AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

DELIBERA 9/23/CONS

ADOZIONE DELLE 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"

NELLA riunione di Consiglio del 25 gennaio 2023;

VISTA la legge 7 agosto 1990, n. 241, recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";

VISTA la legge 14 novembre 1995, n. 481, recante "*Norme per la concorrenza e la regolazione dei servizi di pubblica utilità. Istituzione delle Autorità di regolazione dei servizi di pubblica utilità*";

VISTA la legge 31 luglio 1997, n. 249, recante "*Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle comunicazioni e radiotelevisivo*";

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "*Codice in materia di protezione dei dati personali*" ed i successivi provvedimenti attuativi in materia;

VISTO il decreto legislativo 6 settembre 2005, n. 206 e s.m.i., recante "*Codice del consumo, a norma dell'art. 7 della legge 29 luglio 2003, n. 229*";

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

VISTO, in particolare, l'art. 7-*bis* del decreto-legge 30 aprile 2020, n. 28, rubricato "*Sistemi di protezione dei minori dai rischi del cyberspazio*", il quale dispone quanto segue:

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

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

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

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

VISTO il Regolamento (UE) n. 2015/2120, del 25 novembre 2015, del Parlamento europeo e del Consiglio che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva n. 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il Regolamento (UE) n. 2012/531 relativo al *roaming* sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione;

VISTA la direttiva (UE) 2018/1972, del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche;

VISTO il decreto legislativo 8 novembre 2021, n. 208 recante "*Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/ UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato*";

VISTO il decreto legislativo 8 novembre 2021, n. 207 recante "*Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche*" (nel seguito il "*Codice*");

VISTA la delibera n. 223/12/CONS, del 27 aprile 2012, recante "*Adozione del nuovo Regolamento concernente l'organizzazione e il funzionamento dell'Autorità per le garanzie nelle comunicazioni*", come modificata, da ultimo, dalla delibera n. 434/22/CONS;

VISTA la delibera n. 107/19/CONS, del 5 aprile 2019, recante "*Adozione del regolamento concernente le procedure di consultazione nei procedimenti di competenza dell'Autorità*";

VISTA la delibera n. 160/21/CONS del 24 giugno 2021, recante "*Avvio del procedimento istruttorio finalizzato all'attuazione dell'art. 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di "Sistemi di protezione dei minori dai rischi del cyberspazio"*";

VISTA la delibera n. 16/22/CONS del 20 gennaio 2022, recante "*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*" di seguito anche la "*consultazione*";

VISTE le note inviate in data 2 febbraio 2022 all'Autorità garante per l'infanzia e l'adolescenza (nota prot. n. 36040), al MISE (nota prot.n. 36074), al CNU (nota prot. n. 36182), al Comitato media e minori (nota prot. n. 36132) e all'Onorevole Sottosegretario alla Giustizia Anna Macina (nota prot. n. 36108), al fine di acquisirne gli eventuali commenti e contributi;

VISTA la nota del 18 febbraio 2022 (prot. n. 60093) con cui l'Autorità garante per l'infanzia e l'adolescenza ha inteso dar seguito alla nota dell'Agcom sopracitata;

VISTA la nota del 14 aprile 2022 (prot. n. 127034) con la quale il CNU ha inteso inviare il parere approvato nella seduta del 1° aprile 2022 in merito alla delibera n. 16/22/CONS;

VISTI i contributi pervenuti e i verbali delle audizioni tenutesi nell'ambito della consultazione pubblica di cui alla delibera n. 16/22/CONS, la cui sintesi e le relative valutazioni di dettaglio sono riportate in allegato B al presente provvedimento;

VISTA la nota del 26 aprile 2022 (prot. n. 136083) con cui è stata formulata una richiesta informazioni a tutti gli ISP partecipanti alla consultazione di cui alla delibera n. 16/22/CONS, finalizzata a ottenere maggiori dettagli in ordine ai costi stimati e le possibili alternative tecniche per l'implementazione dei sistemi di *parental control* da parte degli operatori;

VISTE le note con cui gli operatori hanno inteso dare riscontro alla suddetta richiesta di informazioni, qui pervenute in data 26 e 27 maggio 2022;

VISTA la nota del 27 maggio 2022 (prot. n. 171406) con cui è stata formulata un'ulteriore richiesta informazioni agli operatori partecipanti alla *consultazione*, finalizzata a ottenere maggiori dettagli in ordine all'impatto dell'implementazione del Sistema di controllo parentale (di seguito per brevità anche SCP) sulla customer base di ciascun ISP;

VISTA la nota del 20 giugno 2022 (prot. n. 193829) con cui è stata inviata una ulteriore richiesta di informazione sulle specifiche modalità di realizzazione dei sistemi di *parental control*;

VISTE le note con cui gli operatori hanno inteso dare riscontro alla suddetta richiesta di informazioni;

CONSIDERATO che il Regolamento (UE) n. 2015/2120 prevede, all'art. 3, comma 3 alla lettera a), 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*";

RILEVATO che il CNU ritiene opportuno un intervento dell'Autorità per richiedere ai fornitori di servizi di accesso ad Internet non solo di prevedere adeguate e chiare forme di pubblicità sui differenti mezzi di informazione ma anche di verificarne l'efficacia attraverso l'ascolto, cioè con mirate campagne di comunicazione integrata. In questa direzione, il CNU ritiene di fondamentale importanza una comunicazione che permetta, innanzitutto, ai genitori e alle famiglie e, più in generale, agli utenti una corretta informazione sui sistemi di classificazione, sui sistemi di controllo parentale e sui contenuti distribuiti sul web, sulle piattaforme streaming, in televisione, in radio, ecc. Una più diffusa e specifica strategia di comunicazione rende infatti possibile far maturare una maggiore consapevolezza riguardo anche l'uso del *parental control*. Il CNU sostiene che una corretta comunicazione debba essere integrata, incoraggiando in particolar modo attività e campagne di sensibilizzazione a favore degli utenti, anche attraverso un uso coordinato dei diversi mezzi informazione e comunicazione tra i quali la diffusione di informazioni e articoli a mezzo stampa (carta stampata, canali radiofonici, televisivi e piattaforme web), portali multimediali, trailer promozionali, social media, manifestazioni, eventi, spot e campagne di comunicazione istituzionale, ed ogni altra iniziativa tesa a valorizzare gli aspetti di responsabilità e consapevolezza delle famiglie, dei genitori e degli utenti. Tanto andrebbe effettuato sia nella fase di attivazione del *parental control* quanto nella fase successiva, cioè nella fase di gestione del servizio, quando cioè possono sorgere maggiori difficoltà di utilizzo e di comprensione per l'utente. Il CNU, per tali ragioni, ritiene che sarebbe opportuno assicurare modalità di comunicazione più omogenee di gestione da parte dell'utente del SCP (per le operazioni di attivazione, disattivazione, configurazione, ecc.), indipendentemente dal fornitore del servizio e dal dispositivo dell'utente. L'obiettivo infatti dovrebbe essere quello di facilitare l'utente in maniera chiara ed omogenea all'uso del SCP, senza dover essere, di volta in volta, nuovamente istruito in caso di cambio operatore o dispositivo terminale;

RILEVATO che un altro profilo importante per il CNU riguarda la possibilità di personalizzare più facilmente i contenuti oggetto di filtro dei SCP da parte dei titolari del contratto che coinvolge direttamente gli adulti e, in particolare, i genitori, chiamati a svolgere la funzione educativa. A questi ultimi, dovrebbe essere data l'opportunità di aggiungere o rimuovere dalle *black list* e dalle *white list* siti ritenuti inappropriati per i propri figli, di configurare il SCP per fasce orarie, assieme alla possibilità di controllare la navigazione tra i siti visitati. Pertanto, i genitori dovrebbero essere messi in grado di adottare modalità di tutela dei minori orientate ai propri valori e modelli educativi, nonché

di finalizzare le esigenze di sicurezza nella navigazione in rete al godimento dei diritti di formazione, socializzazione, libera espressione della propria personalità che le risorse della rete rendono disponibili per i minori. Inoltre, per quanto riguarda le criticità relative all'aggiramento dei blocchi DNS nella navigazione da parte del minore, sarebbe necessario poter bloccare le richieste relative a domini associati alla presenza di contenuti oggetto di filtro su una pagina web, alla porta 53;

RILEVATO, altresì, che il CNU, sotto il profilo tecnico-funzionale, suggerisce che la guida operativa sul Sistema di controllo parentale debba essere non solo disponibile sul sito web dell'operatore, ma preventivamente sottoposta ad approvazione dell'AGCOM. Si dovrebbero, inoltre, definire le caratteristiche di un SCP, indicando un novero minimo di elementi indispensabili. Contestualmente alla pubblicazione sul sito, l'operatore dovrebbe effettuare una campagna comunicativa (reiterata periodicamente) rivolta a tutti i clienti per informarli dell'esistenza e disponibilità di tale guida e delle forme di assistenza fornite sul SCP. Il CNU ritiene altresì che dette forme di assistenza dovrebbero prevedere almeno un numero gratuito di assistenza telefonica, esclusivamente dedicato al SCP, oltre ad un canale digitale di assistenza sul sito dell'operatore, tipo chat, dove la risposta provenga non solo da un sistema automatico di tipo *chatbot*, ma - se richiesto - preveda anche l'intervento di un operatore umano. La qualità di tali servizi di assistenza dovrebbe essere regolamentata con le stesse regole e criteri previsti, attualmente e in futuro, dall'Agcom per l'assistenza ai clienti dei servizi di comunicazione elettronica;

RILEVATO, infine, che il CNU suggerisce di prevedere un meccanismo di pre-attivazione, disattivazione e configurazione semplice e omogeneo, che renda disponibili i SCP su tutte le linee, a partire dalla data di entrata in vigore della regolamentazione in esame. Tale meccanismo, per le nuove linee, dovrebbe essere disponibile contestualmente all'attivazione della linea stessa; sulle linee pre-esistenti, entro un determinato tempo tecnico, con obbligo di informare periodicamente l'utente della disponibilità del sistema attraverso modalità differenziate (invio ripetuto di SMS, comunicazione in bolletta, in caso di utenti con contratto in abbonamento, e così via). Inoltre, il CNU intende sottolineare l'esigenza che la fornitura dei servizi SCP sia gratuita, come peraltro dovrebbero essere forniti gratuitamente agli utenti tutti i servizi correlati al funzionamento dei SCP. Nessun costo a nessun titolo dovrebbe essere imposto per alcuna operazione ad essi correlata. A tale riguardo, il CNU rileva come non appaia opportuna l'integrazione dei SCP con ulteriori componenti funzionali ad altri scopi. Tuttavia, potrebbe essere concessa all'ISP la possibilità di fornire funzionalità più avanzate 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, lettura di SMS e messaggistica. Inoltre, per ciò che concerne la verifica dell'età essa potrebbe essere agevolata prevedendo almeno tre possibilità di autenticazione in grado di contribuire ad una sempre maggiore tutela dei minori in tale ambito, tra cui anche l'uso dello SPID fatta salva la necessaria preliminare valutazione di impatto sulla protezione dei dati. Infine, il CNU sottolinea l'importanza di considerare l'accessibilità e

l'usabilità universale nella progettazione di ciascuno dei suddetti profili (tecnologico – funzionale, di informazione, comunicazione istituzionale, trasparenza e personalizzazione dei filtri) in virtù del diritto di esercitare il cosiddetto *parental control*, anche da parte di genitori con disabilità, in modo che, utilizzando le opportune tecnologie assistive, siano in grado di interagire con gli strumenti di comunicazione e informazione più diffusi;

RITENUTO che l'adozione delle Linee Guida è coerente con il Regolamento (UE) sopracitato in materia di Open Internet, in quanto effettuato in attuazione della normativa nazionale di cui all'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di "*Sistemi di protezione dei minori dai rischi del cyberspazio*";

RITENUTO, dunque, che, in ottemperanza ai propri compiti istituzionali e ai poteri conferitele dall'art. 7-*bis* del decreto-legge 30 aprile 2020, n. 28, al fine di consentire l'effettiva applicazione dell'intervento legislativo sul punto e la piena attuazione dei diritti da questo attribuiti alla tutela dei minori, l'Autorità debba intervenire sul piano prescrittivo a tutela dei consumatori nell'assicurare che sia loro fornito un sistema di *parental control*, il più efficace e efficiente possibile dal punto di vista tecnico;

RITENUTO, altresì, che la messa a disposizione di un sistema di *parental control* da parte dei fornitori di servizi di comunicazione elettronica debba necessariamente essere accompagnata da informazioni trasparenti, adeguate e aggiornate in merito alla disponibilità e al corretto utilizzo del servizio fornito;

RITENUTO opportuno individuare, attraverso le Linee guida, i requisiti minimi e opzionali dei sistemi di *parental control* rilasciati dagli operatori, in ordine alle modalità di realizzazione degli stessi, alle modalità di configurazione, alla fornitura di informazioni chiare e trasparenti sulle modalità di utilizzo da parte dei titolari dei contratti di servizi di comunicazione elettronica;

CONSIDERATO quanto segue:

I. Individuazione delle categorie e dei contenuti da bloccare

La maggior parte dei rispondenti chiedono che, già in queste Linee guida, siano fornite indicazioni sulle categorie e sui contenuti da bloccare, in modo da poter direttamente procedere alla attuazione della norma.

Secondo i rispondenti la norma dovrebbe subito 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.

A tale proposito, dagli approfondimenti svolti nel corso della consultazione è emerso che gli operatori principali hanno già autonomamente realizzato dei sistemi di *parental*

control mediante *partner* tecnologici che si occupano dell'individuazione dei siti e dei domini di contenuti inappropriati (raggruppati nelle diverse categorie descritte successivamente) e del continuo aggiornamento di tale elenco. Il blocco non agisce, nella maggior parte dei casi, a livello di singolo contenuto, ma a livello di dominio/sottodominio web, sulla base della classificazione/profilatura del sito/dominio o sottodominio fornita dal soggetto terzo e sulla base del blocco impostato o meno dall'utente amministratore della linea

Quindi gli operatori, generalmente, si basano sui servizi di soggetti terzi che mettono a disposizione tanto le soluzioni tecniche che le liste di domini e sottodomini inclusi in determinate categorie.

A tale riguardo, si rileva che lo stesso consumatore viene messo nelle condizioni di poter personalizzare le categorie e liste presentate a seconda del livello di sicurezza che desidera. Il cliente può customizzare la propria protezione aggiungendo o eliminando categorie ai propri blocchi o, se del caso, inserendo specifici nomi a dominio da inserire nella *black list*. In alcuni casi il cliente può impostare i filtri sui contenuti di un'intera categoria oppure solo su determinati domini all'interno di una o più categorie.

Va detto che, nelle soluzioni finora realizzate, i sistemi di *parental control* sono abbinati a servizi di più ampia finalità di accesso alla Rete in sicurezza. Le categorie utilizzate in genere abbastanza ampie sono delle seguenti tipologie:

1. Contenuti per adulti
2. Contenuti ritenuti inquietanti
3. Contenuti relativi a droghe, alcol, tabacco
4. Gioco d'azzardo
5. Contenuti e *download* illegali
6. Contenuti relativi ad armi e violenza
7. Contenuti che incitano all'odio e alla discriminazione
8. Contenuti relativi a pratiche religiose non tradizionali, tipicamente note come "culti", di carattere estremista o coercitivo
9. Siti di Incontri
10. Shopping e aste
11. Pubblicità
12. Siti che facilitano la navigazione anonima
13. Intrattenimento (programmazione di televisione, film, musica, news, etc)
14. File Sharing

15. Forum e newsgroup
16. Hacking e truffa
17. Contenuti su nudità non pornografica, lingerie, etc,
18. Attività criminali, autolesionismo, abuso di minori,
19. Giochi online,
20. Politica,
21. Social network,
22. Streaming di contenuti multimediali
23. Posta elettronica.

Si osserva che, per lo più, per quanto più specificatamente attiene al *parental control*, gli operatori si sono orientati verso le seguenti categorie:

Nome	**Descrizione**
Contenuti per adulti	Siti web riservati ad un pubblico maggiorenne, siti che mostrano nudità totale o parziale in un contesto sessuale pornografico, accessori sessuali, attività orientate al sesso. Siti che supportano l'acquisto online di tali beni e servizi.
Gioco d'azzardo/scommesse	Siti che forniscono informazioni o promuovono il gioco d'azzardo o supportano il gioco d'azzardo online e/o scommesse.
Armi	Siti che forniscono informazioni, promuovono o supportano la vendita di armi e articoli correlati.
Violenza	Siti che presentano o promuovono violenza o lesioni personali, comprese le lesioni autoinflitte, il suicidio, o che mostrano scene di violenza gratuita, insistita o efferata
Odio e discriminazione	Siti che promuovono o supportano l'odio o l'intolleranza verso qualsiasi individuo o gruppo

Nome	**Descrizione**
Promozione di pratiche che possono danneggiare la salute alla luce di consolidate conoscenze mediche	A titolo di esempio siti che promuovono o supportano l'anoressia e/o la bulimia, l'uso di sostanze stupefacenti illegali, di alcol o di tabacco
Anonymizer	Siti che forniscono strumenti e modalità per rendere l'attività online irrintracciabile.
Sette	Siti che promuovono o che offrono metodi, mezzi di istruzione o altre risorse per influire su eventi reali attraverso l'uso di incantesimi, maledizioni, poteri magici o essere soprannaturali.

A tale proposito, nelle Linee guida, l'Autorità ha richiamato l'art. 37 del D.Lgs. n. 208/2021 (TUSMA), recante l'attuazione della direttiva (UE) 2018/1808, relativo alle "*Disposizioni a tutela dei minori nella programmazione audiovisiva"*, nella parte in cui indica, ai commi 1 e 2, le trasmissioni vietate sul territorio nazionale e i correlati compiti dell'Autorità.

Ai sensi del comma 1, *sono vietate le* ***trasmissioni televisive gravemente nocive allo sviluppo fisico, psichico o morale dei minori, e, in particolare, i programmi che presentano scene di violenza gratuita o insistita o efferata ovvero scene pornografiche, nonché i film la cui proiezione o rappresentazione in pubblico ai minori di anni diciotto sia stata vietata dalle Autorità a ciò competenti****, salve le previsioni di cui al comma 3 applicabili unicamente ai servizi a richiesta. Al fine di conformare la programmazione alla disposizione di cui al presente comma, i fornitori di servizi di media audiovisivi si attengono ai criteri fissati dall'Autorità con apposite procedure di co-regolamentazione*.

Sono già individuate, in particolare, alcune categorie quali:

- violenza
- pornografia
- contenuti inquietanti in generale in quanto nocive alla crescita del minore.

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

direttamente poste dal presente articolo, e assicurando che i contenuti classificati ai sensi del comma 1 siano ricevibili e fruibili unicamente nel rispetto delle condizioni fissate ai sensi del comma 5."

Inoltre, in deroga ai divieti stabiliti e in conformità all'art. 37 comma 2 del TUSMA, le trasmissioni vietate possono essere trasmesse una volta adottata, mediante co-regolamentazione e d'intesa con altre istituzioni e soggetti (*Ministero, l'Autorità garante per l'infanzia e l'adolescenza e il Comitato di applicazione del Codice di autoregolamentazione media e minori)*, la disciplina di dettaglio contenente l'indicazione degli accorgimenti tecnici idonei a escludere che i minori vedano o ascoltino normalmente tali programmi.

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

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

Tuttavia, i rispondenti hanno chiesto che l'Autorità, già in esito a questo procedimento, fornisca delle indicazioni concrete sulle categorie e sui contenuti da bloccare.

Si ritiene, pertanto, di precisare nelle Linee guida che l'Autorità si riserva, ai fini dell'art. 7-bis, di fornire, ai sensi del comma 12 dell'art. 37 del D.Lgs. n. 208/2021, criteri per l'individuazione dei programmi e servizi di cui ai commi 1 e 2 dello stesso.

Nelle more, visti gli esiti della consultazione svolta, gli operatori, nel tener conto di quanto già indicato dal comma 1 dell'art. 37 citato, laddove fissa già delle categorie, possono utilizzare le liste di domini/sottodomini e contenuti determinate secondo proprie specifiche di servizio e/o fornite da soggetti terzi individuati sulla base della serietà e capacità professionale avuto riguardo alla idoneità degli stessi a perseguire gli scopi della legge e alle migliori prassi.

Gli operatori dovranno comunicare all'Autorità, per l'espletamento della propria vigilanza, le categorie adottate, i fornitori terzi, e i criteri di selezione da parte del consumatore.

Una volta che l'Autorità avrà definito le categorie gli operatori dovranno, ove occorra, tener conto di quanto stabilito e adeguare i criteri di scelta delle categorie.

II. Ambito di applicazione

La maggior parte dei rispondenti ritiene che le norme in questione si debbano applicare solo ai consumatori e non alla clientela affari.

Le Linee guida fanno genericamente riferimento agli utenti finali che, come noto, includono i clienti del settore *business*.

Si ritiene di accogliere tale precisazione atteso che è il medesimo decreto 28/2020, al comma 2 dell'art. 7-bis, a fare testuale riferimento al "*consumatore*", così delineando l'ambito soggettivo della disposizione.

III. Pre-attivazione dei sistemi di *parental control*

Con riguardo alla pre-attivazione dei SCP, la norma dispone che "*I contratti di fornitura nei servizi di comunicazione elettronica disciplinati dal codice di cui al decreto legislativo 1° agosto 2003, n. 259, devono* ***prevedere tra i servizi preattivati*** *sistemi di* ***controllo parentale*** *ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto."*

Al riguardo, gli operatori rilevano che la pre-attivazione dei sistemi di *parental control* non dovrebbe riguardare le linee sottoscrivibili solo da consumatori maggiorenni, come ad esempio nel caso delle linee fisse. Pertanto, propongono un sistema pre-attivato solo nel caso di offerte riservate a un pubblico di minorenni, presenti nel caso dei servizi mobili, e disponibile su richiesta per tutte le altre offerte.

Ciò premesso, il concetto di pre-attivazione richiede una precisazione.

Come emerso in sede di istruttoria, gli operatori prevedono dei sistemi di *parental control* spesso abbinati con altri servizi di navigazione in sicurezza e protezione, basati su Applicazioni che devono essere scaricate e installate tipicamente tramite un link ricevuto via SMS. Ad esempio, nel caso delle App, a seguito dell'attivazione di un'offerta dedicata ai minori, il Cliente/Genitore riceve un SMS contenente un link per scaricare l'App da installare sul proprio terminale e del minore. Tali applicazioni sono anche, in genere, utilizzabili da smartphone, PC, Tablet. L'APP è infatti talvolta disponibile per il *download* su Google Play per il sistema operativo mobile Android, su App Store per il sistema operativo mobile iOS, ed è anche disponibile per PC con sistema operativo Microsoft e per Mac Apple con sistema operativo macOS.

L'attivazione del servizio comporta un determinato costo mensile per singola licenza e la funzionalità di *Parental control* è spesso abbinata ad altre tipologie di protezione.

Il concetto di pre-attivazione, nella modalità APP, appare, pertanto, presupporre che l'offerta già includa la funzionalità di *Parental control* gratis, cosa che oggi per lo più avviene per le offerte mobili riservate ai minori, ferma restando la necessità di procedere con l'installazione dell'applicazione.

Quando il *parental control* è basato su filtro DNS, non è in generale necessario effettuare l'installazione di alcuna applicazione sullo *smartphone, PC o tablet*. Le funzionalità *parental control* intervengono nella rete.

In conclusione, in generale è previsto, per il *parental control*, un costo mensile di attivazione sia nel caso di APP che per i sistemi basati su DNS, mentre è gratis nelle offerte dedicate ai minori.

Preso atto di quanto sopra si ritiene di meglio chiarire le Linee guida prevedendo che il servizio è incluso, ad esempio con l'invio del link o delle istruzioni per utilizzarlo, per le offerte dedicate ai minori. Per le altre offerte, non dedicate ai minori, il servizio è disponibile a richiesta da parte del consumatore.

In applicazione della legge i servizi di *parental control*, come definiti nella funzionalità base, non sono a pagamento.

IV. Servizi aggiuntivi al semplice blocco dei siti web

Nelle Linee guida al punto 5 è previsto che:

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

In aggiunta al punto 7 si prevede:

> ***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.***

Infine, al punto 10 è previsto che:

> ***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.*

Al punto 5 è riportato che:

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).

Tutti gli operatori ritengono che alcuni servizi aggiuntivi costituiscano un obbligo non proporzionato e complesso da realizzare, non previsto dalla legge, con criticità a livello di *privacy*; altri rilevano siano in violazione dell'autonomia tecnica operatori. Propongono, se del caso, siano considerati come funzionalità aggiuntive a pagamento.

Anche altri rispondenti sono di analogo avviso. Alcuni ritengono che dovrebbe essere concessa all'ISP la possibilità di fornire funzionalità più avanzate (non solo antivirus e simili) a pagamento, mentre altri chiedono che venga assicurata la trasparenza per gli eventuali costi.

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

Al riguardo, è opportuno richiamare il dettato normativo che opera esclusivo riferimento a *"sistemi di* ***controllo parentale*** *ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto"* e non, quindi, a servizi ulteriori.

Si ritiene, pertanto, ragionevole specificare, nelle Linee guida, che la funzionalità da mettere a disposizione gratis è quella di filtro dei domini. Le altre funzionalità di cui ai punti 5 (*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)* e 7 possono essere previste come facoltative.

Nel caso in cui detti servizi aggiuntivi siano a pagamento l'operatore dovrà garantire massima trasparenza sui costi.

Si ritiene, tuttavia, di confermare la previsione di cui al punto 10 sulla possibilità di personalizzare le categorie oggetto di filtro per tutti gli operatori, indipendentemente dalla fascia a cui appartiene l'ISP anche alla luce del riscontro che gli operatori già rendono disponibile detta funzionalità.

V. Autenticazione ai fini della disattivazione del *parental control*

Nelle Linee guida la disattivazione e configurazione del *parental control* richiede l'inserimento di:

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

Al riguardo, gli Operatori rispondenti ritengono le forme di autenticazione proposte nel documento di consultazione (PIN, SPID, autenticazione nell'area riservata, OTP) eccessivamente onerose.

Alcuni degli altri rispondenti ritengono che debba essere sempre disponibile la modalità SPID.

Altri ancora propongono che se si utilizza altra modalità, in alternativa allo SPID, occorre prevedere l'inserimento di una OTP.

Pertanto, visti gli esiti della consultazione e sulla base di un principio di proporzionalità della regolamentazione, si propone di specificare che le modalità proposte sono alternative. Tra le modalità si ritiene opportuno confermare l'invio di una OTP via SMS o e-mail come era comunque già previsto.

VI. Interfacce messe a disposizione del consumatore per attivazione, disattivazione e configurazione del *parental control*

Si richiama che le Linee guida prevedono quanto segue:

> ***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.*

Gli operatori reputano 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 stessi, 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. In generale propongono una interfaccia web o App.

Una associazione rispondente ritiene che l'interfaccia web e la app siano al momento sufficienti e ribadisce l'opportunità di prevedere un'unica interfaccia web e un'unica app del SCP per attivazioni, disattivazioni e configurazioni.

Alcuni rispondenti reputano non sempre tecnicamente fattibile il blocco e lo sblocco in tempo reale.

Ciò premesso, visto gli esiti della consultazione, considerato che l'Autorità ha già proposto come modalità alternative l'APP o il sito web, purché sia garantita una facile utilizzabilità e accessibilità, si ritiene di confermare quanto proposto precisando che le operazioni di attivazione, disattivazione e configurazione dei SCP avvengano con le tempistiche consentite dalla capacità tecnologica disponibile.

VII. Soglie per distinzione tra operatori grandi e minori

Si richiama che le Linee guida hanno graduato gli obblighi in funzione della dimensione dell'ISP:

- Operatori di fascia A: operatori con almeno 100.000 linee dati attive.
- Operatori di fascia B: operatori con almeno 10.000 e fino a 100.000 linee dati attive.
- Operatori di fascia C: tutti gli altri operatori.

I maggiori operatori si sono dichiarati contrari alle soglie, mentre i minori propongono soglie diverse.

Anche parte delle associazioni rispondenti si sono manifestate contrarie alle soglie ritenendo preferibile prevedere obblighi minimi per tutti.

Tenuto conto che si propone di considerare facoltative le funzionalità di cui al punto 5 (sullo sblocco temporaneo del dominio o sito) e 7, che erano previste per gli operatori di fascia A, di rendere obbligatorie per tutti le funzionalità di cui al punto 10, che erano fissate per le fasce A e B, e, come meglio chiarito di seguito, di eliminare il punto 6, in cui si fissavano altri obblighi per la fascia A, si ritiene opportuno eliminare ogni riferimento alle soglie.

VIII. Aspetti tecnici sul filtro dei contenuti a livello di rete

Nelle Linee guida a livello tecnico si proponeva quanto segue:

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

6. ***Gli operatori di fascia A complementano le funzionalità di cui al punto 5, mediante a) l'implementazione di filtri, basati sugli indirizzi IP, dei siti ospitanti contenuti non consentiti o di DNS non sicuri, b) l'implementazione del blocco di quelle funzionalità del terminale che consentono all'utente di utilizzare servizi DNS di altri soggetti, o servizi DNS di tipo DoT (DNS-over-TLS) e DoH (DNS-over-HTTPS), c) la fornitura di applicativi installabili dall'utente sui propri dispositivi per consentire il filtraggio dei singoli contenuti.***

Le posizioni dei rispondenti sono molto articolate.

In linea generale gli operatori ritengono che spetti a loro individuare la soluzione tecnica. Per cui chiedono di emendare interamente il punto 6 delle Linee Guida, ritenendo di dover consentire ampio margine discrezionale circa l'individuazione del metodo più efficace di filtraggio rispetto allo scopo preposto.

In aggiunta sono state evidenziate una serie di criticità rispetto alle proposte del punto 6 delle Linee guida:

- il blocco tramite DNS presenta dei punti di debolezza nella misura in cui la maggior parte dei router o delle CPE permettono all'utente di indicare *resolver* DNS diversi da quelli dell'ISP; recentemente anche i *browser* hanno iniziato a consentire all'utente di indicare un *resolver* diverso da quello dell'ISP, collegandovisi tramite il protocollo cifrato DNSover-HTTPS, progettato appositamente per inoltrare il traffico del protocollo DNS all'interno del traffico Web e renderne impossibile il blocco;
- 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;
- l'inibizione del protocollo DoH, atteso che la porta impiegata è quella utilizzata per tutto il traffico http protetto (porta 443), comporterebbe l'inibizione generalizzata di tutto il traffico https;
- non si ritiene 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;
  - 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.
- un Operatore, con riferimento al punto delle linee guida 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. 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. Il sistema di *routing* generalmente non riconosce i singoli utenti e quindi il blocco si applicherebbe a tutti gli utenti dell'ISP o perlomeno a tutti gli utenti dello specifico accesso Internet, minorenni e maggiorenni. 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.

Inoltre, 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).

- qualche operatore segnala che la richiesta di effettuare un blocco verso indirizzi IP "associati a server DNS", 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.

  Sottolinea comunque come la base legale per tale richiesta non sia 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, restringendo significativamente l'usabilità della rete in generale, disturbando o interrompendo servizi e applicativi che richiedono l'uso di server DNS propri; trattasi di una misura, quindi, presumibilmente incompatibile con il Regolamento 2015/2020.

- 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, incidendo su servizi e applicazioni non correlati necessariamente all'accesso a Internet dei minori, appare andare oltre quanto previsto dal D.L. e di dubbia compatibilità con il Regolamento 2015/2020.

- un operatore fa rilevare che, essendo ormai le comunicazioni delle pagine web crittografate dal protocollo https, la comunicazione avviene sul numero di porta 443

con indirizzamento nell'URL https://; la tecnologia non consente di effettuare, su un dispositivo in rete che non è a uno dei due capi della comunicazione, come sono gli apparati degli ISP, un filtro a livello di contenuti. È possibile effettuare filtri per nome dell'host (filtro DNS oppure analisi del campo SNI del traffico Web) oppure per indirizzo IP (*firewall* e blocchi di *routing*). Propone di inserire nella definizione che il blocco può avvenire solo per interi siti o nomi a dominio, o, se legato a indirizzo IP, per interi server e gruppi di server (spesso ospitanti molti siti). Anche un operatore fa presente che il proprio SCP non agisce a livello di contenuto ma a livello di dominio/sottodominio web.

- un operatore ritiene che la previsione delle Linee guida di cui alla lettera c) la fornitura di applicativi installabili dall'utente sui propri dispositivi per consentire il filtraggio dei singoli contenuti sia di difficile attuazione atteso che tali applicazioni dovrebbero essere sviluppate dai produttori di terminali d'utente piuttosto che dagli operatori ISP.

Alla luce di quanto osservato dal mercato, ritenuto opportuno definire un obbligo di carattere generale valido per tutti gli ISP, si ritiene opportuno eliminare il punto 6 delle Linee guida considerato che l'elevato tecnicismo che lo caratterizza rende la raccomandazione soggetta ai continui cambiamenti delle soluzioni tecniche di accesso ai servizi DNS.

Si condivide, tra l'altro, la richiesta del mercato di lasciare più ampio margine agli operatori e ai *partner* tecnologici al fine di individuare la soluzione tecnica più efficace.

Si ritiene, pertanto, di confermare il punto 5 con un obbligo di mettere a disposizione almeno un sistema di *parental control* che sia basato su DNS o altro filtro a livello di rete o APP scaricabile dal consumatore.

Ne consegue che gli operatori possano individuare le soluzioni tecniche che ritengono maggiormente efficaci.

In caso di segnalazioni di inadeguatezza delle soluzioni messe in campo, l'Autorità – come disposto dalla normativa in materia – potrà intervenire con misure ad hoc.

Gli operatori devono comunicare all'Autorità le soluzioni tecniche implementate, oltre alle categorie da bloccare, ai fini delle attività di vigilanza di competenza.

IX. **Reindirizzamento alla pagina web di errore**

Il punto 5 delle Linee guida prevede che:

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 evidenziano che il reindirizzamento potrebbe risultare tecnicamente impossibile nel caso in cui la pagina cui l'utente finale sta tentando di accedere fosse criptata (HTTPS), come avviene oggi nella quasi totalità dei casi.

Si propone, alla luce di quanto sopra, di specificare che la misura richiesta va implementata laddove tecnicamente fattibile.

X. **Informazione ai consumatori**

Le Linee guida prevedono quanto segue:

> ***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.

Secondo gli operatori gli unici canali di comunicazione utilizzabili, in termini di costi di gestione, sono i seguenti:

- la pubblicazione di contenuti su home-page,
- l'invio di e-mail
- il self-care nell'area cliente
- documento di fatturazione (per i clienti fissi)
- notifica via SMS (per i clienti mobili), nel caso di attivazione del servizio,
- la documentazione contrattuale,
- il call center
- la Carta dei servizi

Gli stessi Operatori escludono la praticabilità della chiamata diretta effettuata dall'operatore in ragione dei costi eccessivi e del possibile fraintendimento da parte del cliente, che la assimilerebbe ad una chiamata di disturbo.

Alcuni rispondenti ritengono non utile ed eccessivamente onerose le modalità via SMS e e-mail.

Altri rispondenti pongono l'accento sull'importanza di campagne informative istituzionali.

Alla luce di quanto sopra, si ritiene di poter confermare quanto proposto nelle Linee guida fatta salva la chiamata *outbound* del *call center* alla luce degli eccessivi e non proporzionati costi anche al fine di non gravare sui consumatori con chiamate a cui potrebbero, visto il fenomeno del *teleselling* illegale, non rispondere.

Si ritiene altresì di consentire la modalità SMS come non obbligatoria.

È stato eliminato l'obbligo per le *pay TV* di dare notizia dell'esistenza dei SCP su fattura o *set-top box*, inserendo un obbligo per tutte le emittenti nazionali di dare evidenza di tali servizi, in quanto si reputa che questa disposizione sia maggiorente conforme a quanto previsto dalla Legge.

XI. Assistenza ai consumatori

Nelle Linee guida sottoposte a consultazione non sono previste specifiche misure.

Gli Operatori ritengono**,** unanimemente, che non siano necessari ulteriori canali di assistenza rispetto a quelli esistenti. Propongono quelli esistenti incluso i canali digitali.

Altri rispondenti propongono:

- l'assistenza tramite chat sul sito dell'operatore,
- 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,
- assistenza tramite e-mail per garantire di diritti degli utenti disabili (audiolesi),
- assistenza canale telefonico, anche con primo livello di risposta automatica.

Si ritiene, in linea generale, adeguato il ricorso agli attuali canali di assistenza come previsti dalla delibera n. 79/09/CSP.

Non si ritiene, pertanto, opportuno introdurre alcuna specifica previsione in queste Linee guida.

XII. Bundling con altri servizi

L'analisi delle offerte di *parental control* degli operatori ha evidenziato che gli stessi sono forniti a titolo oneroso abbinati con altri servizi di protezione e sicurezza.

Gli stessi non hanno preso specifiche posizioni su tale questione nella consultazione.

Altri rispondenti alla consultazione ritengono che i SCP non devono essere associati da parte ISP, in *bundle,* a servizi aggiuntivi a pagamento.

Si ritiene, a tale riguardo, tenuto conto del requisito della gratuità del sistema base di *parental control,* ossia il filtro di domini non consentiti, che la funzionalità dovrà essere garantita gratuita in maniera non abbinata ad altri servizi.

RILEVATO che, trattandosi di *regola tecnica*, lo schema di decisione approvato dal Consiglio nella seduta del 19 luglio 2022, recante l'adozione delle Linee guida per l'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*", è stato notificato alla Commissione europea, ai sensi Direttiva (UE) 2015/1535;

RILEVATO che, con comunicazione acquisita il 23 settembre 2022, la Direzione generale per il mercato, la concorrenza, la tutela dei consumatori e la normativa tecnica del MISE (*Unità Centrale di notifica*) ha informato l'Autorità che:

- il progetto di regola tecnica è stato comunicato alla Commissione europea in data 21 settembre 2022;
- il termine di tre mesi fissato dall'articolo 6, paragrafo 1, della direttiva (UE) 2015/1535 scade il 22 dicembre 2022;

- alla notifica è stato assegnato il numero 2022/0638/I – SERV60.

VISTA la nota con cui la Direzione generale per il mercato, la concorrenza, la tutela dei consumatori e la normativa tecnica del MISE (*Unità Centrale di notifica*) ha informato l'Autorità circa l'assenza di rilievi, osservazioni e/o pareri circostanziati formulati dalla Commissione europea o da altri Stati membri in merito alla notifica 2022/0638/I relativa al progetto recante "*Adozione delle 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"*;

RILEVATO che il MISE nella stessa nota conferma, pertanto, la scadenza del termine di differimento ai fini dell'adozione del provvedimento al 22 dicembre 2022;

RITENUTO, alla luce dell'assenza di rilievi da parte della Commissione, di adottare il provvedimento che conclude il procedimento di cui alla delibera n. 16/22/CONS;

UDITA la relazione del Commissario Laura Aria, relatore ai sensi dell'articolo 31, comma 1, del *Regolamento concernente l'organizzazione e il funzionamento dell'Autorità*;

DELIBERA

Articolo unico

1. Sono approvate le Linee guida per l'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*".
2. Le Linee guida di cui al comma 1 e la sintesi della consultazione pubblica di cui alla delibera n. 16/22/CONS sono riportate rispettivamente negli allegati A e B della presente delibera di cui costituiscono parte integrante e sostanziale.
3. Gli operatori si adeguano alle Linee guida di cui al comma 1 entro nove mesi dalla pubblicazione del presente provvedimento sul sito *web* dell'Autorità.
4. Entro lo stesso termine di cui al comma 3 gli operatori comunicano all'Autorità le soluzioni tecniche adottate, le categorie di contenuti da bloccare individuate e i soggetti terzi utilizzati come *partner* tecnologico ai fini della realizzazione del sistema di *parental control*.
5. In caso di violazione degli obblighi di cui al presente provvedimento, l'Autorità ordina all'operatore la cessazione della condotta e la restituzione delle eventuali somme ingiustificatamente addebitate agli utenti, indicando in ogni caso un termine non inferiore a sessanta giorni entro cui adempiere.

La presente delibera, comprensiva degli allegati A e B, è pubblicata sul sito *web* dell'Autorità e trasmessa alla Commissione europea, ai sensi dell'art. 9-bis, comma 8, del D.lgs.317/86.

Il presente atto può essere impugnato davanti al Tribunale Amministrativo Regionale del Lazio entro 60 giorni dalla pubblicazione dello stesso.

Roma, 25 gennaio 2023

IL PRESIDENTE
Giacomo Lasorella

IL COMMISSARIO RELATORE
Laura Aria

Per attestazione di conformità a quanto deliberato
IL SEGRETARIO GENERALE
Giulietta Gamba