ROGATORIE INTERNAZIONALI E ORDINE DI RIMOZIONE EUROPEO QUALI STRUMENTI DI CONTRASTO AI CRIMINI ANCHE IN ORDINE ALLA DIFFUSIONE DI CONTENUTI TERRORISTICI ON LINE

Rimini, 2 marzo 2022

Indice dell'intervento

Nozione di Rogatoria internazionale

1

La rogatoria internazionale costituisce una forma di **collaborazione giudiziaria** tra diverse Autorità giurisdizionali per il compimento di atti relativi ad un processo, o ad una causa civile, e affonda le proprie radici – in un mondo di Nazioni e popolazioni sempre più aperte agli scambi economici, culturali e sociali, le cui azioni non si esauriscono nell'ambito dei confini nazionali – non solo nella necessità da parte degli Stati di disporre di strumenti idonei alla realizzazione della propria potestà punitiva di fronte al compimento di crimini, ma anche per dare concretezza ai principi universali, costituzionali, comunitari che tutelano il diritto di ciascuna persona al riconoscimento in sede giudiziaria delle proprie ragioni, come affermano gli artt. 7 e 8 della Dichiarazione Universale dei Diritti dell'Uomo, proclamata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948 – 'Tutti sono eguali dinanzi alla legge e hanno diritto, senza alcuna discriminazione, ad una eguale tutela da parte della legge … i diritti di ciascuno sono protetti dalla legge'; l'art. 24 Cost. – 'Tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi'; la Convenzione Europea dei Diritti dell'Uomo, firmata a Roma il 4 novembre 1950 dagli Stati membri dell'Unione Europea – il cui preambolo afferma il loro impegno a rispettare 'la libertà e la preminenza del diritto, a prendere le prime misure atte ad assicurare la garanzia collettiva di alcuni dei diritti enunciati nella Dichiarazione universale [dei diritti dell'Uomo]' e il cui art. 6, recepito dall'art. 111 Cost., impone che ogni causa o processo si svolga 'entro un termine ragionevole', sovente realizzabile solo attraverso un'azione sinergica da parte di diverse Autorità Giudiziarie.

Per queste ragioni il nostro codice di rito, nel libro XI che disciplina i rapporti giurisdizionali con Autorità straniere, dopo avere sancito la tutela dei diritti fondamentali della persona nel mutuo riconoscimento (art. 696 ter c.p.p.), ha regolato i temi dell'estradizione, delle rogatorie internazionali, degli effetti delle sentenze penali straniere e dell'esecuzione all'estero di sentenze penali italiane, dell'assunzione di procedimenti penali dall'estero e del trasferimento di procedimenti penali all'estero, rinviando alle norme di natura pattizia prevedendo la diretta trasmissione ad altra Autorità Giudiziaria, nella reciprocità e sulla base di un accordo

internazionale, della richiesta di assistenza giudiziaria previa trasmissione di copia al ministro della Giustizia, senza ritardo (artt. 723.4 e 727.6 c.p.p.. a seconda che si tratti di rogatorie passive ed attive).
Nello specifico delle rogatorie internazionali si tratta prevalentemente dell'assunzione di legittimi mezzi probatori e del compimento di attività ancillari, quali notificazioni o comunicazioni.
Vi sono due categorie di rogatorie:

1) **dall'estero verso l'Italia**: con la previsione di un doppio sindacato, politico (rimesso al Ministro della Giustizia, che ha un potere di veto della rogatoria per ragioni politiche o di indole giuridica) e giudiziario (di spettanza della Corte d'Appello);
2) **dall'Italia verso l'estero**: con richiesta proveniente da giudici italiani, previo vaglio politico del ministro della Giustizia, che può non dare corso alla rogatoria per motivi attinenti alla sicurezza o ad altri interessi nazionali. Se la richiesta è ritenuta inoltrabile dal Ministro, la rogatoria è trasmessa all'Autorità estera mediante i canali diplomatici.

Fonti nazionali e internazionali di riferimento

Nel nostro ordinamento giuridico – per quanto attiene la materia penale, che qui interessa – le norme di riferimento, come detto, sono contenute nel codice di procedura penale, via via adeguato alla stregua dei trattati internazionali che disciplinano i rapporti giurisdizionali con le Autorità straniere, la cui Parte Seconda regola le rogatorie attive e quelle passive, cioè quella richiesta dall'autorità giudiziaria italiana ad altra Autorità estera e quella proveniente da un'Autorità giudiziaria estera a quella italiana (artt. 723-729 quinquies c.p.p., norma quest'ultima di recente introduzione in materia di **impiego di squadre investigative comuni**), nonché i rapporti giurisdizionali con Autorità straniere (artt. 730-746 c.p.p.) ed i rapporti giurisdizionali con Autorità straniere (artt. 746 bis -746 quater c.p.p.).

La Corte di Cassazione, in tema di rogatoria internazionale, ha costantemente affermato il principio per cui trovano applicazione le norme processuali dello Stato in cui l'atto viene compiuto, con l'unico limite che la prova non può essere acquisita in contrasto con i principi fondamentali dell'ordinamento giuridico italiano, primo fra tutti il diritto di difesa.
È, infatti, principio generale in materia di assistenza giudiziaria penale – peraltro comune alla maggior parte dei Paesi stranieri – che l'atto compiuto all'estero su rogatoria sia regolato non dalla legge del Paese richiedente, ma, costituendo esso tipico esercizio della sovranità del Paese richiesto, dalle norme dell'ordinamento di quest'ultimo, alla cui stregua deve esserne verificata la validità.
Ed invero per la rogatoria internazionale, anche se eseguita con la diretta partecipazione del giudice italiano, trovano applicazione, in virtù del principio 'locus regit actum' e in conformità ai canoni di diritto internazionale della prevalenza della 'lex loci' sulla 'lex fori', non le norme del codice di rito del Paese richiedente, che disciplinano il processo, bensì quelle dello Stato in cui l'atto viene compiuto.

→ *segue*

Un esempio concreto

Un esempio concreto, tratto dalla mia ultra quarantennale esperienza di magistrato inquirente, è costituito dalla rogatoria del pubblico ministero di Padova personalmente eseguita a New York nel 1992, nell'ambito della c.d. 'Tangentopoli', per l'interrogatorio di Giancarlo Grassetto, titolare dell'omonima impresa di costruzioni, venduta a Ligresti Salvatore ad un prezzo comprensivo delle tangenti (rectius: dazioni prive di causa lecita, come propriamente si soleva dire) concordate con esponenti politici di primo piano, locali e nazionali, e poi da quest'ultimo effettivamente versate per la costruzione del nuovo palazzo di Giustizia di Padova.

Detta rogatoria fu eseguita in forza del Trattato del 1982, allora esistente tra gli Stati Uniti d'America e la Repubblica Italiana in materia penale, attraverso la mediazione del nostro Ministero della Giustizia, ma la comune rilevanza delle indagini preliminari in materia di criminalità, specie quella organizzata, hanno ben presto determinato l'Accordo tra Unione Europea e Stati Uniti in materia di estradizione del 25 giugno 2003, a tenore del quale, tra l'altro, 'l'Unione europea provvede a che gli Stati membri confermino con strumento scritto singolarmente concluso con gli Stati Uniti che i Trattati bilaterali sono applicati come convenuto nel presente accordo' (art. 3.1), nonché l'Accordo di mutua assistenza Giudiziaria tra Unione Europea e Stati Uniti sottoscritto a Roma il 3 maggio 2006, avente ad oggetto – soprattutto – le regole relative all'identificazione dei conti e delle transazioni finanziarie e le disposizioni relative alla formazione e alle attività delle squadre investigative comuni.

Convenzione di Strasburgo del 20 aprile 1959

La prima Convenzione europea di assistenza giudiziaria in materia penale, sottoscritta a Strasburgo il 20 aprile 1959 dai Membri del Consiglio d'Europa, ha rappresentato l'ovvio seguito di quella di Parigi del 13 dicembre 1957 in materia di estradizione.
Il suo archetipo è costituito dall'accettazione di regole uniformi per l'assistenza giudiziaria in materia penale, al fine di attuare una più stretta coesione comunitaria come dichiara il suo primo articolo, a tenore del quale 'Le Parti Contraenti si obbligano ad accordarsi reciprocamente, secondo le disposizioni della presente Convenzione, l'assistenza giudiziaria più ampia possibile in qualsiasi procedura concernente reati, la cui repressione, al momento in cui l'assistenza giudiziaria è domandata, è di competenza delle autorità giudiziarie della Parte richiedente', con il limite della sua inapplicabilità all'esecuzione delle decisioni di arresto e di condanna e ai reati commessi dai militari non costituenti reati di diritto comune, cioè di quelli commessi nell'adempimento del loro servizio, o se la domanda si riferisce a reati considerati dalla Parte richiesta come reati politici o come reati connessi con reati politici[1] o come reati fiscali, ovvero se la Parte richiesta ritiene che l'esecuzione della domanda è di natura tale da ledere la propria sovranità, la sicurezza ovvero di essere contraria all'ordine pubblico o ad altri propri interessi essenziali.

Questo primo trattato, basato sul presupposto della reciprocità, della doppia punibilità del reato per il quale si procede e per il quale sia consentita l'estradizione, prevede, per vero, la mediazione del ministro della Giustizia per l'esecutività delle norme in tema di un 'qualsiasi affare penale' e per il trasferimento nello Stato richiedente di una persona detenuta per rendere una testimonianza o essere sottoposta a un confronto, ma già ne afferma in nuce il superamento

[1] La nostra stessa Costituzione afferma, nell'art. 26, che l'estradizione non può in alcun caso essere ammessa per reati politici.

(sostituito dal solo obbligo di informazione) laddove, in primis, prevede che nel **caso di urgenza**, dette commissioni rogatorie possano essere trasmesse direttamente dalle Autorità giudiziarie della Parte richiedente a quelle della Parte richiesta e che gli estratti del casellario giudiziale e tutte le informazioni relative al medesimo possano essere direttamente scambiati tra le Autorità giudiziarie interessate, al pari delle 'domande d'inchiesta preliminare al perseguimento' di un determinato reato con la specificazione che, in siffatti casi, la trasmissione diretta potrà essere effettuata attraverso l'Organizzazione internazionale di Polizia criminale (Interpol) (v. art. 15).

***

Dalla fine degli anni '50 la Comunità Europea è andata sempre più espandendosi, e il mondo globalizzandosi, ed i popoli – nel grande gioco della geopolitica determinato dai contrastanti, più spesso contrapposti, interessi economici e territoriali – si sono dovuti confrontare con le nuove sfide portate dal terrorismo internazionale e dalla cybercriminalità, figlia dell'incredibile progresso tecnologico che ha caratterizzato la fine del secolo scorso e l'inizio dell'attuale.

Per opporvisi i diversi Stati, in specie quelli comunitari, hanno innovato il proprio ordinamento giuridico con la previsione di nuovi reati per attuare una comune strategia di contrasto, ricorrendo a regole comuni di natura pattizia tese ad assicurare interventi diretti e tempestivi da parte delle rispettive Autorità Giudiziarie e di quelle di Polizia, costituenti il loro braccio operativo.

A questo proposito vale la pena ricordare che l'Italia, nel 2001, ha novellato l'art. 270 bis c.p. che prevede il delitto di associazione con finalità di terrorismo o di eversione dell'ordine democratico, ricomprendendo in essa anche l'associazione con finalità di terrorismo internazionale e che, dopo gli attacchi terroristici ai treni di Madrid dell'11 marzo 2004 che uccisero 191 persone e quelli al sistema dei trasporti pubblici di Londra del 7 luglio 2005, che causarono 55 morti e 700 feriti, il legislatore – con d.l. 27 luglio 2005, n. 144 urgentemente convertito nella legge 31 luglio 2005, n. 155 – ha introdotto nel codice penale la norma definitoria delle **condotte con finalità di terrorismo** dell'art. 270 sexies[2], mutuata dalla Direttiva del Consiglio dell'Unione Europea sulla lotta contro il terrorismo del 13 giugno 2002, a sua volta modificata dalla Direttiva del 15 marzo 2017.

Oggi, l'indagine sul reato di violenza politica interna o internazionale richiede l'impiego di **tecniche di accertamento** mediamente più complesse e sofisticate di quelle in uso negli anni '70 e una **professionalità** sia degli operatori di polizia sia dei magistrati ben più matura, estesa e variegata.

In generale, si può dire che nessun segmento della ricerca investigativa può essere lasciato, nella prospettiva di una risposta efficace al crimine, all'improvvisazione e al caso.

Quando la violenza è, per convergenti elementi sintomatici, espressione di **criminalità organizzata,** le tecniche e le metodologie di indagine riflettono, in primo luogo, la struttura del tutto peculiare di tale forma criminale, la cui tipicità consiste nel **carattere reticolare** delle sue strutture le quali si avvalgono di reti di persone non clandestine, inserite quasi sempre nel tessuto sociale ed economico dei paesi in cui vivono, comunicanti fra di loro con l'uso di

[2] Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia.

apparecchi telefonici e telematici, reciprocamente garantite da collaudati schemi di compartimentazione, dotate infine di compiti ora di direzione ora di organizzazione ora di supporto logistico e di incombenti operativi, coordinati all'interno di una preordinata strategia di attacco contro obiettivi antagonisti.
Quando la rete attraversa i confini nazionali e si distende nei territori di più Stati e perfino di più continenti, le tecniche di accertamento incontrano difficoltà crescenti, per superare le quali sono state fino ad ora elaborate e messe in funzione **misure tecnologicamente avanzate** che affiancano le tradizionali opzioni investigative quali le intercettazioni telefoniche, ambientali e telematiche, i pedinamenti e le osservazioni a distanza, le infiltrazioni e l'uso di agenti sotto copertura, le indagini bancarie e le misure di prevenzione patrimoniale previste per la lotta alla mafia, le analisi e la decriptazione dei documenti provenienti dall'organizzazione, le consulenze tecniche e le ricognizioni personali.
Fra le misure di nuovo conio frequentemente utilizzate per dare un volto ed una identità alle persone sospettate di azioni terroristiche ed eversive si ricordano succintamente quelle appresso descritte:

1. Le **smart-cards,** cioè le carte d'identità intelligenti introdotte dopo gli attentati di New York dell'11 settembre 2001, sono destinate a provare l'identità del titolare del documento con margini di errore pressoché trascurabili e si basano sulla biometria, ossia sulla misurazione dell'esatta distanza fra le pupille ed eventualmente altri organi della persona che ne è in possesso.

2. I **prelievi coattivi di campioni biologici, a fini di identificazione della persona indagata**, sono stati introdotti dopo gli attentati di Londra del 5 luglio 2005 dal decreto antiterrorismo Pisanu (n. 144 del 27.7.2005) che, aggiungendo all'art. 349 c.p.p. il comma 2 bis, consente alla polizia giudiziaria di prelevare coattivamente capelli o saliva, previa autorizzazione scritta o orale del pubblico ministero, per identificare l'indagato durante le indagini preliminari.

E' appena il caso di sottolineare che i prelievi possono essere utilizzati come prove dei fatti investigati avendo indubbia efficacia individualizzante della persona sospettata o ricercata, e il d.lgs. 18 maggio 2018, n. 51, istitutivo della Banca Dati Nazionale del DNA, ne ha regolamentato le modalità di repertazione, di analisi e di utilizzazione dei campioni e garantito la correttezza e l'affidabilità delle procedure di identificazione, nonché la durata della loro conservazione, che può essere destinata a scopi identificativi ben al di là dell'indagine che ebbe a occasionarne il prelievo.

3. I **prelievi coattivi di campioni biologici per l'esecuzione di una perizia o consulenza tecnica** finalizzata alla determinazione del profilo del DNA o ad accertamenti medici in genere, che richiedono il compimento di atti idonei ad incidere sulla libertà personale, sono stati introdotti e regolamentati dalla legge 30 giugno 2009 n. 85 che, con le nuove disposizioni degli artt. 224 bis e 359 bis c.p.p., consente al giudice e, in via d'urgenza, al pubblico ministero di disporre il prelievo di capelli, di peli o di mucosa del cavo orale quando manchi il consenso della persona da sottoporre all'esame del perito o del consulente (che può non essere, si badi, la persona indagata o imputata)[3].

4. La raccolta e la conservazione dei dati delle intercettazioni telefoniche e telematiche e la raccolta e la conservazione dei dati identificativi dei passeggeri dei voli

[3] Può essere utile ricordare che negli Stati Uniti si possono utilizzare e conservare a fini identificativi soltanto i dati genetici delle persone condannate in via definitiva per reati contro la libertà sessuale.

internazionali negli aeroporti, che sono notoriamente luoghi di ingresso e di uscita di una mutevole massa non solo di turisti, uomini di affari, lavoratori e studenti, ma anche di clandestini e di terroristi.
Dopo l'11 settembre 2001, molti paesi di vari continenti e, dopo una iniziale resistenza dovuta alla preoccupazione di legittimare una così grave intrusione nella privacy dei viaggiatori, anche i paesi dell'Unione Europea obbligarono le proprie compagnie aeree a conservare i dati relativi ai passeggeri: identità, destinazione, mezzi e modalità di pagamento, scelta dei posti a bordo, preferenze alimentari. Specialmente queste ultime furono ritenute di primaria rilevanza per la ricostruzione dei profili razziali, religiosi, culturali degli utenti e per l'avvio di indagini su importanti filoni del terrorismo medio-orientale, arabo e musulmano.

5. Le cc.dd. "**tecniche di profiling del rischio**", dirette a identificare il profilo fisico, etnico e religioso, ecc. della persona sospettata di terrorismo e fondate in gran parte sull'analisi dei dati provenienti dal traffico aereo negli aeroporti internazionali e dal mondo dei consumi (grandi alberghi, ristoranti, centri commerciali, banche, ecc.), sono le tecniche probabilmente più applicate dai servizi informativi e di sicurezza di ogni Paese, compreso il nostro, nell'attuale tormentata fase della lotta al terrorismo internazionale.
E' evidente che si tratta di tecniche che vanno maneggiate con grande prudenza e alto senso di responsabilità, se solo si pensi all'enorme squilibrio che caratterizza attualmente le strategie di antiterrorismo dei principali paesi occidentali: squilibrio che si manifesta con inusitata intensità ai danni di minoranze arabe e musulmane, sistematicamente e (per lo più) ingiustamente controllate, discriminate, prevaricate dalla multiforme congerie degli strumenti di prevenzione in uso presso i suddetti Paesi, e di tanto è necessario che prendano coscienza i giudici e i pubblici ministeri italiani che, anche per questa ragione, sono chiamati ad esercitare un approfondito e rigoroso lavoro di riscontro della genuinità delle fonti e dell'attendibilità delle informazioni provenienti da organi di polizia giudiziaria nazionali e stranieri.

E' dunque in questo climax che nasce la Convenzione di Budapest del 23 novembre 2001, in materia di cybercriminalità, con la quale si invitano gli Stati membri all'adeguamento della legislazione nazionale – come ha ben fatto lo Stato italiano – per il contrasto a questa tipologia di illeciti.

Convenzione di Budapest del 23 novembre 2001

La Convenzione di Budapest del 23 novembre 2001, approvata dal Consiglio d'Europa, rappresenta il primo vero documento normativo disciplinante i reati commessi attraverso internet o reti elettroniche, ed è sorta per la necessità di prevenire azioni dirette contro la segretezza, l'integrità e la disponibilità di sistemi, reti e dati informatici e di contrastare l'uso improprio di questi sistemi, reti e dati, rendendo punibili i comportamenti in essa descritti e istituendo poteri sufficienti per combattere efficacemente i relativi reati, facilitandone l'individuazione, l'investigazione e il perseguimento sia su scala nazionale che internazionale e adottando provvedimenti per una cooperazione internazionale rapida e affidabile.

In buona sostanza, la Convenzione di Budapest introduce alcuni principi fondamentali in materia di cooperazione internazionale e mutua assistenza nell'ambito dei procedimenti relativi a crimini informatici, con specifico riferimento alla raccolta delle prove in formato digitale.

Essa si divide in due parti, quella sostanziale e quella processuale.

Quella sostanziale invita, o meglio impegna, i moltissimi Stati che l'hanno adottata – da quello albanese a quello ungherese (tra i membri del Consiglio d'Europa) e da quello argentino a quello di Vanuatu in Oceania (tra i non membri del Consiglio d'Europa) – ad introdurre nel proprio ordinamento giuridico, prevedendone la punibilità, anche a titolo di tentativo, con sanzioni efficaci, proporzionate e dissuasive, che includano la privazione della libertà, i reati:

- → di accesso illecito a un sistema informatico o parte di esso;
- → di intercettazione illecita, intesa non come mera captazione di conversazioni telefoniche o telematiche, ma anche come trasmissione di dati digitalizzati tra sistemi informatici;
- → del loro danneggiamento, cancellazione, deterioramento, alterazione o soppressione;
- → di attacco all'integrità di un sistema informatico;
- → di uso abusivo di dispositivi concepiti o utilizzati ai fini illeciti sopra descritti;
- → di falsificazione e frode (rectius: truffa) informatiche;
- → di pedopornografia, il cui presupposto materiale è costituito dalla massiva divulgazione dei propri contenuti attraverso sistemi informatici collegati al web;
- → contro la proprietà intellettuale e diritti affini, oggetto del reato di contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni, già previsti dal nostro art. 473 c.p. che a seguito di una novella del 2009, nel suo ultimo comma, rimanda esplicitamente ai regolamenti comunitari e alle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

E giova sottolineare che l'art. 12 della Convenzione rimanda, sul presupposto della commissione di alcuni degli illeciti sopra indicati, alla responsabilità amministrativa delle società e degli enti, mutuandone la struttura e la natura pecuniaria delle sanzioni dal nostro d.lgs. 8 giugno 2001, n. 231.

La parte processuale, d'altra parte, impegna le parti contraenti a facilitare le indagini finalizzate all'acquisizione delle prove dei reati sopra indicati, commessi attraverso l'utilizzo di computer e della rete digitale, con strumenti idonei e condivisi, quali la perquisizione (cioè, la ricerca) e il sequestro di dati informatici memorizzati, e con l'adozione di misure per la rapida preservazione, conservazione e raccolta in tempo reale di dati digitali memorizzati su sistemi informatici, in guisa tale da ovviare alla loro volatilità.
Le Parti vengono inoltre impegnate ad adottare le misure legislative per ordinare a un soggetto sul loro territorio di fornire specifici dati informatici in suo possesso o sotto il suo controllo, memorizzati in un sistema informatico o su un supporto di salvataggio di dati informatici; e a un fornitore di servizi informatici operante sul loro territorio di cedere i dati in suo possesso o sotto il suo controllo relativi agli utenti e a tali servizi; il che costituisce l'archetipo della Risoluzione di prossima efficacia che ha disciplinato l'ordine comunitario di rimozione dal web di contenuti terroristici, di cui al prossimo paragrafo.
Infine si prevede l'estradizione dei responsabili dei crimini previsti e, come norma di chiusura, la trasmissione spontanea di informazioni nei limiti del proprio diritto interno e senza che ne sia stata fatta domanda, ad imitazione di quanto disciplinato dal nostro ordinamento processual-penalistico, sin dal 1988, con l'art. 371 c.p.p. in tema di indagini collegate tra uffici diversi del pubblico ministero.

Ordine di rimozione
Regolamento UE 29 aprile 2021, n. 784

E' evidente a tutti, ormai, quanto sia rilevante Internet in tutto il mondo e quale sia la sua importanza nell'ambito dell'economia globale, la cui digitalizzazione facilita le relazioni tra imprese e cittadini e il dibattito pubblico attraverso la circolazione di informazioni, opinioni e idee, che contribuiscono in modo significativo all'innovazione, alla crescita economica ed alla creazione di posti di lavoro, non solo nell'Unione Europea, ed è dunque ovvio che in questo contesto i servizi dei prestatori di hosting assumano un'importanza fondamentale.

Com'è scritto nel preambolo del Regolamento del Parlamento Europeo e del Consiglio del 29 aprile 2021, n. 784, che disciplina a livello comunitario l'ordine di rimozione di contenuti terroristici postati on line, i prestatori di servizi di hosting possono, tuttavia, essere utilizzati impropriamente da terzi al fine di perpetrare attività illegali, anche da parte di gruppi terroristici e dei loro sostenitori per diffondere contenuti terroristici allo scopo di propagandare il loro messaggio, radicalizzare e reclutare adepti, nonché facilitare e dirigere attività terroristiche.

Orbene, in considerazione dell'importanza del ruolo che svolgono nonché delle capacità e dei mezzi tecnologici associati ai servizi che forniscono, detti prestatori di hosting hanno particolari responsabilità nei confronti della società sotto il profilo della protezione dei dati in loro possesso dall'uso improprio che potrebbero farne i terroristi e del contributo al contrasto della diffusione di contenuti terroristici, per cui il regolamento in esame 'stabilisce regole uniformi per contrastare l'uso improprio dei servizi di hosting ai fini della diffusione al pubblico di contenuti terroristici' (art. 1), tenendo peraltro in massimo conto l'importanza fondamentale della libertà di espressione, in essa compresa quella di ricevere e comunicare informazioni e idee in una società pluralistica, aperta e democratica.

Il regolamento de quo si compone di 24 articoli suddivisi in 6 sezioni aventi ad oggetto:

1. le disposizioni generali che, tra l'altro, illustrano le locuzioni definitorie;
2. le misure volte a contrastare la diffusione di contenuti terroristici on line, comprendente la disciplina dell'ordine di rimozione, anche dal punto di vista procedurale;
3. gli obblighi di trasparenza per i prestatori di servizi di hosting e da parte delle autorità competenti, nonché i mezzi di reclamo da parte dei primi e dei loro clienti;
4. l'individuazione delle autorità competenti ad emanarli e la cooperazione tra queste ed Europol con i prestatori di servizi di hosting;
5. la competenza territoriale in relazione alla sede dello stabilimento principale di quest'ultimo e la sua rappresentanza legale nell'Unione Europea per il caso in cui detta sede si trovasse fuori dai suoi confini;
6. le disposizioni finali comprendenti le sanzioni per il caso di inadempimento e la data di inizio dell'efficacia del regolamento, **fissata al 7 giugno 2022**.

Le disposizioni generali

Esse innanzitutto affermano il principio regolatore secondo cui gli obblighi di diligenza richiesti ai prestatori di servizi di hosting devono essere conformati ai canoni della ragionevolezza e della proporzione, tenendo ben presente – come detto – il fondamentale diritto alla libertà di espressione, di opinione e di circolazione delle idee, nel contempo sollecitando il

loro senso di responsabilità per evitare la torsione dei loro servizi verso approdi illeciti in tema di terrorismo internazionale, con la previsioni di procedure idonee ad assicurare 'la rapida rimozione dei contenuti terroristici' da parte degli esercenti di servizi di hosting.

I Paesi comunitari vengono impegnati a ricomprendere nella categoria dei reati di terrorismo innanzitutto quelli la cui finalità è indicata nel nostro art. 270 sexies c.p., e poi, ex art. 3 della Direttiva UE 2017/541, specificamente quelli – già da tempo inclusi nel nostro ordinamento giuridico – di:

a) attentati alla vita di una persona che possono causarne il decesso;
b) attentati all'integrità fisica di una persona;
c) sequestro di persona o cattura di ostaggi;
d) distruzioni di vasta portata di strutture governative o pubbliche, sistemi di trasporto, infrastrutture, compresi i sistemi informatici, piattaforme fisse situate sulla piattaforma continentale ovvero di luoghi pubblici o di proprietà private che possono mettere in pericolo vite umane o causare perdite economiche considerevoli;
e) sequestro di aeromobili o navi o di altri mezzi di trasporto collettivo di passeggeri o di trasporto di merci;
f) fabbricazione, detenzione, acquisto, trasporto, fornitura o uso di esplosivi o armi da fuoco, comprese armi chimiche, biologiche, radiologiche o nucleari, nonché ricerca e sviluppo di armi chimiche, biologiche, radiologiche o nucleari;
g) rilascio di sostanze pericolose o il cagionare incendi, inondazioni o esplosioni i cui effetti mettano in pericolo vite umane;
h) manomissione o interruzione della fornitura di acqua, energia o altre risorse naturali fondamentali il cui effetto metta in pericolo vite umane;
i) interferenza illecita relativamente ai sistemi.

L'ordine di rimozione

L'ordine di rimozione consiste nel provvedimento dell'Autorità Giudiziaria di ciascun Stato membro dell'Unione, rivolto ad un prestatore di servizi di hosting, di '**rimuovere contenuti terroristici o di disabilitare l'accesso a contenuti terroristici in tutti gli Stati membri**'.
Tranne i casi di assoluta urgenza, debitamente motivati, il contenuto di tale ordine e le sue procedure devono essere indicate al destinatario con un anticipo di almeno **12 ore**, ma una volta ricevuto dal punto di contatto che ogni prestatore di servizi di hosting operante nell'Unione è obbligato a designare (v. art. 15 del Regolamento) – o, come vedremo, il suo rappresentante legale ivi indicato per il caso in cui la propria sede si trovi fuori dai confini europei – questi deve eseguirlo '**il prima possibile e in ogni caso entro un'ora dal ricevimento dell'ordine di rimozione**'.
Il Regolamento disciplina analiticamente i requisiti sostanziali e formali di tale ordine, compendiabili in modelli uniformi e standardizzati, da inviare attraverso sistemi telematici di trasmissione, in quanto tali tracciabili, che valgano a identificarne con certezza e autenticità l'emittente e il destinatario, ad illustrarne la fonte normativa e la motivazione in riferimento ai contenuti terroristici, ad indicarne i mezzi di impugnazione ed i relativi termini quali previsti dall'ordinamento dell'Autorità Giudiziaria emittente e dalle specifiche norme del Regolamento medesimo in favore del prestatore dei servizi di hosting e del fornitore dei contenuti.
Da parte sua il destinatario, una volta eseguito l'ordine nei termini di legge – eventualmente dopo averne richiesto chiarimenti (non pretestuosi) o rettifiche in caso di evidenti vizi di forma – deve darne comunicazione all'Autorità emittente, assicurando l'avvenuta rimozione dei

contenuti terroristici o della disabilitazione dell'accesso ad essi **in tutti gli Stati dell'Unione**, indicandone la data e l'ora, salvo il caso di impossibilità per cause di forza maggiore o di oggettive impossibilità a lui non imputabile, compresi motivi tecnici giustificabili. Ma una volta venuta meno detta impossibilità l'ordine va eseguito al massimo entro un'ora.
Dal punto di vista sostanziale, per contenuti terroristici si intendono le tipologie di materiali che istigano alla commissione di reati terroristici, quali sopra indicati, o che ne siano apologetici; che tendano al proselitismo; che impartiscano istruzioni per la fabbricazione o l'uso di esplosivi ovvero armi da fuoco o comunque letali o nocive; che in ogni caso costituiscano una minaccia di commissione di reati terroristici (art. 2, punto 7, del Regolamento).
Normalmente può accadere che l'ordine di rimozione abbia quale destinatario un prestatore di servizi di hosting con sede in un Paese comunitario diverso da quelle dell'Autorità emittente: in tal caso l'ordine va trasmesso anche all'omologa Autorità del diverso Paese comunitario che di propria iniziativa, entro 72 ore dal ricevimento della copia di detto ordine, può esaminarlo 'per stabilire se esso violi in modo grave o manifesto il presente regolamento o i diritti e le libertà fondamentali garantiti dalla Carta [Europea dei Diritti dell'Uomo]', eventualmente cassandolo e così privandolo di effetti giuridici, con conseguente ripristino di quei contenuti.
In tal caso, però, l'Autorità emittente dovrà esserne preventivamente informata.

Il destinatario dell'ordine di rimozione avente sede principale in un Paese diverso da quello dell'Autorità emittente, o il suo rappresentante legale, al pari del fornitore di contenuti, hanno il diritto di impugnarlo per motivi sostanziali e formali avanti la competente Autorità di residenza, entro **48 ore** dal ricevimento dell'ordine, e questa, nei tempi e con le modalità sopra descritte (**72 ore**), potrà eventualmente cassarlo.

Come detto, il Regolamento in esame richiama al senso di responsabilità sociale il prestatore dei servizi di hosting sul grave versante dei reati terroristici, impegnandolo – soprattutto ove esposto a contenuti terroristici, quali sopra indicati – ad adottare misure specifiche per evitare che essi possano essere divulgati al vasto pubblico della rete e, per quanto il Regolamento gli assicuri ampia libertà di scelta in ordine alle cautele da adottare, l'art. 5.2 gliene suggerisce alcune incentrate prevalentemente sull'adeguatezza delle risorse umane e tecnologiche e sulla facilità di recepimento di eventuali segnalazioni da parte degli utenti.
Va da sé, però, che la valutazione dell'esposizione di un prestatore di servizi di hosting a contenuti terroristici non appartiene a lui in via esclusiva; al contrario essa è oggettivamente configurata dal Regolamento che la riconosce nel caso in cui quello abbia ricevuto due o più ordini di rimozione nei 12 mesi precedenti.
In tal caso il prestatore di servizi di hosting deve riferire all'Autorità dello Stato di propria residenza o di residenza del proprio rappresentante legale, entro **3 mesi** dalla notifica della realizzazione dell'anzidetto presupposto oggettivo e successivamente su base annuale, quali misure specifiche abbia adottato per rendersi impermeabile a siffatti contenuti, dalla cui efficacia dipenderà la cessazione dell'anzidetto obbligo di comunicazione.

E' di fondamentale importanza sottolineare, peraltro, che la rimozione dei contenuti terroristici non implica affatto la loro distruzione. Al contrario essi vanno conservati nella loro integrità ed in sicurezza a cura del prestatore di servizi di hosting, sia per consentire le eventuali impugnazioni cui ha diritto, sia soprattutto a salvaguardia delle indagini e delle acquisizioni probatorie rispetto alle quali detti dati abbiano rilevanza (v. infra, in tema di commento all'art. 254 bis c.p.p.).

Salvaguardie e rendicontazione

Il Regolamento disciplina dettagliatamente gli obblighi di trasparenza dei prestatori di servizi di hosting e delle Autorità competenti, nei reciproci confronti e per il rispetto dovuto ai fondamentali diritti di libertà delle imprese e degli utenti, ed a salvaguardia di questi delinea mezzi di reclamo innervati dalla possibilità di un doppio reclamo, alla competente Autorità dello Stato emittente dell'ordine di rimozione (v. infra, in tema di commento all'art. 254 bis c.p.p., per quanto concerne il nostro Paese) ed a quella dell'eventuale diverso Stato ove il destinatario dell'ordine ha la propria sede principale o, se questa si trova al di fuori dei confini dell'Unione, ove si trova il proprio rappresentante legale obbligatoriamente designato con le modalità e nei termini, già citati, di cui all'art. 4.

Ai sensi dell'art. 3.9 del Regolamento l'ordine di rimozione diviene definitivo 'alla scadenza del termine per il ricorso o quando non è stato presentato alcun ricorso ai sensi del diritto nazionale o se è stato confermato in esito al ricorso'.

I prestatori di servizi di hosting – detta il Regolamento (art. 7) – 'definiscono chiaramente nelle loro condizioni contrattuali la loro politica volta a contrastare la diffusione di contenuti terroristici …' e, ove abbiano dovuto adottare misure in concreto contro detta diffusione o siano stati obbligati a farlo per ordine dell'Autorità, sono tenuti alla pubblicazione di report annuali, entro il 1° marzo dell'anno successivo, per dar conto di quanto accaduto e di quanto intrapreso per ripristinare la propria impermeabilità al ricevimento e postazione di contenuti terroristici.

D'altra parte, anche le Autorità competenti sono tenute alla pubblicazione di relazioni annuali 'sulla trasparenza relative alle loro attività a norma del presente regolamento' il cui contenuto è chiaramente dettagliato nel relativo art. 8.

Come si è già detto, al pari del prestatore di servizi di hosting, anche il fornitore di contenuti, ha il medesimo diritto di impugnazione quando essi siano stati rimossi o l'accesso ad essi sia stato disabilitato a seguito di un ordine di rimozione; tuttavia gli viene riconosciuta anche una tutela anticipata attraverso un reclamo al prestatore di servizi di hosting allorché questi abbia proceduto alla rimozione o all'oscuramento di quei contenuti propria sponte avendone riconosciuto contenuti terroristici secondo i propri criteri pubblicizzati erga omnes. In tal caso il prestatore di servizi di hosting ha l'obbligo di valutare le ragioni del reclamante e di comunicargliele entro due settimane.

Ovviamente in caso di accoglimento del reclamo i contenuti in oggetto devono essere reintegrati.

Le autorità competenti ad emanarli e la cooperazione tra queste ed Europol con i prestatori di servizi di hosting

Il diritto comunitario esige un'effettiva cooperazione tra le diverse Autorità degli Stati membri, per superare i confini, non tanto territoriali quanto ordinamentali, dai quali sono separate, confini che invece non appartengono ai fruitori del web, sia nella loro veste di prestatori di servizi di hosting che di fornitori di contenuti o di utenti.

Dunque, anche per la materia in esame, vengono dettate norme affinché ciascuno Stato designi le Autorità competenti all'emissione dell'ordine di rimozione e al suo eventuale riesame; alla sorveglianza dei siti dei prestatori di servizi in ordine alle misure predisposte per evitare che siano postati contenuti terroristici e per l'irrogazione delle sanzioni in caso di inadempimento (v. infra) e affinché, nell'ambito di dette Autorità, venga pubblicamente designato o istituito **entro il 7 giugno 2022 un punto di contatto** 'per trattare le richieste di chiarimenti e di riscontro in relazione agli ordini di rimozione emessi da tale Autorità competente', che la Commissione compendierà in un apposito pubblico registro (art. 12).

Inoltre, il Regolamento prevede espressamente che l'effettività e la fluidità di detta cooperazione venga assicurata da Europol, non solo per evitare, in tema di ordini di rimozione, 'una duplicazione di sforzi … e qualsiasi interferenza con indagini in corso nei diversi Stati membri', ma anche, e direi soprattutto, per assicurare l'adozione di effettive ed urgenti misure di sicurezza laddove determinati contenuti terroristici – che in primis dovrebbero essere rilevati e comunicati a Europol dai prestatori di servizi di hosting, attraverso il punto di contatto alla cui designazione anch'essi, come detto, sono tenuti – dovessero comportare la minaccia di attentati alla vita di singole persone o all'integrità di uno Stato (v. art. 14.5).
Viene infine raccomandato l'invio di copia degli ordini di rimozione ad Europol, anche al fine 'di presentare una relazione annuale comprensiva di un'analisi dei tipi di contenuti terroristici oggetto di ordini di rimozione o di disabilitazione dell'accesso'.
Infatti, le relazioni degli Stati membri e di Europol in materia si sono dimostrate uno strumento rapido ed efficace anche per sensibilizzare i prestatori di servizi di hosting in merito a contenuti specifici disponibili attraverso i loro servizi e per consentire loro di intervenire rapidamente. Tali segnalazioni rappresentano altresì un meccanismo inteso ad allertare i prestatori di servizi di hosting in merito alle informazioni che potrebbero essere considerate quali contenuti terroristici, affinché possano – su base volontaria – esaminare la loro compatibilità con le proprie condizioni contrattuali così da poter provvedere, in caso contrario, alla loro rimozione.

La competenza territoriale e la rappresentanza dei prestatori di servizi di hosting

La competenza territoriale in relazione alla sorveglianza sui siti dei prestatori di servizi di hosting (art. 5), al loro monitoraggio in riferimento alle azioni intraprese a norma del Regolamento, che deve costituire l'oggetto di una relazione annuale alla Commissione entro il 31 marzo di ciascun anno (art. 21) e all'irrogazione delle sanzioni (art. 18), spetta allo Stato membro in cui ciascuno di essi ha lo stabilimento principale e, se questo è posto fuori dai confini dell'Unione, allo Stato membro in cui il suo rappresentante legale – che può avere una responsabilità concorrente con quella dei prestatori di servizi di hosting, 'fatte salve le responsabilità e le azioni legali dei prestatori di servizi di hosting' (v. art. 17.3) – risiede.

Infine, è importante sottolineare che 'laddove il prestatore di servizi di hosting che non ha il suo stabilimento principale nell'Unione ometta di designare un rappresentante legale, tutti gli Stati membri sono competenti' (art. 16.2).

Le diposizioni finali

La parte saliente delle disposizioni finali è costituito dal sistema sanzionatorio, che è di natura pecuniaria (salvo il caso di concorso nei reati di terrorismo), l'individuazione del quale è demandato a ciascun Stato membro nel quadro di una loro effettività, proporzionalità e dissuasività, in ragione della natura, della gravità e della durata della violazione; del suo carattere doloso e colposo, la cui graduazione va commisurata alle misure tecniche e organizzative adottate dal prestatore di servizi di hosting per conformarsi al Regolamento; della sua solidità finanziaria e della sua organizzazione; della reiterazione delle violazioni.

L'art. 18.3 del Regolamento prescrive che la sistematica e persistente inosservanza dei suoi obblighi in materia 'sia passibile di sanzioni pecuniarie sino al 4% del fatturato mondiale del prestatore di servizi di hosting del precedente esercizio finanziario'.

Il Regolamento in esame, di data 29 aprile 2021, è entrato in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'Unione Europea, ma la sua efficacia è stata posposta, come detto, al **7 giugno 2022**.

Uno sguardo alle norme dell'ordinamento giuridico italiano poste a presidio del Regolamento

La materia che ci occupa impatta frontalmente le funzioni e l'attività del pubblico ministero – Autorità di riferimento della disciplina dell'ordine di rimozione – essendo evidente che esso, sostanzialmente parificabile a un sequestro, costituirà uno dei mezzi di ricerca della prova del quale il magistrato si avvarrà, secondo le regole del nostro codice di rito e nel rispetto delle garanzie difensive, nell'ambito delle indagini preliminari in tema di reati di eversione e terrorismo internazionale.

Osservando il nostro ordinamento processual-penalisico dal punto di vista di quello sovranazionale, non si può non riconoscere che esso comprende norme sostanziali e processuali che hanno anticipato le esigenze di prevenzione speciale e repressione oggetto delle Convenzioni internazionali e del Regolamento che abbiamo preso in esame, innanzitutto con la modifica (nel 2001) dell'art. 270 bis c.p., in tema di associazioni con finalità di eversione dell'ordine democratico e terrorismo anche internazionale, e con l'introduzione (nel 2005) dell'art. 270 sexies c.p. che ne definisce il concetto, **senza necessità – io credo – di ulteriori integrazioni poiché, per principio consolidato, l'**occasio legis **è irrilevante tutte le volte che la norma possa ritenersi dotata di forza espansiva tale da ricomprendere ipotesi non contemplate all'atto della sua emanazione.**

E lo stesso vale per l'ambito processuale ove già esiste una disposizione posta a presidio dell'attuazione dell'ordine di rimozione, costituita dall'art. 254 bis c.p.p., risalente al 2008, a tenore del quale 'l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali'.

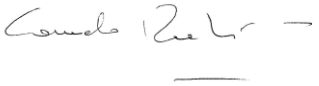
Esattamente come dispone il Regolamento in relazione ai contenuti terroristici in possesso di un prestatore di servizi di hosting, che devono essere conservati nella loro integrità sia perché l'accoglimento delle eventuali impugnazioni potrebbe determinare l'inefficacia dell'ordine di rimozione, sia e soprattutto perché detti contenuti potrebbero avere un'importante rilevanza ai fini investigativi.

Infine, giova rammentare che il mezzo di impugnazione previsto per il caso di specie dal nostro ordinamento giuridico è quello di cui agli artt. 257 e 324 c.p.p., a tenore dei quali l'imputato o la persona sottoposta alle indagini, la persona alla quale le cose sono state sequestrate e quella che avrebbe diritto alla loro restituzione possono proporre richiesta di riesame del decreto di sequestro innanzi al Tribunale distrettuale territorialmente competente, anche nel merito, entro 10 giorni dalla data di esecuzione del provvedimento che lo ha disposto o dalla diversa data in cui l'interessato ne ha avuto conoscenza, la cui decisione, da rendere pubblica nel termine di

10 giorni dalla ricezione degli atti, potrebbe determinare la revoca del provvedimenti di sequestro (rectius: dell'ordine di rimozione).
A propria volta – con un sistema binario, come abbiamo visto – la disciplina propria di questo ne prevede la concorrente impugnazione con la possibilità di un reclamo anche alla competente Autorità dello Stato emittente l'ordine di rimozione ed a quella dell'eventuale diverso Stato ove il destinatario dell'ordine ha la propria sede principale o, se questa si trova al di fuori dei confini dell'Unione, ove si trova il proprio rappresentante legale designato con le modalità e nei termini, già citati, di cui all'art. 4 del Regolamento medesimo.

Rimini, 2 marzo 2022.

Carmelo Ruberto



15