Allegato B alla delibera n. 9/23/CONS

SINTESI DELLA CONSULTAZIONE PUBBLICA

AVVIATA CON DELIBERA N. 16/22/CONS

"AVVIO DELLA CONSULTAZIONE PUBBLICA PER L'ADOZIONE DI LINEE GUIDA FINALIZZATE ALL'ATTUAZIONE DELL'ARTICOLO 7-BIS DEL DECRETO-LEGGE 30 APRILE 2020, N. 28 IN MATERIA DI "SISTEMI DI PROTEZIONE DEI MINORI DAI RISCHI DEL CYBERSPAZIO""

Sommario

La consultazione pubblica

Con la delibera n. 16/22/CONS del 20 gennaio 2022, questa Autorità ha indetto una consultazione pubblica per l'adozione di linee guida finalizzate all'attuazione dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di "sistemi di protezione dei minori dai rischi del cyberspazio", a cui hanno aderito numerosi operatori, anche in forma associativa, Associazioni dei consumatori, Associazioni di genitori e famiglia.

La consultazione pubblica ha inteso sottoporre ai soggetti interessati una serie di quesiti finalizzati ad acquisirne i posizionamenti.

A seguito della produzione di contributi scritti, nel mese di aprile 2022, si sono tenute le audizioni dei partecipanti al procedimento.

I SOGGETTI PARTECIPANTI

Alla consultazione hanno partecipato con propri contributi i seguenti soggetti: Associazione italiana internet provider (di seguito denominata **AIIP**), Assotelecomunicazioni (di seguito denominata **Asstel**), Confindustria Radio TV, Open Xchange a.g. (di seguito denominata **Open Xchange**), Eolo S.p.A. (di seguito denominata **Eolo**), Iliad S.p.A. (di seguito denominata **Iliad**), Irideos S.p.A. (di seguito denominata **Irideos**), Linkem S.p.A. (di seguito denominata **Linkem**), Sky Italia s.r.l. (di seguito denominata **Sky**), Telecom Italia S.p.A. (di seguito denominata **TIM**), Vodafone Italia S.p.A. (di seguito denominata **Vodafone**), WindTre S.p.A. (di seguito denominata **WindTre**), **Federconsumatori, UDICON,** Associazione Centro Elis (di seguito denominata **Centro Elis**)**,** Associazione Pro Vita & famiglia (di seguito denominata **Pro vita**)**,** Coordinamento genitori democratici (di seguito denominata **Cgd**)**, Moige** e il Sig. **Andrea (OMISSIS)**.

Sintesi dei contributi - Considerazioni generali.

OSSERVAZIONI DEI RISPONDENTI

In via preliminare, necessita precisare che le posizioni espresse dal mercato sono particolarmente diversificate e pongono questioni di ampio respiro a partire dall'invito a valutare l'opportunità della regolamentazione fino alla richiesta di un regolamento stringente e dettagliato sui servizi di parental control.

Nel dettaglio, molti partecipanti non hanno inteso rispondere esclusivamente alle domande poste in consultazione dall'Autorità, preferendo partecipare anche con contributi di carattere generale sul tema.

Due rispondenti, con riguardo al percorso di attuazione della normativa primaria intrapreso da questa Autorità, hanno sollevato una questione di carattere metodologico. A valle dell'avvio del procedimento istruttorio di cui alla delibera n. 160/21/CONS, infatti, l'Agcom ha ritenuto di procedere lungo un percorso che si sviluppa su tre distinti momenti temporali: 1) adottare Linee Guida operative che attengono 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; 2) tramite altro e separato procedimento, AGCom intende affrontare 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"); 3) i temi rilevanti (diversi da quelli affrontati nell'ambito delle Linee guida in consultazione) ai fini del rispetto del Regolamento UE n. 2015/2120 in materia di Open Internet, saranno oggetto di separata e successiva valutazione. Ad avviso dei partecipanti sopracitati, sarebbe stato auspicabile seguire un diverso ordine logico nella trattazione delle questioni indicate, facendo precedere le misure di identificazione e inibizione dall'accesso ai contenuti da un previo intervento di classificazione di quest'ultimi. Tale modalità implementativa potrebbe anche minare alla base la corretta implementazione della norma primaria, in quanto l'adozione delle Linee Guida, entro 60 giorni dalla chiusura dell'attuale fase di consultazione, senza conoscere né quali saranno le modalità di classificazione ed individuazione dei contenuti per i quali deve essere pre-attivato un blocco o filtro né se dette modalità celino possibili elementi di conflitto con le regole di net neutrality appare fortemente limitativo. Alla luce di quanto sopra, sarebbe auspicabile affrontare tutte le questioni rilevanti in maniera organica, in seno allo stesso procedimento ovvero in un unico momento. Qualora l'Autorità procedesse comunque su percorsi distinti, si auspica che sia contemplato un confronto non solo con gli Operatori in qualità di internet service provider (anche "ISP") ma anche con quei soggetti che avranno l'onere di classificare i contenuti nonché con coloro che, come i fornitori dei servizi media

audiovisivi e di opere audiovisive destinate al web, hanno già predisposto – anche perché previste dalla regolamentazione attuale - specifiche misure negli ambiti di intervento della Consultazione.

Tanto premesso, **l'associazione** effettua ulteriori considerazioni generali sul documento in consultazione:

1) come riconosciuto espressamente da Agcom, l'individuazione dei contenuti dannosi non spetta agli ISP che beneficiano dell'esenzione di responsabilità di cui all'art. 17 (Assenza dell'obbligo generale di sorveglianza) del decreto legislativo n. 70/2003 recante "Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico". Gli Operatori di comunicazioni elettroniche svolgono infatti un ruolo di "*mere conduit*" dei contenuti offerti da soggetti terzi e l'estrema modificabilità dello scenario di fruizione dei contenuti stessi rende non solo estremamente gravoso addossare ai soli Operatori oneri e responsabilità di verifica che ad essi non appartiene, ma anche praticamente impossibile da garantire.

2) nel settore dei servizi media audiovisivi a richiesta, Agcom ha seguito un processo di co-regolamentazione ai fini dell'adozione di delibere intervenute su temi analoghi a quelli in Consultazione, sulla scorta di quanto previsto dall'art. 34, comma 11, del decreto legislativo 31 luglio 2005, n.177 (anche "TUSMAR") e analogamente a quanto previsto dall'art. 37 decreto legislativo 8 novembre 2021, n. 208 ("TUSMA"). Più precisamente un percorso di co-regolamentazione è stato seguito a proposito dell'adozione di previsioni inerenti:

- Misure tecniche a tutela dei minori - la delibera n. 51/13/CSP recante "Regolamento in materia di accorgimenti tecnici da adottare per l'esclusione della visione e dell'ascolto da parte dei minori di trasmissioni rese disponibili dai fornitori di servizi di media a richiesta che possono nuocere gravemente al loro sviluppo fisico, mentale o morale", che prevede l'adozione di apposite misure in capo ai fornitori di servizi media a richiesta, in quanto unici soggetti a poter offrire contenuti a "visione non libera";
- Classificazione dei contenuti - la delibera n. 52/13/CSP recante "Regolamento sulla classificazione delle trasmissioni televisive che possono nuocere gravemente allo sviluppo fisico, mentale o morale dei minori" con cui si individuano i parametri per poter procedere alla classificazione dei contenuti che possono nuocere gravemente allo sviluppo fisico, psichico o morale dei minori.

3) Ai sensi delle disposizioni del Decreto legislativo 7 dicembre 2017, n. 203, recante: "Riforma delle disposizioni legislative in materia di tutela dei minori nel settore

cinematografico e audiovisivo, a norma dell'art. 33 della legge 14 novembre 2016, n. 220", l'Autorità ha adottato con la delibera n. 74/19/CONS un regolamento in materia di classificazione delle opere audiovisive destinate al web e istituito un tavolo di co-regolamentazione per l'adozione di apposite linee guida relative sia alla specificazione dei criteri di classificazione delle opere audiovisive destinate al web e ai videogiochi, che alle misure tecniche per inibire l'accesso alle opere audiovisive destinate al web. Con delibera n. 359/19/CONS AGCom ha successivamente approvato le Linee Guida redatte ad esito dei lavori del tavolo tecnico di co-regolamentazione e riconosciuto "l'opportunità di istituire un apposito Osservatorio permanente per la co-regolamentazione della classificazione delle opere audiovisive destinate al web e dei videogiochi […]", quale sede di interlocuzione permanente tra l'Autorità ed i soggetti interessati1. Tale Osservatorio, dotato di competenze aggiornate, potrebbe costituire la sede di confronto e di discussione delle misure tecniche compatibili con i vincoli tecnico-commerciali di ciascun attore della filiera (dall'ISP al gestore della piattaforma di contenuti, fino al soggetto "classificatore"), oltreché normativo-regolamentari europei e nazionali.

In linea generale, l'associazione valuta, dunque, le misure poste in consultazione come: a) Inefficaci: non è possibile il blocco generalizzato dei contenuti; b) Incomplete: non sono dettate le procedure applicabili; c) Incerte: i contenuti da controllare sono ignoti, visto il divieto di vigilanza e di net neutrality; d) Parziali: le soluzioni non possono essere locali, posto che si tratta di misure che si ripercuotono su una filiera globale.

In generale, infatti, l'associazione richiama due aspetti che caratterizzano qualunque operazione di blocco dei contenuti online, a prescindere dalla sofisticazione che contraddistingue i Sistemi di blocco approntati: 1) Al fine di evitare violazioni della libertà di espressione, i contenuti da bloccare devono essere sempre indicati da una pubblica autorità; 2) Fintanto che non è inibita la fonte del contenuto da bloccare, è impossibile avere la certezza che i sistemi di blocco non vengano aggirati.

A partire da queste evidenze, secondo l'Associazione, si sta affermando positivamente nel diritto comunitario il principio del c.d. "buon samaritano", declinato dalla proposta di direttiva UE sui servizi digitali (cfr. art. 6 COM/2020/825 final). Tale articolo prevede che i prestatori di servizi intermediari siano ammessi all'esenzione di responsabilità già prevista dal quadro normativo europeo anche nel caso in cui svolgano, a tutela di diritti altrui, indagini volontarie o altre attività di propria iniziativa volte ad individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi, o di adottare le misure necessarie per conformarsi alle prescrizioni del diritto dell'Unione" (naturalmente purché tali iniziative siano state adottate diligentemente ed in buona fede). Mutuando tale impostazione al contesto in questione e tenendo presente che gli Operatori hanno tutti già in essere soluzioni di tutela dei

minori, anche in applicazione di norme di legge e di indicazioni precedenti di codesta Autorità, appare auspicabile salvaguardare quanto più possibile la varietà di meccanismi di tutela presenti sul mercato, per vari motivi che si riassumono sinteticamente nei seguenti punti:

• Nessun sistema di protezione dei minori che operi attraverso un blocco dei contenuti è in grado di assicurare l'inibizione totale dell'accesso a contenuti audiovisivi destinati al web;

• Il fatto che ciascun Operatore ha proceduto a scelte in proprio rispetto alla finalità di tutela dei minori sviluppa una varietà di sistemi che è positiva perché conduce ad un continuo perfezionamento dei sistemi stessi;

• La stessa fornitura di servizi che tutelano i minori in modo differenziato può costituire un elemento su cui valorizzare l'offerta degli Operatori, generando un circolo virtuoso di mercato;

• Gli Operatori hanno sostenuto investimenti ingenti per la messa in opera dei sistemi utilizzati attualmente e non sono stati evidenziati particolari fallimenti di tali sistemi, che anche qualora emergessero potrebbero essere risolti caso per caso, senza costringere tutto il mercato su una unica soluzione che, oltre a dover richiedere ulteriori pesanti oneri tecnici ed economici agli Operatori, presenta le forti limitazioni sopra sintetizzate.

• La natura della fonte adottata dall'Autorità (i.e. Linee Guida) non sarebbe di ostacolo all'efficacia ed osservanza dell'intervento regolamentare. Al contrario, le Linee Guida costituirebbero un riferimento imprescindibile per tutti gli Operatori non appena pubblicate, nonché riferimento del Giudice per ogni profilo interpretativo relativo all'applicazione delle misure disposte.

L'associazione esprime il forte timore che attraverso le misure proposte in Consultazione non sia possibile individuare efficaci strumenti di filtro o blocco di contenuti inappropriati per i minori, atteso che l'attuale sviluppo tecnologico dei terminali d'utente Multi USIM e delle applicazioni/browser disponibili sul mercato consente infatti di passare per esempio dalla rete di un Operatore a quella di altro, oppure di passare dalla rete cellulare alla rete Wi-Fi, oppure permette di utilizzare server Proxy, di attivare VPN o connessioni attraverso la rete TOR in grado di aggirare i filtri configurati sulla Rete, vanificando così qualsiasi sforzo di implementazione delle misure richieste in Consultazione.

Le implementazioni richieste, inoltre, dovrebbero calarsi nel contesto di mercato senza alterare le fisiologiche dinamiche competitive, posto che quand'anche ciascun Operatore fornisse i propri terminali con le ipotizzate limitazioni, l'utente potrebbe rivolgersi all'open market per ottenere così devices "liberi", con il duplice effetto sfavorevole di non tutelare

l'utenza e di favorire impropriamente i produttori di terminali. Diviene pertanto condizione imprescindibile che codesta Autorità garantisca parità di condizioni, assicurando che tutti i produttori di modem, router e smartphone, acquistabili dal cliente sul mercato, siano dotati delle medesime implementazioni hardware e software. Peraltro, se gli Operatori fossero tecnicamente in grado di apportare correttivi real time all'accesso da parte dell'utenza a determinati contenuti, occorrerebbe comunque tener conto del generalizzato divieto di controllo e verifica su quanto visionato dall'utenza, nel rispetto delle rigorose limitazioni poste dalla normativa a tutela dei dati personali oltre che dalla disciplina in tema di net neutrality.

Un operatore aggiunge che la disposizione di legge debba trovare applicazione non su tutte le linee/offerte, ma unicamente su quelle che potremmo definire le offerte di salvaguardia per le quali i SCP sono preattivati, gratuiti e configurati dal genitore/tutore. Si tratta in particolare di offerte caratterizzate da un doppio fattore di "sicurezza", ossia (i) insistono su linee intestate a minori e (ii) sono ideate appositamente per i minori. La legge, infatti, non dovrebbe trovare applicazione laddove le linee siano sottoscrivibili solo da maggiorenni: ciò in ragione del fatto che è la maggiore età, rafforzata dalla responsabilità genitoriale, che deve guidare e non deve certo essere l'operatore a sostituirsi al genitore. Vale la pena rimarcare ulteriormente il fatto che la proposta dell'Autorità di preattivare massivamente i SCP appare davvero eccessiva nella misura in cui assume che tutti gli utenti siano interessati ai servizi in esame senza tener in nessun conto le libertà individuali, le inclinazioni personali, etc. L'Autorità dovrebbe pertanto tenere in massimo conto gli investimenti e le architetture di servizio già realizzate dagli operatori che, ad avviso di un operatore, già soddisfano i requisiti della norma primaria, evitando forme di *over regulation* (si pensi ad esempio alla proposta di estendere i servizi di SCP a tutte le linee fisse e mobili o a quella di intervenire sugli indirizzi IP) di dubbia utilità in termini di incremento della tutela dei minori ma che comporterebbe certamente forti investimenti per gli operatori in termini di dimensionamento di rete, licenze di Threat Intelligence (oltre che distrazione degli investimenti già realizzati) e/o l'adozione di una architettura tecnica difficile poi da gestire.

Un operatore sottolinea che la regolamentazione in essere (come sopra descritta anche da un'associazione) sia già pienamente rispondente alle previsioni di cui all'art. 7-bis in esame e, quindi, che l'intenzione di AGCom di "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")" non debba riguardare anche i servizi media audiovisivi a richiesta. In tal senso, occorre inoltre che l'Autorità mantenga ben distinte le attività di controllo parentale svolte dai diversi fornitori dei servizi in esame: appare non priva di problematiche applicative, e per questo certamente da chiarire, la considerazione

contenuta nel documento di consultazione di avere sistemi di parental control da parte degli ISP dichiaratamente "complementari o sovrapposti a quelli di parental control messi a disposizione dalla piattaforma": il rischio è quello di avere una inutile dispersione di energie/risorse oltre che interventi tra loro contrastanti per limiti oggettivi e tecnici dettati dai rispettivi perimetri di attività.

Un operatore sottolinea come le Linee Guida offerte con la Consultazione in commento rischiano di iper-regolare rispetto a quanto invece stabilito dal quadro normativo e legislativo sancito a protezione dei minori. Il decreto-legge che introduce l'obbligo di SCP prevede esclusivamente un filtro e blocco dei contenuti senza far alcuno riferimento alla possibilità di impostare il tempo di utilizzo dei dispositivi in uso al minore né di monitorarne l'attività. Utile, al riguardo, anche un richiamo alla normativa privacy, per quanto stabilito all'art. 122 Decreto Lgs. 196/2003 – Codice Privacy, comma 1: i) L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate; e comma 2-bis: ii) salvo quanto previsto dal comma 1., è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente. Tutto ciò che non è strettamente previsto dalla legge non potrebbe, dunque, essere introdotto nell'ambito del procedimento in oggetto attraverso delle Linee Guida interpretative del suddetto quadro normativo. Peraltro, si rinvengono ulteriori criticità applicative per alcuni aspetti che riguardano più strettamente temi di natura privacy che non sembrano, allo stato, essere stati presi in considerazione. Per quanto riguarda, la memorizzazione dei siti visitati, il rispondente ritiene opportuno che codesta Autorità, nell'implementazione delle Linee Guida, sviluppi un'interlocuzione con il Garante Privacy in quanto l'intrusione nella sfera privata del minore di un siffatto dispositivo dovrebbe essere accompagnata da misure di bilanciamento della privacy del minore che non deve essere sottoposto ad un cyber stalking (particolarmente importante nella fascia di età 14-17). Nel rispetto, dunque, di un principio di proporzionalità e del corretto *agere* amministrativo, è essenziale che Codesta Autorità tenga conto delle misure (laddove disponibili) già attuate dagli operatori. Si ritiene, inoltre, che le Linee Guida, debbano essere indirizzate in particolare ai fornitori di servizi di comunicazione elettronica che ancora oggi non abbiano implementato misure idonee a tutelare i minori, pur nel rispetto della normativa vigente. In conclusione, su questo punto si auspica:

• Che non vi siano restrizioni all'accesso ad internet per default (cosiddetta pre-attivazione), pena una violazione della normativa sulla Net Neutrality, come meglio sarà precisato in risposta al Q16.

• Che non siano imposte misure tali da violare la normativa della Privacy (sia in termini di identificazione dei minori che in termini di verifica dei contenuti di cui lo stesso avrebbe o meno accesso).

• Che non siano introdotte misure sproporzionate ed eccessive, rispetto all'obiettivo prefissato dalla norma, che non consentono la remunerazione delle attività sottostanti ancor di più se riferite in modo generico a tutta l'utenza.

• Che non siano imposte misure quali l'inibizione di un indirizzo IP senza che vi si sia un ordine degli enti preposti a tal fine, pena oltre alla violazione della normativa sulla Net Neutrality anche il rischio di violare i principi dello stesso Codice delle Comunicazioni Elettroniche laddove riconosce un generale principio di tutela della riservatezza e protezione dei dati personali (art. 1.6) nonché un obbligo di garantire la sicurezza delle reti e dei servizi intesa come la capacità di resistere, a un determinato livello di riservatezza, a qualsiasi azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza di tali reti e servizi, dei dati conservati, trasmessi o trattati oppure dei relativi servizi offerti o accessibili tramite tali reti o servizi di comunicazione (Art. 2);

• Che non siano imposte misure ultronee rispetto a prestazioni già disponibili sul mercato ed in linea con la normativa Berec del 2020.

• Che non siano attuate asimmetrie regolamentari sulla base della dimensione dell'operatore che fornisce un servizio di parental control, rischiando in tal modo una classificazione tra minori di serie A (ovvero minori che sono anche clienti di operatori di maggiori dimensioni) e minori di serie B (ossia, minori che usufruiscono di servizi di operatori di dimensione più piccola). Qualsivoglia misura, se introdotta a tutela dei minori, deve essere indipendente dalla dimensione dell'operatore che fornisce il servizio (anche su questo si dirà meglio infra).

• Che si tenga conto del principio di armonizzazione massima della disciplina tra Stati Membri dell'UE, posto che, come si dirà meglio in risposta al Q16, l'imposizione di un blocco preventivo su base contenuto, rappresenta un'attività di gestione del traffico vietata secondo le regole della Net Neutrality, nonché in violazione della Carta dei diritti fondamentali dell'Unione europea, riguardo alle limitazioni all'esercizio dei diritti e delle libertà fondamentali. Per tale ragione, una norma in deroga a detti principi, deve, quantomeno essere supportata da una norma di medesimo rango primario di derivazione europea, affinché ne venga assicurata una sua applicazione armonica e unitaria in tutta l'Unione.

Un operatore apprezza il riconoscimento dell'Autorità in ordine al fatto che la scelta dei contenuti da bloccare non può essere demandata agli Operatori ma che debba essere un ente terzo ad individuare e segnalare i contenuti da trattare. Tale ente terzo dovrebbe essere

possibilmente uno solo al fine di rendere coerente, efficace ed efficiente il processo di individuazione dei punti terminali di internet da trattare ai sensi della Legge all'origine di questa consultazione e che sarà imprescindibile la definizione di procedure di interscambio dei dati automatiche e tali da minimizzare gli impatti operativi anche al fine di bloccare con la massima tempestività i contenuti rilevanti. La Società ritiene, pertanto, che l'attenzione di codesta Autorità nel definire le modalità attuative dello spirito dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 sia da concentrare non tanto sugli operatori di telecomunicazioni, che operano appunto come "*mere conduit*", bensì sui soggetti che erogano i contenuti e su quelli che producono i dispositivi che ne consento la fruizione. Il medesimo rispondente, alla luce della complessità della tematica trattata, ritiene indispensabile che venga aperto un tavolo di lavoro che coinvolga tutti gli attori presenti nella catena del valore, soprattutto fornitori di router/modem, smartphone, TV, produttori di Sistemi operativi (ad es. Android e IoS) per terminali e App nonché produttori di contenuti a livello internazionale, vista la dimensione globale di internet, al fine di realizzare un disegno consistente in tutte le sue parti, cosa altrimenti di difficile realizzazione.

Un'associazione esprime forti perplessità circa la legittimità, sia a livello normativo che di Linee Guida, di un intervento che imponga agli ISP obblighi e responsabilità diversi da quelli di *mere conduit*, soli ai quali sono tenuti ai sensi dell'art. 12 della Direttiva 31/2000; ne consegue in ogni caso la necessità di una interpretazione quanto più restrittiva dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28, e di un intervento regolatorio che si mantenga entro gli stretti limiti della disposizione. L'articolo 7-bis, presenta inoltre caratteri di indeterminatezza che lo rendono di difficile applicazione e potenzialmente pongono lo stesso, e di riflesso le Linee Guida, in contrasto con norme di rango superiore. È necessario chiarire che le Linee Guida in discorso si applicano solo ai clienti consumer, in ossequio a quanto previsto dall'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28. Di conseguenza, il conteggio delle linee ai fini della determinazione delle fasce, come previsto dalla delibera in consultazione, deve tenere in conto solo le linee di tipo consumer, escludendo i contratti business.
La soluzione di blocco DNS centralizzato, o di blocco a livello IP, non soddisfa il requisito di legge di blocco di "contenuti", in quanto non selettiva; altresì, a differenza di altre attività di inibizione attualmente in uso, è particolarmente oneroso sviluppare la personalizzazione per singolo utente (prevista dalle Linee Guida) del blocco DNS "lato rete", che potrebbe essere invece efficacemente sostituita da un'implementazione di un eventuale SCP lato CPE, con periodico aggiornamento della lista di indirizzi bloccati predisposta da AGCOM e con possibilità di *opt out* autonomo e personale da parte dell'utente stesso, e/o dall'imposizione di un sistema di *tagging* (sul modello di quello IAP) ai fornitori di contenuti. La soluzione proposta dall'associazione, anche considerando che quello al SCP è un *diritto disponibile*,

consente di prevenire eventuali conflitti con il Regolamento EU 2015/2120, che è fonte sovraordinata, lasciando l'utente libero di scegliere di avvalersi di un diverso SCP o di non avvalersene affatto.

Un operatore sottolinea che sarebbe importante tutelare gli investimenti già effettuati dagli operatori per garantire un sistema di parental control agli utenti richiedenti. Auspica, al contempo, la previsione di obblighi regolamentari che non richiedono ingenti investimenti (a titolo esemplificativo, costi di acquisto di licenze annuali per ciascun cliente della customer base dell'operatore a cui applicare il blocco predefinito; costi di gestione del cliente) e che tengano conto delle strutture organizzative e delle risorse economiche anche degli operatori di medie e piccole dimensioni. Tutto ciò al fine di evitare previsioni regolamentari gravose e concretamente insostenibili per gli operatori in quanto eccessivamente impattanti sul bilancio aziendale. Inoltre, per rendere efficace qualsiasi sistema di parental control, è indispensabile trattare e definire in modo congiunto la disciplina dell'individuazione e classificazione dei contenuti da bloccare e il sistema che operativamente dovrebbe bloccarli; tale trattazione dovrebbe, altresì, tenere in debito conto le previsioni del Regolamento europeo in tema di "Net Neutrality". Infine, il medesimo concorda con la distinzione in fasce tra operatori, ma propone di modificarle ed allinearle alle quote di mercato detenute dagli operatori, come risultanti dall'ultimo Osservatorio sulle Comunicazioni pubblicato da AGCOM.

Un altro operatore sottolinea di non concordare con la distinzione in fasce tra operatori, che rischierebbe di generare una discriminazione tra gli utenti. Difatti, gli utenti di operatori minori si ritroverebbero ad avere una minor tutela. Ritiene che l'unica vera tutela dei minori, tecnologicamente efficace, sia un blocco che operi sul terminale utilizzato dal minore e non lato rete. Auspica che la regolamentazione preveda un obbligo generale di fornitura di SCP con misure minime e senza dettagli tecnici sull'implementazione dei sistemi, che dovrebbero essere lasciati alla libertà d'impresa. Infine, sarebbe auspicabile un tavolo tecnico che coinvolga tutti gli operatori della filiera, compresi i fornitori di contenuti e le piattaforme, al fine di addivenire ad una soluzione di sistema che sia effettivamente di tutela dei minori.

Un operatore chiede che le utenze business vengano escluse dalla regolamentazione in ossequio alla finalità della norma da attuare nonché al suo effettivo portato. Inoltre, chiede di valutare se per le utenze mobili il sistema a PIN della SIM possa essere considerato satisfattivo degli obblighi (similmente a quanto disposto dal DM 145/2006). Infine, ritiene che la regolamentazione dovrebbe definire uno strumento base, come quello previsto per gli operatori di fascia C, altrimenti rischierebbe di andare in conflitto con la normativa vigente sul open Internet. Nel caso in cui fossero invece previsti obblighi crescenti con la dimensione dell'operatore, la stessa dovrebbe essere valutata considerando le sole linee impattate (es. escludendo linee business), computate in maniera distinta e separata per tecnologia (es. fisso,

mobile). Ritiene che una regolamentazione organica ed efficace, dovrebbe identificare in primo luogo i contenuti da bloccare (con indicazione di un ente terzo) e poi definire il sistema di blocco attraverso un sistema che operi alternativamente su CPE o su DNS centralizzato.

Un operatore sottolinea come qualsiasi sistema di parental control implichi ingenti investimenti da parte degli operatori, pertanto, sarebbe auspicabile prevedere un obbligo generico di fornitura, lasciando piena libertà sui dettagli di implementazione, che richiedono in ogni caso tempi di realizzazione non trascurabili. Pertanto, è necessario affrontare la questione in maniera sistemica, partendo dalla definizione dei contenuti da bloccare, da parte dell'Autorità, per poi definire il sistema tecnico di blocco. In merito alla proposta di memorizzazione dei siti visitati dagli utenti, di cui non si ha evidenza dalla lettura della normativa primaria, sussiste un problema di capacità degli strumenti di storage, cioè di memorizzazione dei dati, oltre che di tutela della privacy. La Società condivide la soluzione tecnica proposta da Agcom in ordine al blocco a farsi sulla rete piuttosto che su terminale CPE, prevedendo un sistema centralizzato di ON/OFF del filtro applicato basato su DNS.

Un'associazione ricorda che sin dal 2002 le emittenti radiotelevisive nazionali e locali hanno ridefinito, in continuità con precedenti analoghe esperienze, avviate sin dal 1993, regole di autodisciplina contenute nel Codice di autoregolamentazione Tv e Minori, volte a garantire, da un lato, un opportuno livello di tutela avverso trasmissioni nocive o non idonee, dall'altro un'adeguata disponibilità di programmi adatti ai minori e di programmi a loro specificamente rivolti. L'evoluzione tecnologica ha poi reso possibile la fruizione di contenuti anche al di fuori del contesto dei media tradizionali, generando una profonda disparità di trattamento tra i fornitori di servizi di media audiovisivi, la cui attività è pervasivamente disciplinata da un ampio sistema di disposizioni normative, regolamentari e disciplinari, e altri operatori che svolgono le loro attività in rete. A giudizio dell'associazione, l'intervento dell'Autorità costituisce quindi l'occasione di riequilibrare gli obblighi e l'autoregolamentazione potrebbe non essere sufficiente per far sì che ci sia un'assunzione di responsabilità degli utenti. Deve pertanto sussistere in capo alle piattaforme e ai soggetti che operano in rete l'obbligo di adottare tutte le misure tecnologiche idonee a garantire la tutela dei più piccoli e dei ragazzi attraverso l'uso di strumenti tecnologici innovativi di protezione accompagnato dalla diffusione di una corretta educazione dell'utenza all'uso di tali strumenti. È altresì apprezzabile che non si preveda che i fornitori di reti di comunicazione elettronica e gli ISP debbano effettuare essi stessi un controllo preventivo e generalizzato dei contenuti. Va chiarito che l'intervento regolamentare, finalizzato ad assicurare che l'accesso dei minori ai contenuti disponibili in Rete non avvenga in modo indiscriminato, bensì in maniera controllata e sulla base di precise scelte educative, riguardi unicamente il caso in cui siano forniti all'utente servizi di comunicazione elettronica. Nel caso della televisione digitale

terrestre gratuita, la disciplina dei servizi di media audiovisivi, con i correlati obblighi di informazione, assicura già, di per sé, un adeguato livello di tutela dei minori nell'ambito di tali servizi, anche se forniti a pagamento.

Un operatore, in via preliminare, segnala che, come noto, l'art. 7-bis del d.l. 30 aprile 2020, n. 28, integralmente introdotto in sede di conversione, suscita non pochi dubbi di legittimità evidenziati sin dalla sua approvazione, in particolare con riferimento alla conformità dello stesso con il Regolamento (UE) 2015/2120 (Open Internet). Fermo quanto sopra, il medesimo rispondente, come altri operatori che forniscono servizi di connettività, sin dalla data di lancio della propria offerta "(OMISSIS)" - a prescindere, quindi, da eventuali obblighi normativi - ha messo a disposizione dei propri clienti che aderiscono a tale offerta, senza alcun costo aggiuntivo, una funzione di controllo parentale che consente di proteggere la navigazione dei bambini e dei ragazzi inibendo l'accesso ai siti ritenuti non appropriati. Sarebbe dunque auspicabile che ove l'Autorità, nonostante i dubbi di legittimità della norma primaria sopra espressi, intendesse adottare comunque le Linee Guida in oggetto, avviasse sin d'ora un tavolo di confronto con gli operatori interessati, anche nell'ottica di valorizzare i sistemi di controllo parentale già implementati da questi ultimi su base volontaria e con significativi investimenti; diversamente, l'introduzione di nuove regole di dettaglio rischierebbe di penalizzare proprio quei soggetti che si sono dimostrati più virtuosi. Questo *modus procedendi* sarebbe del tutto analogo a quello già seguito in passato dalla stessa Autorità, in particolare, per l'adozione di altri regolamenti in materia di misure a tutela dei minori. Peraltro, tale confronto dovrebbe coinvolgere non solo gli ISP, ma anche, quantomeno, i soggetti -ad oggi non noti- su cui ricadrà l'onere della classificazione ed individuazione dei contenuti per i quali dovrebbe essere pre-attivato un blocco o un filtro, al fine di assicurare una trattazione organica della materia; in ogni caso, le Linee Guida sulle misure tecniche dovrebbero essere definite a valle o, quantomeno, contestualmente ai criteri di classificazione. È ad ogni modo evidente che le emanande Linee Guida non dovrebbero in alcun modo interferire con la disciplina a tutela dei minori prevista dall'art. 37 del TUSMA (ex art. 34) né con le delibere già adottate in materia da questa stessa Autorità per i servizi di media audiovisivi e per le opere audiovisive destinate al web.

Un'associazione dei consumatori sottolinea le seguenti considerazioni:

- Risulta di fondamentale importanza prevedere una comunicazione efficace sulla messa a disposizione del SCP, in modo da garantire all'utenza interessata la dovuta informazione e la possibilità di usufruirne. A titolo di esempio, sarebbe opportuno prevedere che gli operatori mettano a disposizione degli utenti, ciascuno sul proprio sito web, una guida operativa sul funzionamento del SCP e prevedere delle campagne informative anche istituzionali;

SINTESI DEI CONTRIBUTI - CONSIDERAZIONI GENERALI.

- L'assistenza clienti, già implementata dagli operatori, dovrebbe essere adeguatamente formata a fornire supporto all'utente nell'utilizzo degli SCP.

Un'altra associazione dei consumatori ritiene che il testo sottoposto a consultazione sia idoneo a garantire l'introduzione di misure atte a tutelare i diritti dei minori, filtrando i contenuti a loro non adatti, bilanciando il rapporto tra professionista e consumatore/minore. L'Associazione sottolinea, tuttavia, che il SCP non deve prevedere la possibilità di essere associato con servizi aggiuntivi a pagamento da parte degli ISP in quanto, in ottica di tutela del consumatore, una disposizione di tal guisa genererebbe difficoltà nella fase di vigilanza da parte dell'Autorità sulla corretta applicazione della norma.

Un'associazione dei genitori sottolinea le seguenti considerazioni:

- "Il meglio è nemico del bene": non è necessario ottenere subito tutto, perché si rischia di non riuscire a valicare le ragionevoli resistenze degli ISP che non sono enti di beneficenza, ma aziende orientate al profitto.

- L'esperienza di venti anni fa del Codice di autoregolamentazione "Internet e minori" non è stata positiva perché gli ISP non presero iniziative al riguardo non avendo obblighi giuridici.

- Avere una norma è quindi importante, ma se la richiesta nei confronti degli ISP è troppo onerosa, non funzionerà.

- Necessita iniziare subito con il filtraggio DNS, utilizzando servizi internazionali affermati, senza pretendere che l'Autorità definisca criteri di classificazione di contenuti. L'Autorità può identificare alcuni di questi servizi, tra i quali gli ISP possono scegliere: devono però poterne proporre di alternativi, da valutare.

- Il fatto che sia possibile aggirare un qualsiasi sistema di filtraggio non deve costituire un problema: tutte le protezioni fisiche si possono aggirare e quindi anche quelle digitali, più o meno facilmente. I genitori hanno un ruolo formativo verso i figli per far loro capire l'importanza di evitare i rischi con i mezzi opportuni.

- Si può iniziare con l'imporre subito che nei nuovi contratti per le connessioni cablate sia necessario scegliere se attivare o no il filtro DNS facendo anche decidere le categorie da bloccare. Dopo tre mesi, l'Autorità e gli ISP potranno fare un'analisi dell'andamento, per capire quanti utenti l'hanno attivata. In questo modo gli ISP potranno dimensionare i loro servizi di filtraggio in modo graduale, preparandosi al passaggio successivo dedicato a tutti i contratti esistenti. Sarà utile anche fare inchieste sull'accettazione e l'utilizzo del sistema da parte dei nuovi utenti.

SINTESI DEI CONTRIBUTI - CONSIDERAZIONI GENERALI.

- Deve essere sempre possibile attivare un sistema di "biblioteca di casa" (walled garden), cioè navigazione ristretta a un elenco di siti definiti dal genitore.

- Gli ISP devono poter aggiungere ulteriori servizi a pagamento a quelli essenziali di filtraggio DNS.

- Per i contratti dei telefoni mobili ci sono già offerte specifiche per i minori con sistemi di protezione: si può imporre che tutti gli ISP abbiano un'offerta al riguardo, con un costo paragonabile a quella standard per maggiorenni.

- è importante ribadire che non c'è assolutamente nessun problema di "censura" o limitazione di libertà o violazione delle norme europee su Open Internet: il filtro è totalmente disattivabile in qualsiasi momento da un maggiorenne.

Un'altra associazione per la famiglia sottolinea le seguenti considerazioni:

- Le osservazioni dell'Associazione sono ispirate a tre principi, che si ritrovano nella normativa sia europea sia nazionale (si veda ad esempio, l'art. 42 c. 7 del d.lgs n. 208/2021, in riferimento alle piattaforme di condivisione di video): 1. Verifica seria dell'età dell'utente; 2. Controllo parentale effettivo (difficilmente aggirabile dal minore); 3. Ampia informazione sulle misure di protezione e sul loro utilizzo.

- L'Associazione invita a tenere presenti questi principi in tutte le disposizioni che riguardano la predisposizione delle misure di protezione e le diverse fasi di impostazione/modifica delle misure tecniche: 1. adottando quelle soluzioni che implicano standard di autenticazione equivalenti a quelli richiesti per l'accesso ai servizi pubblici per i quali è necessario dimostrare l'identità del richiedente (SPID, CNS, documento di identità); 2. evitando di prevedere, nell'impostazione del SCP o blocco/sblocco di contenuti, la comunicazione di codici che potrebbero comunque facilmente entrare nella disponibilità del minore che utilizza il dispositivo in questione; 3. Disponendo, in riferimento a tutti gli obblighi di informazione, che sia effettuata anche la comunicazione (qualora possibile) all'indirizzo e-mail ordinario dell'utente maggiorenne (anche nel caso di linee già esistenti).

Una associazione dei genitori sottolinea le seguenti considerazioni:

- Le osservazioni e proposte prendono avvio dall'analisi del panorama attuale, che vede la forte diversificazione degli strumenti di filtro e di blocco da parte degli operatori (ISP, emittenti e fornitori di contenuti audiovisivi, ecc.), impostati su sistemi e criteri eterogenei e in ogni caso poco conosciuti dagli utenti, così che di fatto la responsabilità della tutela ricade quasi totalmente sui genitori. A fronte di ciò, il processo di attuazione della nuova norma, oltre a costituire una dovuta applicazione della legge, potrebbe portare ad una maggiore

omogeneità dei sistemi, alla condivisione di responsabilità da parte di tutti i soggetti coinvolti e quindi rendere più efficace la tutela dei minori.

- A valle dell'attuazione del sistema di parental control, sarebbe di fondamentale importanza prevedere una campagna informativa di tipo istituzionale, al fine di formare nella popolazione una cultura digitale adeguata alla fruizione dei servizi Internet da parte dei minori;

- È necessario far passare il messaggio che la sicurezza sul web per i minori non limita la libertà di Internet quanto piuttosto rende possibile il godimento di tutti i loro diritti (informazione, formazione, socializzazione, gioco, ecc.). In questo senso, un sistema di parental control è uno strumento che può aiutare i genitori a garantire il giusto diritto dei minori alla navigazione su Internet;

- Entrando nel merito del provvedimento, la medesima associazione suggerisce di prevedere che il parental control non possa essere abbinato in bundle con altri servizi a pagamento;

- È necessario prevedere un livello essenziale del servizio che sia garantito a tutta la popolazione, indipendentemente dall'ISP utilizzato;

- Altrettanto necessaria è la previsione di canali di assistenza, ad esempio pagine di FAQ, una guida per l'utilizzo del SCP pubblicata sui siti web nonché la possibilità di accedere ad un call center con un contatto umano;

- A valle della messa a disposizione del SCP, sarebbe auspicabile prevedere un periodo di monitoraggio del sistema ai fini della valutazione della customer experience;

Un'altra associazione di genitori sottolinea le seguenti considerazioni:

- Il provvedimento in discorso è di importanza fondamentale per la tutela dei nostri figli, per cui è urgente l'approvazione di linee guida che affrontino in maniera seria e organica il problema della fruizione dei contenuti su Internet da parte dei minori;

- Al contempo, è altrettanto importante che le famiglie vengano a conoscenza dell'esistenza stessa dello strumento. A tal proposito, si propone di prevedere una campagna informativa stringente che coinvolga tutte le istituzioni e anche le associazioni del comparto a tutela dei minori;

- Sarebbe auspicabile che il nuovo sistema di parental control venga almeno pre-attivato sui nuovi contratti. A valle di ciò, preso atto della difficoltà a individuare l'effettivo fruitore (maggiorenne/minorenne) del servizio Internet, si potrebbe prevedere una fase di

sperimentazione di tre/sei mesi per poter procedere gradualmente all'attivazione del SCP sui contratti già attivi.

Sintesi dei contributi - Osservazioni sui singoli quesiti.

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

OSSERVAZIONI DEI RISPONDENTI

Una Società fornisce chiarimenti in merito ad alcune caratteristiche tecniche dei servizi di controllo parentale (SCP) legate all'attuale stato della tecnologia e dei protocolli di trasmissione Internet, segnalando come sia in corso ormai da molti anni la progressiva adozione di protocolli di comunicazione crittografati (il traffico Web viaggi su protocolli crittografati (HTTPS) per percentuali che variano tra il 90 e il 98 per cento secondo i dati resi disponibili ad esempio da parte di Google). L'applicazione di filtri su protocolli non crittografati, più semplice, meno costosa e più flessibile, rappresenta ormai una funzionalità residuale che andrà a scomparire completamente nel giro di pochissimi anni. La Società suggerisce di inserire nella definizione di SCP che il blocco possa avvenire soltanto per interi siti o nomi a dominio, o, se legato all'indirizzo IP, per interi server e gruppi di server (spesso ospitanti decine, migliaia o milioni di siti). Chiarisce infatti che, nell'ambito di comunicazioni applicative crittografate, nessuna delle tecnologie attualmente in uso per il filtro "in network" (ossia, su un dispositivo di rete che non è a uno dei due capi della comunicazione, come

necessariamente sono gli apparati di rete degli ISP) permette di effettuare filtri a livello di singolo contenuto. In base al tipo di tecnologia utilizzata è possibile effettuare filtri per nome dell'host (filtro DNS oppure analisi del campo SNI del traffico Web, quest'ultima peraltro oggetto di nuovi standard di cifratura e destinata a scomparire a breve) oppure per indirizzo IP (firewall e blocchi di routing). Metodi di filtro più complessi per individuare singoli protocolli o contenuti, basati sull'analisi dei pacchetti di traffico crittografato, sono stati concepiti sperimentalmente ma non sono realisticamente applicabili su scala di massa allo stato attuale.

Un operatore ritiene che la regolamentazione non dovrebbe superare la definizione che la norma offre di sistema controllo parentale sia quella di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni 18. La declinazione al singolare di "filtro di contenuti" suggerisce che debba essere previsto un obbligo minimo di SCP di tipo "binario", vale a dire di tipo on-off. Sarebbe quindi ultroneo (*over regulation*) definire ulteriori caratteristiche dei suddetti SCP, generando sistemi troppo rigidi e obbligando gli operatori ad investimenti non strettamente necessari. Per contro, dovrebbe essere lasciata a ciascun operatore la scelta su come implementare il proprio SCP ovvero se limitarsi all'obbligo minimo (come detto prima, di on-off) oppure offrire al cliente un sistema più articolato che, in aggiunta alla funzionalità di base, preveda anche altre caratteristiche (ad es. blocco per fasce orarie, per singole categorie di contenuti, etc.). In tal modo, a giudizio del medesimo operatore si avvierebbe un circolo virtuoso in cui il SCP diventerebbe un elemento competitivo della proposizione commerciale di ciascun operatore in grado di orientare le scelte dei clienti più attenti alla presenza di tali funzionalità. La Società descrive alcune caratteristiche dei propri SCP, evidenziando che il filtro adottato non agisce a livello di singolo contenuto, ma a livello di dominio/sottodominio web, sulla base della classificazione/profilatura del sito/dominio o sottodominio fornita dalla Threat Intelligence e sulla base del blocco impostato o meno dall'utente amministratore della linea. Riguardo alla casistica del blocco operato da "siti web e le applicazioni che prevedono un meccanismo di registrazione con verifica dell'età dell'utente e conseguente filtro dei contenuti accessibili", l'operatore suggerisce di mantenere ben distinte le attività, in termini di controllo parentale, svolte dai diversi fornitori dei servizi. Nel caso di specie, se il fornitore del servizio via sito web/APP è un FSMA, varranno le regole di SCP ad esso già applicate, senza alcun obbligo addizionale e sovrapposto da parte dell'ISP; negli altri casi, occorre prevedere regole per il gestore del sito/APP, senza addossare tutte le responsabilità all'ISP.

Una Società preliminarmente ribadisce di accogliere con favore qualsivoglia iniziativa volta a rendere più sicuro e responsabile l'utilizzo dei servizi di comunicazione elettronica e in particolare di internet a tutela dei minori, senza tuttavia ignorare le norme interne ed europee nel settore dei servizi della società dell'informazione ed in particolare le disposizioni secondo cui gli operatori non possono in alcun modo essere responsabili delle informazioni trasmesse in rete ovvero svolgere attività di sorveglianza generale. Ciò premesso, in merito alla definizione di SCP, la medesima ritiene in parte condivisibile la definizione di cui alla linea

guida 1, chiarendo che, coerentemente con quanto disposto a livello legislativo, e con gli obiettivi prefissati dalla legge (i.e. la tutela del minore), il filtro SCP deve limitarsi a prevedere funzioni di base che possano assicurare la protezione dei minori quali soggetti esposti ai rischi del cyberspazio. Posizione analoga assunta da altro operatore. Le ulteriori funzioni di personalizzazione, quali la previsione di specifiche fasce orarie di utilizzo, tipologia di contenuti, black o white list, etc., potranno costituire funzionalità aggiuntive che possono essere messe a disposizione dagli operatori come servizi opzionali a pagamento in quanto non previste dalla normativa nazionale né europea.

A giudizio di un operatore il filtro SCP deve essere pre-attivato solo nel caso di offerte riservate a un pubblico di minorenni e disponibile su richiesta per tutte le altre offerte, in linea con quanto disposto a livello legislativo europeo, con obbligo per gli operatori di fornire informazioni sulle modalità per attivare il filtro. Il SCP dovrebbe essere costituito da un sistema di semplice soluzione con funzioni di base, che neghi l'accesso ad una serie di contenuti le cui categorie, devono essere definite a monte, di concerto con l'Autorità. Il medesimo chiede che, nel caso un operatore avesse già disponibile un servizio di parental control messo a disposizione gratuitamente per i propri clienti minorenni, ovvero a pagamento per i clienti maggiorenni, non vengano imposti ulteriori adeguamenti che rischiano di essere sproporzionati e non necessari al perseguimento dell'obiettivo individuato dal legislatore, ovvero la tutela del minore. Per quanto riguarda le modalità di classificazione, in categorie, dei contenuti in oggetto e la definizione di filtri per fasce d'età, l'operatore ritiene necessario che la regolamentazione sia contestuale da parte di codesta Autorità, evitando il rinvio ad un separato procedimento e ciò in ragione del fatto che non esiste, allo stato, un elenco univoco e comune dei siti web/applicazioni che includono contenuti inappropriati. In assenza di tale categorizzazione dei contenuti da bloccare, potrebbero riscontrarsi importanti difficoltà tecniche nell'implementare sistemi di SCP.

Una Società ritiene che un filtro applicato all'intero sito web sarebbe una soluzione non pratica, in quanto bloccherebbe il traffico verso le maggiori piattaforme, che sarebbe nei fatti equivalente a non dare proprio la possibilità al minore di accedere ad Internet. In merito alle modalità di classificazione dei contenuti e alla definizione di filtri per fasce d'età che sarà oggetto di separato procedimento, la medesima segnala sin da ora che i principali produttori e distributori di contenuti su piattaforme che possiamo ormai definire "tradizionali" (nella fattispecie: Produttori di videogames, Produttori cinematografici e Televisivi broadcaster TV, gruppi editoriali, ecc.) hanno definito o aderito da molti anni a specifiche modalità di classificazione dei propri contenuti per fasce d'età (ad es.: PEGI - Pan European Game Information; Sistemi di classificazione dei film o delle produzioni TV, ecc.) e che le maggiori criticità, come evidenziato dall'Autorità, riguardano i contenuti prodotti appositamente per essere distribuiti dalle c.d. "nuove" piattaforme digitali e, in generale, i self generated content, spesso divulgati in real time. La stessa Società prevede difficoltà anche nell'imposizione della classificazione ai principali OTT che controllano direttamente o indirettamente le principali piattaforme di distribuzione (YouTube, Facebook, Instagram, Telegram, WhatsApp, Tik Tok,

ecc.) e ai siti web che divulgano, senza alcun accesso condizionato, contenuti pornografici, violenti, lesivi delle diversità e delle minoranze. L'operatore propone che la classificazione si limiti ai contenuti la cui fruizione debba essere filtrata e ai contenuti vietati ai minori. Il medesimo propone, altresì, che per i siti web e le applicazioni che prevedono un meccanismo di registrazione con verifica dell'età dell'utente la restrizione all'accesso dei contenuti sia da fornire a cura del fornitore di contenuti e non da parte dell'operatore, non avendo quest'ultimo alcuna responsabilità in merito al meccanismo di registrazione con verifica dell'età dell'utente. Alla luce di quanto sopra, ribadisce la necessità dell'apertura di un tavolo tecnico per discutere una efficace implementazione del SCP in grado di tutelare il minore.

Due operatori riscontrano numerose potenziali criticità tecniche relative ai SCP proposti nello Schema, con particolare riferimento all'implementazione dei blocchi DNS, della possibilità di sblocco temporaneo all'accesso per i siti web, nonché del blocco delle funzionalità del terminale che consentono all'utente di utilizzare servizi DNS.

Viene rappresentato da un operatore, in particolare, che presupposto imprescindibile affinché si possa procedere all'implementazione dei blocchi DNS è l'identificazione da parte di codesta Autorità dei contenuti da filtrare nonché la definizione delle relative categorizzazioni e specifiche tecniche standard che devono essere condivise tra gli Operatori, atteso che non esistono criteri di classificazione condivisi tra gli ISP, né tantomeno una lista comune dei siti. Tale operazione, inoltre, non può prescindere da una valutazione di opportunità che tenga conto degli obblighi di controllo già previsti in capo ai fornitori dei servizi media audiovisivi in materia di classificazione e misure tecniche a tutela dei minori, al fine di evitare una duplicazione delle misure già implementate in ottica di bilanciamento rispetto agli obiettivi perseguiti con la presente consultazione. Il medesimo segnala che i resolver DNS forniti dagli ISP consentono ad oggi di inibire l'accesso a determinati siti, ma non di filtrare specifici contenuti pubblicati all'interno dei siti stessi, poiché l'ISP si limita a ricevere la categorizzazione dei domini Internet ed è dunque totalmente "trasparente" rispetto ai contenuti ivi presenti. Diretta conseguenza di tale circostanza è che, in presenza di un contenuto soggetto al filtro parental control, gli ISP sarebbero tecnicamente forzati ad inibire l'accesso all'intero sito, limitando indebitamente l'accesso all'Internet degli utenti finali e ponendosi in sostanziale contrasto con i principi di cui al Regolamento UE n. 2015/2120 in materia di Open Internet. Inoltre, il filtro mediante resolver DNS potrebbe rivelarsi inefficace in concreto, in quanto aggirabile utilizzando, ad esempio, VPN ovvero DNS over HTTPs (DoH), frequentemente adottato/consigliato dai browser agli utenti finali per rendere privata la navigazione a tutela della propria privacy. Né è preventivabile l'inibizione del DoH, poiché la porta impiegata per tale protocollo è quella utilizzata per tutto il traffico http protetto (porta 443), e bloccarla comporterebbe l'inibizione generalizzata di tutto il traffico https, in potenziale violazione della sopra citata normativa in materia di Net Neutrality ed Open internet. Il medesimo operatore rileva alcune criticità anche con riferimento all'implementazione del meccanismo di reindirizzamento del minore che tenta di accedere ad un contenuto oggetto del filtro parental control ad una pagina web informativa – fornita

dall'ISP – e della relativa possibilità di sblocco temporaneo all'accesso (cd. "PIN override"). Il reindirizzamento potrebbe risultare tecnicamente impossibile nel caso in cui la pagina cui l'utente finale sta tentando di accedere fosse criptata, come altrettanto non praticabile in maniera selettiva (il filtro DNS non è tipicamente in grado di distinguere tra utente minorenne e maggiorenne). Da ultimo, la Società ritiene che l'introduzione di meccanismi di PIN override presupporrebbe la risoluzione delle numerose criticità già evidenziate in merito, ad esempio, all'identificazione ed autenticazione del soggetto esercente la potestà genitoriale sul minore ed alla tutela dei dati personali dell'utenza finale.

Con riferimento, infine, alla fornitura (richiesta solo agli Operatori di fascia A) di un applicativo che, installato – e in alcuni casi preinstallato – sui dispositivi utilizzati dai minori, effettui un controllo puntuale sui contenuti e filtri quelli ritenuti inappropriati, l'operatore ritiene che l'utilizzo del blocco mediante resolver DNS, ferme le limitazioni sopra descritte, sia ad oggi l'unica soluzione tecnica in grado di garantire l'efficace funzionamento dei SCP.

Il medesimo operatore rappresenta, tuttavia, che la fornitura di applicativi installabili dall'utente sui propri device per il filtro di singoli contenuti non è una soluzione percorribile per gli ISP, che operano a livello di rete e non possono dunque per definizione sostituirsi ai produttori dei device, i quali dovrebbero, come rappresentato in premessa, essere destinatari delle misure volte all'implementazione dei SCP al pari degli ISP stessi.

Con riferimento all'implementazione della possibilità di configurare per fasce orarie l'accesso alla navigazione e di memorizzare gli accessi ad Internet effettuati dal minore (tutti ovvero solo quelli inibiti), ancora una volta prevista solamente per gli ISP di fascia A, l'operatore propone alcune osservazioni di tipo tecnico. Per quanto attiene alla configurabilità dell'accesso per fasce orarie, ritiene che questa sia tecnicamente possibile esclusivamente su rete fissa, e solamente nel caso in cui l'utente finale scelga di utilizzare un router/modem fornito dall'ISP ma facilmente eseguibile solo se applicato indistintamente su tutti i terminali collegati al router/modem. Poiché detta possibilità è intrinsecamente legata al terminale utilizzato dall'utente finale per accedere alla rete e non alla configurazione della rete stessa, il medesimo ritiene necessario il coinvolgimento e confronto con i soggetti produttori di tali terminali, che non possono essere individuati nei soli ISP, al fine di garantire all'utenza un livello di tutela adeguato ed uniforme.

Per quanto riguarda l'ulteriore misura prospettata di memorizzazione degli accessi effettuati dal minore mediante DNS, l'operatore crede che l'introduzione di un tale obbligo comporterebbe oneri estremamente significativi in capo agli ISP, che si troverebbero costretti ad archiviare, per ciascun utente finale, una enorme quantità di dati, con potenziali impatti negativi sulle performance del DNS stesso. Da ultimo il medesimo riporta che un simile sforzo implementativo e gestionale, oltre a risultare sproporzionato se rapportato con il ruolo di mere conduit svolto dagli ISP di cui in premessa, potrebbe risultare critico anche dal punto di vista della cybersecurity e della tutela dei dati personali dell'utenza finale, poiché gli ISP tratterebbero nuove categorie di dati, con conseguente necessità di effettuare tutte le attività

necessarie a garantire la privacy by design dell'attività, anche a livello di corretta e sicura conservazione del dato.

Un operatore fa presente che i fornitori di servizi di accesso ad Internet (ISP) hanno la possibilità di applicare il filtro SCP sui contenuti inappropriati per i minori esclusivamente sulla navigazione web e non "tramite qualunque applicazione", affermando che il blocco di un dominio Internet su server DNS non può tecnicamente avere alcun effetto sull'uso di applicazioni di tipo peer-to-peer (P2P) e sui relativi contenuti.

Due operatori evidenziano che i due requisiti addizionali di un sistema SCP prospettati nel documento di Consultazione - ossia "impostare il tempo di utilizzo dei dispositivi in uso al minore" e "monitorarne l'attività svolta" – sono caratteristiche tipiche di software locali in uso su router/cpe o dispositivi dei clienti e l'implementazione di tali requisiti sui sistemi degli operatori comporterebbe gravi implicazioni sia di natura economica - considerato che un'attività simile richiederebbe sproporzionati costi infrastrutturali, di integrazione e di gestione dei sistemi - sia di natura normativa, in considerazione del fatto che tale implementazione potrebbe fare sorgere criticità in merito al trattamento dei dati di navigazione ad internet da parte dei minori.

Un operatore ritiene necessaria una ulteriore riflessione in merito all'inclusione o meno dei servizi mobili all'interno del perimetro di azione della norma, proponendo una lettura della norma che conduce all'esclusione dei servizi mobili dall'ambito di applicazione della stessa. A riguardo precisa, infatti, che, mentre la nuova disciplina chiaramente si riferisce alla necessità di prevedere strumenti di tutela di minori in un contesto in cui viene esercitato un "controllo genitoriale", i servizi mobili rivestono, invece, per esplicita previsione normativa, un carattere "personale" e, dunque, vengono impiegati dal titolare (e, nel caso, ceduti in uso ad altri) sotto la propria piena responsabilità. Tale distinzione, peraltro, già permea la normativa di settore sul tema. Infatti, il Decreto del Ministero delle Comunicazioni n. 145 del 2006 ("DM"), proprio con riferimento ai sistemi di controllo dell'accesso ai servizi a contenuto, nel riconoscere la natura personale del servizio mobile, fa coincidere tale sistema di protezione con il PIN della SIM, rilasciato in modalità sicura al titolare dell'utenza, opportunamente riconosciuto. Al fine di evitare rilevanti discontinuità con la normativa vigente e di allineare le istruzioni operative qui in discussione con l'ambito di applicazione della norma primaria (che è, ad avviso di chi scrive, l'ambito "domestico" e non quello "personale"), il medesimo suggerisce di prevedere che, per i servizi di comunicazioni mobili e personali, conformemente a quanto già previsto dal sopra citato DM, il sistema di parental control possa coincidere con la consegna di un PIN di abilitazione al servizio, a condizione che il titolare della SIM risulti maggiorenne. Tale sistema potrebbe essere rafforzato con ulteriori strumenti di trasparenza, anche in sede di contrattualizzazione dei nuovi clienti (es. con un richiamo specifico a tali aspetti all'interno delle condizioni contrattuali).

Un altro operatore constata che l'eccessiva genericità della norma ha reso necessario l'intervento dell'Autorità**.** Inoltre, la circostanza che saranno oggetto di separato

procedimento sia le modalità di classificazione, in categorie, dei contenuti di cui si discute nonché la definizione di filtri per fasce d'età non permette di poter individuare compiutamente ogni possibile ulteriore elemento di criticità rispetto ai temi oggi posti in consultazione. Il medesimo sottolinea, infine, che la legittima facoltà riconosciuta al titolare del contratto di disattivare i preimpostati SCP porta con sé un non banale costo gestionale tenuto conto che, sebbene correttamente informato mediante i più diretti e immediati canali di informazione, l'utente medio - non dotato di un'adeguata alfabetizzazione digitale (tale da permettergli di espletare in autonomia la disattivazione/riattivazione dei SCP) – sarà portato ad effettuare tali attività rivolgendosi al servizio di assistenza clienti che, conseguentemente, si troverà a dover gestire un aumento di code a discapito, ad esempio, delle richieste di assistenza vertenti sulla fruibilità del servizio.

Un'associazione di consumatori ritiene poco chiara la definizione di cui al punto 1. delle Linee Guida oggetto di consultazione, di cui si propone la seguente formulazione alternativa: che preveda espressamente la definizione di parental control system (SCP) come sistema finalizzato a limitare o bloccare l'accesso dei minori a contenuti inappropriati forniti attraverso servizi di comunicazione elettronica che consenta al genitore (o chi ne faccia le veci) di bloccare tutti i contenuti riservati ad un pubblico di età superiore agli anni diciotto, di limitare la fruizione dei suindicati contenuti, eventualmente filtrando e bloccando quelli ritenuti inappropriati per i minori, di impostare il tempo di utilizzo dei dispositivi in uso al minore e di monitorare la fruizione dei contenuti sui dispositivi in uso al minore, chiarendo con esempi pratici, quali siano le circostanze che possano determinare l'impossibilità di filtrare il singolo contenuto. **La medesima** propone altresì di includere nel sistema SCP, a titolo di esempio, le applicazioni in cui siano memorizzate modalità di pagamento (come le app di e-commerce o gli app store), in modo che nella fruizione di strumenti comunemente utilizzati dai minori – in primis i giochi online – questi ultimi possano effettuare operazioni di acquisto di beni e/o servizi, nonché l'implementazione del sistema con una funzionalità di alert che, tramite messaggio, segnali al genitore gli eventuali tentativi del minore di accedere a contenuti inappropriati.

Due associazioni di genitori ritengono necessario che le Linee guida prevedano indicazione espressa delle caratteristiche minime di un SCP, elencando lo stretto necessario e non concordano sulla decisione di differire l'individuazione delle modalità di classificazione in categorie. Secondo il giudizio di **una di queste**, la norma dovrebbe invece definire alcuni ambiti generali di classificazione (ad esempio: pornografia, sesso, violenza, droghe, razzismo, scommesse) lasciando libertà di ampliarli, ma soprattutto indicare i fornitori internazionali di classificazione tra i quali scegliere senza impedire all'ISP di generare le proprie categorie in autonomia. L'eventuale errore di classificazione con conseguente blocco provocherebbe conseguenze minime in quanto il blocco è disattivabile dall'adulto. L'Autorità potrà effettuare un monitoraggio per valutare se la protezione è sufficiente e segnalare all'ISP eventuali rafforzamenti necessari.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Un'altra associazione dei genitori ritiene che il punto 1 sia formulato in modo soddisfacente.

Un'associazione di genitori ritiene che le funzionalità riportate nella delibera (restrizioni all'accesso, impostazione tempi di fruizione, monitoraggio dell'attività svolta) costituiscono i contenuti minimi essenziali del SCP, da mettere a disposizione degli utenti. Particolare valore assume la disponibilità di black e white list.

A giudizio di **due associazioni di genitori**, il nuovo contesto di tutela dei minori prefigurato dall'innovazione introdotta dall'art. 7-bis potrà dirsi completato solo a seguito della definizione di un sistema di classificazione dei contenuti cosiddetti "a visione non libera", adempimento attribuito all'Autorità, come viene ribadito dalla stessa delibera n. 16/22/CONS.

A tale proposito, secondo **una di tali associazioni** un valido precedente di riferimento può essere rappresentato dal lavoro di definizione delle Linee guida relative alla classificazione delle opere audiovisive destinate al web, in applicazione del D.Lgs. 203/2017 (cosiddetto "Decreto Franceschini").

Il sig. (OMISSIS) ritiene che il compito dell'applicazione della tecnologia di controllo dei contenuti sia solo dei genitori.

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.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Q2 – QUALI SONO LE CASISTICHE IN CUI IL TITOLARE DEL CONTRATTO PUÒ ESSERE UN MINORE?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione ritiene che la conclusione di un contratto presupponga che il contraente sia maggiorenne, dotato di capacità di agire; pertanto, un ISP può stipulare contratti con utenti che abbiano superato il diciottesimo anno di età.

Gli operatori ((OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS)) dichiarano che, con riferimento alla fornitura di servizi su rete fissa, il titolare del contratto può essere solo un soggetto maggiorenne.

Per quanto riguarda la fornitura di servizi su rete mobile, un operatore riferisce genericamente che titolare del contratto può essere un minore, mentre un altro operatore riporta che in alcuni casi ai minorenni è consentito unicamente l'acquisto di una SIM cosiddetta ricaricabile. Un altro operatore consente l'attivazione di utenze prepagate a soggetti che abbiano compiuto i quattordici anni di età, in linea con la prassi di mercato e con l'evoluzione stessa del diritto, che per consuetudine ammette la sottoscrizione di contratti relativi agli atti della vita quotidiana da parte di soggetti minorenni, come ad esempio un contratto di trasporto tramite l'acquisto del relativo biglietto o l'acquisto di prodotti di varia natura merceologica. Per una Società il limite di età per il contratto mobile è di 15 anni, mentre due operatori non permettono l'adesione alle proprie offerte a utenti di età inferiore ai 18 anni. In merito alle forme di autenticazione proposte da Codesta Autorità nel documento di Consultazione (PIN, SPID, autenticazione nell'area riservata, OTP), un operatore ritiene tali modalità eccessivamente onerose, risultando preferibile richiedere agli operatori l'utilizzo di un'utenza a cui è abbinata una password di rete fornita esclusivamente ai sottoscrittori del contratto maggiorenni da utilizzare per accedere all'area riservata e, eventualmente, in via residuale anche tramite contatto telefonico diretto per le funzionalità di attivazione e disattivazione del filtro.

Un rispondente segnala che, con specifico riguardo ai servizi mobili, con l'approvazione della delibera n. 86/21/CIR, la figura del "reale utilizzatore" – cui spesso il minore ricorreva per essere riconosciuto come possessore dell'utenza mobile datagli in uso da un maggiorenne (tipicamente un genitore) – risulti oramai superata sul piano regolamentare, essendo sempre e comunque necessaria, in caso di cambio del possesso della SIM, una formale procedura di subentro per poter compiere operazioni dispositive sull'utenza. Il medesimo ritiene peraltro

che il concetto di "nuova linea" introdotto dall'Autorità al fine di perimetrare l'applicazione dei diversi meccanismi di opt-in e opt-out (differenziati a seconda che si tratti di utente minorenne o maggiorenne) debba essere perimetrato in modo da non incidere su rapporti di utenza già in essere secondo una disciplina contrattuale previgente.

Un'associazione di consumatori considera annullabile il contratto stipulato da un minore e ritiene opportuno introdurre l'obbligatorietà di indicare i dati personali dell'adulto che eserciti la patria potestà, salvo che l'Autorità non provveda a precisare le casistiche in cui un minore possa essere titolare del contratto, mentre due associazioni di genitori ritengono sempre necessaria la partecipazione di un adulto a tutela.

La medesima associazione di consumatori in merito alla pre-attivazione, disattivazione e configurazione dei SCP, suggerisce di prevedere un meccanismo più snello rispetto a quello indicato nelle Linee Guida, rendendo disponibile il servizio per le nuove linee al momento dell'attivazione ed entro un tempo congruo sulle linee preesistenti (in quest'ultima circostanza con obbligo di informare l'utente con regolari comunicazioni sulla disponibilità del servizio con SMS e messaggi in bolletta).

Il sig. (OMISSIS) ritiene che i contratti di connettività a internet in ambito mobile potrebbero essere fatti dai minorenni. In alcuni casi forse può capitare che sono fatti dai minorenni all'insaputa dei genitori o perché i genitori sono analfabeti digitali e preferiscono delegare il compito al figlio.

Q3 – SI RISCONTRANO ULTERIORI MODALITÀ DI POSSIBILE AUTENTICAZIONE DEL TITOLARE DEL CONTRATTO (O, SE MINORE, DI CHI NE ESERCITA LA POTESTÀ GENITORIALE)?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione dichiara che non ci sono esigenze di autenticazione in quanto l'utente che ha il dovere di usare il servizio secondo la legge e secondo buonafede contrattuale.

Un operatore riferisce in merito ai sistemi di autenticazione già in uso in base ai quali il cliente maggiorenne potrà accedere e modificare le impostazioni del Parental Control utilizzando le credenziali, custodite dal genitore. In fase di configurazione del Parental Control, il cliente può inoltre definire apposito PIN che consente lo skip della pagina pop-up di blocco visualizzata nel caso di selezione URL proibita o malevola (tale skip non è a tempo ma sarà necessario inserire ogni volta il PIN); per i protocolli sicuri (https) tale skip non è sempre possibile.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Un operatore condivide che la gestione del filtro SCP sia rimessa ad un soggetto autorizzato, e ritiene che debba essere lasciata facoltà agli operatori di individuare la soluzione più opportuna, senza che sia previsto un intervento specifico di codesta Autorità mentre un altro operatore chiede che l'Autorità istituisca un Tavolo tecnico per la gestione di questa e di altre criticità.

Una Società ritiene che l'introduzione di un obbligo di identificare il titolare del contratto con le modalità proposte si pone in contrasto con quanto previsto dall'art. 98-undestricies del D.lgs. 259/2003 (anche "Codice delle comunicazioni elettroniche"), secondo il quale gli Operatori di comunicazioni elettroniche debbono identificare gli acquirenti del traffico mobile prepagato tramite "l'acquisizione dei dati anagrafici riportati su un documento di identità, nonché del tipo, del numero e della riproduzione del documento". La medesima osserva peraltro che l'Autorità non è legittimata ad intervenire autonomamente a modificare o comunque integrare i processi di identificazione personale degli utenti, in assenza di qualsiasi norma di legge che le attribuisce un potere in tal senso (incluso il sopra citato art. 98-undetricies del D.lgs. 259/2003).

Secondo un operatore le modalità di autenticazione indicate nella bozza in consultazione sono idonee a riconoscere con un sufficiente grado di certezza il titolare del contratto e dovrebbero essere indicate agli operatori come alternative e non obbligatorie, con la possibilità per gli operatori stessi di individuare ulteriori strumenti resi possibili dalla tecnologia. Per quanto riguarda il riconoscimento del soggetto maggiorenne che esercita la potestà genitoriale sul minore, il medesimo suggerisce di adottare la procedura già in opera in tutti i casi in cui una pubblica amministrazione deve accertarsi di tale fatto, in genere basata sulla raccolta di un'autocertificazione tramite moduli prestampati.

Un operatore, non permettendo l'adesione alle proprie offerte a utenti di età inferiore ai 18 anni e attribuendo a ciascun cliente delle credenziali personali con le quali lo stesso può accedere alla propria area riservata del sito web (c.d. "Area di self care"), ritiene che la certezza della maggiore età e l'identificazione del titolare del contratto risultino ben soddisfatte esclusivamente mediante l'accesso del cliente alla propria Area di self care.

Un'associazione di consumatori e due di genitori non indicano ulteriori modalità di autenticazione rispetto a quelle indicate mentre **un'altra associazione per la famiglia** propone l'uso di Smartcard che rispondano ai requisiti della Carta Nazionale dei Servizi (CNS).

Un'associazione di genitori segnala eventuali criticità che l'utilizzo dello SPID sarà oggetto di preliminare valutazione di impatto sulla protezione dei dati per le possibili conseguenze relative al trasferimento di dati personali degli utenti a soggetti privati quali sono i gestori dell'identità digitale.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Q4 – QUALE (O QUALE COMBINAZIONE) TRA LE SOLUZIONI INDIVIDUATE PER L'AUTENTICAZIONE SI REPUTA PREFERIBILE?

OSSERVAZIONI DEI RISPONDENTI

Secondo un'associazione è sufficiente un'autenticazione semplice come quella normalmente adottata per l'accesso ad aree riservate nei siti di customer care. In tal senso anche tre operatori escludono la praticabilità dello SPID come modalità di identificazione per la scarsa diffusione e per l'onerosità.

Due operatori concordano sul fatto che bisogna consentire all'operatore di scegliere tra più alternative, indicando la natura esemplificativa e non esaustiva della lista proposta

Un operatore ritiene che le modalità di implementazione debbano essere definite nell'ambito del tavolo tecnico.

Un operatore afferma che la criticità più rilevante è costituita dalla inidoneità degli strumenti a comprovare la potestà genitoriale sul minore. A tal fine, l'unica modalità di identificazione in astratto percorribile risulta essere la richiesta dello stato di famiglia del titolare del contratto, ovvero della sentenza di nomina del tutore legale del minore, con evidenti conseguenze in termini di onerosità di gestione per l'operatore ed il conseguente intralcio alle procedure di mobilità dell'utenza di rete fissa e mobile, in aperta violazione degli obblighi di cui all'art. 106 della Direttiva 2018/1972 (anche "Codice Europeo delle comunicazioni elettroniche"), così come recepito dall'98-octies decies del Codice delle comunicazioni elettroniche.

Un'associazione di consumatori ritiene opportuno introdurre una procedura di autenticazione a due livelli, prevedendo prima che l'utente fornisca il codice PIN e poi la conferma con codice OTP.

Un'associazione di genitori ritiene non necessario imporre agli ISP di avere tutte le opzioni possibili di modalità di attivazione e disattivazione, essendo sufficienti l'accesso all'area riservata (che dovrebbe abitualmente prevedere anche SPID) e l'OTP via SMS o e-mail, mentre **un'altra associazione per la famiglia** ritiene preferibili quelle soluzioni che implicano standard di autenticazione equivalenti a quelli richiesti per l'accesso ai servizi pubblici per i quali è necessario dimostrare l'identità del richiedente. Inoltre, per l'abilitazione alla disattivazione o attivazione del SCP tramite codice PIN o OTP inviato a mezzo SMS ritiene necessario che il codice PIN o OTP venga inviato all'indirizzo e-mail del contraente

maggiorenne o tramite SMS ad altro numero telefonico intestato all'utente maggiorenne, indicati da quest'ultimo al momento della verifica dell'età dell'utente

Un'associazione di genitori al contrario ritiene che l'opzione preferibile sarebbe di procedere tramite SPID ma, nel caso di PIN o di altra autenticazione, sarà preferibile affiancare l'OTP via SMS o e-mail.

Un'altra associazione di genitori afferma che, per evitare oneri eccessivi, si potrebbe imporre che l'operatore dia almeno tre possibilità di autenticazione, lasciando sempre possibile quella via SPID.

Sig. (OMISSIS) riporta la preferenza dello SPID che è difficilmente aggirabile da parte del minore che voglia sfuggire al controllo.

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?

OSSERVAZIONI DEI RISPONDENTI

Secondo **un'associazione** in questa sede non è possibile disciplinare ulteriori componenti che non siano espressamente previsti dalla norma.

Una Società osserva che sulle piattaforme non personalizzabili i filtri sono uguali per tutti, mentre sulle piattaforme più avanzate i filtri sono personalizzabili per singolo indirizzo di provenienza, singolo utente e/o singolo dispositivo, pertanto è probabile che gli operatori vadano a fornire un unico servizio di filtro per tutti i tipi di contenuti, che poi verrà configurato

pre-attivando gratuitamente i filtri relativi ai contenuti inadatti ai minori e permettendo invece l'attivazione opzionale, gratuita o a pagamento, di filtri su altri tipi di contenuti. La medesima ricorda comunque che, in base al Regolamento 2015/2020, anche i blocchi mirati al garantire la sicurezza della rete e dei dispositivi o a gestire la congestione di rete (es. blocchi contro attacchi "distributed denial of service") sono permessi ed esenti dalla necessità di consenso dell'utente. Segnala dunque l'opportunità di emendare le linee guida affinché anche questo tipo di blocchi possa, a discrezione dell'ISP, essere pre-attivato e non opzionale, oppure essere attivato anche in un secondo momento dandone informazione all'utente, ma senza necessità di consenso.

Un operatore ritiene che il dettato di legge preveda unicamente l'introduzione di un profilo base di SCP a tutela dei minori, pertanto, deve essere lasciata all'operatore la possibilità di offrire, anche a pagamento, funzionalità/servizi aggiuntive rispetto ai SCP di base: la gratuità dovrebbe riguardare però unicamente i profili di offerta cd. di salvaguardia, intestate e dedicate ai minori, per i quali i SCP sono pre-attivati e configurati dal genitore/tutore.

Tre operatori ritengono che il filtro SCP così come le operazioni correlate devono poter essere fornite gratuitamente ma anche che ciascun operatore deve poter integrare le funzioni del SCP con ulteriori funzioni sia di personalizzazione dello stesso SCP, sia funzionalità aggiuntive e non strettamente correlate, come antivirus, antispam, etc. In particolare, due operatori**,** ribadiscono che ogni ulteriore funzionalità come "impostare il tempo di utilizzo dei dispositivi in uso al minore e di monitorarne l'attività svolta" non costituisce un requisito richiesto dalla legge; pertanto, possano essere offerti a titolo oneroso e non gratuito, a ristoro della onerosità della gestione di detti sistemi. Deve inoltre essere chiaramente precisato che tali servizi aggiuntivi possono essere forniti anche solo in caso di terminale fornito dall'ISP e che non deve essere obbligatorio per l'ISP fornirli anche a quei clienti che adottassero un terminale di loro scelta per il quale non ci sono garanzie di un corretto funzionamento di tali servizi (specie nel caso del fisso, ma anche nel mobile in caso di nuovi sistemi operativi).

Una Società ritiene necessario lasciare alle logiche del libero mercato l'offerta di ulteriori componenti opzionali ai SCP.

Due associazioni di consumatori credono necessario che sia espressamente vietata la fornitura del sistema stesso in bundle con altri servizi a pagamento, come antivirus, antimalware e antispam.

Due associazioni di genitori ritengono che dovrebbe essere concessa all'ISP la possibilità di fornire funzionalità più avanzate (non solo antivirus e simili) a pagamento, come ad esempio il tracciamento della navigazione, l'inibizione della navigazione in alcune ore, l'avviso automatico se il minore tenta di accedere a una risorsa bloccata, la lettura di SMS e messaggistica da parte del genitore mentre un'altra associazione di genitori chiede che venga assicurata la trasparenza per gli eventuali costi, al fine di garantire una scelta consapevole da parte dei genitori.

Sig. (OMISSIS): non favorevole.

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?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione e gli operatori partecipanti ((OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS), (OMISSIS)**)** ritengono unanimemente che non siano necessari ulteriori canali di assistenza rispetto a quelli esistenti. In particolare, una Società reputa che l'assistenza per l'utilizzo del filtro SCP debba essere fornita prevalentemente attraverso l'uso di canali digitali anche per maggiore sicurezza e tutela del cliente. Un'assistenza operativa che consenta, ad esempio di poter bloccare o impostare il parental control tramite richiesta al call center, o tramite assistente digitale, né che possa essere richiesto allo stesso assistente il codice PIN, renderebbe il sistema meno efficace. **Un operatore** fa presente che l'estensione di tutti gli attuali canali di assistenza anche ai SCP accrescerebbe ulteriormente i costi di gestione da parte degli operatori, soprattutto di quelli di medie e piccole dimensioni che, come è noto, sono meno strutturati rispetto ai "big". **Un operatore** evidenzia peraltro che la norma primaria non estende la gratuità dell'attivazione del SCP anche all'eventuale assistenza tramite call center.
Un' osserva che la fornitura, da parte dell'ISP, di applicativi installabili dall'utente sui propri dispositivi per il filtro di singoli contenuti non è una soluzione percorribile, in quanto l'ISP opera a livello di rete e non può certamente sostituirsi al costruttore del dispositivo.
Un'associazione di consumatori di contro ritiene che sia necessario garantire agli utenti da parte degli ISP la possibilità di reperire facilmente informazioni sulla configurazione, attivazione e disattivazione dei SCP nonché l'assistenza gratuita tramite call center e altri canali già previsti per il customer care ed esorta l'Autorità a prevedere un unico sistema di gestione indipendentemente dal fornitore e dal dispositivo utilizzato, chiedendo anche che sia prevista una guida operativa sul SCP sottoposta alla preventiva approvazione dell'Autorità e disponibile sul sito web dell'operatore. Ritiene poi opportuno introdurre l'obbligo per gli

operatori di condurre periodiche campagne di comunicazione al fine di informare i consumatori della disponibilità della guida stesse e delle modalità di assistenza attivate.
Mentre **un'associazione di genitori** crede non convenga gravare ulteriormente gli ISP, **un'altra** chiede che venga assicurata l'assistenza tramite chat sul sito dell'operatore, in quanto modalità intuitiva, semplice e tendenzialmente veloce di contatto.
Un'associazione di genitori ritiene necessaria l'attivazione di un call center con operatore umano e con la previsione di un numero dedicato e la creazione sul sito dell'ISP di una pagina di FAQ e/ un servizio di risponditore automatico.
Sig. (OMISSIS) ritiene sia necessario prevedere un sistema di assistenza tramite e-mail per garantire di diritti degli utenti disabili (audiolesi).

Q7 – L'ASSISTENZA FORNITA ATTRAVERSO IL CALL CENTER RELATIVA AI SCP DOVREBBE AVERE UN NUMERO DEDICATO?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione ritiene che un eventuale call center per il SCP dovrebbe essere a pagamento con tariffazione premium.

Alcuni operatori non ritengono si debbano prevedere altri canali di assistenza né altri numeri dedicati se non quelli già previsti dagli operatori per l'assistenza alla clientela mentre **un operatore** ribadisce che l'assistenza per l'utilizzo del filtro SCP debba essere fornita prevalentemente attraverso l'uso di canali digitali, lasciando l'utilizzo del call center come via residuale di interazione.

Un operatore fa presente che l'estensione di tutti gli attuali canali di assistenza anche ai SCP accrescerebbe ulteriormente i costi di gestione da parte degli operatori.

Un altro operatore ritiene che la norma primaria non estenda la gratuità dell'attivazione del SCP anche all'eventuale assistenza tramite call center e che la fruizione da parte dei clienti finali dei SCP e, quindi, le possibili innumerevoli richieste di attivazione e disattivazione dei medesimi, comporterebbe un eccessivo aggravio lavorativo nel caso di utilizzo del canale tramite call center.

Un'associazione di consumatori ritiene che il servizio di assistenza clienti debba includere almeno un canale telefonico gratuito dedicato e un canale digitale sul sito web dell'operatore che dal punto di vista qualitativo debba rispettare i medesimi criteri previsti per l'assistenza clienti dei servizi di comunicazione elettronica.

A favore dell'attivazione di un call center con operatore umano e con la previsione di un numero dedicato sono due associazioni di genitori, mentre altre due ritengono in alternativa sufficiente garantire la possibilità di scelta di quel tipo di supporto, al primo livello di risposta

automatica, eventualmente aggiungendo sul sito dell'ISP anche una pagina di FAQ e/ un servizio di risponditore automatico.

Sig. (OMISSIS): no

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?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione riporta che sulla base dell'attuale prassi, i resolver DNS forniti dall'ISP consentono di inibire l'accesso a determinati siti, riconducibili alle più comuni categorie di filtro parentale, individuati dall'ISP, eventualmente avvalendosi di soluzioni tecniche di terze parti. Non esistono dunque, allo stato, dei criteri di classificazione condivisi tra gli ISP, né una lista comune dei siti web/applicazioni che possono includere contenuti inappropriati o comunque riservati ad utenti di età superiore agli anni 18. I siti non sono individuati da ISP, visto che questi non operano come master nel filtraggio dei contenuti. Soluzioni di terze parti classificano i siti in base a metriche e consentono di bloccare i siti appartenenti a determinate classificazioni. Tipicamente non esiste poi la classificazione VM18 ma i siti vengono classificati sulla base di categorie individuate per contenuto (a titolo esemplificativo: alcool e tobacco, e-commerce, social, advertisement, entertainment, adult, gambling, politics, online games, etc.). Inoltre, il *resolver* DNS potrebbe consentire di attivare funzionalità di filtro anche nelle ricerche effettuate mediante Google, Bing e Youtube. Fermo quanto sopra, il blocco mediante resolver DNS è applicabile all'intero sito e non ad uno specifico contenuto. Il filtro mediante resolver DNS può risultare a volte inefficace, in quanto aggirabile

utilizzando, ad esempio, DNS over HTTPs (DoH). Di frequente i browser consigliano l'utilizzo di DoH per rendere privata la navigazione a tutela della privacy dell'utente. La porta impiegata per il DoH è inoltre quella standard (443) e bloccarla significherebbe inibire indistintamente tutto il traffico "https". Poiché né i browser né le applicazioni sono sotto il controllo dell'ISP, una soluzione tecnica già implementata da alcuni browser (ad es., Mozilla) è quella di verificare se il filtro delle ricerche di Google, Bing o Youtube è attivo, e, in caso positivo, il browser disattiva automaticamente il DoH per quel device. Con riferimento alla pagina web di reindirizzamento, fornita dall'ISP, in cui viene spiegato all'utente minorenne che non può accedere a quel contenuto poiché considerato inappropriato per la sia età o riservato ad un pubblico maggiorenne, si osserva che tale reindirizzamento non è tecnicamente possibile nel caso in cui la pagina richiesta dall'utente sia criptata. Se la pagina in questione è in formato HTTPs non è infatti garantita la possibilità di visualizzare la pagina di blocco, posto che dipende dal settaggio dell'encryption del sito richiesto e dallo specifico browser usato dall'utente, nessuno dei quali è sotto il controllo dell'ISP. La stessa pagina non può essere indirizzata al singolo utente a seconda che questo sia di minore o maggiore età: è una pagina di blocco che spiega che il sito è bloccato per le regole di navigazione impostate e il DNS non ha modo di avere accesso all'età dell'utente; il funzionamento è più rudimentale: applica il blocco se configurato in tal senso.

Un'altra associazione ritiene che tecnicamente i blocchi DNS e/o IP si siano rivelati efficaci per la gestione del filtraggio di liste generali per l'utenza *at-large*. Per il SCP il filtro dovrebbe essere posto, sia per motivi di scalabilità, sia per ragioni di conformità alla normativa sul trattamento dei dati personali in relazione all'individuazione dei contenuti da bloccare, all'interno del CPE o altro apparato o software in casa cliente e sotto lo stretto controllo dell'utente. Evidenzia, però, che servizi DNS non conformi alla normativa nazionale vengono già messi a disposizione anche da OTT, sia attraverso il meccanismo tradizionale del DNS canonico, sia attraverso forme più innovative come il DoHs permettendo di aggirare i filtri richiesti agli operatori dallo Stato. Raccomanda pertanto che nelle liste generaliste di blocco vengano inclusi questi servizi.

Un operatore è favorevole all'adozione di una soluzione tecnica che prevede l'implementazione di blocchi DNS ai fini dell'implementazione dei SCP. Per quanto attiene alla differenziazione degli obblighi in funzione della dimensione dell'operatore, un operatore ritiene che questa previsione sia non giustificata, eccessiva nonché contraria alla previsione della normativa primaria.

Un altro operatore ritiene che, alla luce anche del proliferare dei siti internet su base minutaria, una funzionalità di blocco mediante DNS sia più adatta a perseguire le finalità in materia di tutela del diritto d'autore. Ricorda inoltre che per il blocco in conseguenza di opere

digitali in violazione del diritto d'autore tale disabilitazione, gestita manualmente, viene applicata su tutto il traffico di rete generato del prestatore di servizi senza alcuna targhettizzazione in base alla tipologia di clientela.

Un operatore ritiene che la progettazione del sistema debba essere definito nell'ambito del tavolo tecnico. Tuttavia, mette in evidenza la possibilità da parte del minorenne di bypassare controlli attivati su DNS sia attraverso la configurazione di un DNS di altra parte (e.g. Google 8.8.8.8) oppure tramite l'uso di strumenti, anche sofisticati, ma comunque disponibili sul mercato come VPN o Browser TOR. Si aggiunge inoltre che blocchi basati su indirizzi IP necessiterebbero di meccanismi in real time di aggiornamento degli indirizzi da bloccare, cosa di cui oggi l'Operatore non dispone.

Un altro operatore, in linea di massima, ritiene che l'implementazione di blocchi a livello di DNS, con "redirect" su una pagina di cortesia, rappresenti la soluzione più efficace ed efficiente per rendere operante l'obbligo sancito dal DL. Come peraltro chiarito in premessa dalla stessa Autorità, il tema cruciale è, tuttavia, quello relativo alla concreta identificazione dei contenuti da bloccare che, in ossequio alle norme di matrice Europea sul commercio elettronico (c.d. principio del *mere conduit*), non può in alcun modo competere all'Internet Service Provider ("ISP"). Pertanto, fermo restando che agli ISP spetterà la messa a disposizione delle funzionalità tecniche di blocco/sblocco all'utenza in accordo alle linee guida, risulta essenziale che ad indicare agli ISP le lista di siti/contenuti da rendere inaccessibili (salvo sblocco) sia un soggetto terzo, al quale competerà anche la manutenzione costante di tale lista. La lista e le relative modifiche dovranno, inoltre, essere redatte con formati, veicolate con canali ed espletate con tempi utili agli ISP per garantire il corretto funzionamento del meccanismo in favore dell'utente finale. Si precisa, inoltre, che, stante la complessità della catena del valore nel comparto delle comunicazioni elettroniche, l'operatore che intrattiene il rapporto contrattuale col cliente finale potrebbe non disporre del controllo di tutte le leve tecniche necessarie per una completa implementazione degli strumenti qui in discussione, necessitando della collaborazione degli operatori più a monte nella catena del valore e risultando, quindi, vincolato dai tempi e dalle modalità implementative scelte da questi ultimi.

Un operatore ritiene che sussistano criticità di natura tecnica relative all'implementazione dei blocchi DNS in quanto il blocco mediante resolver DNS forniti dall'ISP è applicabile all'intero sito - spesso utilizzando soluzioni tecniche acquistate da soggetti terzi che fanno una classificazione in base alla tipologia di contenuto - e non ad uno specifico contenuto. Allo stato attuale, tra l'altro, non risulta che siano stati individuati criteri di classificazione condivisi tra gli ISP e non esiste una lista comune dei siti web e applicazioni che includa contenuti inappropriati o comunque non accessibili ai minori. Si evidenzia, inoltre, che il

blocco mediante resolver DNS ad uno specifico contenuto non sarebbe applicabile in quanto comporterebbe complessità operative e di omogeneità delle soluzioni router/CPE. Si fa, altresì, presente che la pagina web di reindirizzamento fornita dall'ISP "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" non sarebbe tecnicamente attuabile qualora la pagina richiesta dall'utente fosse criptata; inoltre non potrebbe comunque trattarsi di una pagina indirizzata al singolo utente minorenne, in quanto il DNS non può essere a conoscenza di quale tipologia di utente stia navigando (se minorenne o maggiorenne), per cui applica il blocco se questo è configurato.

Un'associazione di consumatori, premettendo di condividere la prospettata integrazione della funzionalità minima di blocco mediante DNS, dei siti ospitanti contenuti oggetto di filtro, al momento non riscontra criticità relative all'implementazione della stessa.

Una Società ritiene che il meccanismo di filtro tramite DNS, pur essendo attualmente la migliore tecnologia disponibile, venga descritto nel testo in maniera troppo semplice e richiedendo funzionalità che tecnicamente non possono essere sempre disponibili, o talvolta non sono proprio realizzabili. In particolare, segnala che i resolver DNS forniti dall'ISP non vengono necessariamente "automaticamente installati quando la connessione è attivata". La maggior parte dei router o dei CPE permettono all'utente di indicare resolver DNS diversi da quelli dell'ISP, che vengono poi comunicati ai dispositivi quando vengono connessi alla rete; inoltre, la maggior parte dei sistemi operativi e dei dispositivi permettono all'utente di configurare resolver DNS diversi da quelli indicati dalla rete, compreso un resolver DNS installato dall'utente stesso sulla propria rete (es. PiHole). Infine, recentemente anche i browser hanno iniziato a permettere all'utente di indicare un resolver diverso da quello dell'ISP, collegandovisi tramite il protocollo cifrato DNSover-HTTPS, progettato appositamente per nascondere il traffico DNS all'interno del traffico Web e renderne impossibile il blocco; alcuni browser suggeriscono anzi attivamente all'utente di utilizzare questa funzionalità per proteggere la propria privacy ed evitare qualunque forma di "censura", ed è possibile che in futuro questa funzionalità venga attivata di default all'installazione del browser. Per quanto indubbiamente la maggior parte degli utenti domestici (si stima almeno il 70-80 per cento) utilizzi al momento l'ISP del proprio provider, l'ISP non può essere ritenuto responsabile dell'eventuale azione dell'utente volta a utilizzare un DNS diverso per aggirare i blocchi, azione che l'ISP, specialmente in caso di uso di protocolli di comunicazione crittografati, non ha sostanzialmente modo di impedire (si veda anche la risposta alla domanda numero 12). Anche la seconda richiesta nel testo, quella di mostrare all'utente minorenne una pagina di spiegazioni, non è tecnicamente realizzabile nel momento in cui l'utente stia tentando di effettuare una connessione Web cifrata (HTTPS), come avviene oggi nella quasi

totalità dei casi. Tale connessione prevede infatti che il browser verifichi l'identità del server a cui si sta connettendo, tramite l'esibizione da parte del server di un certificato crittografico firmato da una autorità riconosciuta (Certification Authority). Nel caso in cui, come richiesto dal testo, l'ISP utilizzi il sistema DNS per redirigere la connessione su un proprio server e mostrare a quell'indirizzo un qualsiasi messaggio, il browser dell'utente bloccherà la connessione; l'ISP, infatti, non ha modo di ottenere un certificato valido per un sito Web che il browser associa a un dominio che non è di sua proprietà. L'unico modo affinché l'ISP possa mostrare una pagina d'errore che venga accettata dal browser è quello di installare sul dispositivo una Certification Authority aggiuntiva, gestita dall'ISP stesso, che gli permetta di realizzare in proprio certificati per domini che non possiede; questa modalità, peraltro tecnicamente complessa e potenzialmente foriera di questioni legali, viene talvolta utilizzata in ambiti (es. reti aziendali) in cui è possibile garantire l'installazione di questa autorità aggiuntiva su tutti i dispositivi connessi alla rete, ma non è realisticamente adottabile in ambienti domestici o comunque aperti alla connessione di nuovi dispositivi; inoltre, essa apre potenziali e molto significativi problemi di sicurezza in caso di compromissione o abuso della nuova autorità di certificazione. Esistono a livello di organismi di standardizzazione diverse proposte tecniche per permettere ai browser di mostrare un messaggio d'errore anche in presenza di comunicazioni cifrate; tuttavia, al momento esse non sono state ancora approvate e i produttori di browser non hanno mostrato interesse alla loro implementazione, ritenendole fonti di potenziali problemi di sicurezza e comunque parte di un tentativo di "censura" alla libertà della rete. Si suggerisce dunque all'Autorità di iniziare una interlocuzione con le società produttrici dei browser più usati (Google, Apple, Microsoft, Samsung e Mozilla) per discutere con loro, con gli ISP e con i vendor DNS una possibile soluzione tecnica per ottenere quanto descritto nel testo, e in particolare per implementare le proposte tecniche mirate a permettere la visualizzazione di un messaggio d'errore adeguato e personalizzabile quando il server DNS blocca l'accesso a un contenuto, e quelle per acquisire e utilizzare automaticamente i server DNS dell'ISP a cui si è attualmente connessi anche nel caso in cui il browser voglia adottare connessioni cifrate (DNSover- HTTPS).

Un'associazione di genitori sottolinea che il problema principale è impostare il server di risoluzione nell'apparato dell'utente: se si tratta di un modem fornito dall'operatore, non è un problema. Se l'utente usa un proprio modem o ha accesso alla configurazione del modem dell'operatore, sarà compito suo impostarlo. Poiché è suo interesse proteggere la navigazione dei minori, si prenderà la responsabilità della sua impostazione. Per evitare l'aggiramento del DNS filtrato attraverso la semplice modifica dell'impostazione nel singolo computer, sarà necessario poter bloccare le richieste alla porta 53 come d'altronde specificato nel punto 6.

Un'altra associazione di genitori ritiene che l'affermazione "i resolver DNS (Domain Name System), forniti dall'ISP e automaticamente installati quando la connessione è attivata" non sempre corrisponde alla realtà, perché l'utente può installare un proprio modem e quindi configurare la connessione autonomamente. Perciò, se è interesse dell'utente proteggere la navigazione dei minori, dovrà impostare il resolver DNS indicato dall'ISP. In tutti i casi, per evitare il semplicissimo aggiramento del DNS filtrato, il modem dovrebbe prevedere la possibilità di bloccare almeno le richieste alla porta 53. Non sembra ragionevole affrontare tutti i metodi di aggiramento e cercare di bloccarli con configurazioni speciali. Ribadisce il ragionamento già fatto esplicitandolo con un'altra analogia: il bambino può togliersi da solo la cintura di sicurezza in auto ma non per questo la blocchiamo con una chiave.

Sig. (OMISSIS): SI. Qualunque blocco DNS può essere scavalcato cambiando server DNS, CON UNA VPN, oppure chiedendo all'amico l'indirizzo IP di quel sito, per poi aggiungere all'interno del file /etc/hosts (è un esempio, specifico dei sistemi operativi a matrice unix) del proprio sistema operativo il nome di dominio e il relativo indirizzo IP dato dall'amico.

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?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione evidenzia che, ponendo come proposto il filtro in casa cliente, il titolare dell'abbonamento può gestire in piena autonomia lo sblocco temporaneo e selettivo.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Un operatore non condivide la proposta di AGCom di prevedere funzionalità aggiuntive/opzionali ai SCP né la proposta della suddivisione in fasce degli operatori. L'intervento regolamentare nei termini sopra descritti appare eccessivo oltre che discriminatorio. Secondo un operatore la norma primaria fa riferimento ad all'obbligo di fornire un SCP. In tal senso dovrebbe essere lasciato alla volontà di ciascun operatore di offrire al cliente un sistema più articolato che, in aggiunta alle funzionalità di base (di per sé sufficienti ad assicurare la compliance con la norma primaria), preveda anche altre caratteristiche (ad es. blocco per fasce orarie, per singole categorie di contenuti, etc.). In tal modo, si avvierebbe un circolo virtuoso in cui gli SCP diventerebbero un elemento competitivo della proposizione commerciale di ciascun operatore in grado di orientare le scelte dei clienti più attenti alla presenza di tali funzionalità.

Un operatore ribadisce che l'attuale sistema di blocco su base DNS utilizzato in materia di violazione di diritto d'autore viene gestito manualmente e soprattutto la disabilitazione del sito internet avviene su tutto il traffico di rete generato dai clienti del prestatore di servizi senza alcuna distinzione rispetto alla tipologia di clientela. A suo avviso, quindi, risulterebbe impossibile effettuare una gestione di sblocco temporaneo e prevedere metodologie di autenticazione per la richiesta di blocco o sblocco dei contenuti da parte del singolo cliente.

Un altro operatore ritiene tale funzionalità estremamente critica e comunque esterna al perimetro di legge che richiede soltanto attività di filtro e di blocco. La previsione di uno sblocco temporaneo all'accesso per i siti web appare in prima analisi molto critica, in quanto assume una notevole complessità anche l'autenticazione del soggetto titolato a richiedere lo sblocco. È necessario implementare a monte un meccanismo di riconoscimento del Cliente per consegnare le chiavi di autenticazione al maggiorenne ed essere certi che non è il minorenne a riceverle, anche con procedure online di assegnazione e di recupero in caso di smarrimento con meccanismi di riconoscimento simili a quelle implementate dagli istituti di pagamento.

Un operatore ritiene che, ai fini dell'attuazione dell'obbligo previsto dal DL, la prestazione di blocco nella formulazione commentata in riscontro al Q8 risulti del tutto sufficiente. Le prestazioni aggiuntive ipotizzate dall'Autorità, per quanto interessanti nell'ottica dell'utenza, dovrebbero pertanto essere qualificate come opzionali per il gestore e potenzialmente oggetto di un corrispettivo applicato all'utenza. Qualora l'Autorità decidesse comunque di sancire tale obbligo nella forma più estesa, non potendo il DL costituire in pieno una base giuridica solida per tale iniziativa, si dovrebbe, secondo il medesimo, rinvenire una diversa base giuridica e valutarne la compatibilità col quadro normativo europeo, in particolare col Regolamento sull'Open Internet. Sul piano tecnico, la possibilità di disattivare temporaneamente l'accesso ai contenuti bloccati comporta un impatto elevato non solo in

merito alla soluzione tecnica da implementare ma anche per la realizzazione di un'interfaccia utente che permetta di fornire quanto richiesto. Tale requisito, infatti, non permette di basarsi su di una soluzione "DNS based", che invece rappresenta la soluzione migliore per rendere operante l'obbligo sancito dal DL.

Un operatore conferma che l'implementazione di un sistema di sblocco temporaneo all'accesso per i siti web richiederebbe un effort economico eccessivo per gli operatori, soprattutto di piccole e medie dimensioni, in considerazione dei costi di acquisto, sviluppo, integrazione e gestione che andrebbero sostenuti.

Un'associazione di consumatori propone il medesimo metodo di autenticazione già descritto nella risposta al Quesito 4

Una Società ribadisce quanto discusso nella risposta precedente, la criticità maggiore è relativa all'impossibilità tecnica di mostrare una pagina d'errore. Nel momento in cui tale criticità venisse risolta, sarebbe anche possibile realizzare una modalità di sblocco. Si ritiene tuttavia preferibile che lo sblocco avvenga mediante modifica della lista di bloccaggio del singolo utente, cosa che il titolare del contratto potrebbe realizzare dalla normale interfaccia di amministrazione, secondo le modalità di autenticazione già implementate per tale accesso; potrebbe dunque essere sufficiente richiedere che la pagina mostri le necessarie istruzioni o contenga un link all'interfaccia stessa.

Tre associazioni di genitori ritengono che il metodo di autenticazione più idoneo sia uno equivalente a quelli indicati in risposta al Q4. **Una di queste** aggiunge che l'autenticazione potrebbe essere eseguita tramite SPID o con credenziali di accesso ad un account già verificato, unitamente all'invio di una OTP. In quest'ultimo caso, a maggior ragione, non dovrebbe essere considerato idoneo l'invio dell'OTP tramite SMS al dispositivo sul quale è avvenuta la richiesta di accesso al sito web bloccato. **Un'altra** aggiunge che lo sblocco temporaneo potrebbe essere una funzione aggiuntiva a pagamento perché parte di un pacchetto di opzioni che il fornitore internazionale offre all'ISP. Nel panorama attuale di sistemi di filtraggio c'è molta varietà e costi molto diversi. L'esperienza di quest'ultima associazione è molto positiva con OpenDNS (anche nella versione gratuita per famiglie) che fornisce molti strumenti di configurazione. ISP come un operatore si appoggiano al filtraggio di Akamai del quale non sono disponibili al pubblico le caratteristiche.

Sig. (OMISSIS): Sì, perché rompe HTTPS in quanto risponde un server diverso da quello che il browser si aspettava, e verrebbe mostrata una pagina di errore HTTPS. Per lo sblocco temporaneo il modo più idoneo è usare lo SPID in quanto si applica a tutti gli utenti maggiorenni in casa.

Q10 – SI REPUTA PROPORZIONATA LA DISTINZIONE DEGLI OPERATORI (ISP) IN FASCE COSÌ COME PROPOSTA?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione propone di conteggiare solo gli utenti residenziali e differenziare le fasce, anche in analogia ai tagli individuati per le fasce contributive che determinano la quantificazione degli oneri ministeriali per l'ottenimento e il mantenimento delle autorizzazioni alla fornitura di servizi di comunicazione elettronica nel seguente modo: Fascia A >1.000.000 utenti, Fascia B > 50.000 utenti e inferiore o uguale a 1.000.000, Fascia C resto del mercato < o = 50.000.

Un operatore, per quanto attiene alla differenziazione degli obblighi in funzione della dimensione dell'operatore, ritiene che questa previsione sia non giustificata, eccessiva nonché contraria alla previsione della normativa primaria.

Un altro operatore evidenzia che misure ultronee o diversificate a seconda della dimensione dell'operatore, non rientrano negli obiettivi del quadro normativo di riferimento e rischiano anzi di determinare situazioni di over-regolamentazione o situazioni di minore protezione non giustificabili. Ritiene pertanto, che non si debbano operare distinzioni in base alla dimensione dell'operatore.

Un operatore non ritiene che le prescrizioni regolamentari debbano essere distinte per fasce di operatori basate sul numero di clienti. La differenziazione di obblighi in funzione del numero di clienti dell'operatore pone diverse criticità, con effetti in grado di alterare la competizione tra gli operatori in quanto una parte della clientela potrebbe essere orientata a scegliere operatori sottoposti a minori vincoli. Si avrebbero infatti diverse user experience in funzione dei diversi obblighi imposti alle diverse fasce di operatori, che potrebbero sia disorientare la clientela sia fornire garanzie diverse ai clienti di operatori di diverse fasce, mentre le garanzie di tutela dei minori dovrebbero essere le stesse per tutti gli utenti indipendentemente dal provider prescelto. Pertanto, ritiene che gli obblighi dovranno essere gli stessi per tutti i fornitori di accesso ad Internet, e non differenziate secondo alcun criterio, men che meno quello legato al numero di clienti.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Un operatore, nel rispondere alla domanda Q10, fornisce in uno la risposta anche alle domande Q13 e Q15, dichiarando che: la distinzione degli Operatori (ISP) in fasce, così come proposta nello Schema, non risulta proporzionata, presenterebbe notevoli criticità. In particolare, si rileva che la prospettata previsione di obblighi differenziati per gli ISP (i quali a seconda della fascia di appartenenza dovrebbero implementare SCP differenti) comporterebbe:

i) in primo luogo, una sostanziale violazione dell'obbligo di non discriminazione degli utenti finali che, oltre a costituire un obiettivo generale della regolamentazione ai sensi dell'art. 4, D.Lgs. 259/2003, è stabilito con specifico riguardo alla fornitura dei servizi agli utenti finali dall'art. 2, comma 12, lettera c) della Legge 481/1995. Infatti, gli utenti degli ISP avrebbero diritto a SCP più o meno avanzati e penetranti solo in base alla "grandezza" dell'operatore da loro scelto per la fornitura di servizi di comunicazioni elettroniche, fisse o mobili che siano. Ciò comporterebbe una grave discriminazione per gli utenti degli ISP di fascia B o C, i quali sarebbero di fatto titolati ad una "classe" di tutela svantaggiata;

ii) in secondo luogo, un significativo squilibrio concorrenziale per gli ISP stessi, poiché quelli appartenenti alle fasce B e C potrebbero essere considerati dall'utenza come "non sicuri", e quindi risentire dello standard di tutela più elevato garantito dagli Operatori più grandi, mentre quelli appartenenti alla fascia A dovrebbero sostenere costi di implementazione dei SCP sensibilmente più elevati e non proporzionati rispetto allo standard minimo presente sul mercato.

Stante quanto sopra considerato, è evidente a parere del rispondente che, al fine di raggiungere fattivamente l'obiettivo di tutelare l'utenza minorenne tramite l'implementazione di SCP, sia necessario stabilire uno standard minimo di tutela comune a tutti gli ISP, senza distinzione alcuna, e lasciare eventuali misure ulteriori e di maggior tutela alla libertà imprenditoriale degli ISP stessi. Ciò anche al fine di evitare fenomeni di cd. "surfing" in cui l'utenza minore, per sfuggire a SCP più stringenti, migra verso Operatori che prevedono meno tutele.

Un altro operatore ritiene che, fermo restando quanto sopra argomentato in merito all'opportunità di far collassare i meccanismi di SCP sull'opzione di base (blocco DNS su base di lista fornita e aggiornata da soggetto terzo riconosciuto da AGCOM), laddove l'Autorità ritenesse comunque di prevedere meccanismi aggiuntivi (es. blocchi temporanei gestibili dall'utente), si ritiene corretto prevedere una differenziazione degli obblighi in funzione della dimensione dell'operatore. Ciò in quanto è necessario che vi sia proporzione tra l'impegno implementativo richiesto e la capacità operativa del gestore nell'ambito impattato (dipendente tipicamente dalla numerosità della base clienti gestita).
A riguardo, precisa che:

- La proposta di sagomare la griglia delle "fasce operatori" sulla base del modello costruito per la misurazione della qualità del servizio internet da postazione fissa appare condivisibile;
- Poiché le implementazioni tipicamente si differenziano tra le diverse tecnologie di accesso gestite dall'operatore (es. fisso e mobile), la posizione di un operatore attivo in più ambiti di servizio dovrebbe essere valutata separatamente in ciascun ambito: ad esempio, un operatore che gestisce 9.000 linee mobili e 9.000 linee fisse dovrebbe risultare in fascia C (<10.000) per entrambi i servizi e non essere considerato in fascia B (tra 10.000 e 100.000) in considerazione del valore ottenuto sommando le due *customer base* (nell'esempio 18.000), che sono però disomogenee;
- Poiché, per quanto argomentato in riscontro alla domanda Q1, le utenze non *consumer* dovrebbero essere escluse dal meccanismo di SCP qui discusso, si ritiene che il computo delle linee dell'operatore ai fini della sua classificazione nelle fasce debba essere effettuato avuto riguardo alle sole utenze interessate dalla normativa, vale a dire quelle *consumer*: ad esempio, un operatore che gestisce 9.000 linee *consumer* e 9.000 linee *business* dovrebbe risultare in fascia C, poiché ai fini del calcolo dovrebbero assumere rilievo le sole linee *consumer*, e non essere considerato in fascia B in virtù del valore ottenuto sommando (erroneamente) le due *customer base* (nell'esempio 18.000);
- Un'ulteriore operazione di decurtamento delle linee dovrebbe poi essere consentita con riguardo alle linee c.d. trafficanti (in quanto, ad esempio, non hanno effettuato alcuna connessione a internet nel corso degli ultimi 12 mesi).

Ad ogni modo, la soluzione di far collassare l'intero impianto di SCP sulla formulazione base (quella prevista per la fascia C), oltra a garantire una migliore aderenza all'impianto normativo generale (DL e citate norme Europee), può semplificare anche tali criticità attuative.

Un operatore condivide la suddivisione degli operatori in fasce, considerato che le stesse riflettono il numero di linee in capo a ciascun operatore e, dunque, di clienti da considerare ai fini della tematica in questione. Tuttavia, si ritiene che le soglie indicate in ciascuna fascia (A, B, C) non riflettano correttamente il contesto concorrenziale nazionale e andrebbero, pertanto, riformulate utilizzando come criterio le quote di mercato detenute dagli operatori.

Analizzando i dati dell'ultimo Osservatorio sulle Comunicazioni pubblicato da Codesta Autorità (n. 4/2021), emerge pertanto che un'equa ripartizione delle soglie potrebbe essere la seguente:

▪ operatori di grandi dimensioni in Fascia A → con più di 2.000.000 di linee dati attive;

▪ operatori di medie dimensioni in Fascia B → con minimo 100.000 e massimo 2.000.000 di linee dati attive;

▪ operatori di piccole dimensioni in Fascia C → tutti gli altri operatori.

La suddivisione proposta, ad avviso della Scrivente, terrebbe dunque conto del fatturato degli operatori ed eviterebbe dunque di applicare gli stessi obblighi previsti per gli operatori "Big" anche ad operatori di dimensioni minori. Come è noto, infatti, le tre menzionate categorie di operatori hanno strutture aziendali e risorse economiche molto diverse tra loro e, pertanto, in ottica di tutela della concorrenza, risulta necessario prevedere una differenziazione tra di esse, così da non rendere eccessivamente gravosa l'attuazione degli obblighi previsti.

Un operatore ha inteso rispondere in uno alle domande Q8, Q9 e Q10, dichiarando quanto segue: premessa la necessaria preventiva indicazione delle categorie di contenuti da porre sotto il controllo di un SCP, è utile ricordare che nessun sistema di protezione che operi attraverso un blocco dei contenuti è in grado di assicurare l'inibizione totale dell'accesso, in quanto per ogni tipo di filtro esistono meccanismi che possono essere utilizzati per aggirarlo. Condividendo un approccio alla gestione centralizzata, il blocco a livello di DNS su singolo cliente, risulta di difficile implementazione, dato che opera un blocco generalizzato per tutti i clienti che si "appoggiano" sullo stesso DNS e non permette allo stato attuale la gestione personalizzata. La Scrivente si riserva, tuttavia, la possibilità di effettuare uno studio di fattibilità che possa confermare gli sviluppi necessari per la messa in campo del requisito di blocco del DNS per ciascun utente.

Un'asssociazione di consumatori non ritiene opportuna la proposta suddivisione in fasce, fermo restando il diritto degli utenti alla parità di trattamento in relazione a qualsiasi aspetto del SCP, indipendentemente dall'operatore con cui è stato stipulato il rapporto contrattuale. Inoltre, se AGCom, analizzando l'impatto regolamentare, ritenga i costi di implementazione eccessivamente onerosi per gli operatori di fascia C, si suggerisce di prevedere un adeguato contributo di solidarietà da parte delle grandi e medie aziende verso i piccoli operatori.

Due associazioni di genitori: sì.

Un'associazione di genitori ritiene che la distinzione degli operatori in fasce, seppure risponda a considerazioni relative alla differente dimensione economica degli stessi, non debba tradursi in una conseguente eccessiva divaricazione dei livelli di tutela tra le diverse fasce di utenti sulle finalità.

Un'altra associazione di genitori considera che in questa sede conviene affrontare con realismo il tema dei costi per gli ISP. Sia che realizzino in proprio il SCP o li acquistino sul mercato internazionale, dovranno prevedere un numero di accessi al filtraggio per

dimensionare il sistema: non è lo stesso fornire il servizio a 10.000 utenti o a 1.000.000. A priori non sapranno quanti utenti lo attiveranno: potranno fare stime in base alle statistiche sociologiche delle famiglie, ma non è prevedibile la risposta degli italiani. Pretendere che un ISP dimensioni il servizio per tutte le proprie utenze è irragionevole: sarebbe un costo insopportabile e inutile. Non tutti i fornitori, a loro volta, avranno la flessibilità necessaria per ampliare o ridurre la dimensione del servizio di filtraggio, modulando opportunamente i costi. Riguardo al blocco degli indirizzi IP, la precisazione "nei casi in cui sia possibile un'associazione biunivoca tra gli stessi e l'indirizzo IP" implica un lavoro di verifica enorme e non sempre realizzabile da parte degli ISP. Per questo motivo riteniamo non ragionevole prevedere il filtraggio su base IP, tranne che per le casistiche già previste dalla legge (ad esempio, pedopornografia, scommesse estere non autorizzate in Italia). Riguardo al blocco delle porte usate da DNS e simili, richiederlo solamente agli ISP di fascia A non è equo e assolutamente non necessario. La medesima associazione ritiene importante non imporre agli ISP oneri inaccettabili e, di conseguenza, ottenere un rifiuto totale. È importante il dialogo con gli ISP di tutte e tre le fasce per raggiungere un accordo sui requisiti minimi applicabili da tutti senza gravami eccessivi.

Sig. (OMISSIS): direi di sì. Un sistema di questo tipo non dovrebbe costare troppo.

6. **Gli operatori di fascia A complementano le funzionalità di cui al punto 5, mediante 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. Attività di vigilanza e programma di lavoro per migliorare la qualità del servizio**

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.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Q11 – SI INDIVIDUANO ALTRE MODALITÀ DI FILTRAGGIO NON ELENCATE E CHE POTREBBERO ESSERE REALIZZATE?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione ribadisce che a suo avviso la soluzione basata sul CPE casa-cliente (o sul terminale mobile per le reti wireless) è la soluzione preferibile per ogni fascia in quanto segrega tutta la complessità e gli alti costi di una modifica peculiare delle architetture di edge e core dei vari operatori che non scalerebbero ad una granularità di personalizzazione per cliente. Ritiene inoltre essenziale che si impongano ai produttori di software che utilizzino meccanismi DNS over TLS o similari che bypassino il protocollo DNS standard, di impiegare indirizzi IP di risoluzione medesimi a quelli già identificati a livello di sistema operativo per il protocollo DNS standard.

Un operatore ritiene che si debba emendare interamente il punto di cui alle Linee Guida n.6, ritenendo di dover lasciare ampio margine discrezionale agli operatori circa l'individuazione del metodo più efficace di filtraggio rispetto allo scopo preposto. Una modalità di filtraggio, al fine di perseguire le finalità dettate al decreto-legge 28/2020, potrebbe essere quella di avvalersi di soluzioni tecniche di terze parti che svolgono attività di catalogazione dei siti internet, anche su base oraria, in base alla tipologia del contenuto e permettano anche alla clientela finale di decidere quali contenuti bloccare/sbloccare attraverso una semplice selezione degli stessi all'interno di un'area clienti. Lasciando agli operatori la facoltà di scegliere la modalità tecnica preferita in vista delle finalità da perseguire, verrebbe richiesto al mercato uno sforzo economico di minore impatto, nel rispetto del principio di massima efficienza dell'agere amministrativo e, in linea con la normativa primaria in materia che prevede soltanto un obbligo di messa a disposizione del filtraggio, lasciando agli operatori libertà nella definizione delle modalità operative più efficaci.

Un operatore non ha individuato modalità di filtraggio ulteriori da proporre.

Un altro operatore ritiene che, alla luce di quanto sopra argomentato, tali meccanismi risultino già esorbitare quanto disposto dal DL di cui in questa sede si discute l'attuazione. Pertanto, non si ritiene di dover aggiungere ulteriori meccanismi nel perimetro delle valutazioni.

Un altro operatore, in merito alla prima funzionalità aggiuntiva a): "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" osserva che gli indirizzi IP possono condividere più servizi ed essere dinamicamente cambiati senza che l'Operatore ne sia necessariamente a conoscenza. La Società nutre tuttavia forti dubbi che tale meccanismo possa fornire uno strumento robusto di filtro di contenuti, considerato il contesto in così rapida evoluzione, come quello delle piattaforme in cloud su Internet. In merito alla seconda funzionalità aggiuntiva b): "blocco delle porte utilizzate dai protocolli DNS e DNSover-TLS per le richieste inviate a server non appartenenti all'operatore", osserva che tale meccanismo non è attualmente standardizzato, e che tale richiesta dell'Autorità, senza un documento tecnico che certifichi che tale soluzione non produca problemi di interoperabilità su servizi, potrebbe rivelarsi fonte di problemi ai clienti finali. Si richiede che AGCOM coinvolga i diversi fornitori di smartphone e/o di terminali d'utente in generale e che standardizzi, a livello italiano, come tali blocchi debbano essere compatibili con le implementazioni degli OTT. In aggiunta esistono anche problemi di tutela del Consumatore per i quali un Cliente potrebbe pagare App o funzionalità, come per esempio iCloud Private Relay, facente parte del servizio Apple iCloud+, e non usufruire della stessa qualora abbia scelto di usare la VPN di Apple. In merito al punto c) relativo alla "fornitura [addirittura preinstallata per gli operatori di fascia A] di applicativi installabili dall'utente sui propri dispositivi per consentire il filtraggio dei singoli contenuti" ritiene che se si preinstalla la stessa funzionalità per tutti gli smartphone, sia per minorenni che per maggiorenni, si potrebbe configurare una discriminazione del canale Operatore sia rispetto al canale Open Market, sia rispetto ad altri Operatori, appartenenti a fasce diverse da quella del rispondente, poiché il filtraggio dei contenuti farebbe propendere la scelta di acquisto di un maggiorenne verso un altro Operatore.

Un operatore non individua ulteriori modalità di filtraggio da realizzare a livello DNS. Il blocco degli indirizzi IP di destinazione associati ai siti oggetto di filtro, nonché il blocco degli indirizzi IP di eventuali altri server DNS utilizzabili dall'utente per aggirare il blocco, non sono pratiche tecnicamente gestibili. Esse, infatti, dovrebbero prevedere una serie di configurazioni e policy su tutti gli apparati di rete, di natura automatica e dinamica: ammesso che possano essere supportate a livello infrastrutturale, dovrebbero venire automaticamente attivate e disattivate conseguentemente all'accensione/spegnimento dei servizi di filtro operati dall'utente finale. Esistono altre soluzioni sul mercato che, non filtrando il traffico DNS, sono agnostiche all'uso di protocolli come DNS-over-TLS e ad eventuali cambi di server DNS operati dall'utente. Tuttavia, anche queste soluzioni sono aggirabili facilmente, ad esempio attraverso l'uso di software VPN forniti gratuitamente sulla Internet.

Un'associazione di consumatori, pur considerando sufficienti le modalità di filtraggio indicate, ritiene che l'impiego di filtri basati direttamente sugli indirizzi IP sia da preferire, quando attuabile, ad un sistema DNS, poiché riduce drasticamente il rischio che i fornitori di contenuti possano by-passare il filtraggio stesso. A tale proposito si ribadisce la necessità di garantire la gratuità di ogni attività e funzionalità impiegata per SCP, compresi i sistemi aggiuntivi come antispam e antivirus.

Un'associazione di genitori suggerisce di prevedere una funzionalità di filtro per parole chiave, che blocca e/o monitora le ricerche nel browser per determinate parole chiave scelte dall'utente maggiorenne.

Un'altra associazione di genitori non ritiene opportuno ampliare la casistica per i SCP obbligatori.

Sig. (OMISSIS) ritiene assolutamente inefficace qualsiasi sistema per filtrare tutti i contenuti inadatti ai minori.

Q12 – SONO PRESENTI CRITICITÀ TRA LE SOLUZIONI TECNICHE ELENCATE?

OSSERVAZIONI DEI RISPONDENTI

Un'Associazione, con riferimento al *"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",* fa notare l'inefficacia di tale previsione posto che gli indirizzi IP sono soggetti a variazioni dinamiche che gli Operatori non soltanto non sono tenuti a verificare, ma che neppure conoscono, con la conseguenza che risulterebbe vanificata ogni strategia di blocco. Le implementazioni richieste, inoltre, dovrebbero calarsi nel contesto di mercato senza alterare le fisiologiche dinamiche competitive, posto che quand'anche ciascun Operatore fornisse i propri terminali con le ipotizzate limitazioni, l'utente potrebbe rivolgersi all'open market per ottenere così devices "liberi", con il duplice effetto sfavorevole di non tutelare l'utenza e di favorire impropriamente i produttori di terminali. Diviene pertanto condizione imprescindibile che l'Autorità garantisca parità di condizioni, assicurando che tutti i produttori di modem, router e smartphone, acquistabili dal cliente sul mercato, siano dotati delle medesime implementazioni hardware e software. Peraltro, se gli Operatori fossero tecnicamente in grado di apportare correttivi *real time* all'accesso da parte dell'utenza a determinati contenuti, occorrerebbe comunque tener conto del generalizzato divieto di controllo e verifica su quanto visionato dall'utenza, nel rispetto delle rigorose limitazioni poste dalla normativa a tutela dei dati personali oltre che dalla disciplina in tema di *net neutrality.* Con riferimento alla fornitura di un applicativo da installare sui dispositivi

utilizzati dai minori segnala che la fornitura, da parte dell'ISP, di applicativi installabili dall'utente sui propri dispositivi per il filtro di singoli contenuti non è una soluzione percorribile, in quanto l'ISP opera a livello di rete e non può sostituirsi al costruttore del dispositivo. Con riferimento a tale previsione, si ritiene opportuno lasciare ampio margine discrezionale agli operatori circa l'individuazione del metodo più efficace di filtraggio rispetto allo scopo preposto ancor di più se sono già disponibili sul mercato soluzioni efficaci volti a tutelare i minori.

Un'altra associazione riporta che le soluzioni proposte presentano elementi di criticità in relazione alla conformità alle normative comunitarie e nazionali di settore, ai costi soprattutto in relazione alle PMI più piccole e agli effetti anticoncorrenziali anche a livello comunitario. Inoltre, provocherebbero impatti sulla stabilità della rete internet e sulla fruibilità delle applicazioni e dei servizi, complicherebbero l'erogazione dei servizi di assistenza e identificazione guasti e aumenterebbero i rischi da sovrafiltraggio e le conseguenti responsabilità per gli ISP. Ribadisce che l'approccio da lei proposto di blocco su CPE lato cliente o terminale mobile consentirebbe di limitare le suddette problematiche.

Un operatore reputa non percorribile la proposta di effettuare il blocco/filtro su base IP. Innanzitutto, si pone un dubbio circa la validità dello strumento, cioè se il blocco dell'IP è funzionale all'obiettivo in esame. Ad uno stesso indirizzo IP possono infatti far capo differenti siti internet (URL) e non è sempre detto che tutti i siti interessati ricadano nella medesima categoria da bloccare tramite i SCP. Esiste quindi un rischio reale di travalicare l'obiettivo della norma, con una censura di internet più ampia rispetto a quanto necessario. In aggiunta, la soluzione sarebbe nei fatti non realizzabile poiché, per quanto di conoscenza, non esiste un fornitore di indirizzi IP organizzati per categorie da filtrare: ciò implicherebbe trasferire sull'ISP l'onere di individuare autonomamente gli IP dannosi, catalogarli, monitorarli nel tempo ed eventualmente bloccarli, aspetto che comporterebbe certamente un profilo di sorveglianza attiva da parte dell'operatore che la stessa Autorità ha escluso in radice, sulla base delle norme vigenti. Inoltre, il blocco di uno specifico IP è estremamente complicato da implementare e da gestire perché 'statico'. Ciò implicherebbe una gestione sostanzialmente manuale da effettuarsi sulla singola linea, fissa o mobile, che ha richiesto il blocco e non consentirebbe di seguire la variabilità dei siti dannosi oltre che la classificazione degli stessi. Per quanto concerne le altre proposte, secondo l'operatore, risulta tecnicamente non fattibile:

- impedire al cliente l'utilizzo di DNS terzi (i.e. Google) o DNS che offrono servizi DoT, DoH, in quanto l'operatore non può intervenire sul client del cliente, impedendogli di modificare il DNS e

- bloccare “le porte utilizzate dai protocolli DNS e DNS-over-TLS per le richieste inviate a server non appartenenti all’operatore”, in quanto l’operatore non può bloccare il traffico dei protocolli DNS over TLS verso DNS selezionati a livello applicativo sui device del cliente. A tal proposito si evidenzia che l’intervento sul DNS operato direttamente dal cliente implica conoscenze informatiche con ogni probabilità non comuni alla maggior parte della popolazione. In tal senso, fermo restando che, nel mondo internet nessuna tecnica informatica assicura la certezza di non essere bypassata, l’Autorità dovrebbe valutare nello specifico la probabilità che l’evento “modifica DNS/uso IP” si verifichi a fronte della certezza degli ingenti investimenti e delle complessità di gestione che richiederebbe un sistema di controllo basato su IP. Riguardo la proposta di installare un applicativo sul terminale dell’utente in grado di filtrare il contenuto, non appare chiara quale sia la finalità della proposta. Se l’obiettivo è spostare sul terminale gli stessi presidi di controllo parentale che sono oggi previsti a livello di linea, ciò implica una inutile duplicazione dei presidi che, in termini incrementali, non comporterebbe alcun miglioramento nell’efficacia dei SCP. Al contrario, si metterebbe in campo una soluzione facilmente eludibile dal minore tramite un semplice cambio di terminale (non venduto dall’operatore) e che implicherebbe un inutile dispendio di risorse per l’operatore per sviluppare l’APP per tutti i sistemi operativi e per tutti i devices disponibili. In aggiunta, tale misura introdurrebbe una discriminazione tra i terminali offerti dall’operatore e quelli disponibili sul libero mercato, che in ultima analisi si tradurrebbe in maggiori costi per gli operatori per quanto detto in precedenza, oltre che nell’offerta di una user experience diversa (a parità di marca di terminale), senza apportare, come detto, alcun beneficio incrementale in termini controllo parentale. Infine, relativamente alla proposta configurare il blocco per accesso tramite di applicazioni installabili sui dispositivi dell’utente, il medesimo operatore evidenzia che l’operatore non riserva un trattamento differenziato alla navigazione Internet a seconda che essa sia originata da browser o da APP. Ne deriva che le logiche di gestione del SCP fin qui descritte sono le stesse in entrambe le fattispecie.

Un operatore ribadisce come gli operatori, sia per gli indirizzi IP che per il blocco delle porte utilizzate dai protocolli, debbano ricevere delle indicazioni di dettaglio puntuali e costantemente aggiornate da parte dell’Autorità in quanto, in qualità di *mere conduit*, non svolgono alcuna analisi sul contenuto delle informazioni trasmesse tramite la propria rete. Inoltre, ricorda come una soluzione tecnica che preveda un blocco su base IP necessita di una continua e costante operatività che oggi non potrebbe essere in alcun modo garantita dagli operatori.

Un altro operatore, in merito al punto c) del paragrafo 6 delle linee guida poste a consultazione:

c) la fornitura di applicativi installabili dall'utente sui propri dispositivi per consentire il filtraggio dei singoli contenuti.

Tale soluzione appare di difficile attuazione in quanto, oltre a tutti i problemi collegati agli aspetti di definizione di tali applicazioni che dovrebbero essere sviluppate dai produttori di terminali d'utente piuttosto che dagli operatori ISP, si segnala che l'Operatore di Telecomunicazioni (ISP) non conosce ad oggi gli Indirizzi IP dei provider di VPN, di servizi di proxy o di servizi DNS, che in linea di principio possono anche cambiare nel tempo e richiedere quindi aggiornamenti periodici. In aggiunta, l'ISP non sa se in corrispondenza di un indirizzo IP è presente un solo servizio, es. DNS, o se sono presenti più servizi. In aggiunta, a conferma della difficoltà dell'implementazione richiesta, si prenda a titolo di esempio il browser TOR, https://blog.torproject.org/, nato con il seguente intento: "gli utenti Internet dovrebbero avere un accesso privato ad un web non censurato". Tale browser implementa una serie di tecniche estremamente sofisticate per permettere di aggirare le censure sulle Reti quando implementate dai Governi. In corrispondenza di meccanismi di blocco basati sugli Indirizzi IP, come quelli richiesti nella Consultazione, tale browser ha implementato come contromisura tecniche più sofisticate per offuscare il traffico e bypassare tali blocchi (https://blog.torproject.org/tor-heart-bridges-and-pluggable-transports/). Il ruolo di un Operatore è quello di mettere in comunicazione i Clienti, permettendo la raggiungibilità di tutti i punti terminali della rete internet e permettendo la libertà di scelta del terminale d'utente, come da regolamentazione 2015/2020 (Open Internet) non quello di studiare tutte le applicazioni disponibili sul mercato, analizzarne i protocolli e implementare tecniche volte a bloccare traffico progettato per aggirare le architetture standard di comunicazione.

Un operatore dichiara che le funzionalità sopra elencate, oltre a presentare le criticità di natura giuridica sopra ampiamente esposte, presentano altresì rilevanti criticità tecniche. In particolare: a) rispetto ai filtri IP, si ripropone la problematica esposta inizialmente relativa alla gestione della lista di indirizzi IP da bloccare. Le informazioni inserite nella stessa non possono essere scelte in maniera arbitraria dal singolo ISP ma è necessario identificare un ente terzo certificato che possa metterla a disposizione degli ISP e che ne garantisca l'aggiornamento; b) Rispetto al blocco DNS terzi, non potendosi intervenire su dispositivi di proprietà del cliente finale viene richiesto il blocco del traffico destinato a server DNS esterni alla rete dell'operatore tramite meccanismi di black-hole del traffico o, nel caso di blocco applicativo per servizi DoT e DoH, tramite l'introduzione di apparati in grado di discriminare il traffico da bloccare utilizzando meccanismi tipici delle azioni di DPI; c) Rispetto agli applicativi su dispositivo, non avendo l'ISP alcun controllo sui dispositivi utilizzati dall'utente in caso di mancata fornitura degli stessi, si ritiene che questa non sia un'opzione

percorribile, data l'impossibilità di individuare la presenza o meno di tali applicativi a bordo dei dispositivi.

Un operatore, in merito alle soluzioni tecniche elencate nel documento di consultazione, ritiene che: 1) l'eventuale blocco degli indirizzi IP non è tecnicamente fattibile su DNS; 2) Il blocco delle porte utilizzate dai protocolli DNS e DNS-over-TLS non può essere effettuato su DNS senza impattare la navigazione (porta TCP 443); 3) la fornitura di un applicativo a protezione dei device dei minori richiede una infrastruttura dedicata, l'acquisto di soluzioni e licenze ad hoc, nonché la pubblicazione di nuovi nodi (es. IP gateway) sulla internet con relativi impatti a livello di cybersecurity. Si tratterebbe, pertanto, di attività che richiedono costi non sopportabili e sproporzionati, soprattutto da parte di operatori di medie dimensioni che rientrano nella Fascia A identificata nel documento di consultazione.

Una Società ritiene che quasi tutte le soluzioni tecniche previste in questa sezione presentino significativi e insormontabili problemi sia tecnici che legali. A proposito della richiesta di aggiungere un blocco dell'accesso verso determinati indirizzi IP "associati ai siti oggetto di filtro, nei casi in cui sia possibile un'associazione biunivoca tra gli stessi e l'indirizzo IP", si segnala che questo requisito introdurrebbe la necessità sostanziale di duplicare il sistema di filtraggio dei contenuti, dato che il server DNS e il sistema di routing che gestisce il passaggio del traffico sono due componenti completamente separate e indipendenti dell'infrastruttura dell'ISP; sarebbe necessario realizzare un secondo sistema di controllo parentale a livello di routing. Inoltre, il sistema di routing generalmente non riconosce i singoli utenti e quindi il blocco si applicherebbe a tappeto a tutti gli utenti dell'ISP o perlomeno a tutti gli utenti dello specifico accesso Internet, minorenni e maggiorenni. A fronte di tutta questa complicazione, il guadagno in termini di efficienza dei filtri sarebbe comunque ridotto, in quanto i siti biunivocamente associati a un solo indirizzo IP sono generalmente pochi; oggi, la maggior parte dei siti utilizza sistemi di CDN (content delivery network) che prevedono la distribuzione di migliaia o milioni di siti dallo stesso indirizzo IP, che può peraltro cambiare ripetutamente anche in tempi molto brevi. Infine, dato che le liste di blocco vengono generalmente fornite sotto forma di lista di nomi a dominio, l'ISP dovrebbe determinare da solo quali di questi nomi a dominio corrispondono a indirizzi IP per cui sia possibile questa associazione biunivoca, operazione peraltro impossibile (non è possibile, dato un indirizzo IP, sapere con semplicità, certezza ed esaustività quali siano i siti Web ospitati sullo stesso) e soggetta comunque a continue correzioni (un minuto dopo il controllo, il nome a dominio può essere spostato altrove oppure possono essere aggiunti o tolti siti Web sullo stesso indirizzo IP). A proposito della richiesta di effettuare un blocco verso indirizzi IP "associati a server DNS", si segnala che la richiesta potrebbe forse essere realizzabile per una lista limitata di server DNS molto noti (8.8.8.8, 1.1.1.1 eccetera); tuttavia, non esiste una lista esaustiva di

tutti i server DNS esistenti al mondo, né è possibile impedire a chiunque di installarne uno e di renderlo accessibile a qualsiasi utente della rete. Si sottolinea comunque come la base legale per tale richiesta non sia affatto chiara, in quanto esistono molti motivi per cui un utente Internet possa voler accedere a server DNS diversi da quello del proprio provider, motivi non legati all'accesso a contenuti inadatti ai minori. Un blocco del genere andrebbe a colpire indiscriminatamente uno dei protocolli essenziali della rete Internet, restringerebbe significativamente l'usabilità della rete in generale, disturberebbe o interromperebbe servizi e applicativi che richiedono l'uso di server DNS propri e quindi non sarebbe considerabile come un sistema di controllo parentale previsto dal D.L. 28/2020; pertanto, in assenza di una solida base legale che autorizzi questo filtro, esso è presumibilmente incompatibile con il Regolamento 2015/2020. Infine, per la richiesta di "blocco delle porte utilizzate dai protocolli DNS e DNS-over-TLS" valgono le considerazioni appena esposte per la richiesta precedente; anche questa sarebbe una richiesta inefficace (in quanto nulla comunque vieta di offrire servizi DNS su porte non standard), estremamente invasiva, che andrebbe a colpire servizi e applicazioni del tutto scorrelati dall'accesso a Internet dei minori, e che quindi va ampiamente oltre quanto previsto dal D.L. e non pare compatibile con il Regolamento 2015/2020. Si richiede dunque di eliminare del tutto i punti a) e b) della sezione in esame e le relative richieste agli operatori. Si suggerisce invece che l'Autorità, se ritiene di dover evitare che l'uso di DNS non forniti da ISP italiani permetta l'aggiramento dei filtri, inizi una interlocuzione con le società fornitrici dei server DNS globali più noti e utilizzati in Italia (Google, Cloudflare, Cisco) per discutere la possibilità di preattivare i filtri parentali anche sui loro servizi quando essi ricevano richieste provenienti dal territorio italiano, permettendo poi agli utenti italiani di autenticarsi e disattivare i filtri se maggiorenni. Questa ipotesi, pur da verificare in termini tecnici e legali e probabilmente realizzabile soltanto in forma di accordo volontario con le suddette aziende, permetterebbe di affrontare il problema senza imporre restrizioni eccessive al normale utilizzo di Internet per tutti gli altri scopi. Più in generale, riteniamo che l'Autorità debba porsi il problema di garantire una equa concorrenza nella fornitura dei servizi DNS tra gli ISP nazionali e i grandi fornitori globali. Aggiungere sulle spalle dei soli ISP italiani requisiti tecnici sempre più complessi e costosi, lasciando liberi gli operatori globali di sottrargli gli utenti offrendo servizi non filtrati e libero accesso a content dell'industria Internet nazionale.

Un operatore ritiene più corretto che tutti gli operatori di servizi DNS per i consumatori, siano essi ISP o piattaforme globali, debbano sottostare alle stesse regole e agli stessi requisiti.

Un'associazione di genitori ritiene poco chiaro se la richiesta di fornitura di applicativo da installare implica l'obbligatorietà del suo utilizzo da parte dell'utente in apparati non forniti dall'operatore. Dovrebbe essere esplicitato che è lasciata all'utente l'opzione di una

protezione aggiuntiva per un controllo puntuale. Ribadisce che questa richiesta potrebbe trovare, in prima battuta, forti resistenze da parte degli operatori di fascia A: pertanto, sarebbe più ragionevole renderla opzionale per accelerare i tempi dell'adozione delle misure minime proposte.

Un'altra associazione di genitori ritiene che la criticità maggiore sia il costo per gli ISP.

Sig. (OMISSIS): decisamente si, come sempre la lista di server DNS è indefinita; il blocco a livello di porta è facilmente bypassabile cambiando la porta; il blocco a livello di IP con un altro indirizzo IP; traffico DoT non sono sicuro che sia individuabile; bloccare DoH significa al limite bloccare il traffico verso la porta 443 cioè tutto il traffico web. I controlli più evoluti richiedono un firewall SPI e quindi comportano un costo maggiore per gli ISP. Per quanto riguarda l'applicativo da installare sui dispositivi utilizzati dai minori c'è il problema di doversi fidare dell'operatore se il software stesso non sia software libero. Inoltre, potrebbe non essere disponibile per tutte le piattaforme e configurazioni (tipo su LineageOS senza microg...) (e come sempre bypassabile con le VPN).

Q13 – .SI REPUTA PROPORZIONATA LA DISTINZIONE IN FASCE COSÌ COME PROPOSTA IN RELAZIONE ALLE LINEE GUIDA DI CUI AI PUNTI 5 E 6?

Un'Associazione concorda con la suddivisione in fasce, condizionatamente alla sua modifica secondo quanto riportato in merito alla Q.10.

Un operatore reputa non pertinente effettuare una distinzione sulle metodologie di blocco da implementare a seconda della grandezza dell'operatore essendo la finalità che deve essere garantita quella di proteggere i minori.

Un altro operatore non ritiene condivisibile la classificazione degli Operatori in fasce. Un sistema di controllo parentale a protezione dei minori non può dipendere, nella sua semplice o articolata attuazione, dal numero di linee dati attive di un Operatore. La Società propone pertanto l'eliminazione della classificazione degli Operatori in Fasce e ogni differenziazione degli obblighi tra gli operatori.

Un operatore ritiene di aver già argomentato con quanto sopra.

Un altro operatore non riscontra criticità purché sia adottata la proposta formulata in risposta al quesito 10 con le relative soglie.

Un operatore ha inteso rispondere in uno alle domande Q11, Q12 e Q13, dichiarando quanto segue: la fornitura di applicativi installabili dall'utente sul proprio dispositivo, ai fini del

filtraggio dei singoli contenuti, non è un'attività che può essere richiesta all'ISP in quanto, operando esclusivamente a livello di rete, quest'ultimo non può sostituirsi ai fornitori dei device e/o delle eventuali app. Si ravvedono criticità anche laddove i sistemi di filtraggio/blocco fossero svolti a livello locale sui terminali forniti dall'operatore. Oltre l'eccessiva onerosità derivante da una reingegnerizzazione dei terminali stessi, sia in termini di hardware che di software, si ravvedono difficoltà legate alla diffusione di soluzioni alternative. Infatti, ove analoghi obblighi non fossero imposti anche ai produttori delle apparecchiature terminali di rete, l'applicazione di sistemi di blocco/filtro a livello locale potrebbe tradursi in una indiretta restrizione del diritto del cliente al c.d. "modem libero".

Un'associazione di consumatori, analogamente a quanto già esposto nella risposta al Quesito 10 e considerando pertanto il diritto degli utenti alla parità di trattamento in relazione all'operatività del SCP indipendentemente dall'ISP, non si ritiene opportuno limitare l'obbligo di fornire le funzionalità complementari ai soli operatori di fascia A.

Un'associazione di genitori: sì.

Un'altra associazione di genitori ritiene che la finalità degli interventi non possa che essere quella di mettere a disposizione di tutti i genitori, e degli adulti in genere, indipendentemente dall'operatore di riferimento un sistema di tutela dei minori da contenuti inappropriati agevole da utilizzare e supportato da modalità accessibili di assistenza.

Un'altra associazione di genitori dichiara che non conviene distinguere in fasce gli ISP: è preferibile imporre a tutti gli stessi obblighi minimali. Quelli di fascia A saranno in grado di aggiungere, con costi molto bassi per l'utente, come già avviene, servizi aggiuntivi di protezione. Per essere più espliciti, un ISP con milioni di utenti può far pagare un solo euro al mese e incassare la cifra sufficiente per fornire servizi avanzati. Invece un ISP con centinaia di utenti non potrà permetterselo con quelle tariffe. Tuttavia, per l'ISP di fascia A non è indifferente far pagare zero invece di uno: dovrebbe investire milioni di euro a fondo perduto.

Sig. (OMISSIS): sì.

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?

OSSERVAZIONI DEI RISPONDENTI

Un'Associazione reputa che l'obbligo di imporre all'ISP la memorizzazione di tutti gli accessi effettuati o solo quelli bloccati mediante DNS appare del tutto sproporzionato, in ragione dell'enorme quantità di dati che l'ISP dovrebbe archiviare per ciascun utente e senza considerare il fatto che tale attività inficerebbe le performances del DNS.

Un'altra associazione rileva che a suo avviso i requisiti indicati non sono previsti per legge e le linee guida sono viziate da eccesso di potere.

Un operatore, per quanto attiene infine la tracciabilità dei siti visitati, riporta che ad oggi monitora unicamente la numerosità degli eventi di blocco, ma non memorizza i siti visitati e non conserva lo storico di navigazione, sia per motivi di privacy sia per motivi tecnici, legati ai dimensionamenti tecnologici necessari per lo storage.

Un operatore ritiene che il filtro SCP debba essere configurato, in linea con il quadro normativo vigente, come un filtro che abbia la sola funzione di bloccare/sbloccare l'accesso ai contenuti riservati a maggiorenni e che il responsabile "amministratore" dello stesso può scegliere di abilitare o disabilitare. Per tutte le funzioni aggiuntive, deve essere lasciata piena autonomia agli operatori di fornire (come alcuni già forniscono) sul mercato soluzioni opzionali a pagamento che potrebbero essere integrate.

Un altro operatore conferma quanto già espresso nelle risposte alle precedenti domande circa la non differenziazione degli obblighi tra gli operatori e il fatto che la legge prevede il filtraggio e il blocco di contenuti a titolo gratuito e che eventuali funzionalità aggiuntive, come quelle inibire l'accesso per fasce orarie o il monitoraggio della navigazione, non debbano risultare tra i servizi offerti gratuitamente bensì, eventualmente, tra quelli offerti a pagamento.

Un operatore, anche in questo caso, ferme le criticità di ordine giuridico già esposte, sussistono rilevanti criticità tecniche collegate alla soluzione prospettata. In particolare, per poter erogare un servizio aderente ai requisiti appena espressi si rendono necessari sia adeguamenti tecnologici invasivi sugli apparati che gestiscono il traffico utente sia sviluppi relativi ai sistemi informativi interni per rendere fruibile all'utente finale, in maniera chiara ed immediata, la soluzione proposta.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Un operatore ritiene che l'implementazione della configurabilità dei SCP per fasce orarie e memorizzazione dei siti visitati, ad avviso della Scrivente, non è implementabile a livello di DNS. Tali soluzioni, infatti, necessiterebbero di integrazioni e sviluppi dedicati su altri apparati e infrastrutture, previa verifica della fattibilità tecnica. Inoltre, la possibilità di memorizzare "tutti gli accessi effettuati o solo quelli bloccati" solleva criticità dal punto di vista della privacy e gestione dei dati.

Un'associazione di consumatori ritiene le funzionalità proposte, indispensabili per una gestione efficace del SCP, si reputano adeguate ma se ne propone l'implementazione con un alert per il genitore così come indicato nella risposta al Quesito 1 nonché con il blocco di alcune attività in base alle fasce orarie: ad esempio, è verosimile ipotizzare che nelle ore pomeridiane della giornata uno studente abbia necessità di svolgere ricerche o approfondimenti utilizzando la rete internet e in ragione di tale premessa si potrebbe appunto impostare il blocco dell'accesso a siti web/app di gioco. Si propone altresì di rendere non cancellabile la cronologia del browser, in modo che il genitore possa sapere su quali siti il minore abbia navigato.

Una Società segnala come la possibilità di "configurare per fasce orarie l'accesso alla navigazione" può essere implementata in modo totalmente affidabile soltanto disabilitando l'accesso Internet dell'utente per tutti i suoi dispositivi nelle fasce orarie indicate. Se invece, come intuibile, ci si riferisce alla possibilità di configurare tramite il sistema di filtro DNS un blocco orario su specifici dispositivi usati dai minori, va riconosciuto come tale funzionalità sarà attiva soltanto se il dispositivo del minore continua a utilizzare il server DNS dell'ISP, ma sarà aggirabile semplicemente configurando un diverso server DNS sul dispositivo in questione o sul suo browser, a meno che tale possibilità non venga bloccata a livello di sistema operativo e di browser del dispositivo (cosa su cui l'ISP non ha modo di intervenire). Riguardo alla possibilità di mantenere un registro degli accessi bloccati o di tutti gli accessi dell'utente, si segnala come un simile registro abbia implicazioni di privacy estremamente rilevanti, compresa la possibilità di rilevare dati personali anche di tipo sensibile (salute, orientamento politico…). Si confida dunque in una interazione dell'Autorità con il Garante della Privacy al fine di assicurare la compatibilità delle linee guida con le determinazioni del Garante stesso e con tutta la regolamentazione in materia di privacy e di conservazione dei dati di traffico, fornendo agli ISP indicazioni chiare e precise su quali dati memorizzare, a chi renderli visibili, in quale modo, e dopo quanto tempo eliminarli.

Un'associazione di genitori ritiene complesse da implementare e perciò non conviene imporre quest'obbligo nell'ambito dei SCP obbligatori: deve essere lasciato alle funzioni aggiuntive a pagamento.

Sig. (OMISSIS): SI, i minori contemporanei tendono stare svegli più a lungo rispetto ai genitori; il blocco diventerebbe bypassabile scaricando i contenuti in un secondo momento e guardandoli in differita. Memorizzare gli accessi effettuati comporterebbe dei grossi problemi di trattamento dati/privacy.

Q15 – SI REPUTA PROPORZIONATA LA DISTINZIONE DEGLI ISP IN FASCE COSÌ COME PROPOSTA?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione concorda con la suddivisione in fasce, condizionatamente alla sua modifica secondo quanto riportato in merito alla Q.10.

Un operatore rinvia a quanto già rappresentato in merito alle domande Q.10 e Q.13.

Un altro operatore ribadisce che la distinzione proposta non è ritenuta proporzionata, anzi pregiudizievole per le dinamiche competitive del mercato. Un sistema di controllo parentale a protezione dei minori non può dipendere, nella sua semplice o articolata attuazione, dal numero di linee dati attive di un Operatore. Si propone pertanto l'eliminazione della classificazione degli Operatori in Fasce e della relativa differenziazione degli obblighi.

Un operatore ritiene di aver già argomentato con quanto sopra.

Un altro operatore reputa proporzionata la previsione sull'implementazione della configurabilità dei SCP per fasce orarie e di memorizzazione dei siti visitati, purché tuttavia sia adottata la proposta formulata in risposta al quesito 10 con le relative soglie.

Un operatore ha inteso rispondere in uno alle domande Q14 e Q15, dichiarando quanto segue: Con riferimento al requisito richiesto di "configurabilità dei SCP per fasce orarie" e "memorizzazione dei siti visitati", si richiamano qui le considerazioni svolte in risposta al quesito 1. Giova, tuttavia, ribadire che tali caratteristiche dei CSP, non rintracciabili nel dato testuale dell'articolo 7-bis del D.L. n. 28/2020, si sostanzia in una declinazione interpretativa di Codesta Spettabile Autorità e che, pertanto, possa agevolmente essere espunta dalle Linee guida sottoposte in consultazione. Appare, inoltre, sproporzionato l'eventuale obbligo in capo agli ISP di memorizzazione di tutti o parte degli accessi effettuati (es. solo quelli bloccati mediante DNS) rispetto all'esigenza di tutela del minore. Tale eventuale obbligo comporterebbe l'archiviazione per ciascun utente di una mole consistente di dati che potrebbe finanche compromettere le performances del sistema di filtraggio.

Un'associazione di consumatori dichiara che analogamente a quanto già esposto nella risposta al Quesito 10 e come ribadito nella risposta al Quesito 13, non si ritiene adeguata la limitazione dell'obbligo di fornire tali funzionalità ai soli operatori di fascia A.

Due associazioni di genitori non concordano con quanto proposto, perché ritiene che queste funzionalità debbano essere opzionali e che l'operatore dovrebbe essere libero di chiedere un costo aggiuntivo per la loro attivazione.

Un'associazione di genitori ribadisce che in ogni caso va evitata la confusione tra le funzionalità dei SCP e i sistemi di protezione aggiuntivi a pagamento.

Sig. (OMISSIS): no, non ha senso perché la funzionalità non comporta una grossa differenza di costi.

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. 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.

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?

OSSERVAZIONI DEI RISPONDENTI

Un'Associazione riscontra che a suo avviso, in linea generale, qualsiasi intervento sul traffico sarebbe potenzialmente in violazione della norma comunitaria, ma che nel caso specifico non ci sono ancora elementi tecnici e regolamentari che consentono di eseguire questa valutazione.

Un operatore osserva che la gestione ragionevole del traffico non richiede tecniche che monitorino i contenuti specifici del traffico di dati trasmesso tramite il servizio di accesso a

Internet. Le Linee guida del Berec del giugno 2020 ("BEREC Guidelines on the Implementation of the Open Internet Regulation") ritengono conforme a tale previsione unicamente la possibilità per gli ISP di fornire il servizio di parental control "over the top", senza effettuare alcun intervento in rete. Ciò conformemente a quanto previsto dal par. 78c che afferma che *"ISPs can also offer [...] end point-based services (e.g. to provide parental control or filtering functions alongside the IAS) in the same way that they are offered by third party CAPs*", ponendo pertanto in rilievo come le funzionalità messe a disposizione degli ISP - ad esempio per sistemi di parental control – debbano essere analoghe a quelle messe in campo da fornitori di tipo OTT (cd. CAPs). Inoltre, le Linee Guida confermano che il traffic management ulteriore rispetto a quello ritenuto "ragionevole" ai sensi del regolamento sia possibile per ottemperare ad un obbligo di legge, ma solo se necessario e limitatamente al tempo necessario. In particolare "*The three exceptions set out in Article 3(3) third subparagraph (a) – (c) have as common preconditions that the traffic management measure has to be necessary for the achievement of the respective exception ("except as necessary") and that it may be applied "only for as long as necessary". These requirements follow from the principle of proportionality*." Pertanto, un obbligo per gli ISP di mettere in campo misure permanenti di filtraggio dei contenuti per l'intera clientela non sarebbe ritenuto conforme al principio di proporzionalità dianzi richiamato, oltre che eccessivamente onerosa e non efficace nel raggiungimento delle finalità che la norma nazionale intenderebbe raggiungere. Le Linee Guida, richiamando il considerato 13 del Regolamento, specificano al successivo par. 82 che "*such legislation or measures must comply with the requirements of the Charter of Fundamental Rights, and notably Article 52 which states in particular that any limitation of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms*". Se anche un ISP fosse capace di gestire tecnicamente interventi in real time rispetto all'accesso a determinati contenuti, continuerebbe a sussistere comunque un generalizzato divieto per gli ISP di adottare misure di limitazione e controllo delle attività espletate in rete dai propri clienti, anche nel rispetto delle disposizioni di privacy oltre a quelle sopra richiamate. Pertanto, misure tecnicamente più invasive, quali ad es. il blocco a livello IP o interventi di imperio sul client installato sul terminale del cliente, si potrebbero rivelare non pienamente rispondenti alla norma eurounitaria. In aggiunta, uno dei punti cardine del Regolamento sulla internet aperta, è quello di tutela della concorrenza: in tal senso, non si rinviene nella proposta dell'Autorità alcuna considerazione circa l'impatto della presente regolamentazione sui mercati dei servizi di controllo parentale. Come noto, i servizi in esame non sono offerti unicamente dagli ISP, ma anche da OTT (es. Google con il Family Link) ed è ormai pacifico che tra OTT e cliente finale si viene ad instaurare un normale rapporto di consumo in cui il prezzo pagato dal consumatore è rappresentato dai dati personali ceduti al professionista (il superamento del concetto di gratuità dei servizi OTT è ormai superato da un punto di vista normativo ed applicativo). Ne deriva che l'attuale proposta di regolamentazione creerebbe una asimmetria tra ISP ed altri

fornitori di SCP e potrebbe anche alterare il gioco competitivo sui mercati. Si ritiene che allo stato attuale della consultazione, e in assenza di informazioni sulle modalità di classificazione ed individuazione dei contenuti nei confronti dei quali dovrebbero intervenire misure generalizzate di restrizione del traffico (addirittura anche per soggetti maggiorenni) basate sul filtraggio dei contenuti, non è possibile che esprimere le considerazioni di ordine generale sopra richiamate e l'adozione della massima attenzione per evitare elementi di potenziale conflitto con le regole di net neutrality.

Un operatore riporta di nutrire forti dubbi sull'applicabilità della deroga di cui all'art. 3, comma 3, lett. a) del Regolamento al caso di specie: sebbene la normativa nazionale (il decreto-legge 30 aprile 2020, n. 28) abbia introdotto l'obbligo per gli operatori di TLC di prevedere un filtro contenuti gratuito e pre-attivato, non sembrano riscontrarsi analoghe previsioni a livello legislativo dell'Unione Europea, in particolare nelle stesse fonti citate (i.e. Direttiva sui servizi di media audiovisivi, e Codice Europeo delle Comunicazioni Elettroniche). Non ritiene, nel caso di specie, che un comportamento contrario alle regole della Net Neutrality, ossia l'introduzione di un filtro per contenuti pre-attivato in tutte le utenze fisse e mobili, possa essere giustificato perché "*necessario e solo per il tempo necessario a*" conformarsi a un atto di legge conforme al diritto dell'Unione. Evidenzia che il Considerando 11 riporta che le eccezioni dovrebbero essere "*soggette a un'interpretazione rigorosa e a requisiti di proporzionalità*"; le misure di blocco o altre misure restrittive non rientranti nel novero delle eccezioni giustificate determinano un impatto negativo sulla scelta dell'utente finale e sull'innovazione e per tale ragione è "*opportuno proteggere specifici contenuti, applicazioni e servizi e loro specifiche categorie*". Il Considerando 13 inoltre specifica che la violazione delle regole Open Internet sarebbe ammissibile solo nel rispetto di uno dei requisiti sanciti a livello della Carta dei diritti fondamentali dell'Unione Europea, riguardo alle limitazioni all'esercizio dei diritti e delle libertà fondamentali. Tutto ciò considerato, l'operatore pone forti dubbi sulla possibilità di applicare "*strictu sensu*" le Linee Guida e le medesime previsioni introdotte con l'art. 7 bis della citata legge nazionale e rende opportuno segnalare all'Autorità, cui la norma rimette la vigilanza sul rispetto degli obblighi in essa definiti, la possibilità anche di considerare la disapplicazione della stessa. In aggiunta a quanto sopra, il medesimo evidenzia anche criticità relative al principio generale per cui gli operatori di accesso non devono conoscere il contenuto delle comunicazioni, né interferire con esso (non solo per i temi di neutralità della rete qui esplicitati) ma, più in generale, in virtu' di previsioni normative a livello di Unione Europea che sembrano sancire principi diametralmente opposti (ad es. la Direttiva sul Commercio Elettronico - Direttiva 2000/31, art. 15).

Un operatore concorda sul fatto che le misure di blocco di specifici punti terminali della rete internet siano possibili solo qualora le indicazioni di blocco siano fornite da un ente

istituzionale terzo rispetto all'operatore, che non può assumersi alcuna responsabilità in merito. Sulle azioni da condurre su specifici punti terminali della rete internet si ritiene che non si possa prescindere dal dettato della legge che si limita ad attività di filtraggio e di blocco di contenuti, senza prevedere la fornitura a titolo gratuito di altre azioni, che sebbene ritenute potenzialmente utili al cliente finale si ritiene debbano essere annoverate tra quelle proponibili a condizioni commerciali. Diverso è invece il caso di altre previsioni della regolamentazione 2015/2120, come ad es. il principio della libertà di scelta del terminale. L'imposizione di obblighi agli operatori sui terminali, sia fissi che mobili, da loro forniti di fatto interviene sul principio di libertà di scelta del terminale; pertanto, la Società è contraria ad ogni obbligo che sia imposto sui terminali sia fissi che mobili forniti dagli operatori. Ogni obbligo relativo ai terminali deve essere imposto ai produttori di tali apparati e non all'operatore di connettività che li fornisce a titolo opzionale, ad integrazione della sua offerta commerciale, anche al fine di non alterare le dinamiche competitive di un mercato che vedrebbe i terminali offerti dagli operatori con funzionalità imposte che ne aumentano la complessità, ne riducono le prestazioni (come ad es. la memoria a disposizione per le App del cliente finale) ostacolando di fatto l'acquisizione dei terminali commercializzati dagli operatori e creando così una discriminazione su tale mercato a vantaggio dei produttori di apparati e dei loro distributori. Si ritiene inoltre doveroso segnalare la necessità di promuovere l'utilizzo dei sistemi di rete che eventualmente potrebbe rendersi necessario porre in essere per ottemperare alla legge, anche per la fornitura, a titolo oneroso, di tutte quelle funzionalità aggiuntive che possono completare efficacemente il Sistema di SCP base previsto dalla normativa.

Un operatore ritiene che la proposta di Linee guida, per come attualmente strutturata, potrebbe contenere previsioni critiche con riferimento al rispetto del Regolamento UE di cui al presente quesito. In particolare, si ritiene che l'impossibilità per gli ISP di inibire tecnicamente l'accesso a contenuti specifici presenti sul web potrebbe comportare l'inaccessibilità per l'utenza a accedere a contenuti pienamente leciti e non soggetti ai SCP. Si pensi, a titolo meramente esemplificativo, al minore che desideri visualizzare un contenuto video sul sito di una testata giornalistica, e che non potrebbe accedervi a causa della presenza all'interno del sito di immagini e/o video non adeguati alla sua età. Il predetto effetto "censorio" risulterebbe peraltro esacerbato dalla pre-attivazione dei SCP su tutte le utenze fisse e mobili (sia nuove linee che sulle linee esistenti), anche intestate a titolari maggiorenni, poiché l'accesso ai predetti contenuti sarebbe de facto inibito all'intera customer base degli Operatori – e quindi alla totalità dei consumatori italiani.

Un altro operatore ritiene che tali criticità siano collegate alla natura stessa del SCP che, appunto, inibisce la raggiungibilità di siti, contenuti e applicazioni di potenziale interesse dell'utente. Ad ogni modo, si ritiene che i punti cardine per garantire il rispetto di quanto

sancito dal DL in una prospettiva di compatibilità col quadro normativo Europeo (incluso il Regolamento Open Internet) siano i seguenti:

- Applicazione dell'obbligo di fornitura del SCP, specie nella forma pre-attivata, entro i limiti sanciti dal DL, senza che siano in alcun modo introdotti aspetti "sovrabbondanti";

- Sistemi trasparenti, semplici e gratuiti per la rimozione del blocco;

- Ruolo di mero esecutore da parte dell'ISP, che non deve essere chiamato in alcun modo a compiere valutazioni discrezionali rispetto all'accesso a determinati siti/contenuti da parte dell'utente.

Un rispondente ritiene che la previsione di un blocco pre-attivato (senza una richiesta espressa da parte dell'utente) di fatto limita il diritto degli utenti ad una "Internet aperta", se si considera che tutti gli utenti– sia maggiorenni che minorenni; sia in presenza di minorenni nel nucleo familiare che in assenza – senza richiederlo espressamente si troverebbero ad avere un blocco automatico da dover rimuovere. La Società ritiene pertanto che possa essere più utile e vantaggioso per il cliente richiedere l'attivazione del blocco ove necessario, chiaramente garantendo informazioni chiare e complete rese dall'operatore in fase di conclusione del contratto e durante l'esecuzione dello stesso. Si invita, pertanto, Codesta Autorità a tenere in debita considerazione i principi e le disposizioni che disciplinano la materia dell'Open Internet nell'adozione delle Linee Guida in questione, al fine di evitare ogni sorta di restrizione che tenda a limitare i diritti degli utenti riconosciuti a livello europeo.

Un altro rispondente dichiara che il Regolamento UE n. 2015/2120 (di seguito "Regolamento") pone regole a tutela della parità e del trattamento non discriminatorio del traffico nella fornitura dei servizi di accesso a Internet e dei relativi diritti degli utenti finali di cui agli articoli 3 e 4. Com'è noto, ai sensi dell'articolo 3, comma 3 del Regolamento "*i fornitori di servizi di accesso a Internet, nel fornire tali servizi, trattano tutto il traffico allo stesso modo, senza discriminazioni, restrizioni o interferenze, e a prescindere dalla fonte e dalla destinazione, dai contenuti cui si è avuto accesso o che sono stati diffusi, dalle applicazioni o dai servizi utilizzati o forniti, o dalle apparecchiature terminali utilizzate*". Il terzo comma prosegue precisando che le uniche misure di traffic management che un ISP può realizzare sono quelle definite come "ragionevoli" (intendendo con ciò le misure di gestione del traffico che sono trasparenti, non discriminatorie e proporzionate) oppure quelle che rientrano in una delle tre eccezioni ivi precisate tra cui, alla lettera a), quelle attuate per "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". Il Regolamento, al considerato n.11, afferma inoltre la necessità che tali eccezioni

siano soggette non solo ad un'interpretazione rigorosa ma anche ai requisiti di proporzionalità.

Un'associazione di consumatori non riscontra particolari criticità.

Una Società ribadisce che il Regolamento 2015/2020 all'articolo 3 non prevede tra le eccezioni al divieto di filtraggio dei contenuti soltanto quella relativa all'implementazione di provvedimenti legislativi che richiedono il blocco di contenuti, ma anche quelle relative ai blocchi mirati alla sicurezza e alla gestione della rete; si suggerisce di allineare le linee guida a tale formulazione. Ribadendo quanto indicato nella risposta alla domanda numero 12, si ritiene che le richieste contenute nelle linee guida alla sezione 6, punti a) e b), siano incompatibili con il Regolamento 2015/2020. Cogliamo comunque l'occasione per segnalare come vi sia una contraddizione filosofica di fondo tra il Regolamento 2015/2020 e gli atti legislativi e giudiziari che richiedono agli ISP di bloccare contenuti di vario genere. Tale contraddizione finisce per scaricare sugli ISP responsabilità legali e morali difficili da gestire, in quanto un banale errore nell'implementazione di un blocco legale può immediatamente costituire una violazione al Regolamento. Sarebbe auspicabile una riconciliazione dell'approccio regolatorio sul tema tra i vari livelli legislativi.

Tre associazioni di genitori non riscontrano criticità, perché si tratta di un servizio totalmente disattivabile e quindi è lasciata totale libertà al titolare del contratto, maggiorenne. Al principio del superiore interesse del minore si corrisponde attraverso la messa a disposizione di un servizio la cui attivazione o disattivazione è affidata alla libera decisione del genitore contraente.

Sig. (OMISSIS): si, è discriminatorio.

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.

SINTESI DEI CONTRIBUTI - OSSERVAZIONI SUI SINGOLI QUESITI.

Q17 – SI RISCONTRANO ULTERIORI REQUISITI PER LE INTERFACCE DEI SCP?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione rileva che la legge non prevede indicazioni in merito a questa funzionalità, evidenziando in particolar modo che l'esecuzione in tempo reale del comando di blocco/sblocco non è prevista dalla legge. Evidenzia inoltre che sarebbe preferibile l'utilizzo di una interfaccia web indipendente dal terminale.

Un operatore reputa che la regolamentazione dovrebbe prevedere unicamente l'implementazione di un blocco minimo di default che consenta all'utente finale di bloccare/sbloccare il SCP, senza obbligare l'operatore ad offrire anche funzionalità/servizi aggiuntivi.

Un altro operatore riporta che l'accesso per l'identificazione tramite PIN/OTP potrebbe essere assicurato piuttosto agevolmente tramite una applicazione (app), disponibile per Android e iOS. Non rileva ulteriori né particolari criticità in merito. Ritiene che l'accesso all'app dovrebbe essere consentito a tutti i clienti che hanno il servizio di telefonia attivo, mentre la gestione del filtro dipenderebbe dal possesso del PIN che viene inviato esclusivamente a un numero di telefono specificato.

Un operatore ritiene che l'adozione di OS diversi da Android e IoS non deve tradursi in una possibile violazione da parte dell'operatore che dovrà essere mantenuto indenne da ogni conseguenza derivate da scelte del cliente finale volte ad aggirare il dispositivo legislativo e regolamentare, come appunto la scelta di terminali con un sistema operativo diverso. Si segnala inoltre che ad oggi, in assenza di una soluzione implementativa definita, non è possibile valutare la sostenibilità della richiesta secondo cui "le impostazioni di blocco/sblocco devono avvenire in tempo reale rispetto alle operazioni di attivazione, disattivazione e configurazione dei SCP da parte degli utenti." La società scrivente rileva che sarà possibile identificare i tempi necessari affinché le impostazioni siano efficaci solo a valle della completa definizione dell'architettura che verrà individuata.

Un operatore ritiene che i requisiti individuati nel testo in consultazione rispetto all'accesso tramite interfaccia siano nel complesso condivisibili e sufficienti a garantire un corretto funzionamento del SCP, fatte salve alcune necessarie precisazioni. In primis, l'indicazione sul funzionamento "in tempo reale" dovrebbe essere sostituita con una formulazione che lasci un tempo tecnico idoneo a consentire ai sistemi di recepire e processare le richieste effettuate del cliente (che dovrebbero, comunque, essere gestite in "near real time"). Inoltre, resta inteso che il requisito del "real time" (rectius "near real time") può riguardare il funzionamento del SCP lato utente ma non l'aggiornamento dello stesso rispetto alla lista dei siti/contenuti da

bloccare (che, come nei casi analoghi di blocco ex lege, ha bisogno di tempi tecnici più consistenti).

Un'associazione di consumatori ribadisce l'opportunità di prevedere un'unica interfaccia web e un'unica app del SCP per attivazioni, disattivazioni e configurazioni, a prescindere dal fornitore del servizio e dal dispositivo utilizzato. L'impiego di un unico sistema di gestione renderebbe più semplice l'utilizzo del SCP da parte dell'utente, che quindi non dovrebbe adeguarsi a nuove modalità in caso di cambio operatore e/o dispositivo.

Un'associazione di genitori reputa eccessiva la misura. Non è necessario imporre app Android e iOS. Può essere sufficiente l'interfaccia web responsive o, più in generale, una webapp. Il requisito imposto "in tempo reale" non è compatibile con la natura dei DNS che richiedono tempi di propagazione nella rete tra tutti i server che offrono lo stesso servizio. Meglio sarebbe richiedere "immediatamente", cioè senza mediazione di tempi di attesa aggiunti rispetto alla normale implementazione delle nuove configurazioni.

Sig. (OMISSIS): si, le app dovranno essere software libero e, nel caso di android, presenti anche in f-droid e funzionanti senza i google mobile services.

Q18 – SI REPUTA CHE LA REGOLAMENTAZIONE DEBBA FORNIRE ULTERIORI SPECIFICHE SULLE MODALITÀ DI IMPLEMENTAZIONE DELLE INTERFACCE DEI SCP?

OSSERVAZIONI DEI RISPONDENTI

Un operatore sottolinea che, ove in linea con quanto previsto nella normativa primaria di riferimento si preveda che gli operatori siano nella possibilità di scegliere la modalità tecnica ritenuta più idonea ed efficace in vista delle finalità da perseguire, verrebbe richiesto al mercato uno sforzo economico di minore impatto, nel rispetto del principio di massima efficienza *dell'agere amministrativo*.

Un operatore ritiene che siano necessarie maggiori informazioni sia sulle interfacce dei SCP, ma soprattutto sull'aggiornamento dei punti terminali di internet da bloccare. In particolare, si richiede che AGCOM certifichi e garantisca che le richieste che verranno formulate non producano effetti indesiderati, sotto ogni profilo, sui servizi che l'Operatore offre. Qualsiasi filtro o blocco che deve essere implementato deve necessariamente seguire una specifica precisa di AGCOM, così come la lista di tutti i blocchi da implementare. Ad esempio, a valle dell'uscita di una nuova App da includere nel sistema di SCP, dovrà essere a cura di AGCOM

segnalare le URL / IP da bloccare, tale attività non può essere ritenuta di responsabilità dell'Operatore.

Un altro operatore non ritiene necessario fornire a riguardo ulteriori osservazioni.

Un'associazione di consumatori ritiene opportuno non limitare la disponibilità delle App solo ai sistemi operativi Android e iOS.

Due associazioni di genitori non ritengono che la regolamentazione debba prevedere ulteriori misure ma deve prevedere che l'Autorità possa segnalare all'operatore migliorie in caso di evidente carenza.

Sig. (OMISSIS): no.

Q19 – SI REPUTA PREFERIBILE UNA INTERFACCIA WEB, UNA APP O SI INDIVIDUANO ULTERIORI MODALITÀ REALIZZATIVE?

OSSERVAZIONI DEI RISPONDENTI

Un operatore ritiene che questa sia una scelta commerciale e di opportunità di sviluppo, dipendente anche da device che si intende utilizzare. In ogni caso, la scelta di avere una interfaccia web sembrerebbe la scelta migliore in quanto, da un lato, risulta essere trasversale a tutti i device ed a tutti i sistemi operativi dei diversi device (senza la necessità di costose customizzazioni) e, dall'altro, appare essere quella più rispondente alle finalità della norma. Infatti, dovendo essere il genitore a gestire il SCP, sarebbe opportuno che il genitore possa intervenire da web senza la necessità di avere in mano il device in uso al minore.

Un altro operatore ritiene che l'app dovrebbe consentire una facile e intuitiva accessibilità a tutti i servizi, ivi compreso quello di controllo/gestione del filtro SCP. Per le funzioni dispositive, e quindi laddove si volessero modificare le impostazioni di utilizzo del filtro, si potrebbe disporre, per ragioni di sicurezza, di un secondo numero di telefono su cui viene inviato il PIN/OTP.

Un operatore al momento non ha particolari osservazioni in merito, ma si riserva di segnalarle in una fase di maggiore definizione delle architetture che verranno proposte.

Un altro operatore risponde in unico alle risposte Q17, Q18 e Q19, dichiarando che: in linea con quanto rappresentato nei riscontri ai precedenti quesiti Q6 e Q7, si reputa che la scelta dei requisiti, delle modalità di implementazione delle interfacce dei SCP e dei canali di attivazione, disattivazione e configurazione dei SCP non possa che essere rimessa agli Operatori, nel rispetto dei principi della libertà imprenditoriale. Quanto sopra, previo

impegno, da parte degli Operatori, a garantire la creazione di interfacce, modalità di attivazione, disattivazione e configurazione dei SCP semplici ed intuitive.

Un operatore, per quanto già sopra argomentato in materia di autenticazione, ritiene che la soluzione basata su interfaccia (o app) debba esser intesa come una soluzione compatibile con le norme sul SCP ma non come soluzione unica e obbligatoria. Il singolo operatore, infatti, in ragione di considerazioni di varia natura (es. volume della customer base impattata, priorità organizzative interne) potrebbe ritenere preferibile gestire la prestazione con strumenti più "tradizionali" – purché egualmente efficienti e sicuri – quali ad esempio il customer care telefonico gratuito.

Un altro operatore intende rispondere in uno alle risposte Q17, Q18 e Q19, dichiara di non individuare ulteriori requisiti per le interfacce dei SCP e ritiene che i requisiti espressi siano già abbastanza elevati. Si ritiene, altresì, che sarebbe opportuno che la regolamentazione fornisca ulteriori specifiche sulle modalità delle interfacce dei SCP, precisando come sia possibile tecnicamente rendere l'interfaccia utente accessibile solo dal titolare del contratto. In merito al Quesito 19, la Scrivente ritiene sia preferibile l'interfaccia web per ragioni di compatibilità. La modalità realizzativa più efficace potrebbe essere un pulsante di attivazione/disattivazione all'interno dell'area riservata cliente sul portale dell'operatore. Le modifiche avrebbero in tempo reale e le nuove impostazioni sarebbero disponibili a seguito del riavvio del router pilotato dal comando sulla interfaccia grafica (GUI).

Un operatore ha inteso rispondere in uno alle domande Q17, Q18 e Q19, dichiarando quanto segue: la Società reputa non definibile a priori una modalità realizzativa per l'implementazione dell'interfaccia dei SCP. Si ritiene che tale modalità debba essere rimessa alla discrezionalità degli ISP anche alla luce dei sistemi di filtraggio che verranno individuati.

Un'associazione di consumatori ritiene che l'interfaccia web e la app siano al momento sufficienti.

Due associazioni di genitori ritengono preferibile la soluzione web app per una maggiore compatibilità con tutti i sistemi.

Un'associazione di genitori concorda con le soluzioni proposte. A questo aggiunge la proposta di prevedere modalità di monitoraggio, soprattutto nelle prime fasi di realizzazione del nuovo sistema, sia predisponendo servizi di raccolta delle opinioni e dei suggerimenti degli utenti da parte degli operatori, sia da parte della stessa Autorità per verificare la corretta applicazione delle Linee guida che saranno emanate.

Sig. (OMISSIS) ritiene che l'interfaccia web per un utilizzo di internet prevalentemente su un browser.

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?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione evidenzia che tale funzionalità è realizzabile lato cliente sia intervenendo sul software del CPE o del terminale mobile, sia installando sempre lato cliente, software locali di parental control sotto il diretto controllo dell'utente.

Un operatore reputa che ciò rientri tra le funzionalità aggiuntive che non dovrebbero essere oggetto di regolamentazione, essenzialmente perché non richiesto dalla norma primaria. L'intervento come proposto nel documento di consultazione appare eccessivamente invasivo e non giustificato.

Un operatore rinvia alle precedenti risposte in merito alle funzioni di base del filtro SCP in linea con quanto previsto dalla normativa di riferimento e all'effettivo ruolo degli operatori di rete.

Un altro operatore ribadisce che la personalizzazione dei contenuti oggetto di filtro, con la possibilità di aggiungere o personalizzare i contenuti oggetto di filtro non sia una prestazione da considerarsi obbligatoria in quanto non prevista dalla legge, e possa essere ricompresa tra quelle che (tutti) gli operatori possono offrire a titolo commerciale e che sia possibile offrirla sugli stessi sistemi utilizzati per ottemperare all'obbligo di legge, anche al fine di rendere più efficace la cd. *User experience*, cioè la facilità d'uso del sistema di SCP e promuoverne l'utilizzo.

Un operatore, ferme restando le significative criticità evidenziate all'interno del presente contributo e l'impossibilità di valutare in maniera efficace gli impatti tecnici delle implementazioni prospettate senza conoscere i criteri di filtraggio e le modalità di classificazione dei contenuti che saranno adottati, non rileva per contro particolari criticità tecniche nella gestione delle *blacklist* e delle *whitelist*.

Un operatore ritiene che tali prestazioni debbano far parte delle funzionalità aggiuntive erogate (nel caso anche a pagamento) dall'operatore su richiesta dell'utente.

Un altro operatore ritiene che non sarebbe tecnicamente possibile gestire black list e white list su DNS. I DNS degli operatori non offrono, infatti, funzionalità per l'inserimento e la rimozione di URL in black/white list da parte degli utenti finali. Inoltre, black list e white list non dovrebbero permettere di visualizzare gli URL permessi o bloccati secondo quanto prevede l'Autorità, andando nella maggior parte dei casi a delegare la gestione dei contenuti agli operatori internet; in generale, i domini Internet o gli URL indicano il contenuto di pertinenza, per tali ragioni le definizioni sulle soluzioni di mercato sono criptate e non visibili.

Un operatore, premettendo che per rispondere compiutamente al quesito occorrerebbe prima conoscere l'esito del procedimento relativo alla classificazione dei contenuti oggetto di filtro/blocco e alla definizione di filtri per fasce d'età, evidenzia fin d'ora criticità circa l'aggiornamento "dinamico" dei contenuti sia ove fosse realizzato lato rete che in altre modalità. In particolare, si ritiene più facilmente realizzabile una soluzione in cui siano disponibili due profili predefiniti ("parental control attivo" e "parental control disattivo") di accesso ai contenuti, dando la possibilità all'utente di poter scegliere rispetto ai suddetti profili messi a disposizione dal ISP. La dinamicità di aggiornamento degli stessi sarebbe in ogni caso legata alle indicazioni fornite dall'Autorità in base alla classificazione dei contenuti. Si ritiene quindi che l'ISP possa aggiornare la black list che determinerà i contenuti non fruibili dal profilo "parental control attivo".

Un'associazione di consumatori concorda con la prospettata introduzione della funzionalità di gestione di black list e white list ma, analogamente a quanto già precisato e per le motivazioni già esposte nelle risposte ai Quesiti 10, 13 e 15, non si ritiene opportuno circoscrivere l'obbligo di fornire le funzionalità in questione ai soli operatori di fascia A e B. A tale proposito si evidenzia inoltre la necessità attribuire anche ai fruitori dei siti web la facoltà di segnalare e di chiedere l'iscrizione nelle liste, poiché sui siti Internet ed i loro contenuti è importante ed opportuno un monitoraggio non solo degli operatori ma anche degli utenti e dei fruitori dei servizi.

Una Società segnala che "black list" e "white list" sono termini il cui uso è ormai sconsigliato a livello internazionale dalle maggiori organizzazioni di standardizzazione di Internet, per via delle implicazioni politicamente scorrette. Sarebbe preferibile utilizzare i termini "blocklist" e "allowlist".

Per **un'associazione di genitori** deve essere possibile attivare solamente la white list, cioè la possibilità di navigare esclusivamente nei siti elencati dal titolare: è la modalità "biblioteca di casa" o walled garden, adatta per i più piccoli.

Un'associazione di genitori sottolinea che **l**a possibilità di gestione di black list e white list acquista un valore che oltrepassa la dimensione del dispositivo tecnico, acquisendo anche un rilievo educativo e culturale più ampio. L'opportunità di aggiungere o rimuovere dalle black list e dalle white list siti ritenuti inappropriati per i propri figli consente ai genitori di orientare le modalità di tutela verso i propri valori e modelli educativi. Ciò, in particolare, laddove i genitori ritengano che i diritti dei minori nella navigazione in rete vadano resi effettivi nella loro completezza, sia per gli aspetti di sicurezza sia per i diritti di socializzazione, formazione, espressione della propria personalità, e così via.

Un'altra associazione di genitori dichiara che alcuni servizi internazionali di filtraggio non le prevedono e questo può essere un problema per gli ISP che li utilizzano. Tuttavia, ritiene fondamentale poter implementare black e white list, inclusa la possibilità della navigazione in sola white list, con la modalità "biblioteca di casa" o walled garden, particolarmente adatta per i più piccoli.

Sig. (OMISSIS): decisamente sì. Le blacklist in questo ambito non sono mai complete, e le whitelist filtrano troppo (che renderebbe difficile, ad esempio, fare una ricerca scolastica su internet).

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?

OSSERVAZIONI DEI RISPONDENTI

Un'associazione ritiene che gli unici canali di comunicazione accettabili, in termini di costi di gestione, siano la pubblicazione di contenuti su home-page, l'invio di e-mail e il self-care nell'area cliente.

Un operatore indica il rinvio per i clienti fissi e mobili ad un'unica pagina web che illustri in modo trasparente le funzionalità dei SCP, l'inclusione delle medesime informazioni nel documento di fatturazione (per i clienti fissi) e in una notifica via SMS (per i clienti mobili), nel caso di attivazione del servizio, mentre esclude la praticabilità della chiamata diretta effettuata dall'operatore in ragione dei costi eccessivi e del possibile fraintendimento da parte del cliente, che assimilerebbe la chiamata ad una chiamata di disturbo. Un operatore ricorda anche che, per quanto riguarda i fornitori di servizi media audiovisivi a pagamento, gli attuali sistemi di controllo parentale sono già regolati e risultano già compliant con la norma primaria; pertanto, gli stessi operatori dovrebbero essere esclusi dall'obbligo di comunicare e promuovere i sistemi i SCP preattivati come per gli operatori di comunicazioni elettroniche.

Un altro operatore ricorda che la specificità del servizio parental control, per definizione, non interessa la totalità dei clienti ovvero potrebbe interessare un cliente in un momento qualunque della sua vita contrattuale, anche molto successivo alla stipula del contratto, pertanto, i canali informativi più efficaci risultano essere canali digitali. In conclusione, il medesimo operatore ritiene che i canali digitali siano da considerarsi gli unici e preferenziali canali informativi in cui inserire, rectius aggiornare, le informazioni circa la presenza di SCP

e le istruzioni su come modificarne la configurazione, disattivarlo e riattivarlo, anche in ossequio del principio di proporzionalità. Della stessa opinione anche un altro operatore mentre **un altro rispondente** afferma che risulterebbe particolarmente onerosa anche l'introduzione dell'obbligo di cui alla lettera d), punto 11 delle proposte Linee guida, poiché risulterebbe necessario sviluppare un IVR ad hoc o dedicare risorse allo scopo di effettuare chiamate dirette verso l'intera *customer base* su rete fissa, ritenendo che la scelta del mezzo dovrebbe essere lasciata alla libertà imprenditoriale.

Un operatore riporta in ordine di preferenza i canali proposti, elencando il sito web dell'operatore attraverso un link dalla home page, la documentazione contrattuale, l'area riservata del sito web e il call center ed esclude per la eccessiva onerosità il documento di fatturazione, l sms/e-mail e la chiamata da parte dell'operatore.

Un altro operatore riconosce utile la pubblicazione sul sito ma non in home page e in un'area dedicata alla tutela dell'utenza a sua volta direttamente accessibile dall'homepage, come anche il customer care e self care area ed eventualmente il documento di fatturazione mentre esclude la chiamata diretta.

Un rispondente, come "adeguate forme di pubblicità", indica per i nuovi clienti la Carta dei servizi e una pagina web ad hoc nella quale declinare tutte le specifiche di dettaglio relativamente ai SCP e alla loro fruizione. Quanto ai clienti delle linee già esistenti sarebbe invece sufficiente un avviso nella relativa sezione del sito web dell'operatore di riferimento e una comunicazione personale da inviarsi mezzo e-mail e/o nell'Area personale dei singoli clienti.

Un'associazione di consumatori reputa che gli obblighi comunicativi, da destinare a tutti i "fornitori di servizi di comunicazioni elettroniche", siano soddisfacenti mentre **un'associazione di genitori**, pur approvandoli, li ritiene addirittura eccessivi, ritenendo più ragionevole lasciare l'indicazione "chiara, trasparente ed esaustiva" e riservare all'Autorità la possibilità di segnalare eventuali carenze dell'ISP.

Un'associazione di genitori consiglia di specificare che le informazioni dovrebbero essere fornite comunque anche tramite e-mail e **un'altra** definisce indispensabile curare il primo livello di informazione/comunicazione da parte degli ISP oltre che delle reti televisive e di comunicazioni elettroniche. **Un'altra ancora** chiede un ampliamento delle modalità comunicative coinvolgendo le associazioni dei genitori e per la tutela dei minori.

Sig. (OMISSIS): è favorevole.