Allegato B alla delibera n. 16/22/CONS

Sommario

I. Premessa

Il decreto-legge 30 aprile 2020, n. 28, coordinato con la legge di conversione 25 giugno 2020, n. 70, ha introdotto *«Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19»*.

In particolare, l'art. 7-*bis*, recante *Sistemi di protezione dei minori dai rischi del cyberspazio*, prevede che:

1. I contratti di fornitura nei servizi di comunicazione elettronica disciplinati dal codice di cui al decreto legislativo 1° agosto 2003, n. 259, devono prevedere tra i servizi preattivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto.

2. I servizi preattivati di cui al comma 1 sono gratuiti e disattivabili solo su richiesta del consumatore, titolare del contratto.

3. Gli operatori di telefonia, di reti televisive e di comunicazioni elettroniche assicurano adeguate forme di pubblicità dei servizi preattivati di cui al comma 1 in modo da assicurare che i consumatori possano compiere scelte informate.

4. In caso di violazione degli obblighi di cui al presente articolo, l'Autorità per le garanzie nelle comunicazioni ordina all'operatore la cessazione della condotta e la restituzione delle eventuali somme ingiustificatamente addebitate agli utenti, indicando in ogni caso un termine non inferiore a sessanta giorni entro cui adempiere.

Alla luce del quadro normativo sopra riportato, e nella prospettiva di rendere il medesimo effettivo, l'Autorità, nell'ambito dei propri compiti istituzionali concernenti

la vigilanza e la garanzia del corretto funzionamento del mercato delle comunicazioni elettroniche, ha richiesto ai principali operatori ed associazioni di categoria[1] di fornire alcune informazioni di dettaglio in relazione alle misure adottate al fine di proteggere i minori dai rischi connessi al *cyberspazio*, con particolare riferimento ai seguenti aspetti*:*

1. classificazione dei contenuti da filtrare e/o bloccare, con specifico riferimento alle modalità di classificazione e alla identificazione delle categorie di contenuti[2]*;*

2. modalità di realizzazione tecnica del filtro o del blocco. A tale riguardo si chiede di chiarire, tra le altre cose, se il servizio è fornito:

- *mediante eventuale installazione da parte dell'utente finale di una applicazione messa a disposizione dell'operatore su PC o smartphone, che controlla la navigazione e filtra i contenuti, gestisce le categorie da bloccare, o altre opzioni; utilizzo di browser specializzato;*
- *mediante filtraggio del contenuto sulla rete a livello di trasporto o applicativo, specifico programma di filtraggio installato su proxy o gateway (es. "lista nera" di URL, DNS, parole chiave, ecc.), impostazione di un servizio DNS per il filtraggio degli indirizzi;*
- *altre modalità, quali, a titolo esemplificativo, la individuazione di aree di accesso con pin o la predisposizione di servizi di controllo parentale;*

3. modalità di utilizzo e disabilitazione o blocco da parte dell'utente;

4. eventuali costi per il servizio in parola, incluso le informazioni o la disabilitazione del servizio o blocco, a carico dell'utente;

5. tempistica di implementazione delle misure adottate e in via di attuazione in ottemperanza alla disposizione sopra richiamata.

Dall'esame dei riscontri trasmessi è emerso che parte degli operatori ha realizzato i sistemi di *parental control* sulla base di proprie soluzioni tecniche e criteri. In alcuni casi, sono previsti costi per i clienti; in altri, il *parental control* è in corso di implementazione. In altri casi ancora, gli operatori attendono indicazioni normative o regolamentari da parte dell'Autorità.

[1] AIIP, ASSTEL, EOLO S.p.A., Fastweb S.p.A., Iliad Italia S.p.A., IRIDEOS S.p.A., Linkem S.p.A., SKY Italia S.r.l., TIM S.p.A., Tiscali Italia S.p.A. Vodafone Italia S.p.A., Wind Tre S.p.A.

[2] Specificazione della distinzione tra i contenuti inappropriati (che sono quelli da filtrare) e contenuti riservati ai maggiori di diciotto anni (da bloccare).

Alla luce delle risultanze della preliminare attività istruttoria svolta, lo stato di implementazione dei sistemi di *parental control* è apparso dunque solo parziale e non pienamente conforme alla normativa stessa sia in relazione ai costi per i clienti sia in merito alle concrete modalità applicative (ad esempio *opt-in vs opt-out*).

Pertanto, dovendo l'Autorità effettuare una specifica attività di controllo finalizzata a ordinare la cessazione di condotte non conformi alla legge e, se del caso, sanzionatoria, si è ritenuto opportuno adottare specifiche Linee guida volte a orientare gli operatori in ordine alle modalità di realizzazione dei sistemi di protezione dei minori, alle modalità di configurazione degli stessi, alla fornitura di informazioni chiare e trasparenti sulle modalità di utilizzo da parte dei titolari dei contratti di servizi di comunicazione elettronica.

Tale approccio è apparso quello maggiormente efficace viste la diversità delle posizioni emerse e la varietà di soluzioni messe in campo, che creano inevitabilmente differenti livelli di protezione per i minori.

Pertanto, con la delibera n. 160/21/CONS del 24 giugno 2021, l'Autorità ha avviato il procedimento istruttorio finalizzato all'approvazione di Linee guida per l'attuazione dell'art. 7-*bis* del decreto-legge 30 aprile 2020, n. 28 e ha previsto all'art.1, comma 4, il successivo avvio di una consultazione pubblica, della durata di 45 giorni, tramite pubblicazione di una delibera dell'Autorità con allegato documento di consultazione in relazione alle suddette Linee guida.

Con il provvedimento qui proposto si provvede, per l'effetto, all'avvio del procedimento di consultazione pubblica sullo schema di Linee guida di seguito riportato.

In via preliminare, tuttavia, appare utile chiarire le modalità di classificazione dei contenuti da filtrare e/o bloccare e di identificazione delle relative categorie mediante richiamo al quadro normativo riveniente dal recepimento della direttiva (UE) 2018/1972, che istituisce il Codice europeo delle comunicazioni elettroniche, nonché della direttiva (UE) 2018/1808, recante la modifica della direttiva 2010/13/UE, (direttiva sui servizi di media audiovisivi), avvenuto, rispettivamente, con l'adozione dei decreti legislativi nn. 207 e 208 dell'8 novembre 2021.

Al riguardo, il considerato n. 7 della direttiva (UE) 2018/1972 (nel seguito anche *nuovo codice delle comunicazioni europeo*) sottolinea che, sebbene sia necessario separare la regolamentazione delle reti e dei servizi di comunicazione elettronica dalla regolamentazione dei contenuti, sussiste convergenza tra i due comparti (comunicazioni elettroniche/contenuti), in particolare al fine di garantire il pluralismo dei mezzi di

informazione, la diversità culturale e la protezione dei consumatori. Ne deriva che, entro i limiti delle loro competenze, le autorità competenti dovrebbero contribuire a garantire l'attuazione delle politiche volte a promuovere tali obiettivi.

Allo stesso modo, l'articolo 103, comma 4 (recepito a livello nazionale dall'articolo 98-quindecies del decreto legislativo n. 207 dell'8 novembre 2021), recante "*Trasparenza, confronto delle offerte e pubblicazione delle informazioni*" recita che "**gli Stati membri possono esigere che i fornitori di servizi di accesso a internet o di servizi di comunicazione** interpersonale basati sul numero accessibili al pubblico, o entrambi, **diffondano gratuitamente**, all'occorrenza, informazioni di pubblico interesse agli utenti finali nuovi ed esistenti tramite i canali che utilizzano normalmente per le comunicazioni con gli utenti finali. In tal caso, **dette informazioni** di pubblico interesse sono fornite dalle competenti autorità pubbliche in forma standardizzata e **riguardano fra l'altro**: … i **mezzi di protezione contro i rischi per la sicurezza personale**, per la vita privata e per i dati personali nella fruizione dei servizi di accesso a internet e dei servizi di comunicazione interpersonale basati sul numero accessibili al pubblico" (enfasi aggiunta).

In sintesi, il sopracitato considerato consente un intervento regolamentare a tutela dei consumatori (nel caso specifico, minori), mentre l'articolo 103, comma 4, su tale scia, lascia spazio ad un intervento dell'Autorità per richiedere ai fornitori di servizi di accesso ad *Internet* (di seguito, anche ISP) di diffondere informazioni a tutela della sicurezza dei consumatori.

Tale conclusione trova fondamento, anche in riferimento ai minori, nel considerato (269) della direttiva recante il nuovo codice, laddove recita testualmente che "*allo scopo di affrontare gli aspetti di interesse pubblico per quanto riguarda l'utilizzazione di servizi di accesso a internet e di servizi di comunicazione interpersonale basati sul numero accessibili al pubblico e allo scopo di incoraggiare la protezione dei diritti e le libertà dei terzi, **gli Stati membri dovrebbero essere in grado di elaborare e diffondere o far diffondere, con l'aiuto dei fornitori di tali servizi, informazioni di interesse pubblico relative all'utilizzazione degli stessi. Tali informazioni dovrebbero poter includere informazioni di interesse pubblico concernenti** le violazioni più comuni e le relative conseguenze giuridiche, ad esempio le violazioni del diritto d'autore, altri usi illegali e la diffusione di contenuti dannosi e consigli e mezzi di protezione contro i rischi alla sicurezza personale, ad esempio quelli che sorgono in seguito alla divulgazione di informazioni personali in alcuni casi, e i rischi alla vita privata e ai dati personali, nonché **la disponibilità di software configurabili di facile uso o di opzioni di software che consentano la tutela dei***

bambini o delle persone vulnerabili. *....* ***Gli Stati membri dovrebbero essere in grado di obbligare i fornitori di servizi di accesso a internet e di servizi di comunicazione interpersonale basati sul numero accessibili al pubblico a diffondere tali informazioni standardizzate a tutti i loro clienti in modo considerato idoneo dalle autorità pubbliche nazionali****. La diffusione di tali informazioni non dovrebbe tuttavia comportare un onere eccessivo per i fornitori. Ove ciò accada gli Stati membri dovrebbero esigere che tale diffusione abbia luogo con i mezzi utilizzati dai fornitori per comunicare con gli utenti finali nel quadro della loro ordinaria attività.*"(enfasi aggiunta).

Quanto sopra esplicita con maggior dettaglio il fatto che lo Stato membro può richiedere agli ISP di divulgare informazioni ai propri clienti su sistemi di *parental control* (*software* configurabili di facile uso a tutela dei minori).

Il considerato 270 specifica che "*In mancanza di norme applicabili di diritto dell'Unione, i contenuti, le applicazioni e i servizi sono considerati legali o dannosi ai sensi del diritto nazionale sostanziale e procedurale.* ***Spetta agli Stati membri, e non ai fornitori di reti o servizi di comunicazione elettronica, decidere, seguendo le normali procedure, se i contenuti, le applicazioni e i servizi siano legali o dannosi****. La presente direttiva e la direttiva 2002/58/CE lasciano impregiudicata la direttiva 2000/31/CE la quale, tra l'altro, contiene una norma detta «semplice trasporto» («mere conduit») per i fornitori intermedi di servizi, quali descritti nella stessa."*

Ne deriva che l'individuazione dei contenuti dannosi non spetta agli ISP bensì agli Stati membri.

Al riguardo, l'art. 37 del D.Lgs. n. 208/2021 (di seguito anche TUSMA), recante l'attuazione della direttiva (UE) 2018/1808, relativo alle "*Disposizioni a tutela dei minori nella programmazione audiovisiva"*, stabilisce, ai commi 1 e 2, le trasmissioni vietate sul territorio nazionale e i compiti dell'Autorità.

Ai sensi del comma 12 dello stesso articolo "*l'Autorità* ***stabilisce con propri regolamenti i criteri per l'individuazione dei programmi e servizi di cui ai commi 1 e 2****. I fornitori di servizi di media audiovisivi e radiofonici e le emittenti radiofoniche si conformano ai menzionati criteri e alla disciplina di dettaglio entro trenta giorni dalla data di entrata in vigore dei regolamenti emessi dall'Autorità, garantendo il rispetto delle condizioni direttamente poste dal presente articolo, e assicurando che i contenuti classificati ai sensi del comma 1 siano ricevibili e fruibili unicamente nel rispetto delle condizioni fissate ai sensi del comma 5*."

In base al comma 5 "*l'Autorità, d'intesa con il Ministero, sentiti l'Autorità garante per l'infanzia e l'adolescenza e il Comitato di applicazione del Codice di autoregolamentazione media e minori, al fine di garantire un adeguato livello di tutela della dignità umana e dello sviluppo fisico, mentale e morale dei minori, adotta,* ***con procedure di co-regolamentazione****, la disciplina di dettaglio contenente l'indicazione degli accorgimenti tecnici idonei a escludere che i minori vedano o ascoltino normalmente i programmi di cui al comma 3,* ***fra cui l'uso di numeri di identificazione personale e sistemi di filtraggio, di verifica dell'età o di identificazione, nel rispetto dei seguenti criteri generali:***

a) ***il contenuto classificabile «a visione non libera»*** *sulla base dei criteri fissati dall'Autorità è offerto con una* ***funzione di controllo parentale*** *che inibisce l'accesso al contenuto stesso****, salva la possibilità per l'utente di disattivare la predetta funzione tramite la digitazione di uno specifico codice segreto che ne renda possibile la visione.*** *L'effettiva imposizione della predetta funzione di controllo specifica e selettiva è condizione per l'applicazione del comma 3*[3]*;*

b) il codice segreto deve essere comunicato con modalità riservate, corredato dalle avvertenze in merito alla responsabilità nell'utilizzo e nella custodia del medesimo, al contraente maggiorenne che stipula il contratto relativo alla fornitura del contenuto o del servizio"(enfasi aggiunta).

Si osserva, inoltre, come il nuovo TUSMA contenga un complesso di previsioni e condizioni affinché *l'Autorità* [possa] *disporre* ***la sospensione provvisoria*** *della ricezione o ritrasmissione dei servizi di media audiovisivi erogati da un fornitore sottoposto alla giurisdizione di un altro Stato membro* (articolo 7, comma 2, del TUSMA).

Inoltre, in deroga ai divieti stabiliti, le trasmissioni vietate possono essere trasmesse una volta adottata, mediante co-regolamentazione e d'intesa con altre istituzioni e soggetti (*Ministero, l'Autorità garante per l'infanzia e l'adolescenza e il Comitato di applicazione del Codice di autoregolamentazione media e minori)*, la disciplina di dettaglio contenente l'indicazione degli accorgimenti tecnici idonei a escludere che i minori vedano o ascoltino normalmente tali programmi.

[3] *3. Le trasmissioni di cui al comma 1 possono essere rese disponibili dai fornitori di servizi di media audiovisivi a richiesta, in deroga ai divieti di cui al comma 1, solo in maniera tale da escludere che i minori vedano o ascoltino normalmente tali servizi e comunque con imposizione di un sistema di controllo specifico e selettivo che vincoli alla introduzione del sistema di protezione di cui al comma 5, alla disciplina del comma 11 ed alla segnaletica di cui al comma 2.*

In particolare, l'Autorità – in ossequio alle richiamate previsioni del decreto di recepimento della nuova direttiva SMAV – ha (già) il compito di determinare una classificazione dei contenuti "a visione non libera" che possono essere offerti con una funzione di controllo parentale che inibisce l'accesso al contenuto stesso, salva la possibilità di disattivare tale funzione mediante codice segreto.

Pertanto, alla luce della già richiamata convergenza tra i due comparti regolamentari in rilievo (comunicazioni elettroniche/contenuti), al fine di garantire il pluralismo dei mezzi di informazione, la diversità culturale e la protezione dei consumatori, consegue che, ai fini dell'art. 7-*bis*, è necessario far riferimento alla classificazione di cui agli artt. 37 e ss. del citato D.Lgs. n. 208/2021, che attribuiscono all'Autorità la competenza a fissare, mediante procedure di co-regolamentazione, i criteri per classificare i contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori.

Concludendo sul profilo in esame, emerge che, sebbene non vi sia un obbligo di sorveglianza attiva da parte degli ISP (come confermato anche nel nuovo codice delle comunicazioni elettroniche), gli stessi non risultano estranei alla materia del contrasto ai contenuti ritenuti dalle Autorità competenti illeciti e sono, invece, tenuti a collaborare con le stesse laddove a conoscenza di fatti rilevanti in materia (in questo senso già gli artt. 14 e 17 del D.Lgs. 9 aprile 2003, n. 70).

Pertanto, la recente normativa comunitaria e nazionale conferma la circostanza che non possono essere direttamente gli ISP a identificare i contenuti lesivi che devono essere bloccati o filtrati dai sistemi di *parental control*.

Al riguardo, le norme richiamate attribuiscono al**l'Autorità la classificazione** dei contenuti "a visione non libera" che possono essere offerti **con una funzione di controllo parentale** che inibisce l'accesso al contenuto stesso, salva la possibilità di disattivare tale funzione mediante codice segreto.

Si individuano pertanto due tipologie di tematiche:

- la prima relativa ai sistemi di controllo parentale offerti dal titolare dei contenuti (che sono aggiuntivi a quelli della norma nazionale che si intende attuare);
- la seconda funzionale alla classificazione dei contenuti cosiddetti "a visione non libera".

Ciò detto, si intende rimettere ad altro e separato procedimento il tema della classificazione ed individuazione dei contenuti per i quali deve essere pre-attivato un blocco o filtro (contenuti cosiddetti "a visione non libera") e, quindi, **limitare il**

presente procedimento alla definizione delle "regole tecniche" che gli ISP dovranno seguire in materia di sistemi di *parental control*.

Tali sistemi, che risultano complementari o sovrapposti a quelli di *parental control* messi a disposizione dalla piattaforma, dovranno essere disponibili per i clienti e immediatamente e facilmente attivabili.

Premesso tutto quanto sopra, nel paragrafo successivo si riportano i contenuti delle Linee guida, che si sottopongono a consultazione, per l'implementazione di *Sistemi di protezione dei minori dai rischi del cyberspazio* in attuazione dell'art. 7-*bis* del decreto-legge 30 aprile 2020, n. 28, coordinato con la legge di conversione 25 giugno 2020, n. 70.

II. Schema di Linee guida

Definizioni

Operatori di fascia A: operatori con almeno 100.000 linee dati attive.

Operatori di fascia B: operatori con almeno 10.000 e fino a 100.000 linee dati attive.

Operatori di fascia C: tutti gli altri operatori.

Linee guida

1. ***I fornitori di servizi di accesso ad Internet (ISP), qualsiasi sia la tecnologia utilizzata per l'erogazione del servizio, mettono a disposizione degli utenti sistemi di parental control ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto.***

Per *parental control system* (SCP) o sistema di controllo genitoriale si intende, ai fini delle presenti Linee Guida, un sistema che permette di limitare o bloccare l'accesso a determinate attività da parte di un minore, ad esempio impedendo l'accesso, tramite qualunque applicazione, a contenuti inappropriati per la sua età, di impostare il tempo di utilizzo dei dispositivi in uso al minore e di monitorarne l'attività svolta.

Le modalità di classificazione, in categorie, dei contenuti in oggetto e la definizione di filtri per fasce d'età sono oggetto di separato procedimento.

Nei casi in cui non sia possibile, sia per ragioni tecniche sia per quantità di contenuti, effettuare un filtro a livello di singolo contenuto, il filtro si applica all'intero sito web o applicazione, seguendo generalmente il criterio più restrittivo sulla base dei contenuti presenti. Per i siti web e le applicazioni che prevedono un meccanismo di registrazione con verifica dell'età dell'utente e conseguente filtro dei contenuti accessibili, si applica la restrizione corrispondente all'età minima richiesta per l'accesso.

Q1. Si forniscano valutazioni su quanto sopra e si indichi se si individuano ulteriori funzionalità che dovrebbero far parte di un SCP?

2. I SCP sono preattivati sulle nuove linee e possono essere disattivati e configurati esclusivamente dal titolare del contratto, se maggiorenne. Sulle linee esistenti i SCP devono essere resi disponibili come attivabili da parte del titolare del contratto, se maggiorenne. Se il titolare del contratto è minorenne, i SCP devono essere attivati automaticamente anche sulle linee preesistenti ed i soggetti che possono eseguire le operazioni di disattivazione, riattivazione e configurazione sono coloro che esercitano la potestà genitoriale sul minore. In caso di disattivazione, i SCP sono sempre riattivabili su richiesta del titolare del contratto.

Onde evitare utilizzi impropri da parte di soggetti non autorizzati, si pone la necessità di identificare il titolare del contratto (o, se minore, chi ne esercita la potestà genitoriale) come unico soggetto che può effettuare le operazioni in argomento. Tra le possibili soluzioni, si possono individuare le seguenti modalità per garantire l'accesso in sicurezza alle funzionalità di attivazione o disattivazione messe a disposizione dall'operatore. In particolare, l'abilitazione alla disattivazione o attivazione avviene tramite:

- codice PIN fornito al titolare del contratto all'atto dell'attivazione dell'utenza, comunicato in forma riservata, ad esempio tramite SMS;
- SPID;
- autenticazione nell'area riservata del sito web dell'operatore;
- OTP inviato via SMS o e-mail.

Q2. Quali sono le casistiche in cui il titolare del contratto può essere un minore?

Q3. Si riscontrano ulteriori modalità di possibile autenticazione del titolare del contratto (o, se minore, di chi ne esercita la potestà genitoriale)?

Q4. Quale (o quale combinazione) tra le soluzioni individuate per l'autenticazione si reputa preferibile?

3. Gli ISP offrono gratuitamente i SCP agli utenti e non impongono costi correlati all'attivazione, alla disattivazione, alla configurazione o al funzionamento degli stessi.

La fornitura dei servizi SCP dev'essere gratuita e tutti i servizi correlati al funzionamento dei SCP devono essere forniti gratuitamente agli utenti. Nessun costo a nessun titolo può essere imposto per qualsiasi operazione ad essi correlata.

È consentito agli operatori di fornire sistemi aggiuntivi – anche integrati con i SCP – che svolgano ulteriori funzionalità non relative ai SCP (ad es. *antivirus, antimalware, antispam,* etc.). Questi eventuali sistemi devono comunque essere sempre opzionali, non preattivati senza il consenso del titolare della linea e attivabili o disattivabili selettivamente dall'utente. Per tutte le funzionalità riconducibili ai SCP eventualmente presenti in questi sistemi nessun costo può essere addebitato all'utente.

Q5. Si reputa che gli operatori possano integrare i SCP con ulteriori componenti, funzionali ad altri scopi, opzionali a pagamento? Se sì, quali?

4. Gli ISP pubblicano sui propri siti web guide chiare ed esaustive per l'utilizzo dei SCP ed offrono assistenza gratuita, anche attraverso call center con operatore umano, per l'attivazione, la disattivazione e la configurazione dei SCP.

Gli utenti devono reperire facilmente informazioni per svolgere le operazioni di configurazione dei SCP e la loro disattivazione e attivazione. Inoltre, devono poter avere assistenza gratuita tramite *call center* e gli altri canali già previsti per l'assistenza clienti.

Q6. Si reputa che debbano essere previsti ulteriori canali di assistenza?

Q7. L'assistenza fornita attraverso il *call center* relativa ai SCP dovrebbe avere un numero dedicato?

5. ***I SCP prevedono, come funzionalità minima, almeno il blocco, mediante DNS, dei siti ospitanti contenuti oggetto di filtro.***

Gli operatori devono fornire, come funzionalità minima, la possibilità di impedire l'accesso ai minori a siti web o ad applicazioni che contengono materiale inappropriato per la loro età.

In particolare, i *resolver* DNS (Domain Name System), forniti dall'ISP e automaticamente installati quando la connessione è attivata, ridirigono le richieste relative a domini associati alla presenza di contenuti oggetto di filtro su una pagina web, fornita dall'operatore, in cui viene spiegato all'utente minorenne che non può accedere a quel contenuto poiché considerato inappropriato per la sua età o riservato ad un pubblico maggiorenne.

Gli operatori di fascia A e fascia B dovranno prevedere nella suddetta pagina la possibilità di sbloccare per un tempo configurabile l'accesso al sito web in oggetto, previa autorizzazione del titolare del contratto (in caso di minore da parte di chi ne esercita la potestà).

Il blocco dovrà essere configurato sia per accesso tramite *browser* sia per il tramite di applicazioni installabili sui dispositivi dell'utente

Il blocco dovrà essere realizzato sia per gli indirizzi IPv4 che per quelli IPv6, ove disponibili.

Q8. Si riscontrano criticità tecniche relative all'implementazione dei blocchi DNS?

Q9. Si riscontrano criticità tecniche relative all'implementazione della possibilità di sblocco temporaneo all'accesso per i siti web? Per tale funzionalità, qual è il metodo di autenticazione che si ritiene più idoneo?

Q10. Si reputa proporzionata la distinzione degli operatori (ISP) in fasce così come proposta?

6. ***Gli operatori di fascia A complementano le funzionalità di cui al punto 5, mediante a) l'implementazione di filtri, basati sugli indirizzi IP, dei siti ospitanti contenuti non consentiti o di DNS non sicuri, b) l'implementazione del blocco di quelle funzionalità del terminale che consentono all'utente di utilizzare servizi DNS di altri soggetti, o servizi DNS di tipo DoT (DNS-over-***

TLS) e DoH (DNS-over-HTTPS), c) la fornitura di applicativi installabili dall'utente sui propri dispositivi per consentire il filtraggio dei singoli contenuti.

Onde evitare la possibilità che i filtri basati sul DNS dell'operatore, di cui al punto 5, siano resi inefficaci dalla configurazione di altri DNS non appartenenti all'operatore di accesso, oppure mediante l'utilizzo della funzionalità di DNS-over-HTTPS presente nelle ultime versioni dei browser più diffusi, gli operatori di fascia A forniscono le seguenti funzionalità aggiuntive:

- blocco degli indirizzi IP associati ai siti oggetto di filtro, nei casi in cui sia possibile un'associazione biunivoca tra gli stessi e l'indirizzo IP, o a server DNS;
- blocco delle porte utilizzate dai protocolli DNS e DNS-over-TLS per le richieste inviate a server non appartenenti all'operatore.

Agli operatori di fascia A è inoltre richiesta la fornitura di un applicativo da installare sui dispositivi utilizzati dai minori che possa effettuare un controllo puntuale sui contenuti, anche eventualmente utilizzando funzionalità di *proxy* implementate nella rete. Nei terminali forniti dall'operatore l'applicazione deve essere preinstallata.

Tutte le funzionalità sopra elencate fanno parte dei SCP anche nel caso in cui siano rese disponibili nell'ambito di sistemi aggiuntivi (ad es. *antivirus, antimalware, antispam*, etc.), se utilizzate per la finalità di *parental control*.

Q11. Si individuano altre modalità di filtraggio non elencate e che potrebbero essere realizzate?

Q12. Sono presenti criticità tra le soluzioni tecniche elencate?

Q13. Si reputa proporzionata la distinzione in fasce così come proposta in relazione alle Linee guida di cui ai punti 5 e 6?

7. Gli operatori di fascia A completano le funzionalità dei SCP mediante l'implementazione della configurabilità degli stessi per fasce orarie e di memorizzazione dei siti visitati.

Gli operatori di fascia A forniscono la possibilità di configurare per fasce orarie l'accesso alla navigazione, inibendone ad esempio totalmente la fruizione a determinati orari, nonché la possibilità, configurabile, di memorizzare tutti gli accessi effettuati o solo quelli bloccati.

Tutte le funzionalità sopra elencate fanno parte dei SCP anche nel caso in cui siano rese disponibili nell'ambito di sistemi aggiuntivi (ad es. *antivirus, antimalware, antispam*, etc.).

Q14. Sono presenti criticità tra le soluzioni tecniche elencate?

Q15. Si reputa proporzionata la distinzione degli ISP in fasce così come proposta?

8. I SCP realizzano esclusivamente le funzionalità necessarie per le finalità dei servizi in argomento, in conformità con il Regolamento UE n. 2015/2120 in materia di Open Internet.

La fornitura di servizi di *parental control* avviene ai sensi del Regolamento UE n. 2015/2120 secondo l'art. 3, comma 3 alla lettera a) il quale prevede, tra le possibili eccezioni per l'adozione di misure di gestione del traffico, la necessità di "*conformarsi ad atti legislativi dell'Unione o alla normativa nazionale conforme al diritto dell'Unione, cui il fornitore di servizi di accesso a Internet è soggetto, o alle misure conformi al diritto dell'Unione che danno attuazione a tali atti legislativi dell'Unione o a tale normativa nazionale, compreso ai provvedimenti giudiziari o di autorità pubbliche investite di poteri pertinenti*".

Ogni ulteriore misura di gestione del traffico, che esula da quanto specificato in queste Linee guida in relazione alle funzionalità di *parental control*, deve essere valutata separatamente in relazione alla sua conformità al Regolamento UE n. 2015/2120.

Q16. Si riscontrano criticità relative alla conformità al Regolamento UE n. 2015/2120 in materia di Open Internet?

9. Le operazioni di attivazione, disattivazione e configurazione dei SCP devono essere realizzabili in modo semplice e intuitivo.

I SCP devono disporre di un'interfaccia utente, accessibile solo dal titolare del contratto (o, se minore, da parte di chi ne esercita la potestà genitoriale), caratterizzata dalla possibilità di utilizzo semplice e intuitivo. Nel caso di interfaccia web, deve essere garantito un alto livello di usabilità e di accessibilità. Nel caso di interfaccia erogata mediante app, questa dev'essere disponibile almeno per Android e iOS. L'efficacia delle impostazioni di blocco/sblocco deve avvenire in tempo reale rispetto alle operazioni di attivazione, disattivazione e configurazione dei SCP da parte degli utenti.

Q17. Si riscontrano ulteriori requisiti per le interfacce dei SCP?

Q18. Si reputa che la regolamentazione debba fornire ulteriori specifiche sulle modalità di implementazione delle interfacce dei SCP?

Q19. Si reputa preferibile una interfaccia web, una app o si individuano ulteriori modalità realizzative?

10. I contenuti oggetto di filtro dei SCP sono personalizzabili dal titolare del contratto, con la possibilità di aggiungere o personalizzare i contenuti oggetto di filtro.

Per gli operatori di fascia A e B deve essere possibile aggiungere e rimuovere siti da *black list* e *white list*, contenenti rispettivamente siti sempre bloccati e siti sempre consentiti.

Q20. Si riscontrano problematiche relativamente alla gestione delle *black list* e *white list*?

11. Gli operatori di telefonia, di reti televisive e di comunicazioni elettroniche assicurano adeguate forme di pubblicità dei SCP preattivati, in modo da assicurare che i consumatori possano compiere scelte informate. In particolare, i SCP dovranno essere pubblicizzati sui siti web degli ISP, nelle carte dei servizi e con campagne di comunicazione mirate.

La presenza dei SCP e le istruzioni su come modificarne la configurazione, disattivarlo e riattivarlo in un secondo momento devono essere fornite in maniera chiara, trasparente ed esaustiva insieme alla documentazione contrattuale e inviate tramite SMS ed *e-mail*.

Nel caso di linee esistenti, nel momento in cui la funzionalità di SCP viene resa disponibile deve esserne data comunicazione al titolare della linea mediante comunicazioni in bolletta, avvisi via SMS e all'interno delle aree riservate su sito *web* e *app*, insieme alle istruzioni su come modificarne la configurazione, disattivarlo e riattivarlo in un secondo momento.

In particolare, si prevede che:

a) Devono essere fornite in maniera chiara, trasparente ed esaustiva informazioni e istruzioni su come modificare la configurazione del SCP, disattivarlo e riattivarlo in un secondo momento.

b) Gli operatori riportano sulle *home page* dei propri siti *web*, dandone ampia evidenza, le informazioni di cui alla lettera a) del punto 11.

c) Gli operatori sono tenuti a fornire le informazioni di cui alla lettera a) del punto 11 anche mediante il ricorso agli strumenti di *self care* (*call center*, aree di *self care* dei *siti web* ed *app*).

d) Gli operatori di comunicazioni su rete fissa sono tenuti a fornire le informazioni di cui alla lettera a) del punto 11 sia tramite apposita comunicazione allegata alla fattura, sia tramite chiamata diretta effettuata dall'operatore, anche tramite sistemi IVR- (*interactive voice response*).

e) Gli operatori di comunicazioni su rete mobile sono tenuti a fornire le informazioni di cui alla lettera a) del punto 11 sia tramite SMS, sia tramite comunicazione veicolata attraverso l'*app* di *self care* e, nel caso in cui l'utente fruisca di servizi post-pagati, attraverso la documentazione di fatturazione.

f) Gli operatori di reti televisive a pagamento sono tenuti a fornire le informazioni di cui alla lettera a) del punto 11 sia tramite la documentazione di fatturazione, sia tramite comunicazione inviata alla *set-top box*.

Q21. Si reputa che i canali di comunicazione individuati siano sufficienti?