensi della proposta, vale a dire la sua applicazione a un intero servizio e non solo a comunicazioni selezionate ([50]), la durata massima di 24 mesi per quanto riguarda materiale pedopornografico noto o nuovo e fino a 12 mesi

([46]) GEPD, «Orientamenti del GEPD sulla valutazione della proporzionalità di misure che limitano il diritto fondamentale alla vita privata e alla protezione dei dati personali» (19 dicembre 2019), pag. 23.
([47]) Cfr. anche GEPD, Parere n. 7/2020 sulla proposta di deroghe temporanee alla direttiva 2002/58/CE ai fini della lotta contro gli abusi sessuali online sui minori (10 novembre 2020), punto 9 e seguenti.
([48]) GEPD, «Orientamenti del GEPD sulla valutazione della proporzionalità di misure che limitano il diritto fondamentale alla vita privata e alla protezione dei dati personali» (19 dicembre 2019), pag. 20.
([49]) Cfr. i dettagli forniti in precedenza, alla sezione 4.5, e in appresso, alla sottosezione 4.8.2.
([50]) Cfr. l'articolo 7, paragrafo 1, della proposta.

per il *grooming*[51] ecc., possono determinare nei fatti una portata molto ampia dell'ordine. Di conseguenza il monitoraggio avrebbe in realtà natura generale e indiscriminata e non sarebbe mirato.

54. Alla luce di quanto precede, l'EDPB e il GEPD sono altresì preoccupati per i possibili effetti dissuasivi sull'esercizio della libertà di espressione e ricordano che tale effetto dissuasivo è ritenuto tanto più probabile quanto minore è la chiarezza della legge.

55. In assenza della specificità, della precisione e della chiarezza necessarie per garantire pienamente la certezza del diritto ([52]), e dato il suo ampio ambito di applicazione, vale a dire tutti i prestatori di servizi della società dell'informazione interessati che offrono detti servizi nell'Unione ([53]), la proposta non garantisce che sia effettivamente attuato solo un approccio mirato alla rilevazione di materiale pedopornografico e del *grooming*. L'EDPB e il GEPD ritengono pertanto che, nella pratica, la proposta potrebbe legittimare una scansione di fatto generalizzata e indiscriminata dei contenuti praticamente di tutti i tipi di comunicazioni elettroniche di tutti gli utenti nell'UE/nel SEE. Di conseguenza la legislazione può indurre le persone ad astenersi dal condividere contenuti legali per timore di essere "attenzionate" a seguito di tale condivisione.

56. Ciò detto, l'EDPB e il GEPD riconoscono che le diverse misure per contrastare gli abusi sessuali su minori online possono comportare diversi livelli di invasività. In via preliminare, essi osservano che l'analisi automatizzata di materiale audio o testuale al fine di individuare potenziali casi di adescamento di minori può costituire un'ingerenza più significativa rispetto all'abbinamento di immagini o video sulla base di casi precedentemente confermati di materiale pedopornografico al fine di rilevare la diffusione di tale materiale. Inoltre dovrebbe essere operata una distinzione tra la rilevazione di «materiale pedopornografico noto» e di «materiale pedopornografico nuovo». L'impatto dovrebbe poi essere ulteriormente differenziato tra le misure rivolte ai prestatori di servizi di hosting e quelle imposte ai prestatori di servizi di comunicazione interpersonale.

4.5.4 Rilevazione di materiale pedopornografico noto

57. Sebbene, in conformità del considerando 4, la proposta sarebbe «tecnologicamente neutra», sia l'efficacia delle misure di rilevazione proposte sia l'effetto di tali misure sulle persone dipenderanno in larga misura dalla scelta della tecnologia applicata e dagli indicatori selezionati. Questo fatto è riconosciuto dalla Commissione nella relazione sulla valutazione d'impatto, allegato 8 ([54]), e confermato da altri studi, come la valutazione d'impatto sostitutiva mirata del Servizio europeo di ricerca parlamentare sulla proposta della Commissione sulla deroga temporanea alla direttiva relativa alla vita privata e alle comunicazioni elettroniche ai fini della lotta contro gli abusi sessuali online sui minori a partire dal febbraio 2021 ([55]).

58. L'articolo 10 della proposta stabilisce una serie di requisiti relativamente alle tecnologie da utilizzare a fini di rilevazione, in particolare per quanto riguarda la loro efficacia, affidabilità e minore intrusività

([51]) Cfr. l'articolo 7, paragrafo 9, della proposta.
([52]) Cfr. la sentenza della Corte di giustizia del 13 marzo 1997, *Commissione delle Comunità europee contro Repubblica francese*, C-197/96, ECLI:EU:C:1997:155, punto 15.
([53]) Cfr. l'articolo 1, paragrafo 2, della proposta.
([54]) Cfr. le informazioni sui tassi di falsi positivi nella relazione sulla valutazione d'impatto, allegato 8, pag. 279 e seguenti.
([55]) Cfr. la proposta della Commissione sulla deroga temporanea alla direttiva relativa alla vita privata e alle comunicazioni elettroniche ai fini della lotta contro gli abusi sessuali online sui minori: valutazione d'impatto sostitutiva mirata (Servizio europeo di ricerca parlamentare, febbraio 2021), pag. 14 e seguenti.

in termini di ingerenza nei diritti degli utenti al rispetto della vita privata e familiare, compresa la riservatezza delle comunicazioni, e alla protezione dei dati personali.

59. In tale contesto l'EDPB e il GEPD osservano che, attualmente, le uniche tecnologie che sembrano in grado di soddisfare in generale tali requisiti sono quelle utilizzate per rilevare il materiale pedopornografico noto, vale a dire le tecnologie di abbinamento basate su una banca dati di hash utilizzati come riferimento.

4.5.5 Rilevazione di materiale pedopornografico precedentemente sconosciuto

60. La valutazione delle misure volte a rilevare materiale pedopornografico precedentemente sconosciuto (vale a dire, nuovo) porta a conclusioni diverse per quanto riguarda la loro efficacia, affidabilità e ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati.

61. In primo luogo, come spiegato nella relazione sulla valutazione d'impatto che accompagna la proposta, le tecnologie attualmente utilizzate per la rilevazione di materiale pedopornografico precedentemente sconosciuto comprendono i classificatori e l'IA. Un classificatore è un algoritmo che suddivide i dati in classi o categorie di informazioni etichettate attraverso il riconoscimento di schemi ricorrenti ([56]). Pertanto queste tecnologie hanno risultati e impatti diversi in termini di accuratezza, efficacia e livello di invasività. Allo stesso tempo, sono anche più soggette a errori.

62. Le tecniche utilizzate per rilevare materiale pedopornografico precedentemente sconosciuto sono simili a quelle utilizzate per rilevare l'adescamento di minori, in quanto entrambe si basano non già su semplici tecnologie di abbinamento, bensì su modelli predittivi che utilizzano tecnologie di IA. L'EDPB e il GEPD ritengono che occorra un livello elevato di cautela nel rilevare materiale pedopornografico precedentemente sconosciuto, in quanto un errore del sistema avrebbe gravi conseguenze per gli interessati, i quali sarebbero automaticamente segnalati come possibili autori di un reato molto grave, con conseguente comunicazione dei loro dati personali e dei dettagli delle loro comunicazioni.

63. In secondo luogo, gli indicatori di prestazione trovati in letteratura, alcuni dei quali sono messi in evidenza nella relazione sulla valutazione d'impatto che accompagna la proposta ([57]), forniscono pochissime informazioni sulle condizioni utilizzate per il loro calcolo e sulla loro adeguatezza rispetto alle condizioni di vita reali, il che significa che le loro prestazioni reali potrebbero essere significativamente inferiori a quanto previsto, con una conseguente minore accuratezza e un tasso più elevato di «falsi positivi».

64. In terzo luogo, gli indicatori di prestazione dovrebbero essere considerati nel contesto specifico dell'uso dei pertinenti strumenti di rilevazione e fornire una visione esaustiva del comportamento di tali strumenti. Quando si utilizzano algoritmi di intelligenza artificiale su immagini o testi, è ben documentato che possono verificarsi distorsioni e discriminazioni a causa della mancanza di rappresentatività di determinati gruppi di popolazione nei dati utilizzati per impostare l'algoritmo. Tali distorsioni dovrebbero essere individuate, misurate e ridotte a un livello accettabile affinché i sistemi di rilevazione siano realmente utili per la società nel suo complesso.

65. Sebbene sia stato effettuato uno studio sulle tecnologie utilizzate per la rilevazione ([58]), l'EDPB e il GEPD ritengono che sia necessaria un'ulteriore analisi per valutare l'affidabilità degli strumenti

([56]) Relazione sulla valutazione d'impatto, allegato 8, pag. 281.
([57]) Relazione sulla valutazione d'impatto, allegato 8, pag. 281-283.
([58]) Relazione sulla valutazione d'impatto, pag. 279 e seguenti.

esistenti. Tale analisi dovrebbe basarsi su indicatori di prestazione esaustivi e valutare l'impatto di potenziali errori in condizioni di vita reale per tutti gli interessati contemplati dalla proposta.

66. Come osservato in precedenza, l'EDPB e il GEPD nutrono seri dubbi quanto alla misura in cui le garanzie procedurali di cui all'articolo 7, paragrafo 6, della proposta siano sufficienti a compensare tali rischi. Inoltre, come già segnalato, essi osservano che la proposta utilizza termini piuttosto astratti e vaghi per descrivere il livello di rischio accettabile (ad esempio «misura sensibile»).

67. L'EDPB e il GEPD temono che queste nozioni ampie e vaghe porteranno a una mancanza di certezza del diritto e causeranno anche forti divergenze nell'attuazione concreta della proposta in tutta l'Unione, a seconda delle interpretazioni che le autorità giudiziarie o altre autorità amministrative indipendenti degli Stati membri daranno a nozioni quali «probabilità» e «misura sensibile». Ciò è preoccupante anche alla luce del fatto che le disposizioni sugli ordini di rilevazione costituiranno «limitazioni» al principio della riservatezza di cui all'articolo 5 della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Pertanto è necessario migliorarne chiarezza e prevedibilità nel regolamento proposto.

4.5.6 Rilevazione dell'adescamento di minori (*grooming*)

68. L'EDPB e il GEPD osservano che le misure proposte in materia di rilevazione dell'adescamento di minori (*grooming*), che comportano un'analisi automatizzata del linguaggio scritto o parlato, possono costituire l'ingerenza più significativa nei diritti degli utenti al rispetto della vita privata e familiare, compresa la riservatezza delle comunicazioni, e alla protezione dei dati personali.

69. Mentre la rilevazione di materiale pedopornografico, sia noto sia nuovo, può essere limitata all'analisi di immagini e video, la rilevazione del *grooming* si estenderebbe per definizione a tutte le comunicazioni sotto forma di testo (ed eventualmente di audio) che rientrano nell'ambito di applicazione di un ordine di rilevazione. Di conseguenza, è molto maggiore l'intensità dell'ingerenza nella riservatezza delle comunicazioni in questione.

70. L'EDPB e il GEPD ritengono che un'analisi automatizzata delle comunicazioni sotto forma di testo trasmesse attraverso servizi di comunicazione interpersonale, avente una natura sostanzialmente generale e indiscriminata, al fine di individuare potenziali casi di adescamento di minori non rispetti i requisiti di necessità e proporzionalità. Anche se la tecnologia utilizzata si limita all'uso di indicatori, l'EDPB e il GEPD ritengono che l'applicazione di tale analisi generale e indiscriminata sia eccessiva e possa persino incidere sulla sostanza stessa del diritto fondamentale al rispetto della vita privata sancito dall'articolo 7 della Carta.

71. Come già indicato, la mancanza di garanzie sostanziali nel contesto delle misure di rilevazione dell'adescamento di minori non può essere compensata unicamente da garanzie procedurali. Inoltre, il problema della mancanza di sufficiente chiarezza e certezza del diritto (ad esempio l'uso di formulazioni giuridicamente vaghe come «in misura sensibile») è ancora più grave nel caso dell'analisi automatizzata delle comunicazioni personali sotto forma di testo di quanto non lo sia nel caso di un confronto fotografico basato sulla tecnologia di «hashing».

72. L'EDPB e il GEPD ritengono inoltre che l'«effetto dissuasivo» sulla libertà di espressione sia particolarmente significativo quando si sottopongono comunicazioni interpersonali sotto forma di testo (o di audio) a scansione e analisi su larga scala, e ricordano che tale effetto dissuasivo è tanto più grave quanto minore è la chiarezza della norma.

73. Inoltre, come indicato nella relazione sulla valutazione d'impatto ([59]) e nello studio del Servizio europeo di ricerca parlamentare ([60]), il tasso di accuratezza delle tecnologie per la rilevazione del *grooming* sotto forma di testo è di gran lunga inferiore al tasso di accuratezza delle tecnologie per la rilevazione di materiale pedopornografico noto ([61]). Le tecniche di rilevazione del *grooming* sono concepite per analizzare e assegnare rating di probabilità a ciascun aspetto della conversazione, pertanto l'EDPB e il GEPD le ritengono anche soggette a errori e vulnerabili agli abusi.

4.5.7 Conclusione sulla necessità e sulla proporzionalità delle misure previste

74. Per quanto riguarda la necessità e la proporzionalità delle misure di rilevazione previste, le preoccupazioni dell'EDPB e del GEPD riguardano soprattutto quelle mirate al materiale pedopornografico sconosciuto e per l'adescamento di minori (*grooming*), a causa della loro invasività dovuta al potenziale accesso su base generalizzata al contenuto delle comunicazioni, della loro natura probabilistica e dei tassi di errore associati a tali tecnologie.

75. Dalla giurisprudenza della CGUE emerge, inoltre, che le misure che consentono alle autorità pubbliche di accedere in modo generalizzato al contenuto di una comunicazione hanno maggiori probabilità di pregiudicare il contenuto essenziale dei diritti garantiti dagli articoli 7 e 8 della Carta. Tali considerazioni sono particolarmente pertinenti per quanto riguarda le misure per la rilevazione dell'adescamento di minori previste dalla proposta.

76. In ogni caso, l'EDPB e il GEPD ritengono che l'ingerenza creata, in particolare, dalle misure per la rilevazione dell'adescamento di minori vada oltre quanto strettamente necessario e proporzionato. Tali misure dovrebbero pertanto essere espunte dalla proposta.

4.6 Obblighi di segnalazione

77. L'EDPB e il GEPD raccomandano di integrare l'elenco degli obblighi specifici di segnalazione di cui all'articolo 13 della proposta con l'obbligo di includere nella segnalazione informazioni sulla tecnologia specifica che ha consentito al prestatore di venire a conoscenza dei contenuti abusivi, nel caso in cui il prestatore sia venuto a conoscenza del potenziale abuso sessuale su minori a seguito di misure adottate per eseguire un ordine di rilevazione emesso a norma dell'articolo 7 della proposta.

4.7 Obblighi di rimozione e blocco

78. Una delle misure previste dalla proposta per attenuare i rischi di diffusione di materiale pedopornografico è l'emissione di ordini di rimozione e blocco che obbligherebbero i prestatori a rimuovere o disabilitare l'accesso o a bloccare il materiale pedopornografico online ([62]).

79. Sebbene l'effetto degli ordini di rimozione sulla protezione dei dati e sulla riservatezza delle comunicazioni sia relativamente limitato, come osservazione di massima l'EDPB e il GEPD ricordano il principio generale da rispettare, secondo cui qualsiasi misura di questo tipo dovrebbe essere quanto più mirata possibile.

([59]) Relazione sulla valutazione d'impatto, allegato 8, pag. 281-283.
([60]) Pag. 15-18.
([61]) Cfr. sopra, punto 40.
([62]) Articoli 14 e 16 della proposta.

80. Allo stesso tempo l'EDPB e il GEPD richiamano l'attenzione sul fatto che i prestatori di servizi di accesso a internet possono risalire all'URL preciso dei contenuti solo se questi ultimi sono resi disponibili sotto forma di testo in chiaro. Ogni volta che i contenuti sono resi accessibili tramite HTTPS, il prestatore di servizi di accesso a internet non potrà risalire all'URL preciso, a meno che non decritti la comunicazione. L'EDPB e il GEPD nutrono pertanto dubbi in merito all'efficacia delle misure di blocco e ritengono che sarebbe sproporzionato imporre ai prestatori di servizi di accesso a internet di decrittare le comunicazioni online per bloccare quelle relative al materiale pedopornografico.

81. Inoltre, più in generale, va osservato che il blocco (o la disabilitazione) dell'accesso a un elemento digitale è un'operazione che ha luogo a livello di rete e la sua attuazione può rivelarsi inefficace in caso di copie multiple (eventualmente simili, ma non identiche) dello stesso elemento. Tale operazione può anche rivelarsi sproporzionata se il blocco interessa altri elementi digitali, non illegali, che siano memorizzati nello stesso server reso inaccessibile mediante comandi di rete (ad esempio, tramite la creazione di una lista nera di DNS o di indirizzi IP). Inoltre non tutte le metodologie per realizzare un blocco a livello di rete sono altrettanto efficaci e alcune possono essere facilmente eluse disponendo di competenze tecniche piuttosto basilari.

82. Infine, dovrebbero essere chiarite le competenze delle autorità coordinatrici per quanto riguarda l'emissione di ordini di blocco . Ad esempio, dall'attuale formulazione dell'articolo 16, paragrafo 1, e dell'articolo 17, paragrafo 1, non è chiaro se alle autorità coordinatrici sia conferito il potere di emettere o solo di richiedere l'emissione di ordini di blocco ([63]).

4.8 Tecnologie e salvaguardie pertinenti

4.8.1 Protezione dei dati fin dalla progettazione e per impostazione predefinita

83. Le prescrizioni della proposta che si applicano alle tecnologie da implementare per la rilevazione di materiale pedopornografico e dell'adescamento di minori non sembrano essere sufficientemente rigorose. In particolare, l'EDPB e il GEPD hanno osservato che, contrariamente alle analoghe disposizioni del regolamento provvisorio ([64]), la proposta non contiene alcun riferimento esplicito al principio della protezione dei dati fin dalla progettazione e per impostazione predefinita e non prevede che le tecnologie utilizzate per scansionare il testo delle comunicazioni non siano in grado di dedurre il contenuto sostanziale delle stesse. La proposta prevede semplicemente, all'articolo 10, paragrafo 3, lettera b), che le tecnologie in questione non devono essere in grado di «estrarre» dalle comunicazioni informazioni diverse da quelle che è strettamente necessario rilevare. Tuttavia tale norma non sembra essere sufficientemente rigorosa, in quanto potrebbe essere possibile *dedurre* altre informazioni dal contenuto sostanziale di una comunicazione senza *estrarre* informazioni in quanto tali.

84. Di conseguenza, il GEPD e l'EDPB raccomandano di introdurre nella proposta un considerando con cui si stabilisca che il principio della protezione dei dati fin dalla progettazione e per impostazione

([63]) L'articolo 16, paragrafo 1, della proposta recita: «L'autorità coordinatrice del luogo di stabilimento ha facoltà di chiedere all'autorità giudiziaria competente dello Stato membro che l'ha designata o ad altra autorità amministrativa indipendente di quello Stato membro di emettere un ordine di blocco [...]», mentre l'articolo 17, paragrafo 1, recita: «L'autorità coordinatrice emette gli ordini di blocco di cui all'articolo 16 [...]» (sottolineatura aggiunta).
([64]) Regolamento provvisorio, articolo 3, paragrafo 1, lettera b).

predefinita di cui all'articolo 25 del regolamento (UE) 2016/679 si applica, a norma di legge, alle tecnologie disciplinate dall'articolo 10 della proposta e, pertanto, non vi è la necessità di ribadirlo nelle disposizioni del regolamento in quanto tali. Inoltre l'articolo 10, paragrafo 3, lettera b), dovrebbe essere modificato per garantire non solo che non siano estratte altre informazioni, ma anche che non siano dedotte altre informazioni, in linea con quanto attualmente previsto dall'articolo 3, paragrafo 1, lettera b), del regolamento provvisorio.

4.8.2 Affidabilità delle tecnologie

85. La proposta presuppone che i prestatori di servizi possano utilizzare diversi tipi di soluzioni tecnologiche per eseguire gli ordini di rilevazione. In particolare parte dal presupposto che vi siano sistemi di intelligenza artificiale disponibili e funzionanti per la rilevazione di materiale pedopornografico sconosciuto e dell'adescamento di minori ([65]) e che alcune autorità coordinatrici potrebbero considerarli conformi allo stato dell'arte. Sebbene l'efficacia della proposta dipenda dall'affidabilità di queste soluzioni tecnologiche, sono disponibili pochissime informazioni sull'uso generalizzato e sistematico di tali tecniche, e questo elemento merita particolare attenzione.

86. Inoltre, sebbene l'EDPB e il GEPD abbiano dovuto utilizzarli nella valutazione della proporzionalità, in assenza di alternative, va osservato che gli indicatori prestazionali delle tecnologie di rilevazione menzionati nella relazione sulla valutazione d'impatto che accompagna la proposta forniscono pochissime informazioni sulle modalità di tale valutazione e sull'effettivo rispecchiamento delle prestazioni delle varie tecnologie. Non vi sono informazioni sui test o sui parametri di riferimento utilizzati dai fornitori di tecnologie per misurare tali prestazioni. In assenza di dette informazioni, non è possibile ripetere i test né valutare la validità delle dichiarazioni prestazionali. A tale riguardo va osservato che, sebbene gli indicatori di prestazione possano essere interpretati nel senso che alcuni strumenti di rilevazione hanno un elevato livello di accuratezza (ad esempio, l'accuratezza di taluni strumenti di rilevazione del *grooming* è pari all'88 %) ([66]), tali indicatori dovrebbero essere considerati alla luce dell'uso concretamente previsto degli strumenti di rilevazione e della gravità dei rischi che comporterebbe per gli interessati l'errata valutazione di un determinato materiale. L'EDPB e il GEPD ritengono inoltre che, con un trattamento soggetto a rischio così elevato, un tasso di insuccesso del 12 % configuri un rischio elevato per gli interessati che sono stati oggetto di falsi positivi, pur in presenza di garanzie finalizzate a prevenire segnalazioni errate alle autorità di contrasto. È altamente improbabile che i prestatori di servizi possano impegnare risorse sufficienti per riesaminare tale percentuale di falsi positivi.

87. Come già menzionato ([67]), gli indicatori di prestazione dovrebbero fornire una visione esaustiva del comportamento degli strumenti di rilevazione. Quando si utilizzano algoritmi di intelligenza artificiale su immagini o testi, è provato che possono verificarsi distorsioni e discriminazioni a causa della mancanza di rappresentatività di determinati gruppi di popolazione nei dati utilizzati per addestrare l'algoritmo. Tali distorsioni dovrebbero essere individuate, misurate e ridotte a un livello accettabile affinché i sistemi di rilevazione siano realmente vantaggiosi per la società nel suo complesso.

88. Sebbene sia stato effettuato uno studio sulle tecnologie utilizzate per la rilevazione ([68]), l'EDPB e il GEPD ritengono che sia necessaria un'ulteriore analisi per valutare in maniera indipendente

([65]) Cfr. la relazione sulla valutazione d'impatto, pag. 281-282.
([66]) Ibidem, pag. 283.
([67]) Cfr. i punti 63 e 64 sopra.
([68]) Cfr. la relazione sulla valutazione d'impatto, pag. 279 e seguenti.

l'affidabilità degli strumenti esistenti nei casi d'uso reali. Tale analisi dovrebbe basarsi su indicatori di prestazione esaustivi e valutare l'impatto di potenziali errori in condizioni di vita reale per tutti gli interessati contemplati dalla proposta. Poiché le suddette tecnologie sono poste a fondamento della proposta, l'EDPB e il GEPD ritengono che tale analisi sia di fondamentale importanza per valutare l'adeguatezza della proposta stessa.

89. L'EDPB e il GEPD osservano, inoltre, che la proposta non definisce obblighi specifici per la singola tecnologia, che sia con riguardo ai tassi di errore, all'uso dei classificatori e alla loro convalida, o ad altre restrizioni, e lascia invece alla prassi l'elaborazione tali criteri nel valutare la proporzionalità dell'uso di una tecnologia specifica, contribuendo ulteriormente alla mancanza di precisione e chiarezza.

90. Data l'importanza delle conseguenze per gli interessati in caso di falsi positivi, l'EDPB e il GEPD ritengono che i tassi di falsi positivi debbano essere ridotti al minimo e che i sistemi in questione debbano essere progettati tenendo presente che la stragrande maggioranza delle comunicazioni elettroniche non comprende né materiale pedopornografico né l'adescamento di minori, e che anche un tasso di falsi positivi molto basso comporterà un numero molto elevato di falsi positivi, considerato il volume di dati che saranno oggetto di rilevazione. Più in generale, l'EDPB e il GEPD sono anche preoccupati per il fatto che le prestazioni degli strumenti disponibili di cui alla relazione sulla valutazione d'impatto non riflettono indicatori precisi e comparabili per quanto riguarda i tassi di falsi positivi e falsi negativi, e ritengono che per tali tecnologie dovrebbero essere pubblicati indicatori di prestazione comparabili e significativi prima di poterle considerare disponibili ed efficienti.

4.8.3 Scansione delle comunicazioni audio

91. Contrariamente al regolamento provvisorio ([69]), la proposta non esclude dal suo ambito di applicazione la scansione delle comunicazioni audio nel contesto della rilevazione del *grooming* ([70]). L'EDPB e il GEPD ritengono che la scansione delle comunicazioni audio sia particolarmente intrusiva, in quanto richiederà di norma intercettazioni attive, continue e «in diretta». Inoltre, in alcuni Stati membri la riservatezza delle comunicazioni orali (il «parlato») gode di una protezione speciale ([71]). In più, dato che in linea di principio dovrebbero essere analizzati tutti i contenuti della comunicazione audio, tale misura può pregiudicare il contenuto essenziale dei diritti garantiti dagli articoli 7 e 8 della Carta. Tale metodo di rilevazione dovrebbe pertanto rimanere estraneo all'ambito di applicazione degli obblighi di rilevazione stabiliti nel regolamento proposto per quanto riguarda sia i messaggi vocali che le comunicazioni in diretta, tanto più se si considera che la relazione sulla valutazione d'impatto che accompagna la proposta non ha individuato rischi specifici o cambiamenti nel panorama delle minacce tali da giustificarne l'uso ([72]).

4.8.4 Verifica dell'età

92. La proposta incoraggia i prestatori ad adottare misure di verifica e valutazione dell'età per identificare gli utenti minori dei propri servizi ([73]). A tale riguardo l'EDPB e il GEPD osservano che attualmente non

([69]) Cfr. il regolamento provvisorio, articolo 1, paragrafo 2.
([70]) Cfr. l'articolo 1 della proposta.
([71]) Cfr. ad esempio il codice penale tedesco, articolo 201.
([72]) Cfr. la relazione sulla valutazione d'impatto.
([73]) Cfr. l'articolo 4, paragrafo 3, l'articolo 6, paragrafo 1, lettera c), e il considerando 16 della proposta.

esiste una soluzione tecnologica in grado di valutare con certezza l'età di un utente in un contesto online senza basarsi su un'identità digitale ufficiale, che in questa fase non è disponibile per tutti i cittadini europei. ([74]) Pertanto l'adozione di misure di verifica dell'età di cui alla proposta potrebbe portare all'esclusione dall'accesso ai servizi online, ad esempio, di adulti dall'aspetto giovanile o all'impiego di strumenti di verifica dell'età molto intrusivi, che potrebbero impedire o scoraggiare l'uso legittimo dei servizi in questione.

93. A tale riguardo, e anche se il considerando 16 della proposta fa riferimento agli strumenti di controllo parentale come possibili misure di attenuazione, l'EDPB e il GEPD raccomandano di modificare il regolamento proposto per consentire espressamente ai prestatori di fare affidamento sui meccanismi di controllo parentale in aggiunta o come alternativa alla verifica dell'età.

4.9 Conservazione delle informazioni

94. L'articolo 22 della proposta limita le finalità per le quali i prestatori a essa soggetti possono conservare i dati relativi al contenuto e altri dati trattati in relazione alle misure prese per ottemperare agli obblighi ivi stabiliti. Tuttavia, la proposta indica che i prestatori possono anche conservare tali informazioni nell'intento di migliorare l'efficacia e l'accuratezza delle tecnologie di rilevazione dell'abuso sessuale su minori online ai fini dell'esecuzione di un ordine di rilevazione, ma non possono memorizzare dati personali a tal fine ([75]).

95. L'EDPB e il GEPD ritengono che solo i prestatori che utilizzano le proprie tecnologie di rilevazione dovrebbero essere autorizzati a conservare i dati per migliorarne l'efficacia e l'accuratezza, mentre coloro che utilizzano le tecnologie fornite dal Centro dell'UE non dovrebbero beneficiare di tale possibilità. Osservano, inoltre, che potrebbe essere difficile garantire nella pratica che nessun dato personale sia memorizzato a tal fine, in quanto i dati relativi al contenuto e altri dati trattati a fini di rilevazione possono essere considerati per la maggior parte dati personali.

4.10 Impatto sulla cifratura

96. Le autorità europee di protezione dei dati hanno sempre perorato l'ampia disponibilità di strumenti di cifratura efficaci opponendosi a qualsiasi tipo di scorciatoia ("backdoor") ([76]). Ciò in quanto la cifratura è importante per garantire il godimento di tutti i diritti umani offline e online ([77]). Inoltre, le tecnologie di cifratura contribuiscono in modo fondamentale sia al rispetto della vita privata e alla riservatezza delle comunicazioni, sia all'innovazione e alla crescita dell'economia digitale, che si basa sull'elevato livello di fiducia e sicurezza che tali tecnologie consentono.

97. Nel contesto delle comunicazioni interpersonali, la cifratura da punto a punto («E2EE») è uno strumento fondamentale per garantire la riservatezza delle comunicazioni elettroniche, in quanto fornisce solide garanzie tecniche contro l'accesso al contenuto delle comunicazioni da parte di persone diverse dal mittente e dal destinatario o dai destinatari, compreso il prestatore. Impedire o scoraggiare in qualsiasi modo l'uso della E2EE, imporre ai prestatori di servizi l'obbligo di trattare i dati

([74]) Cfr. ad esempio CNIL, Recommandation 7: vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée (9 agosto 2021).
([75]) Cfr. l'articolo 22, paragrafo 1, della proposta.
([76]) Cfr. ad esempio Gruppo dell'articolo 29 per la tutela dei dati, dichiarazione del Gruppo dell'articolo 29 sulla cifratura e il suo impatto sulla tutela delle persone con riguardo al trattamento dei dati personali nell'UE (11 aprile 2018).
([77]) Cfr. UNHRC, Resolution 47/16 on the promotion, protection and enjoyment of human rights on the Internet, documento ONU A/HRC/RES/47/16 (26 luglio 2021).

delle comunicazioni elettroniche per fini diversi dalla prestazione dei loro servizi, o imporre loro l'obbligo di inoltrare proattivamente le comunicazioni elettroniche a terzi comporterebbe il rischio che i prestatori offrano servizi meno cifrati al fine di rispettare meglio gli obblighi, indebolendo così il ruolo della cifratura in generale e minando il rispetto dei diritti fondamentali dei cittadini europei. Va osservato che, sebbene la E2EE sia una delle misure di sicurezza più comunemente usate nel contesto delle comunicazioni elettroniche, altre soluzioni tecniche (ad esempio l'uso di altri sistemi crittografici) potrebbero essere o diventare altrettanto importanti per garantire e tutelare la riservatezza delle comunicazioni digitali. Pertanto anche il loro utilizzo non dovrebbe essere impedito o scoraggiato.

98. L'impiego di strumenti per l'intercettazione e l'analisi delle comunicazioni elettroniche interpersonali è intrinsecamente in contrasto con la E2EE, in quanto quest'ultima mira a garantire tecnicamente che una comunicazione rimanga riservata tra il mittente e il destinatario.

99. Pertanto, sebbene la proposta non stabilisca un obbligo sistematico di intercettazione per i prestatori, la semplice possibilità dell'emissione di un ordine di rilevazione potrebbe incidere pesantemente sulle scelte tecniche dei prestatori, soprattutto in considerazione del tempo limitato a loro disposizione per conformarsi a tale ordine e delle pesanti sanzioni cui andrebbero incontro qualora non vi si conformassero ([78]). In pratica ciò potrebbe indurre alcuni prestatori a cessare l'utilizzo della E2EE.

100. È necessario valutare adeguatamente l'impatto che la proposta può avere nel senso di compromettere o disincentivare l'uso della E2EE. Ciascuna delle tecniche presentate nella relazione sulla valutazione d'impatto che accompagna la proposta per eludere la tutela della vita privata garantita dalla E2EE introdurrebbe falle nella sicurezza ([79]). Ad esempio, la scansione lato client ([80]) comporterebbe probabilmente un accesso e un trattamento sostanziali e non mirati di contenuti non cifrati sui dispositivi dell'utente finale. Un tale sostanziale deterioramento della riservatezza colpirebbe soprattutto i minori, dal momento che è più probabile che i servizi che essi utilizzano siano oggetto di ordini di rilevazione, rendendoli vulnerabili al monitoraggio o all'intercettazione. Allo stesso tempo, anche la scansione *lato server* è intrinsecamente incompatibile con il paradigma della E2EE, in quanto dovrebbe essere decrittato il canale di comunicazione, cifrato da pari a pari, , portando così al trattamento massivo di dati personali sui server dei prestatori.

101. Sebbene la proposta affermi che il «regolamento lascia [...] al prestatore la libertà di scegliere le tecnologie da utilizzare per conformarsi efficacemente a un ordine di rilevazione e non dovrebbe essere inteso come un incentivo o un disincentivo all'uso di una determinata tecnologia» ([81]), l'incompatibilità strutturale di alcuni ordini di rilevazione con la E2EE diventa di fatto un forte disincentivo all'uso della E2EE. L'impossibilità di accedere ai servizi che usano la E2EE (che costituiscono l'attuale stato dell'arte in termini di garanzia tecnica di riservatezza) e di usufruirne potrebbe avere un effetto dissuasivo sulla libertà di espressione e sull'uso privato legittimo dei servizi di comunicazione elettronica. La relazione negativa tra la rilevazione di materiale pedopornografico o

([78]) Cfr. l'articolo 35 della proposta.

([79]) Cfr. la sezione 4.2 in Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso, «Bugs in our Pockets: The Risks of Client-Side Scanning», ArXiv abs/2110.07450 (2021).

([80]) La scansione lato client si riferisce in generale a sistemi che scansionano i contenuti dei messaggi alla ricerca di corrispondenze rispetto a una banca dati di contenuti discutibili prima che il messaggio sia inviato al destinatario previsto.

([81]) Cfr. il considerando 26 della proposta.

del *grooming* e la E2EE è riconosciuta anche dalla Commissione quando rileva, nella relazione sulla valutazione d'impatto ([82]), la probabilità che l'implementazione della E2EE prevista da Facebook per il 2023 ponga fine alla scansione volontaria da parte dello stesso Facebook.

102. Per garantire che il regolamento proposto non comprometta la sicurezza o la riservatezza delle comunicazioni elettroniche dei cittadini europei, l'EDPB e il GEPD ritengono che l'articolato della proposta debba indicare chiaramente che nessun elemento del suddetto regolamento dovrebbe essere interpretato come inteso a vietare o indebolire la cifratura, in linea con quanto affermato nel considerando 25 del regolamento provvisorio.

4.11 Vigilanza, attuazione e cooperazione

4.11.1 Ruolo delle autorità nazionali di controllo ai sensi del GDPR

103. La proposta prevede l'istituzione di una rete di autorità nazionali coordinatrici, responsabili dell'applicazione e dell'esecuzione del regolamento proposto ([83]). Sebbene il considerando 54 della proposta affermi che «le norme in materia di vigilanza ed esecuzione di cui al presente regolamento non dovrebbero intendersi tali da incidere sui poteri e sulle competenze delle autorità di protezione dei dati a norma del regolamento (UE) 2016/679», l'EDPB e il GEPD ritengono che dovrebbe essere meglio disciplinata la relazione tra i compiti delle autorità coordinatrici e quelli delle autorità di protezione dei dati e che le autorità di protezione dei dati dovrebbero avere un ruolo più importante nell'ambito del regolamento proposto.

104. In particolare i prestatori dovrebbero essere tenuti a consultare le autorità di protezione dei dati attraverso una procedura di consultazione preventiva di cui all'articolo 36 del GDPR prima di adottare qualsiasi misura di rilevazione di materiale pedopornografico o di *grooming*, e non esclusivamente in relazione all'uso di misure per rilevare l'adescamento di minori, come attualmente previsto dalla proposta ([84]). Tutte le misure di rilevazione dovrebbero essere considerate come «ad alto rischio» per impostazione predefinita e dovrebbero pertanto essere sottoposte a una procedura di consultazione preventiva, indipendentemente dal fatto che riguardino il *grooming* o materiale pedopornografico, come già avviene a norma del regolamento provvisorio ([85]). Inoltre, alle autorità di protezione dei dati competenti, designate a norma del GDPR, dovrebbe essere conferito il potere di esprimere sempre un parere sulle misure di rilevazione previste, e non solo in circostanze specifiche ([86]).

105. Il regolamento proposto dovrebbe inoltre istituire un sistema per affrontare e risolvere le controversie tra le autorità competenti e le autorità di protezione dei dati in merito agli ordini di rilevazione. In particolare, le autorità di protezione dei dati dovrebbero avere il diritto di impugnare un ordine di rilevazione dinanzi agli organi giurisdizionali dello Stato membro dell'autorità giudiziaria o dell'autorità amministrativa indipendente competente che ha emesso tale ordine. A tale riguardo l'EDPB e il GEPD osservano come, nell'attuale versione della proposta, il parere delle autorità di protezione dei dati competenti possa essere ignorato dall'autorità che emette un ordine di rilevazione. Ciò potrebbe portare a decisioni contrastanti, in quanto le autorità di protezione dei dati, come

([82]) Relazione sulla valutazione d'impatto, pag. 27.
([83]) Cfr. l'articolo 25 della proposta.
([84]) Cfr. l'articolo 7, paragrafo 3, secondo comma, lettera b), della proposta.
([85]) Regolamento provvisorio, articolo 3, paragrafo 1, lettera c).
([86]) Cfr. l'articolo 7, paragrafo 3, secondo comma, lettera c), della proposta.

confermato dall'articolo 36, paragrafo 2, GDPR, manterrebbero tutti i propri poteri correttivi ai sensi dell'articolo 58 del suddetto regolamento, compreso quello di ordinare un divieto di trattamento.

4.11.2 Ruolo dell'EDPB

106. L'EDPB e il GEPD osservano che la proposta, all'articolo 50, paragrafo 1, terza frase, stabilisce che «il Centro dell'UE chiede il parere del suo comitato tecnologico e del comitato europeo per la protezione dei dati» prima di aggiungere una tecnologia specifica agli elenchi di tecnologie che i prestatori di servizi di hosting e i prestatori di servizi di comunicazione interpersonale possono prendere in considerazione per eseguire gli ordini di rilevazione. La proposta prevede inoltre che l'EDPB formuli il proprio parere entro il termine di otto settimane, che può essere prorogato di sei settimane in considerazione della complessità della questione. Infine impone all'EDPB di informare il Centro dell' UE dell'eventuale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.

107. I compiti esistenti dell'EDPB sono elencati all'articolo 70 del GDPR e all'articolo 51 della direttiva (UE) 2016/680 (di seguito «LED»)[87]. Nell'ambito di tali compiti è stabilito che l'EDPB fornisce consulenza alla Commissione ed emette pareri su richiesta di quest'ultima, di un'autorità nazionale di controllo o del suo presidente. Mentre l'articolo 1, paragrafo 3, lettera d), della proposta stabilisce che le norme del GDPR e della LED non sono pregiudicate dalla proposta, il conferimento al Centro dell'UE del potere di chiedere pareri all'EDPB va oltre i compiti attribuiti a quest'ultimo a norma dei suddetti atti. Pertanto nel regolamento proposto dovrebbe essere chiarito, almeno in un considerando, che la proposta amplia i compiti dell'EDPB. A tale riguardo l'EDPB e il GEPD apprezzano l'importante ruolo che la proposta attribuisce all'EDPB prevedendone il coinvolgimento nell'attuazione pratica del regolamento proposto. In pratica il segretariato dell'EDPB svolge un ruolo essenziale nel fornire il sostegno analitico, amministrativo e logistico necessario all'adozione dei rispettivi pareri. Per garantire che l'EDPB e i suoi membri possano svolgere i propri compiti è dunque essenziale assegnare risorse finanziarie e di personale sufficienti. Purtroppo però la scheda finanziaria legislativa della proposta non indica che saranno messe a disposizione risorse aggiuntive per l'assolvimento dei compiti supplementari che la proposta assegna all'EDPB ([88]).

108. L'EDPB e il GEPD osservano inoltre che l'articolo 50 della proposta non indica in che modo il Centro dell'UE procederà dopo aver ricevuto un parere da parte dell'EDPB ([89]). Il considerando 27 della proposta si limita ad affermare che il parere dell'EDPB dovrebbe essere preso in considerazione dal Centro dell'UE e dalla Commissione europea. È pertanto opportuno chiarire lo scopo del parere richiesto nel processo di cui all'articolo 50 della proposta nonché le azioni che il Centro dell'UE è chiamato a svolgere dopo aver ricevuto un parere dall'EDPB.

109. L'EDPB e il GEPD ritengono inoltre che, mentre qualsiasi linea guida o eventuale parere dell'EDPB sull'uso delle tecnologie di rilevazione valuterà l'uso di tali tecnologie a livello generale, ai fini di una consultazione preventiva a norma dell'articolo 36 del GDPR l'autorità nazionale di controllo dovrà

([87]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).
([88]) COM(2022) 209 final, pag. 109 e seguenti.
([89]) Cfr. per contro l'articolo 51, paragrafo 4, della LED.

tenere conto delle circostanze specifiche ed effettuare una valutazione caso per caso del trattamento previsto da parte del rispettivo titolare. Essi osservano che le autorità di controllo dovrebbero applicare e applicheranno i criteri di cui all'articolo 36 del regolamento generale sulla protezione dei dati al fine di decidere se sia necessario prorogare il termine stabilito nel suddetto regolamento per fornire i loro pareri in risposta a una consultazione preliminare, e che non vi è necessità di applicare norme diverse quando una consultazione preventiva riguarda l'uso di una tecnologia di rilevazione ([90]).

110. Infine, per quanto riguarda l'applicazione dell'articolo 11 («Orientamenti per gli obblighi di rilevazione»), la proposta prevede che la Commissione possa emanare orientamenti sull'applicazione degli articoli da 7 a 10 del regolamento proposto. L'articolo 11 della proposta dovrebbe essere modificato per chiarire che, oltre alle autorità coordinatrici e al Centro dell'UE, la Commissione dovrebbe consultare anche l'EDPB sul progetto di orientamenti a prescindere dal previsto processo di consultazione pubblica prima di emanare orientamenti per gli obblighi di rilevazione.

111. Pertanto questo compito dell'EDPB, così come il suo ruolo all'interno del quadro giuridico che sarebbe introdotto dalla proposta, merita un'ulteriore valutazione da parte del legislatore.

4.11.3 Ruolo del Centro dell'UE in materia di abuso sessuale su minori

112. Il capo IV della proposta istituirebbe il Centro dell'UE quale nuova agenzia decentrata per l'attuazione della proposta stessa. Tra gli altri compiti, il Centro dell'UE dovrebbe agevolare l'accesso dei prestatori a tecnologie di rilevazione affidabili; mettere a disposizione indicatori creati sulla base di casi di abuso sessuale su minori online verificati da organi giurisdizionali o autorità amministrative indipendenti degli Stati membri a fini di rilevazione; fornire assistenza specifica, su richiesta, in relazione allo svolgimento delle valutazioni del rischio; fornire sostegno nella comunicazione con le autorità nazionali pertinenti ([91]).

113. A tale riguardo l'EDPB e il GEPD accolgono con favore l'articolo 77, paragrafo 1, della proposta che conferma che il trattamento dei dati personali da parte del Centro dell'UE è soggetto alle disposizioni dell'EUDPR e prevede che le modalità di applicazione del richiamato regolamento da parte del Centro dell'UE, anche in relazione alla nomina del responsabile della protezione dei dati dello stesso Centro dell'UE, siano stabilite previa consultazione del GEPD. Tuttavia essi ritengono che diverse disposizioni di questo capo meritino un esame più attento.

114. In primo luogo, l'EDPB e il GEPD osservano che l'articolo 48 della proposta prescrive che «se non giudica la segnalazione manifestamente infondata» ([92]) il Centro dell'UE la inoltra alle autorità di contrasto nazionali e all'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto («Europol»). Tale soglia che consente al Centro dell'UE di inoltrare le segnalazioni alle autorità di contrasto nazionali e a Europol («se non giudica la segnalazione manifestamente infondata») appare troppo bassa, soprattutto se si considera che lo scopo dell'istituzione del Centro dell'UE, come indicato nella relazione sulla valutazione d'impatto della Commissione ([93]), è alleviare l'onere che grava sulle autorità di contrasto e su Europol di filtrare i contenuti erroneamente segnalati come materiale pedopornografico. A tale riguardo non è chiaro per quale motivo il Centro dell'UE, in quanto polo di

([90]) Cfr. il considerando 24 della proposta.
([91]) COM(2022) 209 final, pag. 8.
([92]) L'espressione «manifestamente infondata» è descritta nel considerando 65 della proposta come riferita a una segnalazione «per cui sia immediatamente evidente, senza alcuna analisi giuridica di diritto o di merito, che le attività segnalate non configurano abuso sessuale su minori online».
([93]) Cfr. ad esempio pag. 349 della relazione sulla valutazione d'impatto.

competenze, non possa effettuare una valutazione giuridica e fattuale più approfondita per limitare i rischi che i dati di persone innocenti siano trasmessi alle autorità di contrasto.

115. In secondo luogo, la disposizione relativa al periodo di conservazione dei dati personali da parte del Centro dell'UE appare relativamente elastica se si considera la sensibilità dei dati in questione. Anche se non fosse possibile fissare un periodo massimo per la conservazione di tali dati, l'EDPB e il GEPD raccomandano di fissare nella proposta almeno un termine massimo per riesaminare la necessità di continuare a conservare i dati e per richiedere una giustificazione della conservazione prolungata dopo tale periodo.

116. Inoltre, data l'estrema sensibilità dei dati personali che devono essere trattati dal Centro dell'UE, l'EDPB e il GEPD sono del parere che il trattamento debba essere soggetto a garanzie supplementari, in particolare per garantire una vigilanza efficace. Ciò potrebbe includere l'obbligo per il Centro dell'UE di registrare le operazioni di trattamento in sistemi di trattamento automatizzato dei dati (in linea con le prescrizioni relative ai dati personali operativi di cui al capo IX dell'EUDPR), compresa la registrazione della raccolta, della modifica, dell'accesso, della consultazione, della comunicazione, dell'interconnessione e della cancellazione di dati personali. Le registrazioni delle consultazioni e delle comunicazioni consentono di stabilire la motivazione, la data e l'ora di tali operazioni, di identificare la persona che ha consultato o comunicato i dati personali operativi, nonché, nella misura del possibile, di stabilire l'identità dei destinatari. Tali registrazioni sarebbero usate ai fini della verifica della liceità del trattamento, dell'autocontrollo e per garantire l'integrità e la sicurezza e, su richiesta, sarebbero messe a disposizione del responsabile della protezione dei dati del Centro dell'UE e del GEPD.

117. Inoltre, la proposta fa riferimento all'obbligo per i prestatori di informare gli utenti in merito alla rilevazione di materiale pedopornografico tramite ordini di rilevazione, nonché al diritto di proporre reclamo presso un'autorità coordinatrice ([94]). Tuttavia non stabilisce procedure per l'esercizio dei diritti degli interessati, anche tenendo conto dei molteplici luoghi dove i dati personali possono essere trasmessi e conservati nell'ambito della proposta (Centro dell'UE, Europol, autorità di contrasto nazionali). La prescrizione relativa all'informazione degli utenti dovrebbe prevedere l'obbligo di informare le persone del fatto che i loro dati sono stati inoltrati a e sono trattati da soggetti diversi, se del caso (ad esempio da parte delle autorità di contrasto nazionali e di Europol). Inoltre dovrebbe essere prevista una procedura centralizzata per ricevere e coordinare le richieste di esercizio del diritto di accesso, di rettifica e alla cancellazione o, in alternativa, l'obbligo per il soggetto che riceve una richiesta dell'interessato di coordinarsi con gli altri soggetti interessati.

118. L'EDPB e il GEPD osservano che, a norma dell'articolo 50 della proposta, il Centro dell'UE ha il compito di specificare l'elenco delle tecnologie che possono essere utilizzate per eseguire ordini di rilevazione. Tuttavia, a norma dell'articolo 12, paragrafo 1, della proposta, i prestatori sono tenuti a segnalare tutte le informazioni che rivelino casi di potenziale abuso sessuale su minori online nei loro servizi, e non solo quelle derivanti dall'esecuzione di un ordine di rilevazione. È altamente probabile che una quantità significativa di tali segnalazioni provenga dall'applicazione delle misure di attenuazione adottate dai prestatori, conformemente all'articolo 4 della proposta. Appare pertanto fondamentale determinare quali potrebbero essere queste misure, la loro efficacia, il loro tasso di errore nella segnalazione di potenziali abusi sessuali su minori e il loro impatto sui diritti e sulle libertà delle persone. Sebbene l'articolo 4, paragrafo 5, della proposta preveda che la Commissione, in

([94]) Cfr. l'articolo 10, paragrafo 6, e, in seguito alla trasmissione di una segnalazione al Centro dell'UE, l'articolo 12, paragrafo 2, della proposta.

cooperazione con le autorità coordinatrici e il Centro dell'UE, dopo aver condotto una consultazione pubblica, possa emanare orientamenti pertinenti, l'EDPB e il GEPD ritengono importante che il legislatore includa all'articolo 50 il compito del Centro dell'UE di fornire anche un elenco di misure di attenuazione raccomandate e di migliori pratiche che siano in particolare efficaci nell'individuare potenziali abusi sessuali su minori online. Poiché tali misure possono interferire con i diritti fondamentali alla protezione dei dati e al rispetto della vita privata, si raccomanda inoltre che il Centro dell'UE chieda il parere dell'EDPB prima di pubblicare tale elenco.

119. Infine, le prescrizioni in materia di sicurezza di cui all'articolo 51, paragrafo 4, della proposta dovrebbero essere più specifiche. A tale riguardo è possibile trarre ispirazione dalle prescrizioni in materia di sicurezza stabilite in altri regolamenti relativi ai sistemi su larga scala che comportano un trattamento ad alto rischio, quali il regolamento (CE) n. 767/2008 ([95]) (cfr. articolo 32), il regolamento (CE) n. 1987/2006 ([96]) (cfr. articolo 16), il regolamento (UE) 2018/1862 ([97]) (cfr. articolo 16) e il regolamento (UE) n. 603/2013 ([98]) (cfr. articolo 34).

4.11.4 Ruolo di Europol

120. La proposta prevede una stretta cooperazione tra il Centro dell'UE ed Europol. A norma del capo IV della proposta, una volta ricevute le segnalazioni da parte dei prestatori su presunti casi di materiale pedopornografico, il Centro dell'UE le controlla per valutare quelle sulla cui base sia possibile agire («se non giudica la segnalazione manifestamente infondata») e le inoltra a Europol e alle autorità di contrasto nazionali ([99]). Il Centro dell'UE concede a Europol l'accesso alle sue banche dati di indicatori e alla banca dati delle segnalazioni per assisterlo nelle indagini su presunti reati di abuso sessuale su minori ([100]). Inoltre il Centro dell'UE disporrebbe di un accesso «il più ampio possibile» ai sistemi di

([95]) Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS) (GU L 218 del 13.8.2008, pag. 60).
([96]) Regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 381 del 28.12.2006, pag. 4).
([97]) Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).
([98]) Regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013 che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (GU L 180 del 29.6.2013, pag. 1).
([99]) Cfr. l'articolo 48 della proposta.
([100]) Cfr. l'articolo 46, paragrafi 4 e 5, della proposta.

informazione di Europol ([101]). Le due agenzie condivideranno anche i locali e alcune infrastrutture (non operative) ([102]).

121. L'EDPB e il GEPD osservano che diversi aspetti relativi alla cooperazione tra il Centro dell'UE proposto ed Europol destano preoccupazione o richiedono ulteriori precisazioni.

A proposito dell'inoltro delle segnalazioni da parte del Centro dell'UE a Europol (articolo 48)

122. L'articolo 48 del regolamento proposto prevede che il Centro dell'UE inoltri le segnalazioni che non sono giudicate manifestamente infondate, unitamente a qualunque complemento di informazione pertinente, a Europol e alla o alle autorità di contrasto dello Stato membro o degli Stati membri che possono essere giurisdizionalmente competenti a indagare o perseguire il caso di potenziale abuso sessuale su minori. Sebbene questo articolo attribuisca a Europol il ruolo di individuare l'autorità di contrasto competente ove non sia chiaro quale sia lo Stato membro interessato, la disposizione prevede in effetti che tutte le segnalazioni siano trasmesse a Europol indipendentemente dal fatto che l'autorità nazionale sia stata individuata e abbia già trasmesso la segnalazione ricevuta dal Centro dell'UE.

123. Tuttavia la proposta non chiarisce quale sarebbe il valore aggiunto del coinvolgimento di Europol né quale ruolo si prevede svolgerebbe Europol al ricevimento delle segnalazioni, in particolare nei casi in cui l'autorità di contrasto nazionale sia stata individuata e notificata in parallelo ([103]).

124. L'EDPB e il GEPD ricordano che il mandato di Europol si limita al sostegno dell'azione delle autorità competenti degli Stati membri e della loro reciproca cooperazione nella prevenzione e nella lotta contro la criminalità grave che interessa due o più Stati membri ([104]). L'articolo 19 del regolamento (UE) 2016/794 ([105]), modificato dal regolamento (UE) 2022/991 ([106]) («regolamento Europol modificato») stabilisce che un organismo dell'Unione che fornisce informazioni a Europol è tenuto a determinare la o le finalità per le quali tali informazioni devono essere trattate da Europol, nonché le condizioni per il trattamento. È inoltre responsabile di garantire l'esattezza dei dati personali trasferiti ([107]).

125. Un inoltro generalizzato di segnalazioni a Europol sarebbe pertanto in contrasto con il regolamento Europol modificato e comporterebbe una serie di rischi per la protezione dei dati. La duplicazione del trattamento dei dati personali potrebbe comportare la conservazione parallela di più copie degli stessi

([101]) Cfr. l'articolo 53, paragrafo 2, della proposta.
([102]) In particolare quelli riguardanti la gestione delle risorse umane, le tecnologie dell'informazione (IT) (compresa la sicurezza informatica), l'edificio e le comunicazioni.
([103]) Il considerando 71 della proposta fa solo un riferimento generale all'esperienza di Europol nell'individuare le autorità nazionali competenti in situazioni poco chiare e alla sua banca dati di intelligence criminale che può contribuire a individuare collegamenti con indagini in corso in altri Stati membri.
([104]) Cfr. l'articolo 3 del regolamento Europol modificato.
([105]) Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 24.5.2016, pag. 53).
([106]) Regolamento (UE) 2022/991 del Parlamento europeo e del Consiglio, dell'8 giugno 2022, che modifica il regolamento (UE) 2016/794 per quanto riguarda la cooperazione di Europol con le parti private, il trattamento dei dati personali da parte di Europol a sostegno di indagini penali, e il ruolo di Europol in materia di ricerca e innovazione (GU L 169 del 27.6.2022, pag. 1).
([107]) Cfr. l'articolo 38, paragrafo 2, lettera a), del regolamento Europol modificato.

dati personali altamente sensibili (ad esempio presso il Centro dell'UE, Europol, l'autorità di contrasto nazionale), con rischi per l'accuratezza dei dati a causa della potenziale desincronizzazione delle banche dati, nonché per l'esercizio dei diritti degli interessati. Inoltre la soglia bassa stabilita nella proposta per la condivisione delle segnalazioni con le autorità di contrasto («se non giudica la segnalazione manifestamente infondata») implica un'elevata probabilità che nei sistemi di informazione di Europol siano conservati falsi positivi (ossia contenuti erroneamente segnalati come abusi sessuali su minori), potenzialmente per periodi prolungati ([108]).

126. L'EDPB e il GEPD raccomandano pertanto che la proposta specifichi e limiti le circostanze e le finalità per le quali il Centro dell'UE potrebbe inoltrare segnalazioni a Europol, conformemente al regolamento Europol modificato. Dovrebbero essere esplicitamente escluse le circostanze in cui le segnalazioni sono state trasmesse all'autorità di contrasto dello Stato membro interessato e che non implicano una dimensione transfrontaliera. Inoltre la proposta dovrebbe includere l'obbligo per il Centro dell'UE di trasferire a Europol solo dati personali adeguati, pertinenti e limitati allo stretto necessario. Devono anche essere previste garanzie specifiche per garantire la qualità e l'affidabilità dei dati.

Articolo 53, paragrafo 2, sulla cooperazione tra il Centro dell'UE ed Europol

127. L'articolo 53, paragrafo 2, della proposta prevede che Europol e il Centro dell'UE si consentano reciprocamente «il più ampio accesso alle informazioni e ai sistemi di informazione pertinenti, se necessario per l'assolvimento dei rispettivi compiti e conformemente agli atti di diritto dell'Unione che disciplinano detto accesso».

128. L'articolo 46, paragrafi 4 e 5, della proposta specifica inoltre che Europol ha accesso alle banche dati degli indicatori e alla banca dati delle segnalazioni del Centro dell'UE, mentre l'articolo 46, paragrafo 6, stabilisce la procedura per consentire tale accesso: Europol presenta una richiesta, specificando lo scopo perseguito e il grado di accesso necessario per conseguirlo, che è debitamente valutata dal Centro dell'UE.

129. I criteri e le garanzie cui sono subordinati l'accesso di Europol e il successivo utilizzo dei dati ottenuti dai sistemi di informazione del Centro dell'UE non sono specificati. Inoltre non è spiegato per quale motivo sia necessario concedere a Europol un accesso diretto ai sistemi di informazione di un'agenzia estranea al settore del contrasto, contenenti dati personali altamente sensibili, per i quali potrebbe non essere stato accertato alcun collegamento con le attività criminali e con la prevenzione della criminalità. Al fine di garantire un livello elevato di protezione dei dati e il rispetto del principio della limitazione della finalità, l'EDPB e il GEPD raccomandano che la trasmissione di dati personali dal Centro dell'UE a Europol avvenga solo caso per caso, a seguito di una richiesta debitamente valutata e tramite uno strumento di comunicazione per lo scambio sicuro, come SIENA ([109]).

([108]) Secondo la relazione della Commissione sulla valutazione d'impatto, Europol è stato in grado di esaminare solo il 20 % dei 50 milioni di immagini e video unici di materiale pedopornografico contenuti nella sua banca dati, il che implica una mancanza di risorse per agire sulla base dei contributi attualmente ricevuti in relazione al materiale pedopornografico. Cfr. la relazione sulla valutazione d'impatto che accompagna la proposta di regolamento che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori [SWD(2022) 209, pag. 47 e 48].

([109]) Secure Information Exchange Network Application (SIENA, applicazione di rete per lo scambio sicuro di informazioni).

130. L'articolo 53, paragrafo 2, contiene l'unico riferimento della proposta all'accesso del Centro dell'UE ai sistemi di informazione di Europol. Non è quindi chiaro per quali scopi, e in base a quali garanzie specifiche, tale accesso avrebbe luogo.

131. L'EDPB e il GEPD ricordano che Europol è un'agenzia di contrasto istituita a norma dei trattati dell'UE con il mandato fondamentale della prevenzione e della lotta contro la criminalità grave. I dati personali operativi trattati da Europol sono pertanto soggetti a norme e garanzie rigorose in materia di trattamento dei dati. Il Centro dell'UE proposto non è un organismo di contrasto e in nessun caso dovrebbe avere accesso diretto ai sistemi di informazione di Europol.

132. L'EDPB e il GEPD osservano, inoltre, che gran parte delle informazioni relative a un interesse condiviso dal Centro dell'UE e da Europol riguarderà i dati personali delle vittime di presunti reati, i dati personali di minori e i dati personali relativi alla vita sessuale, che si qualificano come categorie particolari di dati personali ai sensi del regolamento Europol modificato. Il regolamento Europol modificato impone condizioni rigorose per quanto riguarda l'accesso alle categorie particolari di dati personali. L'articolo 30, paragrafo 3, del regolamento Europol modificato stabilisce che solo Europol ha accesso diretto a tali dati personali, in particolare solo un numero limitato di funzionari Europol debitamente autorizzati dal direttore esecutivo ([110]).

133. L'EDPB e il GEPD raccomandano pertanto di chiarire la formulazione dell'articolo 53, paragrafo 2, della proposta al fine di rispecchiare adeguatamente le limitazioni in vigore a norma del regolamento Europol modificato e di specificare le modalità di accesso da parte del Centro dell'UE. In particolare l'accesso ai dati personali trattati nei sistemi di informazione di Europol, ove ritenuto strettamente necessario per l'assolvimento dei compiti del Centro dell'UE, dovrebbe essere concesso solo caso per caso, dietro presentazione di una richiesta esplicita che documenti lo scopo specifico e la motivazione. Europol dovrebbe essere tenuto a valutare attentamente tali richieste e a trasmettere i dati personali al Centro dell'UE solo se strettamente necessario e proporzionato allo scopo perseguito.

Articolo 10, paragrafo 6, sul ruolo di Europol nell'informare gli utenti in seguito all'attuazione di un ordine di rilevazione

134. L'EDPB e il GEPD accolgono con favore l'obbligo di cui all'articolo 10, paragrafo 6, della proposta che impone ai prestatori di informare gli utenti i cui dati personali possono essere interessati dall'esecuzione di un ordine di rilevazione. Tali informazioni devono essere fornite agli utenti solo dopo aver ottenuto conferma, da Europol o dall'autorità nazionale di contrasto dello Stato membro che ha ricevuto la segnalazione a norma dell'articolo 48 della proposta, che la fornitura di informazioni agli utenti non è tale da compromettere le attività di prevenzione, accertamento, indagine e perseguimento dei reati di abuso sessuale sui minori.

135. Vi è tuttavia una mancanza di specificità per quanto riguarda l'attuazione pratica di tale disposizione. Quando le segnalazioni sono inoltrate sia a Europol che a un'autorità di contrasto di uno Stato membro, la proposta non stabilisce se sia necessaria una conferma da parte di uno o di entrambi i destinatari, né specifica le procedure/modalità per ottenere tale conferma (ad esempio se le conferme devono essere trasmesse attraverso il Centro dell'UE). Tenuto conto dell'elevato volume di materiale pedopornografico che Europol e le autorità di contrasto nazionali potrebbero essere tenute a trattare

([110]) A norma del regolamento Europol modificato sono previste eccezioni a tale divieto per le agenzie dell'Unione istituite sulla base del titolo V del TFUE. Tuttavia, data la base giuridica della proposta (articolo 114 del TFUE, relativo all'armonizzazione del mercato interno), tale eccezione non includerebbe il Centro dell'UE proposto.

e della mancanza di un termine preciso per fornire la conferma («senza indebito ritardo»), l'EDPB e il GEPD raccomandano di chiarire le procedure applicabili al fine di garantire la realizzazione pratica di tale salvaguardia. Inoltre l'obbligo di informare gli utenti dovrebbe includere anche le informazioni relative ai destinatari dei dati personali in questione.

Raccolta dei dati e obblighi di trasparenza (articolo 83)

136. L'articolo 83, paragrafo 3, della proposta prevede che il Centro dell'UE raccolga dati e generi statistiche in relazione a una serie di compiti di cui al regolamento proposto. A fini di monitoraggio, l'EDPB e il GEPD raccomandano di aggiungere a tale elenco le statistiche sul numero di segnalazioni inoltrate a Europol a norma dell'articolo 48, nonché sul numero di richieste di accesso ricevute da Europol a norma dell'articolo 46, paragrafi 4 e 5, compreso il numero di richieste accolte e respinte dal Centro dell'UE.

5. CONCLUSIONI

137. L'EDPB e il GEPD, pur accogliendo con favore gli sforzi della Commissione volti a garantire un'azione efficace contro gli abusi sessuali su minori online, ritengono che la proposta susciti serie preoccupazioni in materia di protezione dei dati e rispetto della vita privata. Invitano pertanto i colegislatori a modificare il regolamento proposto, in particolare per garantire che gli obblighi di rilevazione previsti soddisfino le norme applicabili in materia di necessità e proporzionalità e non comportino un indebolimento o una compromissione della cifratura a livello generale. L'EDPB e il GEPD restano disponibili a offrire sostegno durante il processo legislativo, qualora il loro contributo fosse ritenuto necessario per affrontare le problematiche poste in evidenza nel presente parere congiunto.

Per il Garante europeo della protezione dei dati Il Garante europeo della protezione dei dati (Wojciech Wiewiorowski)	Per il comitato europeo per la protezione dei dati La presidente (Andrea Jelinek)