



Il contrasto alla propaganda terroristica online nell'ambito dell'Unione europea: tutela attuale e prospettive future

DI VIVIANA SACHETTI*

Sommario: 1. Introduzione. – 2. Il quadro normativo pregresso. – 2.1 La Direttiva *eCommerce* e la responsabilità degli *hosting provider*. – 2.2 La specifica disciplina in materia di terrorismo della Direttiva 2017/541. – 3. Verso l'innovazione della normativa europea. – 3.1. La Raccomandazione 2018/334 sui contenuti illeciti *online*. – 3.2 Il contrasto alla propaganda terroristica *online* nella Proposta di Regolamento 2018/640. – 4. Prime misure introdotte nell'Unione europea in via volontaria. – 5. Osservazioni conclusive.

1. Introduzione

In considerazione dell'aumento esponenziale del numero di reati commessi attraverso il mezzo di Internet¹, con speciale riguardo alla diffusione di contenuti illeciti *online* concernenti il terrorismo, la Commissione europea ha adottato, il 12 settembre del 2018, la Proposta di Regolamento 2018/640², che costituisce un parziale sviluppo della precedente Raccomandazione 2018/334³.

* Dottoranda di ricerca in Diritto dell'Unione europea, Università degli Studi Roma Tre.

¹ È primariamente necessario considerare una distinzione, nel novero dei *computer crime*, tra quei reati realizzati per mezzo dello strumento Internet e quei reati preesistenti all'avvento informatico, che ha costituito piuttosto una semplificazione nel raggiungimento dello scopo criminale, riferendosi proprio a questa seconda categoria la Proposta di Regolamento oggetto di analisi nel presente contributo. Più dettagliatamente, sulla illustrata distinzione, v. M. DURANTE, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Torino, 2008, p. 39. Ulteriore categoria rinvenibile negli studi dottrinari è poi quella degli illeciti perpetrati contro Internet, quale ad esempio è considerata da taluni l'attività di *cyberterrorism* e in generale quanto posto in essere dagli *hacker* (cfr. A. G. PARISI, *Il commercio elettronico*, in S. SICA, V. ZENO-ZENCOVICH (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, Padova, 2015, p. 433).

² Proposta di Regolamento del Parlamento europeo e del Consiglio relativa alla prevenzione della diffusione di contenuti terroristici online, COM(2018)640 final, del 12 settembre 2018 (in seguito, Proposta di Regolamento). Tale proposta è stata approvata in prima lettura da parte del Parlamento europeo il 17 aprile 2019, con

In virtù delle «particolari responsabilità sociali che ricoprono»⁴, la nascente disciplina si rivolge, oltre agli Stati membri dell'Unione europea, anche e direttamente ai prestatori di servizi di *hosting* (in seguito, *hosting provider*), ossia al «prestatore di servizi della società dell'informazione consistenti nella memorizzazione di informazioni fornite da un destinatario del servizio su richiesta di quest'ultimo ai sensi dell'articolo 14 della direttiva 2000/31/CE, che rivolge la sua attività a consumatori residenti nell'Unione, indipendentemente dal suo luogo di stabilimento»⁵.

In particolare, la Commissione prende atto di una serie di accordi sulle predette materie, assunti su base volontaria ed intercorsi nell'ambito di una serie di Forum⁶, promossi dall'Unione europea soprattutto nell'ultimo quadriennio, ritenendo necessario l'impegno da parte degli *hosting provider* nel contrastare la proliferazione di contenuti illeciti mediante misure efficaci ed appropriate, garantendo al tempo stesso interventi diligenti e proporzionati nella rimozione di siffatti contenuti informatici o nella disabilitazione dall'accesso agli stessi.

Pur nel riconoscere il merito dei predisposti strumenti di cooperazione, la Commissione europea ravvisa altresì dei limiti nell'impiego di meccanismi meramente volontari, individuandone degli ostacoli alla loro adeguatezza nell'impossibilità di coinvolgere in concreto tutti gli attori di tale contesto e nell'insufficienza della portata e del ritmo dello sviluppo degli strumenti per arginare i pericoli posti dalla propaganda terroristica *online*⁷.

Prima di passare all'analisi della legislazione che si prospetta entrare in vigore nel prossimo futuro, appare necessario ricostruire quanto costituisce attualmente il quadro normativo di riferimento in materia, evidenziando le criticità che emergono dal combinato disposto di tali atti europei. Come si vedrà, detta normativa viene richiamata a fini integrativi dalla Proposta di Regolamento: sarà dunque opportuno analizzare i profili di compatibilità della disciplina in fase di approvazione con quanto già vigente, anche al fine di comprenderne più adeguatamente i principali tratti innovativi.

2. Il quadro normativo pregresso

2.1 La Direttiva eCommerce e la responsabilità degli hosting provider

emendamenti concernenti peraltro il titolo ("Regolamento del Parlamento europeo e del Consiglio relativo alla lotta alla diffusione di contenuti terroristici online").

³ Raccomandazione (UE) 2018/334 della Commissione europea del 1° marzo 2018 sulle misure per contrastare i contenuti illegali online (in seguito, Raccomandazione 334).

⁴ Considerando n. 15, Raccomandazione 334.

⁵ Art. 4, lett. a), Raccomandazione 334. Il che comporta oltretutto la veicolazione e la pubblicazione delle informazioni a seguito della concessione di uno spazio fisico digitale al cliente sul *server* del *provider*: cfr. I. P. CIMINO, *I contratti degli internet providers e per i data services on line*, in G. CASSANO, I. P. CIMINO (a cura di), *Diritto dell'Internet e delle nuove tecnologie telematiche*, Milano, 2009, p. 19. A titolo esemplificativo, si considerano *hosting provider*: i mercati virtuali, le piattaforme di condivisione di video, i *social network*, i *blog*, i siti su cui vengono pubblicate recensioni e, più in generale, quelli che consentono la pubblicazione dei commenti degli utenti.

⁶ Considerando n. 2, Raccomandazione 334; Proposta di Regolamento, p. 2.

⁷ La possibilità di giungere all'uso di strumenti normativi di maggiore pervasività giuridica era già stata considerata sin dalla Comunicazione della Commissione europea del 2017 con la quale ha avuto concretamente inizio il dialogo istituzionale con le piattaforme informatiche e i principali portatori di interessi in materia (*Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, 'Tackling Illegal Content Online – Towards an Enhanced Responsibility of Online Platforms'*, 2017/555, Bruxelles, 28 settembre 2017, p. 20).

A fondamento della disciplina per il contrasto dei contenuti illeciti *online*, la Proposta di Regolamento considera come quadro normativo generale ed applicabile per qualsivoglia ambito di reati quello predisposto dalla c.d. “Direttiva *eCommerce*”⁸, con particolare riferimento al Capo II, Sezione 4, riguardante la responsabilità dei *provider* di servizi intermediari⁹. Pur mirando infatti a regolamentare il commercio di tipo elettronico, integrandolo nella legislazione europea e nazionale dei singoli Stati membri a giovamento del mercato unico interno, la Commissione sembra ritenere che tale Direttiva possa trovare una più ampia applicazione in tutte le ipotesi in cui sia implicata la responsabilità dei prestatori di servizi informatici, soprattutto per quel che concerne l’immagazzinamento di informazioni elettroniche¹⁰.

Trattasi innanzitutto, nel caso dei *provider*, di una responsabilità che la dottrina ha definito di tipo secondario o indiretto¹¹, ossia risultante dalla condotta illecita degli utilizzatori dei servizi informatici, e ciò per una duplice ragione: la prima, evidentemente di natura giuridica, concerne la oggettiva difficoltà di controllo preventivo delle informazioni conservate presso i *provider*, prima che tali contenuti possano raggiungere il pubblico; la seconda, di matrice economica, riguarda soprattutto i prestatori di servizi di piccole dimensioni che non riuscirebbero con tutta probabilità ad assorbire i costi dell’implementazione di mezzi informatici particolarmente avanzati, capaci di analizzare preventivamente tutti i dati oggetto di *hosting*¹².

L’art. 12 della Direttiva *eCommerce* considera generalmente privo di responsabilità il *provider*, purché in presenza di tre condizioni determinate: (i) non sia la fonte della trasmissione dei dati informatici; (ii) non abbia la funzione di selezionare il destinatario di detta trasmissione; ed infine, (iii) non interferisca sulle informazioni oggetto della trasmissione apportandovi modifiche o selezioni¹³.

Il successivo art. 14, che appare di primario interesse in relazione al contenuto della Proposta di Regolamento in esame, disciplina nello specifico l’esenzione da responsabilità per

⁸ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell’8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell’informazione, in particolare il commercio elettronico, nel mercato interno (in seguito, Direttiva *eCommerce*). In Italia, è stata pedissequamente recepita con il D. Lgs. 70/2003.

⁹ È però opportuno sottolineare come la Direttiva presenta alcune restrizioni, escludendo di fatto l’applicabilità della propria disciplina ai soggetti che non risultano rientranti nelle definizioni di imprenditori o di professionisti (sul punto, M. DE CATA, *La responsabilità civile dell’Internet Service Provider*, Milano, 2010, p. 186).

¹⁰ In apparente contrasto con quanto previsto dalla Comunicazione 555, nella quale espressamente si statuisce «[i]t is important to stress that this legal framework does not define, let alone harmonise, what constitutes “illegal” content». Si veda *infra* §3.2 su come, al contrario, la Proposta di Regolamento 2018/640 miri proprio all’armonizzazione della disciplina in materia tra gli Stati membri dell’Unione europea.

¹¹ Così G. SARTOR, *Providers Liability: From the eCommerce Directive to the Future*, 2017, disponibile presso www.europarl.europa.eu/, p. 4.

¹² Sui riflessi ulteriori di tale seconda questione, *infra* §3.1. Sul punto, cfr. R. JULIA-BARCELO, *Liability for Online Intermediaries: A European Perspective*, in *European Intellectual Property Review*, 1998, p. 7.

¹³ Peraltro, qualora non dovessero rispettarsi questi requisiti da parte dei *provider*, la loro responsabilità sarà determinata dal diritto nazionale dei singoli Stati membri in cui la violazione è avvenuta, limitandosi la Direttiva *eCommerce* a stabilire le eccezioni alla stessa in ragione dello specifico servizio fornito (per una possibile prospettazione alla luce della prevista riforma della Proposta di Regolamento, si veda *infra* §3.2). Cfr. P. BAISTROCCHI, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in *Santa Clara High Technology Law Journal*, 2003, p. 118. Come affermato costantemente nella giurisprudenza della Corte di Giustizia dunque, l’attività del *provider* deve limitarsi ad essere “di ordine meramente tecnico, automatico e passivo” (da ultimo sul tema, Corte di Giustizia UE, 7 agosto 2018 *Coöperatieve Vereniging SNB-REACT U.A. c. D.M.*, C-521/17, §47).

gli *hosting provider*, la cui attività, «consistendo in una forma di memorizzazione a carattere tendenzialmente duraturo, è di per sé maggiormente pericolosa»¹⁴. In aggiunta, dunque, ai requisiti indicati dall'art. 12, nel peculiare caso dei prestatori di servizi di memorizzazione di contenuti informatici, la responsabilità di costoro viene meno qualora, cumulativamente: (i) essi non siano a conoscenza dell'attività o informazione di natura illecita e, in relazione ad azioni di tipo risarcitorio, l'attività o l'informazione non sia manifestamente illegale; e (ii) nell'apprendere dell'illegale utilizzo dei propri servizi, il *provider* si attiva immediatamente per inibire o far cessare la violazione avvenuta. Perplesso ha tuttavia destato la mancanza di specificità di tale norma per quanto concerne l'estensione dell'uso dei servizi di *hosting* da parte degli utilizzatori e la determinazione degli illeciti che dovrebbero essere individuati dal *provider*, con le decisioni giurisprudenziali in materia nei singoli Stati membri che hanno assunto un prevedibile orientamento oscillante¹⁵.

Seguendo l'ordine normativo, appare rilevante soffermarsi sulla questione della cooperazione con le autorità. È infatti lo stesso art. 14 a prevedere «la possibilità, per un organo giurisdizionale o un'autorità amministrativa [...] di esigere che il prestatore ponga fine ad una violazione o la impedisca». Ed ancora, detto disposto lascia impregiudicata la facoltà per gli Stati membri di «definire procedure per la rimozione di informazioni o la disabilitazione dell'accesso alle medesime», al contempo prevedendo la mancanza di un obbligo generalizzato di sorvegliare sulle informazioni memorizzate o di attivarsi al fine di ispezionare «fatti o circostanze che indichino la presenza di attività illecite», negando addirittura l'art. 15 la possibilità che gli Stati membri impongano un simile obbligo ai *provider* per via normativa¹⁶. Resta tuttavia salva la possibilità per gli Stati di determinare un dovere, in capo ai prestatori di servizi informatici, di procedere a comunicare «senza indugio» alle autorità del rinvenimento di «presunte attività o informazioni illecite», o a fornire alle stesse dati circa gli utenti dei servizi di memorizzazione dei dati informatici¹⁷.

In tema di poteri attribuiti direttamente agli Stati dalla Direttiva *eCommerce*, riveste un ruolo di primaria importanza la previsione dell'art. 3, dove rispetto al generale divieto per gli stessi di «limitare la libera circolazione dei servizi» provenienti da altro Stato membro¹⁸, viene sancita una importante deroga, prevedendosi in capo all'autorità pubblica il potere di

¹⁴ A. MAIETTA, *Il sistema delle responsabilità nelle comunicazioni via Internet*, in G. CASSANO, I. P. CIMINO (a cura di), *Diritto dell'Internet e delle nuove tecnologie telematiche*, Milano, 2009, p. 523.

¹⁵ DLA PIPER, 'Liability of Online Intermediaries', in *European Union Study on the Legal Analysis of a Single Market for the Information Society: New Rules for a New Age?*, novembre 2009 (disponibile presso www.ec.europa.eu).

¹⁶ Art. 15, par. 1, Direttiva *eCommerce*. Il divieto è stato ribadito dalla giurisprudenza europea, che ha ritenuto contrastante con la normativa in esame l'emissione di un decreto ingiuntivo che obblighi un *provider* ad introdurre un sistema di rilevazione degli indirizzi IP dai quali provengano contenuti illeciti, non garantendo un equo bilanciamento con la libertà di iniziativa economica, il diritto alla *privacy* e la libertà di espressione e potendo portare al blocco di dati leciti (Corte di Giustizia UE, 24 novembre 2011, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10). Deve tuttavia considerarsi una recentissima pronuncia della Corte, che, nell'interpretare l'art. 15 della Direttiva *eCommerce*, ha stabilito come il giudice nazionale possa legittimamente ordinare ad un *provider* la rimozione di informazioni che siano identiche o sostanzialmente equivalenti ad altri contenuti di cui sia già stata dichiarata l'illiceità, purché ciò non costringa il prestatore di servizi ad effettuare un'autonoma valutazione di tali informazioni, potendo finanche ingiungerne la rimozione «a livello mondiale, nell'ambito del diritto internazionale pertinente» (Corte di Giustizia UE, 3 ottobre 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, C-18/18).

¹⁷ Art. 15, par. 2, Direttiva *eCommerce*.

¹⁸ Art. 3, par. 2, Direttiva *eCommerce*.

adottare provvedimenti, proporzionati ed in relazione ad un servizio lesivo degli obiettivi considerati dallo stesso articolo o costituenti «un rischio serio e grave di pregiudizio a tali obiettivi». Detti fini meritevoli di tutela sono suddivisi in tre gruppi: (i) l'ordine pubblico, «in particolare per l'opera di prevenzione, investigazione, individuazione e perseguimento in materie penali»; (ii) la sanità pubblica; (iii) la pubblica sicurezza e la difesa nazionale¹⁹.

La Direttiva, se da una parte ammette dunque evidentemente la possibilità per il *provider* di identificare autonomamente il contenuto illecito tra le informazioni immagazzinate presso lo stesso, dall'altra sembra limitare il meccanismo di segnalazione da parte di terzi di tali dati (c.d. *notice and take down mechanism*) unicamente alla pubblica autorità nazionale, con scarsa o assente possibilità di trasmettere le comunicazioni ai prestatori di servizi direttamente da parte degli altri utilizzatori. Anche a volerne ammettere la difficile praticabilità tecnica nell'anno di approvazione della Direttiva, la procedura ora nominata riveste, quasi vent'anni dopo, nel mondo del “*Web 4.0*”, una importanza fondamentale, costituendo difatti la primaria forma di segnalazione prevista nella Raccomandazione 2018/334.

2.2 La specifica disciplina in materia di terrorismo della Direttiva 2017/541

Ben maggiore rilevanza assume invece la recente Direttiva 2017/541 in materia di lotta al terrorismo (in seguito, Direttiva 541)²⁰: proponendo l'armonizzazione delle legislazioni nazionali in materia, tale atto normativo intende al contempo dare una attuazione maggiormente adeguata agli «obblighi giuridici cui l'Unione e gli Stati membri sottostanno a norma del diritto internazionale»²¹, sottolineando sin da subito l'opportunità di sanzionare le condotte «messe in atto attraverso Internet, inclusi i social network»²².

E proprio in merito alle condotte, è l'art. 3 a prevedere, con un elenco tassativo, quali di queste costituiscano reati di terrorismo, trattandosi di una serie di atti intenzionali, «che, per la loro natura o per il contesto in cui si situano, possono arrecare un grave danno a un paese o a un'organizzazione internazionale», quando commessi al fine di: (i) intimidire gravemente la

¹⁹ Art. 3, par. 4, Direttiva *eCommerce*. La procedura in questione presenta peraltro ulteriori complessità, prevedendosi ai paragrafi successivi dello stesso art. 3 che lo Stato, prima di adottare i provvedimenti, debba chiedere all'eventuale altro Stato membro implicato di attivarsi adeguatamente e, qualora ciò non accada, sarà esso stesso a provvedere, previa notificazione all'altro Paese e alla Commissione, che ne dovrà valutare la compatibilità con il diritto dell'Unione europea. Fase quest'ultima attuabile *ex post* solo in caso di urgenza, i cui motivi dovranno essere debitamente specificati nella predetta notificazione.

²⁰ Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio del 15 marzo 2017 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio. La Direttiva, recepita dagli Stati membri entro l'8 settembre 2018, prevede che la Commissione presenti una relazione entro due anni al Parlamento e al Consiglio che valuti le misure adottate dagli Stati, spettando poi alla Commissione stessa valutare entro l'8 settembre 2021 «il valore aggiunto della presente direttiva riguardo alla lotta al terrorismo» (art. 29, Direttiva 541). Di essa non sono parte il Regno Unito, l'Irlanda e la Danimarca (considerando n. 41 e 42, Direttiva 541).

²¹ Tra gli obblighi internazionali che devono rispettarsi nell'attuare la Direttiva, vi sono certamente quelli relativi ai diritti umani. In particolare, al considerando n. 35 si fa obbligo di tenere conto della Convenzione europea per i diritti dell'uomo e del Patto internazionale sui diritti civili e politici. Vi è tuttavia un macroscopico difetto di coordinamento tra le varie versioni linguistiche della direttiva: mentre ad esempio la versione inglese, in linea con le altre, prevede anche l'obbligo del rispetto di «other human rights obligations under international law», la versione italiana considera, molto più in generale, gli “altri obblighi di diritto internazionale”.

²² Considerando n. 6, Direttiva 541.

popolazione; (ii) costringere i pubblici poteri o una delle organizzazioni internazionali a «compiere o astenersi dal compiere *qualsiasi* atto» [corsivo aggiunto]; ovvero (iii) destabilizzare gravemente o distruggere le strutture politiche, costituzionali, economiche o sociali fondamentali di un paese o di un'organizzazione internazionale²³.

È peraltro penalmente rilevante anche la minaccia di compiere uno degli atti elencati dall'art. 3, con un conseguente arretramento della soglia di punibilità in relazione ad alcune delle condotte ivi previste. Il dato appare alquanto preoccupante se si considera che ciò porterebbe a sanzionare con pene particolarmente severe (in conformità a quanto stabilito dall'art. 15 della Direttiva 541) condotte quali la minaccia di interferire illecitamente nei sistemi informatici²⁴: il che condurrebbe, nel caso ora astrattamente ipotizzato, ad una reclusione non inferiore nel massimo ad anni otto qualora l'autore del reato sia a capo di un gruppo terroristico, come espressamente sancito dall'art. 15, par. 3²⁵.

Per quanto qui maggiormente rileva, desta attenzione l'art. 5 della Direttiva 541, riguardante la pubblica provocazione alla commissione dei reati di terrorismo. Gli Stati membri devono infatti adottare le misure reputate necessarie a reprimere l'intenzionale «divulgazione di un messaggio, con qualsiasi mezzo, sia online che offline», che sia volto ad istigare e tale da promuovere la commissione di un reato di terrorismo²⁶, «ad esempio mediante l'apologia di atti terroristici»²⁷. La condotta deve dunque essere idonea a creare le condizioni di «pericolo [perché] uno o più di tali reati possano essere commessi»²⁸, da desumersi dalle circostanze specifiche dell'atto e dal contesto di commissione dello stesso, considerando ulteriormente «l'entità e [...] la natura verosimile del pericolo»²⁹.

La Direttiva incoraggia poi la collaborazione con gli Stati terzi al fine di consentire la rimozione dai *server* dei territori di questi ultimi dei contenuti illeciti, esortando gli Stati membri, qualora il meccanismo illustrato non si rendesse attuabile, a predisporre sistemi in grado di bloccare direttamente l'accesso ai dati di natura terroristica nel proprio territorio³⁰. La formulazione della norma è peraltro piuttosto oscura quanto ai mezzi di eliminazione dei dati informatici e soprattutto ai limiti di questa azione, dettati anche dalla giurisdizione, stabilendo che gli Stati «[s]i adoperano inoltre per ottenere la rimozione di tali contenuti

²³ L'art. 4, Direttiva 541, prevede poi i «[r]eati riconducibili a un gruppo terroristico», trattandosi di atti intenzionali e consistenti nella direzione o partecipazione al gruppo stesso, nell'ambito del quale il contributo rilevante è dato dalla fornitura di mezzi materiali o di informazioni ai membri del gruppo, apparendo dunque sufficiente, a parere di chi scrive, una mera condotta agevolatrice, purché connotata dalla «consapevolezza che tale partecipazione contribuirà alle attività criminose del gruppo terroristico».

²⁴ Come derivante dalla lettura del combinato disposto delle lett. i) e j), art. 3, Direttiva 541.

²⁵ Una ulteriore specificazione a riguardo è fornita dal considerando n. 8: «[l]a minaccia di commettere tali atti intenzionali dovrebbe altresì essere considerata un reato di terrorismo laddove si accerti, *sulla base di circostanze oggettive*, che tale minaccia sia stata posta in essere con un tale scopo terroristico» [corsivo aggiunto].

²⁶ Con l'esclusione della sola condotta di minaccia di cui alla lett. j), art. 3, Direttiva 541.

²⁷ Nel considerando n. 10 della Direttiva 541 sono elencati, a titolo esemplificativo: l'apologia; la giustificazione del terrorismo; la diffusione *online* od *offline* di immagini o messaggi, anche riguardanti le vittime delle azioni terroristiche.

²⁸ Desta dubbi la formulazione dell'ultima parte dell'art. 5, Direttiva 541, che sembra ammettere la possibilità della punibilità dei c.d. «reati di pericolo di pericolo» se considerato in combinato disposto quantomeno con le condotte di cui alle lettere d), g) e h) dell'art. 3. Categoria questa considerata come un «non reato» dalla dottrina penalistica: cfr. ad esempio F. MANTOVANI, *Diritto penale – Parte generale*, Padova, 2013, p. 213.

²⁹ Considerando n. 1, Direttiva 541.

³⁰ Art. 19, paragrafi 1 e 2 e considerando n. 22, Direttiva 541.

ospitati al di fuori del loro territorio» [corsivo aggiunto]. Quest'ultima questione, peraltro, sembra aprire un profilo di contrasto con la Direttiva *eCommerce*: l'art. 19 della Direttiva 541 prevede che, qualora sia commesso un reato di terrorismo, ciascuno Stato «può estendere la propria giurisdizione quando il reato è stato commesso nel territorio di un altro Stato membro», mentre si ricorderà come l'art. 3 della Direttiva *eCommerce* sancisca il divieto per gli Stati di porre limitazioni alla libera circolazione dei servizi provenienti da un altro Stato membro³¹.

Nel consentire la diffusione del già menzionato *notice and take down mechanism*, procedura questa ormai considerata di facile realizzazione soprattutto per i grandi *hosting provider*, la Direttiva 541 da una parte impone agli Stati membri di far salvi i diritti garantiti dalla Carta di Nizza e la possibilità di adire l'autorità giudiziaria per gli utenti i cui contenuti siano stati ritenuti illeciti, dall'altra, al contempo, ribadisce il divieto di creare un obbligo generale di sorveglianza per i fornitori di servizi, in conformità dunque con il dettato normativo dell'art. 15 della Direttiva *eCommerce*³².

Si ritiene tuttavia che, all'atto applicativo, il regime di esenzione dalla responsabilità delineato nell'ambito della Direttiva *eCommerce* potrà trovare una deroga se raffrontato con l'art. 17 della Direttiva 541, laddove è prevista la responsabilità penale delle persone giuridiche qualora un individuo, che ricopre una posizione preminente nell'ambito della stessa³³, abbia potuto perpetrare un reato a suo vantaggio, e ciò sia avvenuto in conseguenza della carenza di sorveglianza o controllo esercitata nell'organizzazione della persona giuridica, gravando sugli Stati membri l'obbligo di prevedere le misure necessarie per stabilire tale responsabilità in capo alla persona giuridica³⁴.

Per quanto concerne specificamente i contenuti *online* di matrice terroristica, la Direttiva 541 impone agli Stati di predisporre un sistema di garanzie che possa bilanciare il penetrante intervento della rimozione o del blocco dei dati illeciti, e ciò creando delle procedure trasparenti, limitando «allo stretto necessario e [in modo] proporzionato» detto intervento e provvedendo altresì ad informare gli utenti circa le ragioni che hanno condotto all'adozione di simili misure³⁵. E al riguardo non può che sollevare qualche perplessità il considerando n. 21 della Direttiva 541, che nel premettere il dovuto rispetto del diritto alla protezione dei dati personali anche nel corso delle indagini in materia di terrorismo, da attuarsi con gli stessi strumenti impiegati «nella lotta contro la criminalità organizzata o altre gravi forme di criminalità», autorizza e sollecita espressamente all'uso della «sorveglianza

³¹ Art. 19, par. 1, Direttiva 541. Un meccanismo di coordinamento è poi delineato dal par. 3, che, nel caso di giurisdizione concorrente di più Stati membri, richiede la collaborazione tra questi per determinare quale tra essi avvierà l'azione penale, anche avvalendosi di Eurojust e tenendo conto di una serie di elementi ivi elencati.

³² Considerando n. 23, Direttiva 541.

³³ Nello specifico, tale soggetto deve avere un potere di rappresentanza, la facoltà di adottare decisioni ovvero di esercitare il controllo a qualsiasi titolo all'interno della struttura della persona giuridica.

³⁴ Lasciando peraltro libertà agli Stati nello stabilire se le relative sanzioni avranno natura penale o meno: cfr. art. 18, Direttiva 541. Sanzioni accessorie, stabilite dal citato art. 18, potranno consistere in: a) esclusione dal godimento di contributi o sovvenzioni pubblici; b) interdizione temporanea o permanente dall'esercizio di un'attività commerciale; c) assoggettamento a vigilanza giudiziale; d) liquidazione giudiziaria; e) chiusura temporanea o permanente dei locali usati per la commissione del reato.

³⁵ Art. 21, par. 3, Direttiva 541. A questo quadro giuridico deve certamente aggiungersi quello predisposto dal 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 – c.d. GDPR).

discreta, compresa la sorveglianza elettronica, la captazione, la registrazione e la conservazione di audio all'interno di veicoli o di luoghi privati o pubblici, nonché di immagini di persone all'interno di veicoli e di luoghi pubblici», con una libertà di mezzi e soprattutto di modalità che sembra dare quasi alcun peso alle corrispondenti necessarie garanzie. Si afferma in ogni caso il divieto di limitare la possibilità di ricorrere per via giudiziaria³⁶ e la necessità di lasciare impregiudicati i diritti e i principi giuridici fondamentali previsti dall'art. 6 TUE³⁷, rimettendo poi alla determinazione della normativa nazionale la possibilità di prevedere opportune garanzie procedurali qualora si incorra nell'ambito della determinazione o della limitazione della responsabilità della stampa e degli altri mezzi di comunicazione³⁸.

3. Verso l'innovazione della normativa europea

3.1. La Raccomandazione 2018/334 sui contenuti illeciti online

Come già precedentemente menzionato, la recente Proposta di Regolamento 2018/640 costituisce lo sviluppo della Raccomandazione 334, benché, come si vedrà, deliberatamente parziale.

Detta Raccomandazione presenta una serie di aspetti di novità rispetto al quadro normativo sinora analizzato: nel promuovere l'adozione di *standard* minimi generali nella prevenzione e rimozione dei contenuti illeciti *online*³⁹, prescindendosi dunque dalla materia, dedica una sezione autonoma al terrorismo, settore per cui si è sentita la necessità «di una risposta più rapida ed efficace»⁴⁰.

Per quanto concerne la parte riferibile a tutti i tipi di illeciti, la Raccomandazione dedica ampio spazio alla questione delle segnalazioni sottoponibili ai *provider*, auspicando una diffusa adozione del *notice and take down mechanism* al fine di agevolare il compito del prestatore di servizi nel trovare e valutare se sia opportuno rimuovere o disabilitare determinati contenuti che si assumono essere di natura illecita, rilevandosi peraltro come siano intervenute, a seguito della Direttiva *eCommerce*, una serie di «prescrizioni giuridiche [nazionali] tra loro diverse per contenuto e per campo d'applicazione»⁴¹. Differentemente da quanto stabilito dalla Direttiva 2000/31 ed in considerazione delle tecnologie intervenute negli

³⁶ Art. 21, par. 3, Direttiva 541.

³⁷ Specificazione questa peraltro evidentemente superflua, ponendosi l'art. 6 TUE come *lex superior* rispetto alla Direttiva 541.

³⁸ Art. 23, Direttiva 541. L'ultima parte dell'articolo non è andata esente da critiche in considerazione dell'estrema ampiezza che sembra lasciare agli Stati nel decidere a livello normativo circa la responsabilità, in particolare dei *media*: sul punto, A. CAIOLA, *The European Parliament and the Directive on Combating Terrorism*, in *ERA Forum*, 2017, p. 423.

³⁹ La parte generale menziona tuttavia, come ambiti di particolare allarme ed interesse, i reati legati alla pedopornografia e alla proprietà intellettuale, quest'ultima disciplinato compiutamente dalla Direttiva 2004/48/CE. Per quanto invece concerne il primo tipo di illecito, è certamente rilevante l'art. 25 della Direttiva 2011/93/UE, riguardante le misure da adottare contro i siti che contengono o diffondono materiale di tipo pedopornografico, imponendo per gli Stati l'obbligo di assicurarne la tempestiva eliminazione e chiedendo loro di adoperarsi «per ottenere la rimozione di tali pagine ospitate al di fuori del loro territorio» [corsivo aggiunto]. Le misure adottate devono in ogni caso assicurare procedure trasparenti, adeguate quanto alle garanzie (compresa la possibilità di adire l'autorità giudiziaria), proporzionate e limitate «allo stretto necessario», dovendo informare gli utenti quanto al motivo che ha portato alla rimozione dei contenuti ad essi appartenenti.

⁴⁰ Considerando n. 31, Raccomandazione 334.

⁴¹ Considerando n. 11, Raccomandazione 334.

ultimi anni, è dunque ora ammessa e fortemente incoraggiata la segnalazione proveniente da qualsiasi utente dell'*hosting provider*, e ciò mediante la predisposizione di meccanismi facilmente accessibili per costoro. Per consentire ai prestatori di servizi di adottare «una decisione coscienziosa e informata quanto al seguito da dare a tali segnalazioni», queste ultime dovranno essere «adeguatamente motivate e sufficientemente precise»⁴². E tuttavia, ai fini della valutazione della responsabilità di cui all'art. 14 della Direttiva *eCommerce*, si evidenzia come non viene meno per i *provider* l'opportunità di procedere ad autonoma individuazione dei contenuti illeciti, non apparendo sufficiente l'eventuale giustificazione, ai fini dell'esenzione dalla responsabilità, della mancata specificità della segnalazione ricevuta.

Resta in ogni caso di preminente importanza l'attività svolta dalla figura del c.d. segnalatore attendibile, ossia quel soggetto «che un prestatore di servizi di hosting ritiene abbia particolari competenze e responsabilità ai fini della lotta ai contenuti illegali online»⁴³, le cui comunicazioni dirette ai *provider* dovrebbero essere considerate in via prioritaria mediante la predisposizione di procedure accelerate, previa verifica delle necessarie competenze e della prestazione dell'attività diligente e neutrale dell'attività di segnalazione⁴⁴.

Le più recenti tecnologie consentono inoltre l'adozione di strumenti automatizzati, in grado di identificare autonomamente i contenuti considerati illeciti e di reagire in modo estremamente più rapido qualora simili dati vengano immagazzinati presso l'*host*. Tuttavia, stante ancora il costo non indifferente per un *provider*, l'adozione di tali misure non può allo stato richiedersi in via generalizzata, rendendosi necessarie considerazioni circa le dimensioni e la scala di operatività del prestatore di servizi stesso⁴⁵. Non potendosi dunque prescindere da considerazioni di natura economica, è fortemente incoraggiata la collaborazione tra gli stessi *hosting provider*, che «ove opportuno, dovrebbero condividere tra loro esperienze, soluzioni tecnologiche e migliori prassi per contrastare i contenuti illegali online, anche nel contesto delle iniziative di collaborazione già in corso relative a codici di condotta, protocolli d'intesa e altri accordi volontari»⁴⁶.

Se evidenti sono i benefici che i mezzi automatici di rilevazione sono in grado di apportare al contrasto degli illeciti *online*, altrettanto manifesta è la necessità di implementare, in relazione agli stessi, misure di salvaguardia ancora più stringenti, «efficaci e appropriate per garantire l'accuratezza e la fondatezza delle decisioni relative a tali contenuti» da parte degli *hosting provider*. Tra le misure richieste figura in particolare la possibilità di procedere con una ulteriore verifica, posta in essere da persone fisiche, in tutte le circostanze in cui ciò si renda opportuno e, in ogni caso, qualora vi sia espressa richiesta⁴⁷. Nell'impiegare questi strumenti, è fatto salvo ancora una volta il disposto del citato art. 15, par. 1, della Direttiva

⁴² Artt. 5 e 6 e considerando nn. 16 e 17, Raccomandazione 334.

⁴³ Art. 4, lett. g), Raccomandazione 334. Costituisce invece una segnalazione qualificata «qualunque comunicazione indirizzata a un prestatore di servizi di hosting da un'autorità competente o da Europol in merito a contenuti memorizzati da tale prestatore di servizi di hosting e considerati contenuti terroristici dall'autorità competente o da Europol, con cui si chiede al prestatore di servizi di hosting di procedere su base volontaria alla rimozione di tali contenuti o alla disabilitazione dell'accesso ai medesimi» (art. 4, lett. k), Raccomandazione 334. Sulla importanza della cooperazione degli *hosting provider* con Europol, si veda anche il considerando n. 28 della Raccomandazione 334.

⁴⁴ Artt. 23 e 27, Raccomandazione 334.

⁴⁵ Cfr. considerando n. 24, Raccomandazione 334.

⁴⁶ Art. 28, Raccomandazione 334.

⁴⁷ Art. 20, Raccomandazione 334.

eCommerce, concernente il divieto per gli Stati di imporre un obbligo giuridico di sorveglianza generale in capo ai *provider*, peraltro anche in relazione ai contenuti terroristici⁴⁸.

Rilevanza assume altresì l'art. 14 della Direttiva *eCommerce*: la Commissione europea ha ritenuto che l'adozione di misure proattive (l'impiego di strumenti automatizzati costituendone meramente un esempio) non implica l'automatica perdita del beneficio dell'esenzione di responsabilità⁴⁹. Il contesto migliore di utilizzo di questi strumenti è costituito dalle situazioni in cui «sia già stata accertata la natura illegale dei contenuti o questi ultimi siano tali da renderne superflua la contestualizzazione», ancora una volta evidenziandosi la preminenza delle segnalazioni provenienti «da Europol o dalle autorità preposte all'applicazione della legge»⁵⁰.

Benché la Raccomandazione ritenga opportuna la creazione, in favore degli utenti, di meccanismi atti a informarli e a fornire loro la possibilità di contestare la rimozione dei contenuti o il blocco dell'accesso agli stessi e capaci di garantire una adeguata considerazione di tali repliche⁵¹, le procedure non dovrebbero trovare impiego «qualora risulti evidente che i contenuti in questione sono illegali e fanno riferimento a reati gravi che comportano una minaccia per la vita o la sicurezza delle persone»⁵². Nell'ottica di piena collaborazione che la Raccomandazione in esame si propone di perseguire, il meccanismo non dovrebbe peraltro essere impiegato qualora sia pervenuta richiesta in tal senso da un'autorità competente, nazionale od europea, «per motivi di ordine pubblico o di pubblica sicurezza e in particolare a fini di prevenzione, indagine, accertamento e perseguimento di reati»⁵³. Per meglio rispondere alle previste finalità, gli Stati membri sono inoltre esortati ad imporre normativamente agli *hosting provider* un obbligo di «informare tempestivamente le autorità preposte»⁵⁴ qualora vengano a conoscenza, nell'esercizio delle proprie attività, di «elementi di prova di presunti reati gravi che comportano una minaccia per la vita e la sicurezza delle persone»⁵⁵.

Quanto ai contenuti illeciti *online* costituenti reati di terrorismo, la Raccomandazione prevede aggiuntivamente⁵⁶ che gli Stati membri forniscano alle loro autorità competenti «le capacità e le risorse sufficienti per rilevare e identificare efficacemente i contenuti terroristici e presentare segnalazioni qualificate»⁵⁷, e ciò anche attraverso una collaborazione particolarmente attiva con Europol⁵⁸. Tali comunicazioni dovrebbero essere esaminate dagli *hosting provider* entro un'ora dalla ricezione⁵⁹, gravando sugli stessi l'onere di «inviare senza

⁴⁸ Così il considerando n. 36, Raccomandazione 334.

⁴⁹ Comunicazione 555, p. 5.

⁵⁰ Considerando n. 25, Raccomandazione 334.

⁵¹ Artt. 9 e 11-13 della Raccomandazione 334, auspicandosi anche che i *provider* forniscano una risposta informativa circa le motivazioni che hanno portato alla rimozione o al blocco dei contenuti.

⁵² Individuati a titolo esemplificativo dal considerando n. 21, Raccomandazione 334, nei reati previsti dalle Direttive (UE) 2017/514 e 2011/93/UE.

⁵³ Art. 10, Raccomandazione 334. A tal proposito, il considerando n. 21 della stessa Raccomandazione prevede: «[n]ella misura in cui tutto ciò comporti una restrizione del diritto a essere informati in merito al trattamento di dati personali, dovrebbero essere soddisfatte le pertinenti condizioni di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio».

⁵⁴ E ciò peraltro in conformità all'art. 15, par. 2, della Direttiva *eCommerce*.

⁵⁵ Art. 24, Raccomandazione 334.

⁵⁶ Per espressa previsione dell'art. 29, Raccomandazione 334.

⁵⁷ Art. 32, Raccomandazione 334.

⁵⁸ Art. 40, Raccomandazione 334.

⁵⁹ Art. 34, Raccomandazione 334. E ciò in virtù di una duplice constatazione: da un lato, a causa della maggiore probabilità di produrre danni nella prima ora della pubblicazione di tali contenuti; dall'altro, «considerate le

indebiti ritardi una conferma dell'avvenuto ricevimento delle segnalazioni qualificate»⁶⁰. In merito agli strumenti automatizzati di rilevazione dei contenuti illeciti, essi dovrebbero essere predisposti in questo specifico settore anche al fine di impedire una rinnovata pubblicazione dei dati informatici che abbiano già subito la rimozione o cui l'accesso sia stato disabilitato⁶¹. Si auspica inoltre che «[l]addove sia tecnologicamente possibile dovrebbero essere rilevati tutti i formati di diffusione dei contenuti terroristici» (art. 38), e ciò anche mediante il miglioramento della c.d. banca dati di *hash*, ossia un *database* concernente tutti i contenuti terroristici *online* conosciuti⁶².

Da ultimo, in quella che si prospetta diventare una deroga alla previsione dell'art. 15, par. 2, della Direttiva *eCommerce*, ripresa dalla successiva Proposta di Regolamento, la Raccomandazione suggerisce agli *hosting provider* di «adottare tutte le misure ragionevoli per impedire e, ove possibile, *prevenire* la memorizzazione di contenuti terroristici» [corsivo aggiunto]⁶³.

3.2 Il contrasto alla propaganda terroristica online nella Proposta di Regolamento 2018/640

L'esigenza sentita nella Raccomandazione di dedicare uno spazio autonomo al terrorismo trova piena continuità nella Proposta di Regolamento 2018/640, che delimita il proprio *focus* unicamente sulla prevenzione della diffusione di contenuti terroristici *online*, rivolgendosi, oltre che agli Stati membri, direttamente agli *hosting provider*.

È da ritenersi che tale scelta ristretta quanto alla materia individuata dalla Commissione europea derivi da una serie di fattori. Se certamente si tratta del settore che necessita di una normativa cogente ed uniforme con la maggiore urgenza, in considerazione dell'allarmante diffusione dei contenuti ora menzionati⁶⁴, è altresì da rilevarsi come nelle altre materie, quali ad esempio pedopornografia e violazione delle normative a tutela della proprietà industriale, vi sono stati già considerevoli sforzi, sinora su base volontaria, che hanno consentito di

competenze e le responsabilità specifiche delle autorità competenti e di Europol» (considerando n. 35, Raccomandazione 334). La misura era peraltro già stata adottata ad esempio dalla società Facebook, che grazie agli strumenti automatici di identificazione dei contenuti illeciti si afferma capace di rimuovere il 99% dei contenuti entro detto limite temporale, talvolta agendo addirittura in via preventiva (EUROPEAN COMMISSION, *Fighting Terrorism Online: Internet Forum Pushes for Automatic Detection of Terrorist Propaganda*, 6 dicembre 2017, disponibile presso www.europa.eu/).

⁶⁰ Art. 33, Raccomandazione 334.

⁶¹ Art. 37, Raccomandazione 334.

⁶² Art. 38, Raccomandazione 334. Tale banca dati, lanciata nel 2017, ha raccolto in pochi mesi oltre 40.000 immagini e video rilevanti (sul punto, EUROPEAN COMMISSION, *ult. op. cit.*). Risale peraltro già al dicembre 2016 la creazione di un simile *database*, nato dal comune accordo delle società Facebook, Twitter, Microsoft e YouTube, che prevede la condivisione tra dette imprese di video ed immagini rimossi dai propri servizi di *provider* (disponibile presso www.newsroom.fb.com/).

⁶³ Considerando n. 33, Raccomandazione 334.

⁶⁴ Significativamente, la Commissione riporta come i principali portatori di interessi europei abbiano ritenuto che i contenuti terroristici *online* costituiscano una seria minaccia, oltre che per la società in generale, anche per i modelli aziendali degli *hosting provider*. Invero, il 65% degli intervistati ha ritenuto che *Internet* non costituisca un ambiente sicuro per i suoi utilizzatori, mentre il 90% di loro ha ritenuto necessario un intervento per limitare la diffusione di contenuti illeciti (cfr. Proposta di Regolamento, p. 6).

raggiungere risultati evidentemente valutati come sufficienti dall'Unione europea⁶⁵. Trattasi di una decisione oculata anche sotto un altro profilo: invero, gli obblighi che discenderanno dal futuro Regolamento per gli *hosting provider*, come di seguito si illustrerà, potrebbero rivelarsi allo stato eccessivamente gravosi per i fornitori di servizi, specie se di piccole-medie dimensioni, tanto per motivi tecnologici quanto economici, qualora si dovessero trovare gravati dal vincolo giuridico di prevenire la diffusione di qualsiasi contenuto di natura illecita.

Base giuridica del futuro Regolamento sarà l'articolo 114 del Trattato sul Funzionamento dell'Unione europea (TFUE): la Commissione ritiene infatti che l'atto legislativo andrà a creare un quadro giuridico chiaro e armonizzato in materia, e ciò al fine di garantire il corretto funzionamento del Mercato unico digitale, assicurando un contesto operativo ai *provider* connotato da certezza giuridica. Tali esigenze sono sentite come di importanza preminente, al punto da ritenere l'art. 114 TFUE come una base giuridica appropriata per imporre obblighi anche ai *provider* che forniscano i loro servizi all'interno del territorio comunitario, pur avendo la sede legale al di fuori: a tal fine, è infatti sufficiente che il *provider* abbia un «collegamento sostanziale» con uno o più Stati membri, dato ad esempio dall'avere il fornitore la propria sede nell'Unione europea, ovvero dall'avere un significativo numero di utilizzatori o dall'indirizzare le proprie attività in uno o più degli Stati membri⁶⁶. Sulla scorta di queste considerazioni, la Commissione ha ritenuto che la forma giuridica più appropriata per l'atto oggetto di proposta sia il regolamento, in quanto eventuali divergenze normative fra gli Stati membri, ancorché limitatamente alla fase applicativa, potrebbero danneggiare l'attività di prestazione di servizi qualora il *provider* operi in più Stati⁶⁷.

Il futuro Regolamento si pone dunque come necessaria fase di completamento della disciplina stabilita dalla Direttiva *eCommerce* per quel che concerne la responsabilità dei *provider* e della Direttiva 541, relativamente alle definizioni di condotte costituenti terrorismo⁶⁸.

In relazione alla prima Direttiva, due sono le questioni che si prospettano di principale interesse. Innanzitutto, nel sollecitare l'impegno proattivo degli *hosting provider*, la Proposta di Regolamento evidenzia come ciò non debba tradursi in un obbligo di sorveglianza generale, in conformità al più volte citato art. 15 della Direttiva *eCommerce*. È evidente come il legislatore europeo si mostri ancora inspiegabilmente reticente nell'ammettere una deroga specifica per i contenuti terroristici al regime imposto dall'art. 15, nato in ben altro contesto tecnologico, nonché nell'imporre l'uso di strumenti automatizzati, prevedendo unicamente la possibilità per l'autorità competente di adottare misure specifiche e mirate per il *provider* che

⁶⁵ Come appare confermato dalla stessa Proposta di Regolamento: «[s]e non sono state adottate misure supplementari, verranno portate avanti le azioni volontarie previste nello scenario di base, con effetti sulla riduzione dei contenuti terroristici online. Tuttavia, è improbabile che tutti i prestatori di servizi di hosting esposti a tali contenuti adottino misure volontarie e potrebbe conseguire un'ulteriore frammentazione giuridica, che frapporrebbe ulteriori barriere alla fornitura di servizi transfrontalieri» (Proposta di Regolamento, p. 6).

⁶⁶ Proposta di Regolamento 2018/640, pp. 2-4 e art. 2, n. 3.

⁶⁷ Si vedrà tuttavia *infra* come il Regolamento espressamente riservi allo Stato membro la possibilità di decidere che tipo di responsabilità sorge in capo al *provider* che non benefici del regime di esenzione di cui all'art. 14 della Direttiva *eCommerce*.

⁶⁸ È da ritenersi come il rinvio alle definizioni di reati di terrorismo contenute nella Direttiva 541 non verrà meno neanche qualora dovesse essere adottato l'emendamento del Parlamento europeo alla Proposta di Regolamento, volto ad eliminare l'art. 2, n. 4 dell'atto della Commissione che operava un espresso rimando all'art. 3 della Direttiva 541. E ciò anche in considerazione dei diversi altri richiami alla Direttiva che la Proposta di Regolamento opera, senza aver subito modifiche da parte del Parlamento in prima lettura.

abbia ricevuto «un numero significativo di ordini di rimozione» e purché risulti necessaria all'esito di un bilanciamento tra la tutela della pubblica sicurezza e i diritti fondamentali coinvolti⁶⁹. A ben vedere, due sembrano gli scenari che potranno prospettarsi: (i) le autorità competenti valutano tale necessità sussistente *ex ante*, e dunque effettivamente contravvengono alla disciplina dell'art. 15 Direttiva *eCommerce*, imponendo un obbligo generalizzato di sorveglianza, sebbene limitato alla materia del terrorismo; ovvero (ii) la necessità si rivela esistente *ex post*, il che di fatto disattende il fine dell'azione preventiva che si propone il Regolamento in questione.

In secondo luogo, assumerà certamente fondamentale importanza la scelta degli Stati membri in relazione all'ampio margine di discrezionalità per quel che concerne la qualificazione della responsabilità degli *hosting provider* in relazione ai contenuti *online* costituenti terrorismo qualora il prestatore di servizi non rimuova tali dati nel tempo ritenuto congruo dalla disciplina europea, ovvero manchi di adeguarsi ad un eventuale obbligo di rimozione imposto dalle autorità competenti. Invero, la Proposta di Regolamento si limita a stabilire che dovranno essere imposte sanzioni particolarmente gravose qualora il *provider* non sia in grado di disabilitare l'accesso alle informazioni di natura terroristica in modo sistematico e persistente entro un'ora dalla ricezione del *removal order* emesso dalle autorità competenti⁷⁰, tenendo in ogni caso in adeguata considerazione la capacità economica del fornitore di servizi e assicurandosi altresì che l'imposizione di tali sanzioni non determini il *provider* a rimuovere contenuti in modo indiscriminato per evitare di incorrere in penalità. L'unica indicazione proveniente dalla Proposta, oltre a doversi caratterizzare la sanzione per effettività, proporzionalità e carattere dissuasivo⁷¹, è quella di poter arrivare ad esigere dal *provider* una sanzione sino al 4% del fatturato dell'ultimo anno, ancora una volta non specificando dunque la natura giuridica di tale penale⁷².

Appare ragionevole ritenere che tre saranno le possibili soluzioni adottate nel definire detta responsabilità: (i) di natura civile, per *culpa in vigilando*, in funzione sanzionatoria; (ii) di natura penale, per concorso omissivo nel reato commissivo altrui; (iii) ancora di natura penale, ma per concorso commissivo, agevolando il fornitore dei dati informatici mediante una condotta materiale o morale.

Alla luce delle menzionate normative europee attualmente vigenti, è da ritenersi come la soluzione a carattere civilistico sia da preferirsi, quantomeno in una prima fase, soprattutto in considerazione del livello di adattamento tecnologico che sarà inevitabilmente richiesto alle società fornitrici di servizi di memorizzazione di dati, apparendo questa soluzione un equo bilanciamento rispetto alle esigenze di pubblica sicurezza che la legislazione si propone di tutelare.

⁶⁹ Art. 6, par. 4, Proposta di Regolamento, come emendata in prima lettura dal Parlamento europeo.

⁷⁰ Viene fatta salva in ogni caso la possibilità per il *provider* di segnalare all'autorità competente l'impossibilità, di fatto o dovuta a forza maggiore, di rimuovere i contenuti segnalati: cfr. art. 4 Proposta di Regolamento.

⁷¹ I criteri da considerarsi ai fini della commisurazione della pena ed indicati dall'art. 18 (come emendato dal Parlamento europeo), onde rispettare tali principi direttivi, sono i seguenti: a) la natura, la gravità e la durata della violazione; b) il carattere intenzionale o meramente negligente della condotta; c) gli eventuali precedenti illeciti attribuibili alla persona giuridica; d) la capacità economica della persona giuridica; e) il livello di collaborazione dell'*hosting provider* con le autorità competenti, al fine evidentemente di individuare i responsabili della creazione dei dati illeciti; e-bis) la natura e le dimensioni del *provider*.

⁷² Art. 18 e Considerando n. 38, Proposta di Regolamento. Peraltro, l'art. 18 impone agli Stati membri di comunicare, entro sei mesi dall'entrata in vigore del Regolamento, quali siano le misure a tal fine adottate.

E certamente una potenziale scelta in questa direzione da parte dei legislatori nazionali non dovrà pregiudicare del tutto la terza opzione, pur ponendosi come *extrema ratio*, conformemente ai principi generali del diritto penale. Peraltro, è necessario richiamare quanto previsto dall'art. 17 della Direttiva 541, che nel disciplinare la responsabilità penale delle persone giuridiche in materia di terrorismo⁷³, stabilisce già quale sia la natura della conseguenza per la persona giuridica qualora una persona ricoprente ruolo apicale al suo interno ponga in essere tali delitti: trattasi, evidentemente, di potenziali ipotesi di concorso nella commissione del reato, atteso il vantaggio che deve derivarne per la società ai fini della configurabilità della responsabilità in questione.

Infine, sebbene la Proposta di Regolamento non dedichi specifica attenzione al *notice and take down mechanism*, è richiesta l'adozione di misure specifiche da parte dei fornitori di servizi, pur nel rispetto dei diritti fondamentali concernenti in particolar modo la libertà di espressione e di informazione⁷⁴. E, a tal riguardo, la futura normativa europea richiede che i dati rimossi o disabilitati a seguito di un ordine dell'autorità ovvero dell'impiego di misure specifiche di rilevamento di contenuti illeciti dovranno essere conservati per un periodo pari a sei mesi, al fine di consentire un ricorso amministrativo o giudiziario della decisione di rimozione o, al contrario, per favorire le eventuali investigazioni sulla fonte di tali informazioni⁷⁵. Peraltro, il termine, che appare perentorio, si troverà manifestamente in contrasto con quanto stabilito dalla attuale disciplina italiana in materia di *data retention*, che, nell'attuare la Direttiva 541, ha stabilito che i *provider* dovranno conservare i dati telefonici e telematici a fini di indagine per un periodo pari a sei anni⁷⁶.

4. Prime misure introdotte nell'Unione europea in via volontaria

In piena conformità già alle previsioni della Raccomandazione 2018/334, sono state realizzate fin da subito una serie di attività a livello europeo, con l'obiettivo di raggiungerne i fini prefissati. Innanzitutto, è opportuno considerare come al centro dei progetti che Europol si propone di compiere nel prossimo triennio vi sia il miglioramento delle capacità cibernetiche e forensi dei propri organismi, con lo scopo di arginare la proliferazione di contenuti illeciti *online*, rivolgendo particolare attenzione al settore dei reati di terrorismo. E proprio a riguardo, è prevista una stretta cooperazione con gli esperti in tale ambito degli Stati membri e degli *hosting provider*, cui spetta l'obbligo di fornire informazioni su richiesta della stessa Europol. Peraltro, è stabilito il monitoraggio continuo delle attività sui *social network* e in generale

⁷³ Vedi *supra* §2.

⁷⁴ Art. 6, Proposta di Regolamento. Tali diritti dovranno trovare adeguata tutela anche garantendo agli utilizzatori un adeguato potere di revisione umana e, più in generale, di verifica dei contenuti rimossi o bloccati in modo automatizzato, creando dunque per gli *user* un meccanismo effettivo di reclamo.

⁷⁵ Art. 7, Proposta di Regolamento.

⁷⁶ Art. 24, L. 20 novembre 2017, n. 167, recante le Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017. Piuttosto evidente come tale normativa già presenti profili di incompatibilità con la normativa europea, ed in particolare alla luce della lettura costante della giurisprudenza lussemburghese a partire dal *leading case* in materia, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources et al. and Kärntner Landesregierung et al.*, 8 aprile 2014, C-293/12 e C-594/12, Grand Chamber. Da ultimo, sul punto, v. anche il Parere 1/15 della Corte di Giustizia dell'Unione europea, reso il 26 luglio 2017 dalla Grande Sezione e concernente il Progetto di accordo tra il Canada e l'Unione europea sul trasferimento dei dati del codice di prenotazione passeggeri aerei (c.d. "PNR") dall'Unione al Canada.

nell'ambiente informatico: ancora una volta, l'attività appare difficilmente attuabile senza procedere in un futuro prossimo all'imposizione di un generale obbligo di sorveglianza in capo agli *hosting provider*⁷⁷.

Nel giorno immediatamente successivo all'approvazione della Raccomandazione 334, e dichiaratamente in esecuzione della stessa, è stato peraltro attivato un progetto pilota tra la *Internet Referral Unit* (IRU) di Europol, Belgio, Francia e Olanda, con l'obiettivo di migliorare i sistemi di rilevazione, analisi e deferimento di contenuti *online* di matrice terroristica⁷⁸. La IRU ha poi provveduto, in collaborazione con diversi Stati membri⁷⁹, ad un'azione congiunta per la individuazione di tali contenuti su *blog* e siti di *video-hosting*, segnalando quanto si è ritenuto costituire illecito ai moderatori dei *provider*, affinché questi potessero stabilire se fosse opportuna la rimozione dei dati, in conformità alle clausole di termini e condizioni da essi determinati, agendo dunque pienamente come segnalatore qualificato⁸⁰.

L'attività coordinata di segnalazione di contenuti mediante la collaborazione degli Stati e degli *hosting provider*, che Europol intende promuovere con una cadenza regolare, costituisce con evidenza un'attuazione delle esortazioni proposte nell'ambito della Raccomandazione 334 e dei fini che si propone la Proposta di Regolamento 640, dovendosi positivamente segnalare come l'Unione europea si stia altresì impegnando nella ricerca attiva di forme di investigazione diverse dalla raccolta dati di massa⁸¹.

5. Osservazioni conclusive

Devono certamente accogliersi favorevolmente gli sforzi sin qui compiuti dalle istituzioni europee, dapprima mediante la Raccomandazione 2018/334, nonché quelli in corso con la Proposta di Regolamento 2018/640, che mostra il grande pregio di adattare il quadro normativo preesistente alle nuove sfide poste dal progresso tecnologico nel campo della repressione della diffusione di contenuti terroristici *online*.

Con il presente contributo si è cercato tuttavia di individuare ed analizzare quanto potrebbe lasciare ancora spazio di incertezza, nonostante una disciplina nel complesso da giudicarsi positivamente. E, con tutta probabilità, la questione aperta maggiormente preoccupante sotto un profilo strettamente giuridico è la mancata determinazione della natura

⁷⁷ EUROPOL, *Draft Europol Programming Document 2018 – 2020*, 30 gennaio 2017, 48-52, disponibile presso www.parleu2017.ee/. Il coordinamento di tali attività dovrà avvenire per mezzo dell'ECTC (*European Counter-Terrorism Centre*), istituito nel 2016 nell'ambito di Europol.

⁷⁸ EUROPOL, *Europol's EU Internet Referral Unit Partners with Belgium, France and The Netherlands to Tackle Online Terrorist Content*, 2 marzo 2018: "The project is developed under Europol's EU IRU mandate to coordinate and share detection tasks (flagging) of online terrorist content with relevant partners, and to carry out and support referrals quickly, efficiently and effectively in close cooperation with the industry. Furthermore, the initiative is in line with the latest Recommendation of the European Commission of 1 March 2018 to reinforce the EU's response to illegal content online" (disponibile presso www.europol.europa.eu/).

⁷⁹ Belgio, Francia, Olanda, Slovenia e Regno Unito (quest'ultimo Stato non è peraltro parte della Direttiva 541).

⁸⁰ EUROPOL, *More Than 900 Instances of Online Terrorist Propaganda Uncovered*, 16 marzo 2018, disponibile presso www.europol.europa.eu/.

⁸¹ Invero, tale ultima soluzione è stata recentemente riconosciuta da Europol come "difficult, expensive, not necessarily effective and highly problematic from the perspective of civil liberties and privacy rules" (così EUROPOL, *The Evolution of Online Terrorist Propaganda*, 19 aprile 2018, disponibile presso www.europol.europa.eu/).

della responsabilità in capo al *provider*, in relazione ai contenuti terroristici, qualora non trovi applicazione l'esenzione stabilita dall'art. 14 dell'ormai parzialmente obsoleta Direttiva *eCommerce*. Rimane dunque da domandarsi se l'armonizzazione che il futuro Regolamento si propone di raggiungere al fine di fornire certezza normativa – e, conseguentemente, economica – ai *provider* che operano nell'Unione europea sia effettivamente conseguibile nonostante tale lacuna.

Auspicabile appare considerare due ulteriori fattori, che non risultano essere stati oggetto di analisi nei documenti sinora prodotti dalle istituzioni e dalle agenzie europee: (i) l'implementazione di forme più avanzate di responsabilità dei *browser* rispetto ai *provider* in generale; (ii) una attenzione particolare ai fenomeni del *Dark Web* e del *Deep Web*⁸².

Quanto alla prima questione, si ritiene possibile prevedere, allo stato attuale dello sviluppo dell'informatica, che una diversa, più stringente forma di responsabilità debba ricadere in capo ai *browser*, ossia a quei programmi utilizzati per la navigazione in Internet in grado di mostrare una interfaccia HTML⁸³. Ed invero, non si vede perché non possano essere esortate le relative aziende, anche mediante strumenti di *soft law*, ad implementare meccanismi che siano in grado di rilevare contenuti, quali ad esempio quelli immagazzinati nelle c.d. banche di *hash*⁸⁴, portando ad un immediato oscuramento di tali informazioni mediante criptazione delle stesse. Di conseguenza, i dati non figurerebbero più tra i risultati di ricerca proponibili all'utenza, restringendo notevolmente il campo di diffusione dei contenuti illeciti.

Quanto al secondo punto, la mancata presa di cognizione negli strumenti normativi europei di tali universi informatici è forse l'aspetto più preoccupante sia della Raccomandazione 334 che della successiva Proposta di Regolamento, in quanto sia il *Deep Web* che, soprattutto, il *Dark Web* costituiscono notoriamente il maggior campo di proliferazione degli illeciti *online* e della propaganda degli stessi, in particolare di matrice terroristica⁸⁵.

Conclusivamente, nonostante le inevitabili perplessità che permangono anche in relazione alla disciplina *in fieri*, appare evidente come l'Unione europea abbia assunto piena consapevolezza del maggior punto di forza per la repressione degli illeciti *online*: indirizzare le proprie richieste direttamente agli operanti nel settore tecnologico, nell'ottica di una piena collaborazione tra questi, le autorità nazionali ed Europol.

⁸² A differenza del c.d. *Surface Web*, cui chiunque disponga di una connessione ad Internet può accedere, il *Deep Web* costituisce il materiale *online* non accessibile con una semplice ricerca (prevedendo codici di decriptazione di grado superiore rispetto al *Surface Web*), mentre al *Dark Web* si può accedere unicamente mediante appositi software che consentono, *inter alia*, una navigazione sulla rete assolutamente anonima e non tracciabile (cfr. A. D. ROMEO, *Hidden Threat: The Dark Web Surrounding Cyber Security*, in *Northern Kentucky Law Review*, 2016, pp. 75-76).

⁸³ Tra i più noti e comunemente usati *browser*, a titolo esemplificativo: Chrome, Edge, Internet Explorer, Firefox.

⁸⁴ Sulle quali v. *supra*, nota 62.

⁸⁵ Consentendo peraltro ai terroristi di comunicare facilmente, organizzarsi e scambiare quanto necessario per perpetrare le loro attività terroristiche: A. D. ROMEO, op. cit., p. 79. Qualche fugace menzione al *Dark Web* è presente unicamente in *Draft Europol Programming Document 2018 – 2020*, 30 gennaio 2017, 48-52, disponibile presso www.parleu2017.ee/.