Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurìdico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

FRANCESCA DI GIANNI*

PROTEZIONE DEI MINORI *VS.* TUTELA DEI DATI PERSONALI: PROFILI CRITICI DELLA PROPOSTA DI REGOLAMENTO SULLA PREVENZIONE E LA LOTTA CONTRO L'ABUSO SESSUALE SUI MINORI *ONLINE*

1. *Introduzione*

La transizione digitale ha determinato la necessità di elaborare un quadro normativo in grado di bilanciare il libero sviluppo del cyberspazio con la repressione dei contenuti di natura illecita, avendo particolare riguardo alla peculiare posizione di vulnerabilità in cui versano i minori. Cyberbullismo, *fake news*, *hate speech* e induzione all'autolesionismo sono solo alcuni dei pericoli cui sono esposti bambini e bambine a causa dello sviluppo tecnologico e della diffusione dei mezzi di comunicazione via Internet[1].

Il problema della sicurezza dei minori *online* appare particolarmente preoccupante se si considera la vasta gamma di abusi sessuali – quali l'adescamento, la pornografia infantile, il turismo sessuale e il traffico sessuale di minori, l'invio di materiale osceno (richiesto e) non richiesto – cui i minori si trovano sempre più esposti a causa dell'utilizzo sempre più massiccio delle tecnologie digitali nella vita quotidiana.

Secondo il Rapporto annuale 2022 dell'Internet Watch Foundation (IWF), il numero delle segnalazioni relative alla diffusione di immagini e video contenenti *child sexual abuse*

* Dottoressa di ricerca in Principi giuridici e istituzioni tra mercati globali e diritti fondamentali, Università degli studi di Bari Aldo Moro.

[1] N. BILIGOTTI, *La tutela dei minori nel cyberspazio. Parental Control di Stato e libera circolazione dei contenuti: un delicato equilibrio*, in *Rivista di Diritto dei Media*, 2023, p. 358-368, in particolare p. 359.

material (CSAM) è raddoppiato rispetto ai livelli del 2019[2] e, solo nell'Unione europea (UE), il numero di denunce per abusi sessuali sui minori *online* è passato da 23.000 nel 2010 a oltre 72.500 nel 2019, con un drastico peggioramento determinato dalla pandemia da Covid-19[3].

Insieme all'aumento della richiesta e della ricerca di materiale pedopornografico *online* in tutto il mondo[4], si attesta anche un abbassamento dell'età delle vittime, essendo coinvolti soprattutto bambini e bambine di età compresa tra i 3 e i 13 anni[5], nonché il ricorso a metodologie di adescamento sempre più diversificate tra cui l'estorsione finanziaria[6].

Sebbene l'abuso e lo sfruttamento sessuale dei minori e la diffusione di materiale pedopornografico costituiscano reato in tutta l'UE in virtù della direttiva 2011/93/UE sulla lotta contro l'abuso sessuale e la pornografia minorile[7], la dimensione *online* del fenomeno rappresenta una sfida ulteriore che richiede adeguata attenzione e un'azione specifica da parte dell'UE e dei suoi Stati membri.

2. *L'azione dell'Unione europea nella lotta contro gli abusi sessuali sui minori online*

Come è noto, in forza degli artt. 3, par. 3 e 5 del Trattato sull'Unione europea (TUE) la promozione della tutela dei diritti dei minori viene annoverata tra i principali obiettivi cui si ispira l'azione dell'UE[8]. Difatti, con l'entrata in vigore del Trattato di Lisbona ha inizio un

---

[2] Internet Watch Foundation, *The Annual Report 2022*, reperibile *online*: https://annualreport2022.iwf.org.uk/wp-content/uploads/2023/04/IWF-Annual-Report-2022_FINAL.pdf, p. 37

[3] Si vedano in proposito i dati raccolti dalla organizzazione no profit *National Center for Missing and Exploited Children* (NCMEC) che si occupa della raccolta delle segnalazioni trasmesse dalle aziende che hanno rimosso contenuti pedopornografici. I rapporti così realizzati vengono poi messi a disposizione delle forze dell'ordine di tutto il mondo per facilitarne il lavoro di contrasto al fenomeno degli abusi sessuali online sui minori, rendendo l'organizzazione un punto di riferimento fondamentale nel settore, anche per l'Unione europea: https://www.missingkids.org/theissues/csam. Inoltre, sul punto EUROPOL, *Exploiting Isolation: Sexual Predators Increasingly Targeting Children During COVID pandemic. A Further Increase in Sharing of Child Abuse Material Online, Sexual Coercion and Extortion of Children is Expected*, 19 giugno 2020, reperibile *online*: https://www.europol.europa.eu/media-press/newsroom/news/exploiting-isolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic.

[4] Con l'espressione "materiale pedopornografico" si intende il materiale che configura pornografia minorile o spettacolo pornografico ai sensi dell'art. 2, lett. c) ed e) della direttiva 2011/93/UE e, quindi, si riferisce a pornografia infantile e prestazioni pornografiche e ricomprende tutto il materiale coperto da quei termini, nella misura in cui può essere diffuso attraverso i servizi in questione (nella pratica: video e immagini).

[5] INHOPE, *Annual Report 2022*, consultabile *online*: https://inhope.org/media/pages/articles/annual-reports/14832daa35-1687272590/inhope-annual-report-2022.pdf, pp. 38-39

[6] Come evidenziato dal Federal Bureau of Investigation (FBI) degli Stati Uniti, dall'inizio del 2023 sempre più frequenti sono i casi di estorsione finanziaria, con cui attraverso l'utilizzo di account falsi i minori vengono avvicinati sulle piattaforme digitali, costretti a inviare foto o video espliciti e minacciati che vengano resi pubblici a meno che non inviino il pagamento richiesto: FBI, *International Law Enforcement Agencies Issue Joint Warning About Global Financial Sextortion Crisis*, 7 February 2023, reperibile *online*.

[7] Direttiva 2011/93/UE del Parlamento europeo e del Consiglio del 13 dicembre 2011 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio, in *G.U.U.E L 335/1* del 17 dicembre 2011.

[8] Si legge, infatti, che «[l]'Unione combatte l'esclusione sociale e le discriminazioni e promuove la giustizia e la protezione sociali, la parità tra donne e uomini, la solidarietà tra le generazioni e *la tutela dei diritti del minore*» (corsivo aggiunto) e «[n]elle relazioni con il resto del mondo [..] contribuisce […] alla tutela dei diritti umani, in particolare dei diritti del minore […]». In dottrina, si rinvia, *ex multis*, a P. F. LOTITO, *Art. 24 – Diritti del bambino*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali*

processo di valorizzazione degli interessi dei soggetti di minore età e dei principi di derivazione internazionale posti a tutela dei loro diritti fondamentali[9].

Nel sistema giuridico dell'UE il principale parametro di riferimento in materia è costituito dall'art. 24 (intitolato "Diritti del bambino") della Carta dei diritti fondamentali (d'ora in poi "Carta" o "Carta di Nizza")[10] – a cui è stato riconosciuto rango primario a partire dall'entrata in vigore del Trattato di Lisbona[11] – che rappresenta la sintesi dei principi e dei diritti fondamentali già riconosciuti a livello internazionale nella Convenzione delle Nazioni Unite sui diritti del fanciullo, conclusa a New York nel 1989[12], e nei suoi Protocolli facoltativi[13]. Riprendendo quanto definito dalla Convenzione del 1989, la Carta statuisce il diritto dei bambini alla protezione e alle cure necessarie per il loro benessere e, in ossequio al principio del *best interest of the child*[14], che in tutti gli atti che li riguardino, siano essi compiuti

dell'Unione europea, Milano, 2001, p. 185 ss.; C. CARLETTI, M. BOVA (a cura di), *Promozione, protezione e attuazione dei diritti dei minori: strumenti normative, politiche e strategie a livello internazionale ed europeo*, Torino, 2014, p. 15 ss.; F. CASOLARI, *Art. 24 della Carta dei diritti fondamentali dell'Unione europea*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'Unione europea*, II ed., Padova, 2014, pp. 1734-1739; A. RIZZO, *Uguaglianza*, in A. TIZZANO, *Trattati dell'Unione europea*, II ed., Milano, 2014, p. 2605 ss.; L. RATTI, *Art. 24 – Diritti del minore*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'unione europea*, Milano, 2017, p. 476 ss.

[9] A. GARDE, *Children and the European Union. Rights, Welfare and Accountability*, 2012, p. 8 ss.; O. LIND-HALDORSSON, R. O'DONNELL, *The Eu and Child Protection Systems: The Role and the Impact of the EU in Advancing Children's Protection Rights*, in I. IUSMEN, H. STALFORD (eds), *The EU as a Children's Rights Actor. Law, Policy and Structural Dimension*, Lancaster, 2015, p. 101 ss.; A. KISUNAITE, S. DELICATI, *The European Union and the United Nations Convention on the Rights of the Child. Towards a Fully-fledged European Union Child Rights Strategy*, in E. MARRUS, P. LAUFER-UKELES (eds), *Global Reflections on Children's Rights and the Law. 30 Years After the Convention on the Rights of the Child*, 2021, pp. 47 ss.

[10] In *G.U.U.E. C 364/1* del 18 dicembre 2000.

[11] In forza dell'art. 6 TUE, la Carta possiede la stessa efficacia vincolante dei Trattati istitutivi. Sul valore e sugli effetti della Carta si vedano, a titolo puramente esemplificativo, G. DI FEDERICO (ed.), *The EU Charter of Fundamental Rights, From Declaration to Binding Instrument*, Dordrecht, 2011; P. MORI, *Autonomia e primato della Carta dei diritti fondamentali dell'Unione europea*, in G. NESI, P. GARGIULO (a cura di), *Luigi Ferrari Bravo il diritto internazionale come professione*, Trento, 2015, 169 ss.; L. D'ANDREA, G. MOSCHELLA, A. RUGGERI, A. SAITTA (a cura di), *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, Torino, 2016; F. PAPPALARDO, *Preambolo*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *op. cit.*, p. 14 ss.

[12] United Nations, *Convention on the Rights of the Child*, United Nations General Assembly resolution 44/25, New York, 20 November 1989. In dottrina, *ex multis*, E.E. SHUTERLAND, *Implementing Article 3 of the United Nations Convention on the Rights of the Child. Best Interest, Welfare and Wellbeing*, Cambridge, 2016; Autorità garante per l'infanzia e l'adolescenza, *La Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza. Conquiste e prospettive a 30 anni dall'adozione*, 2019, reperibile *online*; U. KILKELLY, T. LIEFAARD, *International Human Rights of Children*, 2020; W. VANDENHOLE, G. E. TÜRKELLI, S. LEMBRECHTS, *Children's Rights. A Commentary on the Convention on the Rights of the Child and its Protocols*, Cheltenham, 2019; S. SONELLI, *I minori e i loro diritti: una tutela a più dimensioni*, Torino, 2022.

[13] *Optional Protocols to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict and on the Sale of Children, Child Prostitution and Child Pornography*, United Nations General Assembly, resolution A/RES/54/263, 16 March 2001; *Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict*, United Nations General Assembly, resolution A/RES/54/264ì3, 20 May 2000; *Optional Protocol to the Convention on the Rights of the Child on a Communications Procedure*, United Nations General Assembly, resolution A/RES/66/138, 27 January 2012.

[14] Per una ricostruzione storica del concetto si veda L. LENTI, *Note critiche in tema di interesse del minore*, in *Rivista di diritto civile*, 2016, p. 86 ss. Inoltre, in dottrina, si vedano, segnatamente C. FOCARELLI, *La Convenzione di New York sui diritti del fanciullo e il "best interests of the child"*, in *Rivista di diritto internazionale*, 2010, p. 981 ss.; E. LAMARQUE, *Prima i bambini. Il principio dei best interests of the child nella prospettiva costituzionale*, Milano, 2016; M. L. PADELLETTI, *Salvaguardia dei minori e best interests of the child secondo la Convenzione di New York sui diritti del fanciullo*,

da autorità pubbliche o da istituzioni private, l'interesse superiore del minore deve essere considerato preminente. Viene stabilito, dunque, un obbligo di metodo e di risultato, in virtù del quale il superiore interesse del minore deve sempre essere tenuto in considerazione nel bilanciamento degli altri diritti e interessi in gioco[15].

In questa prospettiva, nella Strategia dell'UE per una lotta più efficace contro gli abusi sessuali sui minori del 2020, la Commissione europea ha identificato la lotta contro il *child sexual abuse* (CSA) come una delle sue priorità[16]. Delineando una risposta globale alla crescente minaccia di abuso sessuale sui minori sia *offline* che *online*, la Strategia del 2020 ha delineato un quadro giuridico di protezione basato su otto iniziative e sul coinvolgimento di tutti le parti interessate nella prevenzione, nella protezione e nel sostegno ai minori[17].

A questa strategia si sono aggiunte altre iniziative dedicate. In particolare, il 24 marzo 2021 la Commissione europea ha adottato la Strategia dell'UE sui diritti dei minori, una prima strategia globale sui diritti dei bambini che intende porre questi ultimi e il loro superiore interesse al centro delle politiche dell'UE, con l'ambizione generale di rendere migliore possibile la loro vita nell'Unione europea e in tutto il mondo attraverso misure rafforzate di protezione avverso tutte le forme di violenza, incluso l'abuso e lo sfruttamento *online*[18]. Significativo, all'interno di questa strategia, appare l'invito rivolto dalla Commissione alle imprese operanti nel settore delle tecnologie dell'informazione e della comunicazione (ITC) ad implementare il loro impegno nella rilevazione, segnalazione e rimozione di contenuti illegali *online*, con particolare attenzione all'abuso sessuale sui minori, dalle loro piattaforme e dai loro servizi[19].

Con l'obiettivo ultimo di «promuovere un modello europeo per la trasformazione digitale, che metta al centro le persone, sia basato sui valori europei e sui diritti fondamentali dell'UE, riaffermi i diritti umani universali e apporti benefici a tutte le persone, alle imprese e alla società nel suo complesso», la recente proposta di Dichiarazione europea sui diritti e i principi digitali ha incluso tra i suoi obiettivi l'impegno a promuovere un ambiente digitale sicuro per i bambini e a proteggerli dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi *online* e ad impedire che il cyberspazio sia utilizzato per la commissione o il favoreggiamento di reati[20].

---

in *La Comunità Internazionale*, 2018, pp. 413-428, in particolare pp. 419-422; A. GAUDIERI, *Il principio dei "best interests of the Child" e la tutela della vittima minorenne nello spazio giuridico e giudiziario europeo*, in *Freedom, Security and Justice*, 2019, pp. 106-138; M.C. BARUFFI, *Il principio dei best interests of the child negli strumenti di cooperazione giudiziaria civile europea*, in A. DI STASI, L.S. ROSSI (a cura di), *Lo spazio di libertà, sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere*, Napoli, 2020, pp. 233-253.

15 P. F. LOTITO, *Art. 24*, cit. p. 185; F. CASOLARI, *Art. 24*, cit.

16 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'UE per una lotta più efficace contro gli abusi sessuali sui minori*, COM(2020) 607 final, Bruxelles, 24 luglio 2020, p. 2.

17 In particolare, garantire la piena ed efficace attuazione della legislazione vigente, individuare le lacune legislative, le migliori pratiche e le azioni prioritarie, rafforzare le azioni di contrasto e di prevenzione a livello nazionale e dell'Unione, istituire un centro europeo per la prevenzione e la lotta agli abusi sessuali sui minori, sostenere gli sforzi dell'industria volti a garantire che i prodotti assicurino la protezione dei minori e migliorare la protezione dei minori attraverso la cooperazione multipartecipativa.

18 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'UE sui diritti dei minori*, Bruxelles, 24 marzo 2021, COM(2021)142 final.

19 *Ibidem*, p. 17-20.

20 Dichiarazioni comuni, Parlamento europeo, Consiglio, Commissione europea, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, 23 gennaio 2023, in *G.U.U.E. C 23/1*, p. 22, lett. c) e d). In dottrina si rinvia,

Importante *trait d'union* tra i documenti indicati è il riconoscimento del ruolo svolto dai prestatori di servizi di *hosting* o di comunicazione nel contesto considerato, il cui comportamento responsabile risulta fondamentale per la costruzione di un ambiente *online* sicuro in cui sia garantito l'esercizio dei diritti e delle libertà fondamentali[21]. E in effetti, a fronte dell'aumento dei casi di abusi sessuali su minori nel cyberspazio, alcuni prestatori hanno iniziato ad utilizzare volontariamente apposite tecnologie di rilevamento, segnalazione e rimozione di CSAM. Ad esempio, già nel 2012 Facebook aveva avviato un'analisi di messaggi insoliti sulla sua piattaforma per l'individuazione di casi di adescamento di minori[22]; Microsoft, in collaborazione con il Dartmouth College, ha lavorato allo sviluppo di *PhotoDNA*, una tecnologia che aiuta a individuare e rimuovere immagini note di sfruttamento minorile, oggi utilizzato da organizzazioni di tutto il mondo[23]; e, nell'agosto 2021, Apple ha annunciato l'avvio di una nuova iniziativa per la rilevazione di materiale pedopornografico noto, poi rinviata per la forte opposizione ricevuta[24].

Tuttavia, considerate l'esiguità del numero di prestatori che vi fa ricorso e la diversità delle misure attuate e della qualità delle segnalazioni, questa azione volontaria si è rivelata insufficiente[25]. Cosicché, stante il carattere limitato di simili misure, alcuni Stati membri

segnatamente, a P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *Il Diritto dell'Unione europea*, marzo 2022, p. 1-15.

[21] Sul tema e per ulteriori riferimenti bibliografici, si veda in generale M. TADDEO, L. FLORIDI, *The Responsabilities of Online Service Providers*, London, 2017; F. WILMAN, *The Responsibility Of Online Intermediaries for Illegal User Content in the EU and in the US*, Cheltenam, 2020; M. L. MONTAGNANI, *Internet, contenuti illeciti e responsabilità degli intermediari*, Milano, 2018, in particolare pp. 71-129; G. MORGESE, *Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE*, in *Federalismi.it*, 2022, n. 1, p. 80 ss.; e G. M. RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet*, in *Rivista italiana di informatica e diritto*, 2022, pp. 17-24.

[22] J. MENN, *Social Networks Scan for sexual Predators, with Uneven Results*, 12 July 2012, reperibile *online*.

[23] Per informazioni dettagliate sul processo di sviluppo e sul funzionamento di questa tecnologia è possibile consultare la pagina dedicata sul sito ufficiale di *Microsoft*: https://www.microsoft.com/en-us/photodna.

[24] J. WAKEFIELD, *Apple Delays Plan to Scan iPhones for Child Abuse*, 3 September 2021, reperibile *online*.

[25] Secondo la Commissione europea, l'azione volontaria varia in modo significativo tra le imprese, è sensibile ai cambiamenti nelle politiche aziendali, lascia le decisioni che incidono sui diritti fondamentali ai fornitori di servizi e manca di garanzie armonizzate, rivelandosi inefficace: Commission Staff Working Document, *Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse*, SWD(2022)209 final, Bruxelles, 11 May 2022.

dell'UE (Germania[26], Francia[27], Olanda[28] e Austria[29]) hanno già adottato o sono in procinto di adottare norme nazionali volte a contrastare l'abuso *online* sui minori. Inevitabilmente, queste misure non seguono un modello unico, così rischiando di accentuare la frammentazione del mercato unico digitale dei servizi. Ciò ha determinato l'esigenza di un'armonizzazione delle norme di rilevazione, segnalazione e rimozione di casi di abuso sessuale sui minori *online* al livello dell'UE[30] e, quindi, l'elaborazione di una disciplina che integri la normativa sui servizi digitali ed elimini gli ostacoli esistenti.

Con l'intento di eliminare tali divergenze e prevenire l'insorgere di ostacoli determinati dall'ulteriore sviluppo di norme nazionali troppo diversificate tra loro, l'11 maggio 2022 la Commissione ha presentato la proposta di regolamento CSAM che "definisce norme uniformi per contrastare l'uso improprio dei servizi della società dell'informazione interessati a fini di abuso sessuale su minori online nel mercato interno"[31], in modo da stabilire un quadro giuridico chiaro e armonizzato in materia di prevenzione e contrasto all'abuso sessuale sui minori *online*[32]. Per conseguire questo obiettivo, la proposta prevede l'introduzione di obblighi di valutazione e attenuazione del rischio integrati da obblighi di rilevazione, segnalazione e rimozione di CSAM cui devono attenersi i prestatori che offrono determinati tipi di servizi *online* nel mercato unico digitale.

Tuttavia, considerati i molteplici diritti ed interessi in gioco, fin dalla sua presentazione la proposta CSAM ha suscitato non poche critiche e dubbi sulla sua effettiva capacità di riuscire a stabilire un giusto equilibrio tra le esigenze di tutela dei minori e dei loro diritti

---

[26] Si veda il *Netzwerkdurchsetzungsgesetz o Network Enforcement Act (NetzDG)* del 2018, che mira a combattere reati di odio e fake news e a migliorare l'applicazione del diritto penale tedesco online, in particolare in termini di cancellazione di contenuti illegali, e la *Gesetz zur Bekämpfung von Rechtsextremismus und Hasskriminalität im Internet* del 30 marzo 2021, la quale prevede l'obbligo per i prestatori di servizi online di adottare misure precauzionali strutturali, adeguate ed efficaci per proteggere i minori da contenuti pericolosi, proteggere i loro diritti individuali e i loro dati e sviluppare strumenti per favorire l'alfabetizzazione digitale.

[27] In particolare, si veda la *Loi n. 2020-766 du 24 juin 2020 visan à lutter contre le cotenus haineux sur internet*, che obbliga i fornitori di servizi online a rimuovere entro 24 ore qualsiasi contenuto che sia stato segnalato da qualsiasi utente (persona fisica o giuridica) o dalla polizia come manifestamente illegale. Il limite temporale per ottemperare all'obbligo di rimozione è ridotto a un'ora e si applica non solo alle piattaforme, ma a qualsiasi sito web qualora il contenuto sia stato segnalato come propaganda terroristica o materiale pedopornografico. V. anche il *Projet de Loi visant à sécuriser et réguler l'espace numerique du 5 juillet 2023*, che intende garantire protezione dai rischi associati all'uso di Internet per i privati e le imprese, nonché ad armonizzare le norme nazionali con quelle europee nell'ambito del progetto di creazione di un mercato unico digitale europeo. In particolare, rispetto alla tutela online dei minori, è prevista l'introduzione di un obbligo per i prestatori di rimuovere i contenuti pedopornografici, su ordine dell'autorità amministrativa, entro 24 ore. Ulteriori informazioni sul contenuto del progetto di legge sono reperibili al sito: https://www.senat.fr/travaux-parlementaires/textes-legislatifs/la-loi-en-clair/projet-de-loi-visant-a-securiser-et-reguler-lespace-numerique.html.

[28] Si veda la proposta di legge *Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal* del 16 febbraio 2021, che introdurrebbe l'obbligo per i prestatori di servizi online di rimuovere i contenuti terroristici e pedopornografici.

[29] Rilevante è il *Federal Act on measures to protect users on communication platforms (Communication Platforms Act)*, entrato in vigore il 1° gennaio 2021, il quale prevede l'obbligo per tutte le piattaforme di comunicazione rientranti nel suo ambito di applicazione di nominare un rappresentante responsabile di segnalare eventuali abusi sessuali online a danno di minori.

[30] Sul problema della frammentazione del mercato unico digitale e degli ostacoli al suo corretto funzionamento si veda Commission Staff Working Document, *Business Journey on the Single Market: Practical Obstacles and Barriers*, SWD(2020)54 final, Bruxelles, 10 March 2020, p. 29 ss.

[31] Art. 1, par. 1, della *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori*, 11 maggio 2022, COM(2022)209 final.

[32] *Ivi*, p. 3.

anche *online* e alcuni diritti e libertà fondamentali delle altre parti interessate, in specie la *privacy* di utenti e prestatori di servizi digitali.

Ciò posto, il presente contributo intende esaminare alcune delle problematiche giuridiche che sono state sollevate all'indomani della presentazione della suddetta proposta, chiedendosi se, stante l'attuale formulazione, la normativa oggetto di discussione sia davvero in grado di stabilire un giusto equilibrio tra i diritti e gli interessi che vengono in rilievo nel contesto considerato.

3. *Dal regolamento (UE) 2021/1232 (c.d. regolamento ePrivacy) alla proposta di regolamento CSAM*

La proposta di regolamento CSAM è diretta ad elaborare una normativa che sostituisca il regime temporaneo introdotto dal regolamento (UE) 2021/1232[33] (c.d. regolamento *ePrivacy*), con cui è stata prevista una deroga a talune disposizioni della direttiva 2002/58/CE (c.d. direttiva *ePrivacy*)[34] finalizzate a prevenire e combattere la diffusione di materiale pedopornografico e l'adescamento di minori *online*. La deroga temporanea introdotta dal regolamento *ePrivacy* è intervenuta a colmare una lacuna della direttiva *ePrivacy* – preposta a garantire il diritto alla vita privata e alla riservatezza in relazione al trattamento dei dati personali nel settore delle comunicazioni elettroniche[35] – determinata dalla mancanza di disposizioni specifiche sul trattamento dei dati personali da parte dei fornitori di servizi di comunicazione elettronica per l'individuazione, segnalazione e rimozione di materiale pedopornografico *online* dai propri servizi.

Fino alla entrata in vigore del regolamento *ePrivacy*, invero, il trattamento di comunicazioni e dati per il rilevamento di simili pratiche era stato affidato prevalentemente all'azione volontaria di alcuni fornitori, basata su tecnologie specifiche (ad es. la tecnologia *hashing* per le immagini e i video, classificatori, intelligenza artificiale per l'analisi del testo o di dati sul traffico), rivelatasi fondamentale per l'identificazione delle vittime, la riduzione dell'ulteriore diffusione di materiale pedopornografico e l'individuazione degli autori dei reati. Queste attività però rischiavano di interferire con alcune disposizioni della direttiva *ePrivacy*, priva di una base giuridica esplicita per il trattamento volontario di contenuti o dati sul traffico per il rilevamento di casi di CSA.

Il ricorso alle procedure volontarie di individuazione, segnalazione e rimozione di CSAM avrebbe dovuto realizzarsi, a norma dell'art. 15 della direttiva 2002/58/CE, sulla base di misure legislative adottate dagli Stati membri tese a limitare la portata dei diritti e degli obblighi di cui agli artt. 5 e 6[36], che tutelano rispettivamente la riservatezza delle

---

[33] *Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori*, in *G.U.U.E. L 274/41* del 30 luglio 2021.

[34] *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, in *G.U.U.E. L 201/37* del 31 luglio 2002.

[35] Per approfondimenti e ulteriori riferimenti si rinvia, *ex multis*, a C. KOENIG, A. BARTOSCH, J. D. BRAUN, M. ROMES, *EC Competition and Telecommunications Law*, Alphen aan den Rijn, 2009; G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, 2014; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

[36] *Regolamento (UE) 2021/1232*, 10° considerando.

comunicazioni elettroniche e i dati sul traffico. Pertanto, in mancanza di specifiche misure legislative nazionali, l'applicazione della direttiva *ePrivacy* privava i fornitori di servizi di comunicazione interpersonale della necessaria base giuridica per la realizzazione delle azioni dirette a rilevare abusi sessuali sui minori nei loro servizi.

Considerata l'importante funzione delle suddette attività volontarie nella lotta agli abusi sessuali su bambini e bambine *online*, il regolamento (UE) 2021/1232 ha introdotto una deroga, operativa dal 2 agosto 2021 fino al 3 agosto 2024, agli artt. 5, par. 1[37] e 6, par. 1[38] della direttiva *ePrivacy* per consentire ai fornitori di servizi di comunicazione interpersonale indipendenti dal numero (NI-ICS)[39] di continuare ad utilizzare tecnologie specifiche per il trattamento di dati personali e di altro tipo nella misura strettamente necessaria a individuare, segnalare e rimuovere il materiale pedopornografico *online* dai loro servizi (art. 1)[40].

Il monitoraggio indiscriminato delle comunicazioni private ha sollevato fin da subito numerosi dubbi circa la compatibilità della misura con il diritto alla *privacy*, manifestati dal Consiglio d'Europa[41] e dal Garante europeo della protezione dei dati (EDPS)[42]. Durante l'*iter* di elaborazione, avviato nel 2017, il regolamento è apparso problematico sia per l'incapacità di realizzare il necessario equilibrio *ex* artt. 7 e 8 della Carta tra il diritto al rispetto della vita privata e alla protezione dei dati degli utenti dei servizi rientranti nell'alveo del regolamento *ePrivacy* e le necessità di protezione dei bambini *online*, sia per il rischio di un alto tasso di errori di accertamento delle diverse tecnologie utilizzate.

Cosicché, nella sua versione finale, il testo dell'art. 3 del regolamento del 2021 prevede alcune condizioni per l'applicazione delle norme citate da parte dei fornitori. In particolare, che il trattamento dei dati sia strettamente necessario alle finalità previste, proporzionato e

---

[37] «Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare, essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza».

[38] «I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1».

[39] Dall'entrata in vigore della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche (*G.U.U.E. L 321/36* del 17 dicembre 2018) rientrano nell'ambito di applicazione della direttiva *ePrivacy* tutti i servizi indicati dall'art. 2 del Codice, inclusi i servizi di comunicazione interpersonale indipendenti dal numero. Con questa espressione si intende «un servizio di comunicazione interpersonale che non si connette a risorse di numerazione assegnate pubblicamente – ossia uno o più numeri che figurano in un piano di numerazione nazionale o internazionale – o che non consente la comunicazione con uno o più numeri che figurano in un piano di numerazione nazionale o internazionale» (art. 2, par. 7).

[40] D. LETTIG, L. BERTUZZI, *L'UE ha autorizzato le piattaforme a controllare le chat private per contrastare gli abusi sui minori*, 13 luglio 2021, reperibile *online*: https://euractiv.it/section/digitale/news/lue-ha-autorizzato-le-piattaforme-a-controllare-le-chat-private-per-contrastare-gli-abusi-sui-minori/; G. MORGESE, *Moderazione e rimozione*, cit., pp. 93-95.

[41] Council of Europe, *Respecting Human Rights and the Rule of Law when Using Automated Technology to Detect Online Child Sexual Exploitation and Abuse*, Indipendent Experts' Report, June 2021, consultabile *online*: https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee.

[42] EDPS, *Opinion 7/2020 on the Proposal for temporary Derogations from Directive 2002/58/EC for the Purpose of Combating Child Sexual Abuse Online*, 10 November 2020, consultabile *online*: https://edps.europa.eu/sites/default/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf.

limitato alle tecnologie utilizzate e ai dati sul contenuto e sul traffico (par. 1, lett. a), *sub* i). Peraltro, i fornitori sono tenuti a garantire che le tecnologie utilizzate, preventivamente valutate dalle autorità nazionali (par. 1, lett. c) e d)), siano conformi allo stato dell'arte del settore, le meno intrusive della vita privata (lett. b) e sufficientemente affidabili per limitare il tasso di errori (lett. e). Al contempo, è richiesta la predisposizione di procedure e meccanismi di ricorso adeguati a garantire che le persone colpite dalle suddette misure possano presentare un reclamo ai fornitori e ottenere la rettifica di eventuali errori, qualora determinati contenuti siano stati erroneamente qualificati come CSAM (par. 1, lett. g), *sub* ii); che garantiscano che il materiale non sia stato precedentemente identificato come materiale pedopornografico *online* o che l'adescamento di minori non sia stato segnalato alle autorità o alle organizzazioni di contrasto agli abusi sessuali sui minori senza previa conferma umana (*sub* iii); la previsione di procedure e meccanismi di ricorso adeguati affinché gli utenti possano presentare reclami (*sub* iv); che gli stessi siano informati dell'impatto del ricorso alla deroga sulla riservatezza delle comunicazioni (*sub* v), nonché delle modalità di presentazione dei ricorsi, della possibilità di presentare un reclamo all'autorità di controllo e del diritto ad un ricorso giurisdizionale qualora il loro contenuto sia stato rimosso (*sub* vi).

Tuttavia, nonostante la previsione del soddisfacimento di queste condizioni per garantire il carattere proporzionato della limitazione dei diritti al rispetto della vita privata e alla protezione dei dati personali determinata dall'applicazione della deroga, il regolamento ha suscitato non poche perplessità. Basti pensare che, all'interno del Parlamento europeo, alcuni gruppi hanno contestato la normativa sostenendo che non tutelasse i minori, ma esponesse questi ultimi e gli altri utenti dei servizi coinvolti a gravi rischi di violazioni dei loro diritti fondamentali dal momento che una scansione generalizzata e indiscriminata del contenuto delle comunicazioni private è da considerarsi inaccettabile in quanto lesiva del diritto alla vita privata[43]. Peraltro, come già anticipato, nonostante l'importante contributo di alcuni prestatori, la sola disposizione di azioni volontarie contro l'abuso sessuale sui minori *online* si è rivelata insufficiente, dato il numero esiguo di prestatori che vi fa ricorso[44]. Senza considerare la durata limitata del regolamento che, come già indicato, resterà in vigore fino al 3 agosto 2024 essendo una deroga temporanea.

È in questo quadro che si inserisce la citata proposta di regolamento CSAM, volta a sostituire il regolamento provvisorio del 2021 con un quadro a lungo termine che possa assicurare il migliore equilibrio possibile tra tutela dei minori, *privacy* degli utenti e sicurezza delle comunicazioni.

Imperniata sull'art. 114 del Trattato sul funzionamento dell'Unione europea (TFUE), che prevede, come noto, l'adozione di misure atte a garantire il funzionamento del mercato interno, la proposta CSAM mira ad eliminare le barriere esistenti alla prestazione dei servizi interessati nel mercato unico digitale e a contrastare l'abuso sessuale sui minori perpetrato attraverso un uso improprio dei servizi dell'informazione e della comunicazione. A tal fine, viene prefigurato un quadro giuridico chiaro e armonizzato in materia attraverso l'introduzione di obblighi a carico dei prestatori dei servizi della società dell'informazione

[43] A questo proposito, si veda la *Relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE del Parlamento europeo e del Consiglio per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali sui minori*, A9-0258/2020, 11 dicembre 2020, p. 42.

[44] COM(2022)209 final, p. 2-3.

che offrono detti servizi nell'UE indipendentemente dal luogo di stabilimento principale (art. 1, par. 2 della proposta).

Iniziando a esaminare l'articolato, viene anzitutto ampliata la nozione di "abuso sessuale sui minori *online*" così da includervi non solo il materiale pedopornografico già rilevato e indentificato (c.d. "noto"), ma anche quello non ancora rilevato né identificato come tale (c.d. "nuovo") e le attività di adescamento di minori (c.d. "*grooming*")[45].

Nella prospettiva di un rafforzamento della protezione dei minori nell'ambiente digitale, il regolamento in esame stabilisce norme armonizzate per i prestatori di servizi della società dell'informazione e i prestatori di servizi di *hosting* e di comunicazione interpersonale cui vengono imposti, sotto il profilo regolatorio, obblighi di valutazione e attenuazione del rischio di un uso improprio dei loro servizi, di rilevazione, segnalazione, blocco e rimozione di materiale pedopornografico noto e nuovo. Più di preciso, l'art. 3 impone ai questi soggetti di valutare i possibili rischi di un uso improprio dei loro servizi per la diffusione di CSAM o di adescamento (par. 1), tenendo conto dei casi già individuati come tali (par. 2, lett. a), dell'esistenza di una strategia e di funzionalità per contrastare simili rischi (lett. b), del modo in cui il servizio è ideato e gestito e utilizzato dagli utenti (lett. c) e d)), dell'età dei minori che utilizzano il servizio (lett. e), *sub* ii) e della presenza di funzionalità che possano dar luogo al rischio di *grooming* (*sub* iii).

Per ridurre al minimo i rischi eventualmente individuati, i prestatori potranno adottare misure di attenuazione efficaci, proporzionate e mirate in relazione al rischio individuato e applicate in maniera diligente e non discriminatoria (art. 4). Per ragioni di trasparenza, inoltre, dovranno riferire sull'esito della valutazione e sulle relative misure di attenuazione alle autorità coordinatrici designate dagli Stati membri, le quali determineranno se la valutazione del rischio e le relative misure di attenuazione siano conformi a quanto stabilito dagli artt. 3 e 4 (art. 5). Infine, ai prestatori di negozi di applicazioni *software* è imposto di valutare se le applicazioni per cui fungono da intermediari presentino il rischio di essere utilizzati a fini di adescamento e, nel caso in cui sia significativo, dovranno mettere in atto misure ragionevoli, identificare gli utenti di minore età ed impedire loro di accedere al servizio in questione (art. 6).

Tra le principali novità previste dalla proposta, vi è la previsione del potere riconosciuto all'autorità coordinatrice nazionale di chiedere all'autorità giudiziaria competente dello Stato membro che l'ha designata di emettere un "ordine di rilevazione" nei confronti di un prestatore di servizi di *hosting* o di servizi di comunicazione interpersonale rientrante nella giurisdizione dello Stato in questione (art. 7, par. 1). L'ordine di rilevazione impone al prestatore di adottare le misure di cui all'art. 10 per rilevare casi di CSA su un servizio specifico qualora l'autorità coordinatrice ritenga che sussista un rischio significativo di un suo uso improprio[46]. Tuttavia, la mera constatazione di un simile rischio non è considerata motivo sufficiente per emettere un ordine di rilevazione, considerate le conseguenze sproporzionate che potrebbe produrre sui diritti e gli interessi legittimi delle altre parti interessate, in specie gli utenti. È opportuno, quindi, che l'autorità competente

[45] *Ibidem*, p. 15.

[46] La qualificazione di un rischio come "significativo" è fatta dipendere dal tipo di CSA oggetto dell'ordine di rilevazione. Pertanto, relativamente al materiale pedopornografico noto, un simile rischio sussiste laddove vi siano prove che il servizio è stato utilizzato negli ultimi 12 mesi, in misura sensibile, per la diffusione di CSAM noto (par. 5). Mentre, per quanto attiene al materiale nuovo, un rischio significativo sussiste se vi sono prove che il servizio sia stato utilizzato, in misura sensibile, negli ultimi 12 mesi per la diffusione di CSAM nuovo (par. 6).

valuti obiettivamente, diligentemente e caso per caso la probabilità e la gravità delle potenziali conseguenze negative di un uso improprio del servizio e degli effetti sui diritti fondamentali degli altri attori coinvolti prima di procedere all'emissione dell'ordine, nonché delle capacità tecnologiche e finanziarie del prestatore, onde evitare l'imposizione di oneri eccessivi[47].

Qualora adottato, l'ordine di rilevazione deve essere individuato e specificato dall'autorità competente in modo tale da limitare le conseguenze negative per i diritti e gli interessi legittimi di tutte le parti interessate, così da garantire un giusto equilibrio tra i diritti fondamentali in gioco (par. 8). Pertanto, qualora il rischio sia limitato ad una parte o componente identificabile, l'autorità coordinatrice e l'autorità giudiziaria o amministrativa indipendente dovranno assicurare che le misure richieste trovino applicazione solo rispetto a questa parte o componente (lett. a), siano disposte garanzie proporzionate ed effettive (lett. b), e il periodo di applicazione dell'ordine sia limitato a quanto strettamente necessario (lett. c).

La proposta CSAM prevede, inoltre, disposizioni relative alla segnalazione, alla rimozione e al blocco di materiale pedopornografico.

Qualora il prestatore venga a conoscenza dell'esistenza di un caso di potenziale abuso sessuale sui minori nei suoi servizi, dovrà segnalarlo tempestivamente all'Agenzia dell'UE per la prevenzione e la lotta contro l'abuso sessuale sui minori ("Centro dell'UE sull'abuso sessuale sui minori" o "Centro dell'UE")[48] e informarne l'utente interessato, indicando il motivo alla base della segnalazione e le sue conseguenze nonché i possibili strumenti di ricorso a sua disposizione (art. 12, parr. 1 e 2).

Se, a seguito di diligente valutazione, l'autorità coordinatrice del luogo di stabilimento identifica un caso di CSAM potrà richiedere all'autorità giudiziaria competente dello Stato membro che l'ha designata di emettere un "ordine di rimozione" ed un "ordine di blocco" a carico di un prestatore di servizi di *hosting* e di accesso ad Internet. Per effetto dell'eventuale ordine di rimozione, il prestatore interessato dovrà disabilitare o rimuovere l'accesso in tutti gli Stati membri a uno o più elementi specifici del materiale in questione entro 24 ore (art. 14, parr. 1 e 2), a meno che non sia impossibilitato per cause di forza maggiore – inclusi motivi tecnici o operativi (par. 5) – oppure per errori manifesti o informazioni insufficienti per l'esecuzione (par. 6).

Contestualmente, a norma dell'art. 16, l'autorità coordinatrice ha la facoltà di richiedere anche l'emissione di un ordine di blocco con il quale è imposto al prestatore di servizi di accesso ad Internet di adottare misure ragionevoli per impedire agli utenti di accedere al materiale pedopornografico noto (par. 1), previa valutazione di una serie di elementi volta a determinare la sussistenza delle condizioni di cui al par. 4 (par. 2). In merito a queste ultime, rileva evidenziare che, prima di procedere alla richiesta di un ordine di blocco, l'autorità coordinatrice dovrà verificare che il servizio considerato è stato utilizzato negli ultimi 12 mesi e in misura sensibile per accedere o tentare di accedere al materiale pedopornografico indicato dagli identificatori uniformi di risorse di cui all'art. 44 (par. 4, lett. a); che l'ordine in questione è necessario per prevenire la diffusione del materiale pedopornografico, tutelare i diritti delle vittime e favorire l'attuazione di una politica del prestatore volta a scongiurare il rischio di tale diffusione (lett. b); che gli identificatori uniformi indicano l'esistenza di materiale pedopornografico in misura sufficientemente affidabile (lett. c); e che i motivi per l'emissione dell'ordine prevalgono sulle conseguenze negative per i diritti e gli interessi

[47] COM(2022)209 final, 22° considerando.

[48] Si tratta dell'agenzia europea che, secondo quanto prefigurato, dovrebbe sostenere e agevolare l'attuazione delle disposizioni del regolamento in esame (art. 40 della proposta).

legittimi di tutte le parti interessate, considerata «l'esigenza di garantire un giusto equilibrio tra i diritti fondamentali di queste parti, a partire dall'esercizio della libertà di espressione e d'informazione degli utenti e della libertà d'impresa del prestatore» (lett. d). Inoltre, in ragione di questa esigenza, è stabilito che l'emissione dell'ordine di blocco sia accompagnata dall'indicazione di limitazioni e garanzie effettive e proporzionate tese a limitare a quanto strettamente necessario le conseguenze negative e la durata del periodo di applicazione del blocco (par. 5, lett. a) e b)[49].

Un contributo fondamentale alla realizzazione dell'obiettivo perseguito dalla proposta in esame dovrà essere assicurato dal citato Centro dell'UE sull'abuso sessuale sui minori, che risponde alla necessità di definire responsabilità chiare in capo ai prestatori e di contribuire alla rimozione degli ostacoli al mercato interno[50]. In quanto organismo dell'Unione dotato di personalità giuridica (art. 41), gli viene attribuita la funzione di sostenere e agevolare l'attuazione delle disposizioni del regolamento, raccogliere e condividere informazioni e supportare la cooperazione tra le parti interessate, pubbliche e private, in materia di prevenzione e contrasto avverso l'abuso sui minori, in particolare *online* (art. 40). Nello specifico, lavorando a stretto contatto con l'Europol[51] e con le organizzazioni partner pertinenti[52], il Centro dell'UE dovrà provvedere all'istituzione di banche dati di tre tipi di indicatori di abuso sessuale sui minori *online*: quelli per rilevare la diffusione di materiale pedopornografico noto, quelli per il materiale pedopornografico nuovo e, infine, quelli per l'adescamento di minori (art. 44, par. 1), nonché di una banca dati contenente le segnalazioni trasmesse dai prestatori di servizi di *hosting* e di comunicazione interpersonale (art. 45). Si specifica che i suddetti indicatori dovranno essere applicati dai prestatori per ottemperare ai loro obblighi di rilevazione e formare la base degli eventuali ordini di blocco affinché sia garantita coerenza, efficienza ed efficacia e possa ridursi al minimo il rischio di elusione[53].

4. *Considerazioni sul bilanciamento operato dalla proposta di regolamento CSAM tra protezione dei minori* online *e tutela della vita privata e dei dati personali degli utenti.*

La proposta di regolamento CSAM costituisce un nuovo tassello del processo di costruzione di un sistema di moderazione e rimozione dei contenuti illegali *online* nell'Unione

[49] Il periodo di blocco non dovrà comunque superare i cinque anni, come prescritto dall'art. 16, par. 6.
[50] COM(2022)209 final, p. 3.
[51] L'Europol ha il compito di sostenere gli Stati membri nella prevenzione e nella lotta contro tutte le forme gravi di criminalità organizzata e internazionale, criminalità informatica e terrorismo. A tal fine, collabora anche con molti Stati partner non membri dell'UE e con diverse organizzazioni internazionali. Per informazioni dettagliate sulla struttura e sulle funzioni di Europol è possibile consultare il sito ufficiale: https://www.europol.europa.eu/.
[52] Tra cui il Centro nazionale statunitense per minori scomparsi e sfruttati (*U.S. National Centre for Missing and Exploited Children - NCMEC*) o la rete di *hotline* dell'Associazione internazionale delle linee telefoniche di emergenza per Internet (*International Association of Internet Hotlines - INHOPE*).
[53] COM(2022)209 final, 33° considerando.

europea[54], sistema oggi governato dal c.d. *Digital Services Act* (DSA)[55] rispetto al quale la proposta qui esaminata, qualora approvata, costituirà *lex specialis*[56]. In maniera analoga al DSA, infatti, la proposta CSAM risponde alla necessità di definire un sistema di norme armonizzate in materia di moderazione, rimozione e disabilitazione dei contenuti *online*[57], riproponendo anche in questo frangente la delicata questione del bilanciamento tra esigenze di sicurezza e tutela dei diritti fondamentali[58].

Da una prima lettura, sembrerebbe che l'elaborazione della proposta di regolamento CSAM sia avvenuta avendo riguardo alle possibili implicazioni che il nuovo regime potrebbe avere sul godimento di alcuni diritti fondamentali da parte dei soggetti coinvolti, in specie gli utenti e i prestatori dei servizi di comunicazione interpersonale. Riteniamo, infatti, che le disposizioni in essa contenute mostrino il riconoscimento delle sfide e delle problematiche intrinseche connesse ai nuovi obblighi posti a carico dei prestatori di tali servizi, prefigurando l'individuazione di un equilibrio tra diversi diritti e libertà fondamentali in gioco[59].

Tuttavia, così come avvenuto con il regolamento *ePrivacy*, la normativa proposta è apparsa fin dall'inizio molto controversa, in particolare per la dubbia capacità di garantire un

---

[54] Per "contenuto illegale" si intende «qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto»: art. 3, lett. h) del *regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)*, in *G.U.U.E. L 277/1* del 27 ottobre 2022. Tale concetto fa riferimento, in particolare, a tutte quelle informazioni che ai sensi del diritto applicabile sono di per sé illegali, tra cui l'incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori illegali, o che le norme applicabili rendono illegali in quanto relative ad attività illegali, come la condivisione di materiale pedopornografico (12° considerando del DSA).

[55] Per un'analisi del DSA si rinvia, tra gli altri, a L. WOODS, *Overview of Digital Service Act*, in *EU Law Analysis*, 16 dicembre 2020, reperibile *online*; G. CAGGIANO, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in G. CAGGIANO, G, CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, pp. 3-31; G. MORGESE, *Proposta di Digital Service Act e rimozione dei contenuti illegali online*, *ivi*, pp. 31-57; G. M. RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet*, in *Rivista italiana di informatica e diritto*, 2022, pp. 17-24; H. ZECH, *General and Specific Monitoring Obligations in the Digital Services Act*, in *Verfassungsblog*, 2 September 2021, reperibile *online*: https://verfassungsblog.de/power-dsa-dma-07/.

[56] COM(2022)209 final, 8° considerando.

[57] Sul tema si rinvia, segnatamente, a G. MORGESE, *Moderazione e rimozione*, cit.; A. DE STREEL, *Online Platforms' Moderation of Illegal content Online. Law, Practice and Options for Reform*, June 2020, reperibile *online*: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf; R. BELLANOVA, M. DE GOEDE, *Co-Producing Security: Platform Content Moderation and European Security Integration*, in *Journal of Common Market Studies*, 2022, pp. 1316-1334; D. C. NUNZIATO, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, in *Chicago Journal of International Law*, 2023, p. 115-128.

[58] Sul punto, B. CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, 2013; G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, Atti del Convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno", Messina, 26-27 maggio 2017; M. DISTEFANO (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017. Sul bilanciamento tra tutela della sicurezza nazionale e protezione dei dati personali, nonché sulla nota "saga *Schrems*", v. per tutti S. CRESPI, *L'influenza del diritto dell'Unione europea sulla sicurezza nazionale: l'art. 4, par. 2, TUE alla prova della recente giurisprudenza UE tra l'altro in materia di* privacy, in *Eurojus*, 2022, n. 4. Infine, sulla vicenda del software di sorveglianza delle comunicazioni (*spyware*) Pegasus, v. G. SARTOR, A. LOREGGIA, *The impact of Pegasus on fundamental rights and democratic processes*, Study requested by the European Parliament's PEGA Committee, 2022, reperibile *online*.

[59] P. DUNN, G. DE GREGORIO, *A New Tile for the EU Content Moderation Governance Mosaic? The Proposal for a Child Sexual Abuse Material Regulation*, in *MediaLaws*, 21 aprile 2023, reperibile *online*.

adeguato bilanciamento tra le esigenze di tutela dei minori e la protezione dei diritti e delle libertà degli interessati[60]; dubbi manifestati anche dall'European Data Protection Board (EDPB)[61] e dall'European Data Protection Supervisor (EDPS)[62], principali autorità di controllo della protezione dei dati, in un parere congiunto[63].

Nello specifico, perplessità sono sorte in merito alla conformità dell'ordine di rilevazione di cui all'art. 7 proposta CSAM con gli artt. 7, 8 e 11 della Carta dei diritti fondamentali, che assicurano rispettivamente la tutela della vita privata, la protezione dei dati personali e la libertà di espressione. Se, da un lato, è indubbio che un simile ordine persegua una finalità di interesse generale – quale la prevenzione e la lotta contro l'abuso sessuale sui minori, che costituisce un reato di particolare gravità – dall'altro, introduce significative limitazioni ai diritti considerati.

Ciò che ci si chiede è se tali limitazioni siano sufficientemente regolate all'interno della proposta da non compromettere l'essenza dei diritti considerati e, quindi, da garantire la necessaria proporzionalità rispetto all'obiettivo perseguito. In questa prospettiva, non è di poco momento ricordare che, secondo quanto stabilito dall'art. 52, par. 1 della Carta, qualsiasi limitazione all'esercizio dei diritti e delle libertà da essa riconosciuti deve essere prevista dalla legge e rispettare l'essenza di tali diritti e libertà; essenza che risulta lesa nel momento in cui il diritto considerato è svuotato del suo contenuto fondamentale, al punto da impedirne l'esercizio[64]. In altre parole, le limitazioni sono possibili solo se rispondenti ad obiettivi di interesse generale perseguiti dall'Unione e non costituiscano, rispetto allo scopo prefissato, un intervento sproporzionato e inaccettabile, tale da ledere il contenuto sostanziale del diritto così garantito[65]. Si ricorda che, per costante giurisprudenza sia della Corte di giustizia dell'Unione europea (CGUE) sia della Corte europea dei diritti dell'uomo (Corte Edu),

---

[60] Si veda, in tal senso, il reclamo formale presentato dall'European Digital Rights (EDRi) alla Commissione europea ancor prima della presentazione della proposta dell'11 maggio 2022, *Scanning Private Communication in the EU*, 9 February 2022, reperibile *online*: https://edri.org/wp-content/uploads/2022/02/EDRi-principles-on-CSAM-measures.pdf. Si vedano, inoltre, la petizione presentata da 15 organizzazioni per i diritti umani e la giustizia nella campagna "*Stop Scanning Me EU*", *Sign Now. Privacy Emporwers, Surveillance Weakens*, consultabile *online*: https://stopscanningme.eu/en/; la richiesta di ritiro della proposta di regolamento presentata da 134 organizzazioni della società civile, *European Commission: Uphold Privacy, Security and Free Expression by Withdrawing New Law*, 8 June 2022, reperibile *online*: https://edri.org/wp-content/uploads/2022/06/European-Commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law.pdf.

[61] Il Comitato europeo per la protezione dei dati (EDPB) è un organismo europeo indipendente che riunisce le autorità nazionali per la protezione dei dati dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati (EDPS). Per approfondimenti in merito alle sue funzioni e alla sua struttura è possibile consultare il sito ufficiale: https://edpb.europa.eu/edpb_en.

[62] Il Garante europeo della protezione dei dati è un'autorità indipendente che si adopera per la protezione dei dati dell'Unione europea (UE). Per informazioni dettagliate sul suo mandato è possibile consultare il sito ufficiale: https://edps.europa.eu/_en.

[63] EDPS-EDPB, *Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse*, 28 July 2022, reperibile *online*: https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf.

[64] Sul punto, si vedano la sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, *Maximillian Schrems* c. *Data Protection Commissione*r, causa C-362/14, ECLI:EU:C:2015:650, parr. 94 e 95; la sentenza dell'8 aprile 2014, *Digital Rights Ireland e al.*, cause riunite C-293/12 e C-594/12, EU:C:2014:238, ECLI:EU:C:2014:238, par. 39; la sentenza *Tele2 Sverige*, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970, par. 123. Si veda, inoltre, EDPS, *Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data*, 19 dicembre 2019, reperibile *online*, nonché S. CRESPI, *op. cit.*

[65] Sentenza della Corte di giustizia dell'Unione europea del 14 gennaio 2021, *OM*, causa C-393/19, ECLI:EU:C:2021:8, par. 53.

questo requisito implica che l'atto che consente l'ingerenza con un determinato diritto debba definire, esso stesso, in maniera chiara e precisa la portata della limitazione all'esercizio del diritto considerato[66].

Sebbene la proposta di regolamento sembri apparentemente conforme al primo requisito di cui all'art. 52, par. 1 della Carta, data la previsione di un insieme composito di norme sulla valutazione, mitigazione e segnalazione di rischi di CSAM e sulla conseguente emissione di un ordine di rilevazione, alcuni elementi paiono compromettere una simile conclusione.

Innanzitutto, la terminologia utilizzata appare particolarmente ampia, risultando caratterizzata da un notevole grado di vaghezza. Relativamente alla valutazione e alla mitigazione del rischio, l'art. 3 della proposta obbliga i fornitori di servizi di *hosting* e di servizi di comunicazione interpersonale a identificare, analizzare e valutare il rischio di utilizzo del servizio ai fini di abuso sessuale sui minori *online* e a cercare di ridurre al minimo il rischio individuato richiedendo di ricorrere a "misure di mitigazione ragionevoli e adeguate" (artt. 3 e 4 della proposta): sebbene il par. 2 dello stesso art. 3 indichi quali elementi debbano essere presi in considerazione nella valutazione del rischio, alcuni dei criteri mancano di chiarezza, determinando il rischio che i prestatori possano interpretare i propri obblighi in modi differenti al punto da compromettere la valutazione iniziale da cui si fa dipendere l'eventuale emissione di un ordine di rilevazione.

In secondo luogo, non vengono specificate in modo sufficientemente dettagliato la natura e le caratteristiche delle tecnologie da utilizzare nell'attuazione di un ordine di rilevazione. In particolare, manca qualsiasi indicazione su cosa si intenda per "tecnologie di rilevazione sufficientemente affidabili" e quale sarebbe il "tasso di errore" relativo alla rilevazione da considerare accettabile in termini di equilibrio tra efficacia e misure che siano meno intrusive possibile[67]. Così facendo, la proposta di regolamento riconosce un'ampia discrezionalità interpretativa ai prestatori di servizi di comunicazione, affidando ad essi la scelta delle tecnologie cui fare ricorso e, quindi, anche la responsabilità sulle conseguenze del loro funzionamento sui diritti in gioco.

Ciò posto, riteniamo che, sebbene le norme proposte siano formulate in maniera aperta e flessibile, ciò non significa necessariamente che il requisito dell'art. 52, par. 1, della Carta non possa essere soddisfatto. Vale la pena di ricordare, infatti, che la CGUE ha osservato come tale requisito non escluda una formulazione di tale limitazione in termini sufficientemente ampi da potersi adattare a fattispecie differenti e a eventuali cambiamenti di situazioni[68] e la possibilità che essa stessa possa, se necessario, precisarne la portata sia

---

[66] Si vedano, *ex multis*, la sentenza *Schrems II* in cui la CGUE afferma che «[…] il requisito secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato»; la sentenza CGUE del 16 luglio 2020, *Data Protection Commissioner* c. *Facebook Ireland Limited e Maximillian Schrems*, Causa C-311/18, par. 175; e la sentenza della Corte Edu nel caso *Big Brother Watch and Others v. The United Kingdom, (Applications n. 58170/13, 62322/14 and 24960/15)* del 25 maggio 2021, in cui il giudice di Strasburgo ha sottolineato che «[i]t is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures […]» (par. 333 e giurisprudenza *ivi* citata).

[67] *Joint Opinion 4/2022*, cit., pp. 16-17. Inoltre, sul punto, v. il documento SWD(2022)209 final, cit., pp. 281-283.

[68] Sentenza della Corte di giustizia dell'Unione europea del 26 aprile 2022, *Polonia* c. *Parlamento europeo e Consiglio*, causa C-401/19, ECLI:EU:C:2022:297, par. 74 e giurisprudenza ivi menzionata.

rispetto ai termini della normativa di cui trattasi sia rispetto all'impianto sistematico e agli obiettivi da essa perseguiti, come interpretati alla luce della Carta dei diritti fondamentali[69]. Questa circostanza giustificherebbe, quindi, il riconoscimento ai prestatori di servizi di comunicazione di una certa discrezionalità nella determinazione delle misure concrete da adottare per raggiungere l'obiettivo perseguito.

Pertanto, nonostante la poca chiarezza e la scarsa completezza dell'attuale formulazione del regolamento, non ci sembra che si possa affermare con assoluta certezza la non conformità della proposta alla disposizione di cui all'art. 52, par. 1 della Carta. Inoltre, è importante non trascurare che, nel caso di specie, le contestate discrezionalità e flessibilità verrebbero esercitate nell'ambito di un quadro normativo dettagliato, che prevede importanti limiti e garanzie. Una di queste è rappresentata dalla previsione che gli ordini di rilevazione siano emessi dalle autorità giudiziarie competenti o dalle autorità amministrative indipendenti di uno Stato membro previa "obiettiva, diligente e specifica valutazione", e siano preparati ed eseguiti sotto la supervisione e con il supporto di altre autorità pubbliche indipendenti, in particolare il Centro dell'UE e le autorità nazionali per la protezione dei dati[70].

Ad ogni modo, ciò non esclude la necessità di un'integrazione di elementi di maggior dettaglio sia sui limiti ai diritti coinvolti sia rispetto alla tecnologia cui i prestatori possono far ricorso, onde evitare che la discrezionalità riconosciuta a questi ultimi assuma la forma di una illimitata libertà d'azione tale da dar vita ad un controllo che, come verrà osservato in seguito, potrebbe favorire un accesso indiscriminato alle comunicazioni interpersonali.

5. Segue: *Il "precedente" della saga giurisprudenziale sulla c.d.* "data retention".

Prima di esaminare le specifiche questioni su cui è stato instaurato il dibattito, si rammenta che, al fine di proteggere i diritti fondamentali degli utenti dei servizi dell'informazione e della comunicazione (specificamente quelli stabiliti negli artt. 7, 8 e 11 della Carta), sono previsti una serie di limiti alla misura in cui i fornitori di tali servizi possono conservare e monitorare i dati sulle loro reti. Sebbene la questione richiederebbe ben altri approfondimenti, ci pare opportuno richiamare alcuni elementi fondamentali della disciplina della materia.

Ispirandosi ad un obiettivo di tutela della riservatezza e della protezione dei dati, la citata direttiva 2002/58/CE ha stabilito, *inter alia*, il divieto di memorizzazione di dati e metadati (dati relativi al traffico e all'ubicazione) prodotti dai servizi di telecomunicazione (art. 5), ponendo a capo dei *service provider* l'obbligo di cancellare o rendere anonimi i dati sul traffico relativi ai propri utenti nel momento in cui tali informazioni fossero diventate non più necessarie per la trasmissione della comunicazione stessa o per le fatturazione (art. 6)[71].

In deroga a questa regola generale, come precedentemente indicato, la direttiva *ePrivacy* ha previsto un regime eccezionale a norma dell'art. 15, par. 1 attribuendo agli Stati membri la facoltà di adottare normative dirette a limitare i diritti e gli obblighi dell'art. 6 «qualora tale

---

[69] Si vedano in tal senso la sentenza della Corte di giustizia dell'Unione europea del 26 aprile 2022, *Polonia* c. *Parlamento e Consiglio*, causa C-401/19, parr. 64 e 74, nonché la giurisprudenza *ivi* citata; e la sentenza del 21 giugno 2022, *Ligue des droits humains ASBL* c. *Conseil des ministres*, causa C-817/19, par. 114.

[70] Art. 7, parr. 1, 2 e 3 e art. 9, parr. 3 e 4 della proposta CSAM.

[71] G. FORMICI, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino, 2021, p. 56.

restrizione costituisca […] una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative che prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo».

L'art. 15 ha riconosciuto agli Stati membri un'ampia autonomia in merito alla determinazione degli obblighi di conservazione, in mancanza di specifiche condizioni e limitazioni, aprendo così ad una forma di *data surveillance* generalizzata per scopi securitari. Tuttavia, l'eccessiva discrezionalità attribuita ai legislatori nazionali unitamente alla vaghezza della disposizione di cui all'art. 15 ha dato vita ad un quadro normativo fortemente frammentario che ha sollevato non poche problematiche[72].

Avverso questa frammentarietà, è intervenuta la direttiva 2006/24/CE[73], atto contenente norme armonizzate in materia di conservazione dei dati contenuti nelle comunicazioni elettroniche[74], che ha segnato il graduale passaggio dalla *data protection* alla *data retention*[75]. La nuova disciplina ha stabilito che gli Stati membri devono adottare «misure per garantire che i dati, qualora generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati […], siano conservati conformemente alle disposizioni della presente direttiva» (art. 3, par. 1), per assicurarne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi (art. 1, par. 1). Tuttavia, non è stata predisposta una delimitazione dei soggetti i cui metadati dovevano sottoporsi a conservazione, cosicché la memorizzazione riguarda tutti gli utenti e tutte le comunicazioni elettroniche, senza la necessità di un collegamento tra *data retention* e indagini né di un'autorizzazione da parte di un'autorità nazionale competente. Inoltre, la conservazione – la cui durata è stabilita dal legislatore nazionale e deve essere comunque ricompresa tra sei mesi e due anni – deve riguardare unicamente i metadati indicati dall'art. 5[76], mentre restano esclusi i dati relativi al contenuto delle comunicazioni.

Molteplici sono i profili critici che hanno destato fin da subito profonde preoccupazioni circa l'impatto della normativa sui diritti fondamentali e sulla proporzionalità delle misure rispetto all'obiettivo perseguito[77]; criticità che hanno reso ben presto necessario

---

[72] *Ibid*., p. 57.

[73] *Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, in *G.U.U.E. L105/54* del 13 aprile 2006.

[74] In particolare, le informazioni volte a rintracciare la fonte di una comunicazione (numero telefonico o identificativo dell'utente di un servizio Internet o di posta elettronica), la destinazione di una comunicazione (come il numero del destinatario di una telefonata), data, ora e durata della comunicazione, il tipo di comunicazione e l'attrezzatura utilizzata, i dati relativi all'ubicazione delle apparecchiature.

[75] C. JONES, B. HAYES, *The EU Data Retention Directive: A Case Study in the Legitimacy and Effectiveness of EU Counterterrorism Policy*, in *Securing Europe Through Counter-Terrorism – Impact, Legitimacy and Effectiveness*, 2013, p. 1 ss.

[76] L. FEILER, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, in *European Journal of Law and Technology*, 2010, p. 1 ss.

[77] Per un approfondimento delle principali problematiche sollevate in riferimento alla direttiva 2006/24/CE si rinvia, *ex multis*, a F. BIGNAMI, *Protecting Privacy Against the Police in the European Union: the Data Retention Directive*, in *Melanges en l'honneur de Philippe Léger*, Parigi, 2006, p. 109 ss.; M. TAYLOR, *The EU Data Retention Directive*, in *Computer Law and Security Report*, 2006, p. 309 ss.; C. BONES, B. HAYES, *op. cit*.; E. GUILD, S. CARRERA, *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trial of the Data Retention Directive*, CEPS Paper in Liberty and Security in Europe, 2014, p. 7 ss.; G. CAGGIANO, *Il bilanciamento*, cit.

un intervento da parte della Corte di giustizia dell'UE, chiamata a pronunciarsi in più occasioni sulla *data retention*. Nello specifico, e per quanto ci interessa, rilevano alcune pronunce in materia di compatibilità della conservazione dei dati con i diritti fondamentali sanciti dagli artt. 7, 8, 11 e 52, par. 1 della Carta di Nizza, attraverso le quali la CGUE ha elaborato una serie di principi e indicazioni che, oltre ad aver determinato un ripensamento del bilanciamento tra esigenze securitarie e di tutela della *privacy* e della protezione dei dati, appaiono rilevanti nell'analisi in corso. Difatti, sebbene la Corte di Lussemburgo non abbia mai avuto modo, fino ad oggi, di esaminare la questione nel contesto della lotta alla diffusione di materiale pedopornografico, la base giurisprudenziale elaborata in riferimento alla conservazione e al monitoraggio dei metadati può fornire alcuni utili criteri per una valutazione di alcuni elementi della proposta CSAM.

Innanzitutto, la Corte di giustizia ha chiarito, nella nota sentenza *Digital Rights Ireland*[78], che la conservazione dei metadati pone il rischio di una grave lesione della vita privata, potendo rivelare informazioni in merito alla vita privata delle persone interessate[79], tale da generare da parte di queste ultime «la sensazione che la loro vita privata sia oggetto di costante sorveglianza» (par. 37). Di conseguenza, per poter essere legittimo, l'obbligo di conservazione deve soddisfare i requisiti indicati dall'art. 52 della Carta, vale a dire rispettare il contenuto essenziale dei diritti in gioco ed essere conforme al principio di proporzionalità. Sotto il primo profilo, la CGUE ha ritenuto che, sebbene la conservazione dei dati costituisca un'ingerenza particolarmente grave del diritto al rispetto della vita privata e degli altri diritti sanciti dall'art. 7 della Carta, non è tale da pregiudicarne il contenuto essenziale, dal momento che non permette di venire a conoscenza del contenuto delle comunicazioni elettroniche (par. 39). Al contempo, tale conservazione non è neppure idonea a pregiudicare il contenuto essenziale del diritto alla protezione dei dati personali di cui all'art. 8 della Carta poiché i fornitori sono tenuti a rispettare taluni principi di protezione e di sicurezza dei dati (par. 40). Invece, per quanto attiene il profilo della proporzionalità – per il quale gli atti delle istituzioni dell'Unione devono essere idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi e non superare i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi[80] – la CGUE si è limitata a stabilire che i metadati costituivano per le autorità competenti uno strumento supplementare di accertamento dei reati gravi e quindi la loro conservazione risultava proporzionata in quanto rispondente all'obiettivo securitario perseguito dalla normativa di riferimento (par. 49).

D'altro canto, la direttiva è stata giudicata non conforme al requisito della stretta necessità data la mancanza di regole chiare e precise sulla portata e l'applicazione della misura e sui requisiti minimi necessari affinché le persone interessate dispongano di sufficienti garanzie per la protezione dei loro dati personali avverso il possibile rischio di abusi, nonché contro eventuali accessi o usi illeciti di tali dati (par. 54); garanzie che risultano tanto più importanti «allorché i dati personali sono soggetti a trattamento automatico» (par. 55). A ben

[78] *Digital Rights Ireland*, cfr. nota 62, par. 39.

[79] Tra cui, le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali e gli ambienti sociali frequentati.

[80] Si vedano, in tal senso, la sentenza della Corte di giustizia dell'Unione europea dell'8 luglio 2010, *Afton Chemical Limited* c. *Secretary of State for Transport*, causaC-343/09, EU:C:2010:419, par. 45; la sentenza del 9 novembre 2010, *Volker und Markus Schecke GbR e Hartmut Eifert* c. *Land Hessen*, cause riunite C-92/09 e C-93/09, EU:C:2010:662, par. 74; la sentenza del 23 ottobre 2012, *Nelson e al.* c. *Deutsche Lufthansa AG*, cause riunite C-581/10 e C-629/10, EU:C:2012:657, par. 71; la sentenza del 22 gennaio 2013, *Sky Österreich GmbH* c. *Österreichischer Rundfunk*, causa C-283/11, EU:C:2013:28, par. 50; nonché la sentenza del 17 ottobre 2013, *Herbert Schaible* c. *Land Baden-Württemberg*, Causa C-101/12, EU:C:2013:661, par. 29.

vedere, da un lato, la direttiva 2006/24/CE obbliga i fornitori ad una conservazione generalizzata riguardante qualsiasi persona e qualsiasi mezzo di comunicazione elettronica, nonché tutti i dati relativi al traffico senza distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi (par. 57). Dall'altro, la conservazione non è subordinata all'esistenza di una relazione tra i dati e una minaccia per la sicurezza pubblica, né di indizi tali da far credere che il comportamento delle persone interessate possa avere «un nesso, ancorché indiretto o lontano, con reati gravi» (parr. 57 e 58).

Nel complesso, per poter essere legittima e proporzionata, la conservazione dei dati deve risultare limitata «a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate» coinvolte, in qualche modo, in un reato grave o «la conservazione dei cui dati […] potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi» (par. 59). Peraltro, la CGUE ha rilevato non solo mancanza di tali limiti, ma anche di criteri oggettivi volti a delimitare «l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento e di indagini» riguardanti reati che potessero essere considerati sufficientemente gravi da poter giustificare l'ingerenza nei diritti fondamentali di cui agli artt. 7 e 8 della Carta (par. 60). Infine, i giudici di Lussemburgo hanno ritenuto che la disciplina non definisse una durata della conservazione fondata su criteri obiettivi (parr. 64 e 65) né garanzie sufficienti avverso eventuali accessi e usi illeciti dei dati (parr. 67 e 68)[81].

Tutto quanto considerato, la normativa in questione non è stata ritenuta conforme al principio di proporzionalità alla luce degli artt. 7, 8 e 52, par. 1 della Carta.

Come è noto, con la decisione *Digital Rights Ireland* la Corte di giustizia UE ha imposto una rivalutazione dell'approccio alla *data retention*, evidenziando la necessità di un adeguato bilanciamento tra conservazione di massa dei dati ed esigenze di tutela della vita privata e della protezione dei dati[82]. In questa prospettiva, come ribadito nella sentenza *Tele2 Sverige*, uno Stato membro può adottare una normativa che permetta la conservazione dei metadati, purché tale conservazione «sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario» (par. 108)[83]. In altri termini, la normativa in questione deve prevedere norme chiare e precise che definiscano la portata della misura considerata, fornendo alle persone interessate sufficienti garanzie avverso eventuali rischi di abuso, e la conservazione deve rispondere a criteri oggettivi, così da delimitare la portata della misura e i soggetti coinvolti, nonché da rivelare una connessione, almeno indiretta, con gli atti di criminalità grave per i quali la misura è adottata[84].

Difatti, in considerazione della gravità dell'ingerenza nei diritti fondamentali in questione, solo la lotta avverso la criminalità grave è idonea a giustificare la conservazione dei metadati, fermo restando che questo obiettivo di interesse generale, per quanto fondamentale, non può considerarsi sufficiente a giustificare la necessità di una misura di conservazione generalizzata e indiscriminata dei dati (parr. 102 e 103).

Tutto quanto considerato, una normativa che manchi degli elementi appena indicati va al di là dei limiti dello stretto necessario e non può ritenersi fondata sulla disposizione di cui

---

[81] M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, in *European Law Review*, 2014, p. 849.
[82] G. FORMICI, *op. cit.*, p. 76; A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Diritto pubblico comparato ed europeo*, 2014, p. 1224 ss.
[83] *Tele2 Sverige*, cfr. nota 62.
[84] *Ibidem.*, parr. da 109 a 111.

all'art. 15, par. 1 della direttiva 2002/58/CE letto alla luce degli artt. 7, 8, 11 e 52, par. 1 della Carta dei diritti fondamentali (par. 107).

6. Segue: *il rischio di compressione dell'"essenza" dei diritti fondamentali nella proposta CSAM*

Alla luce di quanto detto nel paragrafo precedente, possiamo allora ritenere che un ordine di rilevazione, come quello prefigurato dalla proposta di regolamento CSAM, diretto all'individuazione di materiale pedopornografico e di casi di adescamento di minori implichi, *de facto*, l'accesso e l'analisi indiscriminati di tutti i contenuti del servizio di comunicazione interpersonale interessato, determinando una forma di monitoraggio dei dati su base generalizzata[85].

Il dibattito è sostanzialmente incentrato su due aspetti: da un lato, la capacità della normativa in esame, e in particolare dell'ordine di rilevazione, di preservare l'"essenza" dei diritti considerati; essenza che, come indicato, deve essere in ogni caso rispettata anche qualora sia prevista una loro restrizione[86]. Dall'altro, la proporzionalità della misura rispetto all'obiettivo perseguito e, quindi, l'individuazione di un giusto equilibrio tra i molteplici diritti ed interessi in gioco. Possono peraltro ritenersi condivisibili, almeno in parte, i dubbi che si pongono rispetto ai possibili effetti che potrebbero derivare dall'emanazione di un ordine di rilevazione sul godimento del diritto alla vita privata garantito dall'art. 7 della Carta e del diritto alla protezione dei dati personali di cui all'art. 8; dubbi che sono stati manifestati anche dal Servizio giuridico del Consiglio dell'Unione europea in un parere del 26 aprile 2023[87].

Per meglio comprendere le ragioni alla base del dibattito, rileva evidenziare che, in linea di principio, l'analisi automatizzata conseguente ad un ordine di rilevazione non consente di identificare gli utenti i cui dati sono soggetti a siffatta analisi. Tuttavia, qualora i dati in questione costituiscano "dati personali", ciò consentirebbe l'identificazione della persona o delle persone interessate. Secondo la definizione di cui all'art. 4, par. 1, del regolamento generale sulla protezione dei dati (GDPR)[88], per "dato personale" si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile» e si considera identificabile «la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Pertanto, poiché lo *screening* delle comunicazioni che verrebbe attuato per effetto del suddetto ordine presuppone l'accesso sistematico e l'elaborazione delle informazioni in esse contenute, ciò

---

[85] O. Van Daalen, *Does monitoring your phone affect the essence of privacy?*, in *European Law Blog*, 7 June 2022.

[86] M. Brkan, *The Concept of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core*, in *European Constitutional Law Review*, 2018, pp. 332-368; K. Lenaerts, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, in *German Law Journal*, No. 20, 2019, pp.779-793; EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, cit., p. 8.

[87] *Opinion of the Legal Service, Proposal for a Regulation laying down rules to prevent and combat child sexual abuse – detection orders in interpersonal communications – Articles 7 and 8 of the Charter of Fundamental Rights – Right to privacy and protection of personal data – proportionality*, 8787/23, Bruxelles, 26 April 2023.

[88] *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, in *G.U.U.E. L 119/1* del 4 maggio 2016.

può consentire, in una fase successiva, l'identificazione di tutti gli utenti interessati da tale analisi automatizzata.

A questo proposito, rileva quanto indicato dalla CGUE nella sentenza *La Quadrature du Net* del 6 ottobre 2020, in cui è stata esaminata una normativa belga che, al fine di salvaguardare la sicurezza nazionale, imponeva ai fornitori di servizi di comunicazione elettronica di implementare, sulle proprie reti, misure che consentissero l'analisi automatizzata dei dati di traffico e di ubicazione[89]. In particolare, secondo la Corte l'analisi automatizzata dei dati implica, per i fornitori di servizi di comunicazione elettronica interessati, l'attuazione di un trattamento generalizzato e indifferenziato dei dati come definito dall'art. 4, par. 2 GDPR[90] (par. 172). Ciò posto, una normativa nazionale che autorizza una siffatta analisi dei metadati, oltre a costituire una deroga rispetto a quanto disposto dall'art. 5 della direttiva 2002/58/CE a garanzia della riservatezza delle comunicazioni elettroniche e dei dati correlati, costituisce un'ingerenza nei diritti fondamentali di cui agli artt. 7 e 8 della Carta e può comportare effetti dissuasivi sull'esercizio della libertà di espressione stabilita al successivo art. 11 (par. 173). A detta della CGUE, infatti, l'ingerenza così determinata ha un elevato livello di gravità in quanto coinvolge in maniera generalizzata e indifferenziata i dati di tutti coloro che usufruiscono del servizio considerato, cosicché l'analisi automatizzata opera anche nei confronti degli utenti per i quali non esiste alcun elemento che possa indurre a ritenere che il comportamento tenuto possa rappresentare un nesso, sia pur indiretto o remoto, con un atto criminoso (par. 174).

Poiché la normativa nazionale oggetto di analisi nella sentenza considerata presenta una serie di punti in comune con l'ordine di rilevazione della proposta CSAM[91], le risultanze cui è giunta la Corte nel caso *La Quadrature du Net* risultano utili per una valutazione delle possibili ingerenze con alcuni diritti fondamentali cui potrebbe dar luogo il regime prefigurato dalla proposta in esame.

---

[89] Sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2020, *La Quadrature du Net e al.* c. *Premier ministre e al.*, cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, in particolare il par. 171. Per un'analisi della questione, si rinvia a J. SAJFERT, *Bulk Data Interception/Retention Judgments of the CJEU – A victory and a Defeat for Privacy*, 26 October 2020, reperibile *online*: https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/; M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione europea*, Torino, 2021, pp. 93-194; X. TRACOL, *The Two Judgments of the European Court of Justice in the Four Cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is Trying to Hard to Square the Circle of Data Retention*, in *Computer Law and Security Review*, July 2021, pp. 1-13; I. CAMERON, *Metadata Retention and National Security: Privacy International and La Quadrature du Net*, in *Common Market Law Review*, 2021, pp. 1433-1472; e S. ROYER, S. CAREEL, *Access Denied – CJEU Reaffirms La Quadrature du Net and Clarify Requirements for Access to Retained Data*, 23 March 2021, reperibile *online*: https://www.law.kuleuven.be/citip/blog/access-denied-cjeu-reaffirms-la-quadrature-du-net-and-clarifies-requirements-for-access-to-retained-data/.

[90] Ricordiamo che ai sensi della disposizione considerata per "trattamento" si intende «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

[91] In entrambi i casi, i prestatori sono tenuti a valutare automaticamente i dati delle comunicazioni, il cui *screening* è basato su una serie di "indicatori" elaborati dalle autorità pubbliche. Inoltre, entrambe le misure riguardano i servizi di comunicazione elettronica e possono rivelare la natura delle informazioni in esse contenute e trovano applicazione anche nei confronti dei soggetti per i quali non sussistono elementi idonei a far ritenere che il loro comportamento possa avere un collegamento, anche indiretto con i reati considerati.

Anzitutto, la circostanza che l'ordine di rilevazione sia indirizzato ad uno specifico prestatore, e non a tutti i servizi di comunicazione interpersonale non ci sembra che costituisca un argomento sufficiente per poter ritenere che la misura considerata non abbia carattere generalizzato e indiscriminato. Sebbene indirizzati a uno specifico *provider*, l'ordine di rilevazione determinerebbe una scansione del contenuto di tutte le comunicazioni interpersonali relative a tale servizio (o alla parte o componente interessata di esso)[92] mediante strumenti automatizzati. Di conseguenza, il trattamento dei dati non sarebbe limitato alle comunicazioni di quegli utenti rispetto ai quali sussistono fondati motivi per ritenere che siano coinvolti in una qualche forma di abuso sessuale sui minori *online* o presentino un nesso, anche indiretto, con casi di CSA. Peraltro, non solo non è contemplato alcun tipo di salvaguardia sostanziale a fronte di un simile rischio, ma pare fondato il timore che, al fine di scoraggiare l'uso di altri servizi a fini di abuso sessuale di minori, possa configurarsi un'estensione degli ordini di rilevazione ad altri prestatori e, quindi, dar vita ad una sorveglianza permanente di tutti i servizi di comunicazione interpersonale[93]. Ciò causerebbe un'ingerenza particolarmente grave nei diritti in gioco, dal momento che lo *screening* non riguarderebbe i metadati (come nel caso *La Quadrature du Net*) ma il ben più semsibile contenuto della comunicazione, risultando quindi molto più invasivo.

Il controllo generalizzato del contenuto delle comunicazioni per la rilevazione di materiale pedopornografico richiederebbe, tra l'altro, l'indebolimento o l'elusione di alcune misure di sicurezza informatica cui fanno oggi ricorso i prestatori di servizi di comunicazione interpersonale (come Signal, Telegram, Messenger di Facebook, WhatsApp e Direct Message di Instagram), in specie la crittografia c.d. "da punto a punto" (*End-to-End Encryption* o E2EE). Attualmente, le app di messagistica più popolari applicano questo strumento di sicurezza in virtù del quale, nel momento in cui le comunicazioni lasciano gli *endpoint*, vale a dire il dispositivo dell'utente (telefono o computer), l'accesso al loro contenuto non è più possibile senza la chiave di decrittazione, che è a disposizione solo del mittente e del destinatario della comunicazione[94].

Come abbiamo evidenziato, i *provider* non sono tenuti ad utilizzare una specifica tecnologia, ma è sufficiente che quest'ultima soddisfi le condizioni stabilite nella proposta, tra cui una condizione di efficacia che dovrebbe essere garantita anche in un ambiente crittografato. Tale condizione di efficacia implicherebbe, quindi, che l'ordine di rilevazione debba essere finalizzato all'analisi degli *endpoint*, vale a dire prima che la comunicazione venga crittografata, o che la crittografia debba essere modificata per consentire al prestatore di analizzare il contenuto delle comunicazioni "in transito" attraverso i *server*[95].

Di conseguenza, per adempiere agli obblighi posti a loro carico, ai fini dell'analisi dei dati personali ivi contenuti i prestatori dovrebbero prendere in considerazione l'abbandono della crittografia *end-to-end*, oppure l'introduzione di una sorta di "*back-door*" per accedere al contenuto crittografato o, ancora, il ricorso alla c.d. "scansione lato *client*" (l'accesso al contenuto sul dispositivo dell'utente prima che lo stesso venga crittografato). Tecnologie che si rivelerebbero molto invasive[96] e che, secondo alcuni, potrebbero trasformarsi in uno

[92] Art. 8, par. 1, lett. d) della proposta CSAM.
[93] Sul punto, si veda Council of the European Union, *Opinion of the Legal Service,* cit., parr. 44-48.
[94] B. LUTKEVICH, M. BACON, *End-to-End Encryption (E2EE)*, June 2021, consultabile *online*: https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE.
[95] *Opinion of the Legal Service*, cit., p. 17.
[96] In merito ai possibili effetti negativi della rimozione della crittografia E2E su alcuni diritti fondamentali, si veda il rapporto di Business Social Responsibility (BSR), *Human Rights Impact Assessment, Meta's Expansion of End-to-End Encryption*, 4 April 2022, reperibile *online*.

strumento di sorveglianza di massa[97]. Senza considerare i timori per il rischio di sfruttamento dell'indebolimento della crittografia da parte di altri soggetti, comprese le agenzie di *intelligence* straniere e le organizzazioni criminali[98]. Simili misure di sicurezza svolgono, infatti, un ruolo chiave per garantire che non venga pregiudicata la sostanza del diritto alla protezione dei dati personali di cui all'art. 8 della Carta. Dunque, le soluzioni tecniche volte a garantire e proteggere la riservatezza delle comunicazioni elettroniche, comprese le misure di crittografia, sono essenziali per garantire il godimento dei diritti fondamentali[99].

A ciò si aggiunge l'ulteriore constatazione secondo cui la comunicazione di dati personali a un terzo, come un'autorità pubblica, costituisce una chiara ingerenza nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta, al di là dell'uso ulteriore delle informazioni comunicate, e lo stesso vale per la conservazione dei dati personali nonché per l'accesso agli stessi ai fini del loro uso da parte delle autorità pubbliche[100]. Ciò indipendentemente dal fatto che le informazioni relative alla vita privata siano informazioni sensibili o che gli interessati abbiano subito eventuali inconvenienti[101]. Di conseguenza, una normativa che consenta alle autorità pubbliche «di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche» potrebbe pregiudicare il contenuto essenziale dei diritti considerati[102].

Alla luce di quanto indicato, ci sembra conclusivamente che si ponga la necessità di apportare modifiche all'accesso generalizzato al contenuto delle comunicazioni previsto dalla proposta CSAM, soprattutto in considerazione della possibile compromissione dell'essenza del diritto al rispetto della vita privata nonché del diritto alla tutela dei dati personali che ne deriverebbe. Sebbene la tecnologia cui il prestatore può fare ricorso non debba essere in grado di estrarre dalle comunicazioni pertinenti informazioni diverse da quelle strettamente necessarie per rilevare CSAM, debba essere conforme allo stato dell'arte nel settore e il meno invadente possibile in termini di impatto sui diritti degli utenti alla *privacy* e alla vita familiare, nonché alla protezione dei dati[103], ciò non esclude, di per sé, il rischio che l'analisi automatizzata coinvolga tutti i dati delle comunicazioni di ciascun utente del servizio a cui è rivolto l'ordine, senza neanche un collegamento diretto o indiretto con reati di abusi sessuali su minori.

È evidente, dunque, il rischio di ingerenza nei diritti garantiti dagli artt. 7 e 8 della Carta, nella misura in cui venga istituito un sistema di sorveglianza generalizzata, indiscriminata e sistematica, che include la valutazione automatizzata di dati personali di tutti gli utenti che utilizzano il servizio di comunicazione interpersonale interessato[104].

---

97 In tal senso, si veda H. ABELSON e al., *Bugs in our Pockets: The Risks of Client-Side Scanning*, 14 October 2021, reperibile *online*; nonché le dichiarazioni della Presidente della Signal Foundation, Meredith Whittaker, rilasciate in occasione del ventesimo anniversario dell'EDRi, *President of Signal Foundation Meredith Whittaker's speech for EDRi's 20th anniversary*, 13 April 2023, reperibile *online*.

98 Sul punto, H. ABELSON e al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications, Computer Science and Artificial Intelligence Laboratory Technical Report*, 6 July 2015, reperibile *online*.

99 Human Rights Council, *Resolution 47/16 on the Promotion, Protection and Enjoyment of Human Rights on the Internet*, UN Doc. A/HRC/RES/47/16, 26 July 2021, p. 2.

100 In tal senso, *Digital Rights Ireland*, parr. da 33 a 35; sentenza *Schrems I*, cfr. nota 64, par. 87.

101 *Ligue des droits humains,* cfr. nota 67, par. 96.

102 *Schrems I*, par. 94.

103 Art. 10, par. 3, lett. b), c) e d) della proposta di regolamento.

104 Sul punto, si vedano, per analogia, le risultanze cui è giunta la CGUE nella sentenza *Ligue des droits humains*, parr. da 92 a 111.

7. *In tema di proporzionalità della proposta CSAM rispetto all'obiettivo perseguito*

Sotto il profilo della proporzionalità, come già evidenziato, le limitazioni imposte da atti di diritto dell'Unione ai diritti e alle libertà sanciti dalla Carta non devono eccedere i limiti di quanto idoneo e necessario al conseguimento degli scopi legittimi perseguiti e, laddove siano disponibili più misure appropriate, vanno scelte quelle meno restrittive e i cui inconvenienti non siano sproporzionati rispetto agli scopi perseguiti[105]. Anche sotto questo profilo, appare significativa la metodologia sviluppata dalla Corte di giustizia per valutare la proporzionalità di ingerenze particolarmente gravi con alcuni diritti fondamentali nel contesto della conservazione dei dati o dell'accesso ai metadati.

Per quanto ci interessa, la CGUE ha affermato che le disposizioni di cui agli artt. 7, 8, 11 e 52, par. 1, della Carta non ostano a misure legislative che, ai fini della lotta alla criminalità grave e della prevenzione di gravi minacce alla pubblica sicurezza, prevedono «una conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario»[106]. Al contempo, ha stabilito che «anche gli obblighi positivi che possono derivare, a seconda dei casi, dagli artt. 3, 4 e 7 della Carta e che riguardano […] l'istituzione di norme che consentano una lotta effettiva contro i reati non possono avere l'effetto di giustificare ingerenze tanto gravi quanto quelle che comporta una normativa che prevede una conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta […] senza che i dati degli interessati siano idonei a rivelare una connessione, almeno indiretta, con l'obiettivo perseguito»[107].

In secondo luogo, la Corte ha affermato che il diritto dell'UE non osta, ai fini della lotta alla criminalità in generale, alla conservazione generalizzata dei dati relativi all'identità anagrafica e agli indirizzi IP[108]. La conservazione degli indirizzi IP di tutte le persone fisiche che possiedono apparecchiature che consentono l'accesso a Internet potrebbe essere l'unico mezzo per indagare sui reati commessi *online*, anche nei casi di reati di pedopornografia di particolare gravità, quali l'acquisizione, la diffusione, la trasmissione o la messa a disposizione *online* di materiale pedopornografico, ai sensi dell'art. 2, lett. c), della direttiva 2011/93/UE.

Tuttavia, la Corte ha precisato, da un lato, che l'identità anagrafica degli utenti, oltre ai dati di contatto, come i loro indirizzi, non fornisce alcuna informazione sulle comunicazioni inviate e, conseguentemente, sulla vita privata degli utenti. Pertanto, l'ingerenza che comporta la conservazione di tali dati non può, in linea di principio, essere considerata grave. Per quanto riguarda invece gli indirizzi IP, pur facendo parte di dati di traffico, non rivelano, in quanto tali, alcuna informazione relativa a terzi soggetti che sono stati in contatto con la persona che ha effettuato la comunicazione: tale categoria di dati è quindi meno sensibile di altri dati relativi al traffico[109].

---

[105] Sul punto, sentenza del 17 dicembre 2020, *Centraal Israëlitisch Consistorie van België e al.*, causa C-336/19, ECLI:EU:C:2020:1031, par. 64 e giurisprudenza ivi indicata.
[106] Sentenza del 20 settembre 2022, *Bundesrepublik Deutschland* c. *SpaceNet AG e Telekom Deutschland GmbH*, cause riunite C-793/19 e C-794/19, ECLI:EU:C:2022:702, par. 75.
[107] *La Quadrature du Net*, par. 145.
[108] Sentenza *SpaceNet*, par. 99.
[109] *La Quadrature du Net e al.* c. *Premier ministre e al.*, parr. da 152 a 158.

Infine, secondo la CGUE, la grave ingerenza determinata dall'analisi automatizzata generalizzata dei dati relativi al traffico e all'ubicazione può soddisfare il requisito di proporzionalità solo in situazioni in cui ci si trovi di fronte a una grave minaccia alla sicurezza nazionale, che si dimostra reale e presente o prevedibile, e a condizione che la durata di tale conservazione sia limitata a quanto strettamente necessario. Solo in simili circostanze una valutazione generale e indiscriminata di dati idonei a rivelare la natura delle informazioni consultate in rete e che si applichi indipendentemente da un collegamento, anche indiretto o remoto, con attività illecite può essere considerata giustificata alla luce dei requisiti derivanti dagli artt. 7, 8 e 11 e dall'art. 52, par. 1, della Carta[110].

Guardando alla proposta di regolamento CSAM, i menzionati criteri non sembrano essere soddisfatti.

Come detto prima, gli ordini di rilevazione non indicano gli utenti specifici le cui comunicazioni devono essere esaminate al fine di rilevare l'eventuale presenza di materiale pedopornografico o casi di adescamento di minori. A tal proposito, ricordiamo che la CGUE ha stabilito nella sentenza *Commissioner of An Garda Síochána* che una misura di conservazione può ritenersi giustificata solo se "mirata", vale a dire solo qualora sia fondata su criteri oggettivi e non discriminatori e si rivolga a quei soggetti i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave e, in particolare, quelli precedentemente identificati come una minaccia per la sicurezza pubblica o la sicurezza nazionale (parr. 76, 77 e 78)[111].

Ciò posto, poiché l'ordine di rilevazione non prevede l'indicazione dettagliata dei destinatari le cui comunicazioni dovrebbero essere sottoposte a monitoraggio, la misura non configura una forma di sorveglianza "mirata", risultando quindi sproporzionata rispetto allo scopo perseguito. Una sproporzione ulteriormente aggravata dalla durata della rilevazione, visto che, ai sensi dell'art. 7, par. 9 della proposta CSAM, il periodo di applicazione dell'ordine di rilevazione di materiale pedopornografico e di casi di adescamento può durare, rispettivamente, 24 mesi e 12 mesi. Non può non notarsi che, a fronte della notevole durata del periodo di monitoraggio, non è prevista una rivalutazione della necessità del provvedimento né un limite al suo eventuale rinnovo; circostanza che apre al rischio di dar vita ad una sorveglianza che, oltre ad essere generalizzata ed indiscriminata, potrebbe assumere anche carattere permanente[112].

Peraltro, rispetto ai metadati, il problema della proporzionalità appare ancora più preoccupante se si considera il livello di sensibilità dei dati delle comunicazioni interpersonali, da cui potrebbero ricavarsi informazioni relative alla personalità della persona interessata, alle sue relazioni sociali e alle sue attività quotidiane.

Alla luce di questi elementi, è difficile comprendere come la menzionata giurisprudenza possa fornire la base giuridica necessaria per giustificare un provvedimento, come quello in esame, che mira a combattere reati indiscutibilmente gravi ma non collegati a minacce alla sicurezza nazionale. Al riguardo, la Corte ha ritenuto che «l'obiettivo di preservare la sicurezza nazionale corrisponde all'interesse primario di tutelare le funzioni essenziali dello

---

[110] *Ibidem*, parr. da 172 a 180.

[111] Sentenza della Corte del 5 aprile 2022, *G.D.* c. *The Commissioner of An Garda Síochána e al.*, Causa C-140/20, ECLI:EU:C:2022:258. Inoltre, si vedano le sentenze *Tele2 Sverige*, parr. 110 e 111, e *La Quadrature du Net*, parr. 148 e 149.

[112] In tal senso, si veda European Parliamentary Research Service, *Proposal for a Regulation Laying Down the Rules to Prevent and combat Child Sexual Abuse. Complementary Impact Assessment*, April 2023, reperibile *online*: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)740248, p. 59-61.

Stato e gli interessi fondamentali della società" mediante la prevenzione e la repressione delle attività che possano "destabilizzare le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare la società, la popolazione o lo Stato in quanto tale, quali in particolare attività di terrorismo»[113]. Inoltre, a differenza della criminalità, anche particolarmente grave, una minaccia alla sicurezza nazionale «deve essere reale ed attuale o, quanto meno, prevedibile», circostanza che presuppone «il verificarsi di circostanze sufficientemente concrete, da poter giustificare una misura di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, per un periodo limitato». È evidente, quindi, la distinzione tra una simile minaccia, caratterizzata da una natura, una gravità e una specificità particolari, dal rischio di tensioni o di perturbazioni, anche gravi, della pubblica sicurezza o da quello di reati gravi, inclusi gli abusi sessuali sui minori[114].

Pertanto, poiché la conservazione dei metadati è stata giudicata dalla Corte di giustizia proporzionata solo ai fini della salvaguardia della sicurezza nazionale, non ci sembra che lo *screening* del contenuto delle comunicazioni interpersonali avverso l'abuso sessuale sui minori *online* prefigurato dalla proposta CSAM, nonostante l'importanza degli obiettivi che si prefigge, possa ritenersi altrettanto proporzionato data la diversa natura di tale reato rispetto alle minacce poste alla sicurezza nazionale, rivelandosi quindi suscettibile di ledere l'essenza dei diritti in parola.

8. *Considerazioni conclusive*

Il cyberspazio e le tecnologie dell'informazione e della comunicazione rappresentano un importante strumento per lo sviluppo dei minori. L'accesso ad Internet e a tutte le sue risorse offre, infatti, molteplici opportunità di crescita, scambio e socializzazione per bambini e bambine, grazie al venir meno delle barriere spaziali e temporali[115]. Tuttavia, la condizione di particolare vulnerabilità in cui versano i minori li espone a rischi sempre maggiori e diversificati, rendendo indispensabili misure di tutela efficaci che possano garantirne la protezione anche in Rete.

Come si è avuto modo di osservare, a conferma dell'impegno nella prevenzione e nel contrasto avverso le minacce e i pericoli derivanti dal progresso tecnologico per i soggetti di minore età[116], l'Unione europea ha adottato numerosi atti di *soft law* e ha elaborato una serie di misure giuridicamente vincolanti che mirano a creare un ambiente digitale sicuro e affidabile. Tra questi ultimi, un ruolo fondamentale va riconosciuto alla direttiva 2011/93/CE che, con l'intento di assicurare la protezione dei minori avverso ogni forma di violenza, ha favorito l'introduzione di norme di contrasto efficaci alle principali fattispecie di

[113] *La Quadrature du Net*, par. 135; sentenza del 5 aprile 2022, *Commissioner of An Garda Síochána*, causa C-140/20, ECLI:EU:C:2022:258, par. 61.
[114] *La Quadrature du Net*, par. 136 e 137; *Commissioner of An Garda Síochána*, par. 62.
[115] G. VOTANO, *Protezione e tutela dei minori in internet*, in G. CASSANO, S. PREVITI (a cura di), *Il diritto di internet nell'era digitale*, Milano, 2020, p. 118.
[116] *Ibid.*

abuso sessuale alimentato dall'evoluzione del Web, che rende sempre più agevole, *inter alia*, l'accesso e la diffusione del materiale pedopornografico[117].

Alla luce delle molteplici sfide che si pongono nel cyberspazio, si è visto come la Commissione abbia proposto l'adozione di questa nuova normativa che determina una rielaborazione in chiave digitale della tutela dei diritti dei minori, fondato su una maggiore responsabilizzazione dei prestatori di servizi di comunicazione e di servizi di *hosting*. L'attuale sistema basato sull'azione volontaria di rilevazione dei casi di abuso sessuale *online* sui minori da parte delle aziende si è rivelato infatti insufficiente a garantire un'adeguata protezione dei bambini e, in ogni caso, i prestatori di servizi di comunicazione rientranti nell'ambito di applicazione della direttiva *ePrivacy* non disporranno più della base giuridica necessaria per continuare ad attuare tali attività su base volontaria in vista della imminente scadenza del regime derogatorio introdotto dal regolamento (UE) 2021/1232, prevista per il 3 agosto 2024.

La proposta di regolamento CSAM, come si è detto, intende sostituire il regime temporaneo, stabilendo norme chiare e armonizzate volte a contrastare l'abuso sessuale perpetrato nei confronti dei minori attraverso l'uso improprio dei servizi ICT e imponendo ai prestatori di tali servizi obblighi di valutazione e attenuazione del rischio di un simile uso, di rilevazione, segnalazione, blocco e rimozione di materiale pedopornografico, sia esso noto o nuovo, e di casi di *grooming*.

Tra i nuovi obblighi posti a carico dei fornitori di servizi ICT rientranti nell'ambito di applicazione della normativa, numerose perplessità sono state sollevate in relazione all'obbligo di rilevazione che, sebbene costituisca una misura di ultima istanza cui fare ricorso solo laddove le misure preventive di attenuazione si dimostrino inefficaci, presenta non pochi profili critici. In particolare, ci sembrano condivisibili i dubbi in merito alla conformità dell'ordine di rilevazione di cui all'art. 7 della proposta CSAM con gli artt. 7, 8 e 11 della Carta dei diritti fondamentali e, quindi, con la tutela della *privacy*, la protezione dei dati personali e la libertà di espressione. Sebbene la prevenzione e la lotta contro l'abuso sessuale sui minori costituiscano un importante obiettivo di interesse generale, l'attuale formulazione del regolamento rischia di introdurre notevoli limitazioni ai diritti indicati al punto da non soddisfare i requisiti di cui all'art. 52, par. 1 della Carta.

Contrariamente a quanto prefigurato dalla proposta di regolamento, nel cui *memorandum* esplicativo si rileva l'intenzione di voler stabilire un quadro giuridico e armonizzato in materia di abusi sessuali sui minori *online* che garantisca certezza giuridica ai prestatori di servizi, stabilendo un giusto equilibrio tra le misure di protezione dei minori e i loro diritti fondamentali e i diritti fondamentali degli altri utenti e dei prestatori[118], è stato osservato in questo lavoro come, in base all'attuale formulazione della normativa, molteplici elementi impediscano la predisposizione di un adeguato bilanciamento.

Oltre a quanto già indicato, riteniamo che le stesse misure che dovrebbero contribuire a ridurre le possibilità che bambini e bambine diventino vittime di abusi sessuali *online* presentino un potenziale rischio per la tutela del loro diritto alla *privacy* e della loro libertà di espressione, laddove rivelino il contenuto delle loro comunicazioni così interferendo con la loro capacità di costruire la propria identità *online* e di esprimersi liberamente.

---

[117] Sul punto, M. TROGLIA, *Lotta contro l'abuso, lo sfruttamento sessuale dei minori e la pornografia minorile: alcune riflessioni sulla direttiva 2011/93/UE del Parlamento e del Consiglio del 13 dicembre 2011*, in *Cassazione penale*, 2012, p. 1906-1918.

[118] COM(2022)209, p. 3.

Il timore manifestato dalle autorità di controllo sulla protezione dei dati e dai servizi giuridici di tutte le Istituzioni europee coinvolte nel processo di adozione dell'atto rispetto al rischio che, in mancanza di adeguate garanzie a tutela della vita privata e dei dati personali, la normativa proposta apra la porta alla sorveglianza di massa, sembra essere condiviso dagli stessi soggetti che la normativa vorrebbe proteggere. Il 66% degli adolescenti europei di età compresa tra i 13 e i 17 anni ha espresso, infatti, la propria contrarietà alla proposta, per il timore che il monitoraggio del contenuto delle comunicazioni possa compromettere la loro libertà di espressione e la possibilità di esplorare la propria sessualità[119].
Tutto quanto considerato, lascia perplessi il sostegno espresso per la proposta di regolamento CSAM dalla maggior parte degli Stati membri dell'UE[120], che condividono la posizione della Commissione europea in merito alla legittimità e alla proporzionalità degli ordini di rilevazione di CSAM fondata sull'assunto che i diritti in gioco non sono diritti "assoluti", ma devono essere considerati in relazione alla loro funzione sociale[121]; circostanza che giustificherebbe l'attuale struttura della normativa in esame. Ciò nonostante, una parte degli Stati membri, seppur minoritaria, continua a sostenere la necessità di una modifica della normativa oggetto di discussione[122] affinché ad un innalzamento del livello di protezione dei minori nel cyberspazio corrisponda la garanzia di un'adeguata tutela di tutti gli ulteriori diritti e libertà fondamentali coinvolti.

---

[119] P. BEYER, *#ChatControl Survey: Children Don't Want to be "Protected" by Scanning or Age-Restricting Messenger and Chat Apps*, 7 March 2023, reperibile *online*: https://www.patrick-breyer.de/en/chatcontrol-survey-children-dont-want-to-be-protected-by-scanning-or-age-restricting-messenger-and-chat-apps/.
[120] EDRi, *Despite Warning from Lawyers, EU Governments Push for Mass Surveillance of our Digital Private Lives*, 4 July 2023, reperibile online: https://edri.org/our-work/despite-warning-from-lawyers-eu-governments-push-for-mass-surveillance-of-our-digital-private-lives/.
[121] Commission Services, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse – Balancing the Rights of Children with Users' Rights*, 2022/0155(COD), Bruxelles, 16 May 2023, p. 3-4.
[122] Si vedano, in tal senso, la risoluzione del Senato francese del 20 marzo 2023, *Résolution européenne sur la proposition de règlament du Parlament européen et du Conseil établissant des règles en vue de prévenir et de combattre lesa bus sexuels sur enfents – COM(2022)209 final*, No. 77; la risoluzione del Parlamento austriaco del 3 novembre 2022, *Binding Resolution of the Austrian Parliament against the Child Sexual Abuse Regulation*; la comunicazione del Bundestag tedesco del 1° marzo 2023, *Sachverständige üben breite Kritik an Plänen zur Chatkontrolle*; la lettera dell'Houses of the Oireachtas irlandese del marzo 2023, *Political Contribution on Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse.*