NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

Il *Position Paper* dell'Italia sull'applicabilità del diritto internazionale nel cyberspazio, la sentenza del Tribunale UE nel caso Google Shopping e l'Oxford Statement sulla regolamentazione internazionale degli attacchi *ransomware*[*]

di Flavia Zorzi Giustiniani[**]

Il **4 novembre** scorso l'Italia ha pubblicato la sua posizione sul diritto internazionale e il cyberspazio[1]. Il documento é stato realizzato dal Ministero degli Affari Esteri in collaborazione con la Presidenza del Consiglio dei Ministri e il Ministero della Difesa. Così facendo il nostro Paese si colloca tra gli Stati che, dando seguito alle raccomandazioni espresse in tal senso dall'ONU, ha espresso la sua visione sul tema[2].

Nel suddetto documento l'Italia intende presentare la sua opinione su molteplici aspetti riguardanti l'applicazione del diritto internazionale nel cyberspazio. Il *Paper* esordisce facendo proprie le conclusioni raggiunte dal Gruppo di esperti governativi delle Nazioni Unite (GGE) e dal Gruppo di lavoro aperto (OEWG) sulla sicurezza informatica, secondo cui "il diritto internazionale e in particolare la Carta delle Nazioni Unite nella sua interezza, è applicabile ed è essenziale per mantenere la pace e la stabilità e promuovere un ambiente ICT aperto, sicuro, stabile, accessibile e pacifico"[3]. Il documento evidenzia poi come le nozioni di pace e di sicurezza internazionale trascendano la mera dimensione militare, con la conseguenza che le norme di diritto internazionale applicabili nel cyberspazio non sono soltanto quelle relative al divieto dell'uso della forza nelle relazioni internazionali. Quanto poi al diritto internazionale umanitario (DIU), ovvero lo *jus in bello*, l'Italia lo considera restrittivo in quanto mira a limitare la condotta dei belligeranti che colpiscono civili e obiettivi civili in un conflitto armato. Pertanto, il riconoscimento della sua applicabilità al cyberspazio non equivale a incoraggiare o consentire

[*]Contributo sottoposto a *peer review*.

[**] Professoressa associata di diritto dell'Unione europea, Link Campus University

[1]https://www.esteri.it/MAE/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

[2] Sull'analogo *Position Paper* della Germania sia permesso il rinvio alla rassegna disponibile al link https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2021/06/ZorziRassegnaNomos-Maggio-21.pdf.

[3] Cfr. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, 24 giugno 2013, par. 20; *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 luglio 2015, par. 24; *Open-ended working group on developments in the field of information and telecommunications technologies in the context of international security*; UN Doc. A/75/816, 18 marzo 2021, par. 7.

ISSN 2279-7238

l'uso della forza come strumento di aggressione e/o come mezzo per la risoluzione delle controversie internazionali.

Con riguardo alla tutela della sovranità, l'Italia attribuisce un'importanza fondamentale al principio di sovranità nel cyberspazio e ritiene che nel mondo digitale si applichino sia gli aspetti interni che gli aspetti esterni della sovranità. Al riguardo, il documento fa riferimento in particolare ad azioni di influenza come la manipolazione delle elezioni o la manomissione delle infrastrutture sanitarie[4].

Il documento dedica poi un'intera sezione al diritto della responsabilità degli Stati nel cyberspazio[5]. Qui si affronta in primis la questione – spinosa – dell'attribuzione degli attacchi informatici. Secondo l'Italia l'attribuzione, come pure la decisione di renderla pubblica, é una prerogativa nazionale e come tale dovrebbe fondarsi su prove sufficientemente affidabili quanto alla fonte delle attività in questione e all'identità dei responsabili. L'Italia assegna una particolare importanza, al riguardo, alla trasparenza, pur consapevole che la stessa non sia oggetto di un preciso obbligo di diritto internazionale. Il Paese concorda poi con l'opinione che la materia é governata dalle norme consuetudinarie sulla responsabilità degli Stati come codificate nel relativo Progetto di articoli della Commissione del diritto internazionale delle Nazioni Unite del 2001.

In tema di *due diligence*, il documento esordisce affermando che i relativi obblighi si applicano nel cyberspazio, per cui gli Stati, come affermato dalla Corte Internazionale di Giustizia nel caso di scuola Corfu Channel del 1949, non devono permettere che il loro territorio sia utilizzato per atti contrari al diritto di altri Stati, né tantomeno che la loro infrastruttura ICT (*Information and Communication Technology*) sia impiegata per la condotta di attività cibernetiche illecite da parte di attori statali o non statali[6]. Viene tuttavia ricordato che il dovere di diligenza è un obbligo di condotta e che pertanto uno Stato, fintantoché compie tutti gli sforzi possibili, non può essere ritenuto responsabile se alla fine non è in grado di prevenire, mitigare o porre termine ad attività informatiche illecite avviate o in transito attraverso il suo territorio.

Con riguardo alle contromisure[7], l'Italia ritiene che uno Stato ha il diritto di ricorrere a siffatte misure in risposta ad operazioni cibernetiche che costituiscono un illecito internazionale al di sotto della soglia del conflitto armato. Il *Paper* sottolinea tuttavia che nella specie l'adozione di contromisure potrebbe rivelarsi problematica, tra l'altro, per la difficoltà di individuare il responsabile degli attacchi. Inoltre, adempimenti preventivi quali la previa notifica potrebbero risultare inapplicabili laddove una reazione immediata fosse necessaria per far valere i diritti dello Stato leso e impedire danni ulteriori. In ogni caso le contromisure devono essere proporzionate al danno patito e non possono consistere nella minaccia o nell'uso della forza.

Le operazioni cibernetiche sono soggetto al generale divieto di uso della forza nella relazioni internazionali di cui all'art. 2 par. 4 della Carta delle Nazioni Unite[8]. L'Italia considera un'aggressione cibernetica equivalente ad un attacco armato, che in quanto tale giustifica una reazione in legittima difesa ex art. 51 della Carta ONU, solo allorché le sue dimensioni e i suoi

[4] Cfr. la parte I del documento.
[5] Cfr. la parte II del documento.
[6] Cfr. la sezione II b).
[7] Cfr. la sezione II c).
[8] Cfr. la sezione III.

effetti sono comparabili, con conseguenti danni a proprietà, lesioni a persone o perdita di vite umane. Sono specificamente incluse quelle operazioni che, come il recente attacco informatico alla Regione Lazio[9], possono determinare l'interruzione di servizi essenziali pur non causando un danno fisico. La decisione su quando un'operazione cibernetica che equivale a un attacco armato conduca all'autodifesa collettiva sarà presa caso per caso.

Con specifico riguardo all'uso della forza nel cyberspazio, il *Paper* riconosce poi l'applicabilità dello *jus in bello* – il cosiddetto diritto internazionale umanitario (DIU) – e, nei conflitti armati internazionali, del diritto della neutralità. Ne consegue, tra l'altro, che uno Stato non potrebbe fornire o negare l'accesso alla sua infrastruttura ICT a una sola parte.

L'Italia ritiene che il diritto internazionale dei diritti umani si applichi nel cyberspazio allo stesso modo in cui si applica nel mondo reale[10]. In particolare, ogni Stato deve tutelare siffatti diritti, a cominciare dalla libertà di opinione e di espressione, il diritto all'accesso alle informazioni e il diritto alla privacy. Al riguardo l'Italia riconosce poi la responsabilità (*accountability*) anche del settore privato, conformemente ai *Guiding Principles on Business and Human Rights* delle Nazioni Unite del 2011.

La cooperazione è uno strumento essenziale nel dominio cibernetico[11]. Non a caso, nel documento si afferma che l'Italia promuove la cooperazione internazionale per migliorare la resilienza cibernetica e la stabilità internazionale, facendo leva anzitutto sulle misure di rafforzamento della fiducia tra Paesi e sulla condivisione delle informazioni, nonché assegnando un particolare rilievo alla cooperazione a livello regionale e bilaterale. Considerato il ruolo di primo piano degli stakeholders privati nel cyberspazio, l'Italia considera essenziale la cooperazione pubblico-privato, al fine precipuo di garantire la sicurezza informatica e un efficace rafforzamento delle capacità (*capacity-building*)[12].

Il **10 novembre** scorso il Tribunale dell'Unione europea si è pronunciato nella Causa T-612/17, *Google LLC, in precedenza Google Inc. e Alphabet, Inc. contro Commissione europea*, sul ricorso volto all'annullamento della decisione con cui la Commissione aveva sanzionato *Google LLC* e la sua società madre *Alphabet Inc.* (di seguito "Google") per aver violato l'art. 102 del Trattato sul Funzionamento dell'Unione Europea (TFUE) e l'art. 54 dell'Accordo sullo Spazio Economico Europeo (Accordo SEE)[13]. Con tale decisione Google era stato condannato al pagamento di 2,42 miliardi di euro per aver trattato più favorevolmente, sia in termini di posizionamento sia di visualizzazione nelle sue pagine generali dei risultati di ricerca, il proprio servizio di comparazione degli acquisti rispetto ai servizi dello stesso genere offerti da operatori concorrenti. La sentenza del Tribunale, che qui si riassume per sommi capi, è di indubbio rilievo pur non brillando per chiarezza e sinteticità[14].

[9] Tale attacco é avvenuto il 30 luglio 2021 (v. https://www.regione.lazio.it/notizie/attacco-hacker).
[10] Cfr. la sezione IV.
[11] Cfr. la sezione VI.
[12] Cfr. la sezione V.
[13] Si veda la decisione della Commissione C(2017) 4444 final del 27 giugno 2017.
[14] "We would not expect the judgments to have the elegance of Justice Cardozo, the verve of Lord Denning or the lucidity of

Il Tribunale ha anzitutto confermato che la condotta tenuta da Google debba qualificarsi come anticoncorrenziale giacché il ricorrente ha reso praticamente impossibile la concorrenza nel mercato dei servizi di comparazione. Per giungere a tale conclusione i giudici europei hanno tenuto conto del traffico di dati generato da Google, del comportamento degli utenti i quali si soffermano in genere sui primi risultati forniti dal flusso di dati che è stato deviato dai servizi di comparazione concorrenti, e last but not least della "vocazione universale" di Google[15]. A quest'ultimo riguardo il Tribunale ha rimarcato come la promozione di un solo tipo di risultati specializzati – i propri – costituisce una chiara "anormalità" per un motore di ricerca programmato per indicizzare i risultati delle ricerche di ogni genere, e contraddice la natura stessa di Google come infrastruttura aperta. Il Tribunale UE ha poi confermato l'approccio della Commissione secondo il quale Google deve essere considerato alla stregua di una infrastruttura essenziale (*essential facility*) fintantoché nel mercato non saranno disponibili delle infrastrutture alternative. Tuttavia ha rigettato la tesi di Google volta a giustificare la sua condotta sulla base della giurisprudenza *Bronner*[16]. Il precedente Bronner, risalente al 1998, concerne un "rifiuto di fornire un servizio" e precisa quali condizioni debbano essere soddisfatte perché una condotta possa definirsi abusiva. Siffatta giurisprudenza non è stata ritenuta rilevante perché nel caso di specie l'abusività, come precisato dal Tribunale, non riguarda un rifiuto di fornitura di servizi bensì il carattere discriminatorio della preferenza assegnata da Google ai propri servizi di comparazione[17].

Il Tribunale UE ha poi confermato gli effetti negativi per la concorrenza prodotti dalla condotta in esame. Giova ricordare al riguardo che la fattispecie di abuso di posizione dominante ai sensi dell'art. 102 TFUE richiede la dimostrazione della semplice idoneità della condotta de qua a limitare la concorrenza. Secondo il Tribunale, nel caso di specie la Commissione nella sua Decisione aveva sufficientemente dimostrato gli effetti anticoncorrenziali della condotta di Google. In particolare la Commissione aveva dimostrato che il traffico di dati dirottato dalle pagine dei risultati generali di Google verso Google Shopping aveva una entità notevole e non poteva essere efficacemente sostituito da altre fonti di traffico quali le pubblicità (*AdWords*) o le applicazioni di comparazione, né tantomeno dalle piattaforme commerciali (una per tutte Amazon), che fanno parte di un mercato diverso. Pur confermando in larga parte l'analisi della Commissione, il Tribunale ha tuttavia statuito che la stessa non aveva fornito evidenza del fatto che la condotta di Google abbia avuto effetti sul mercato dei servizi di ricerca generica[18].

Al fine di giustificare la propria condotta da un punto di vista oggettivo, Google aveva asserito anzitutto che l'esibizione dei prodotti raggruppati (*Product Universals)* e degli annunci pubblicitari su tali prodotti (*Shopping Units) si fondasse su presunte caratteristiche pro-concorrenza della condotta, data la sua capacità di migliorare la qualità del servizio. Secondo Google vi erano poi dei vincoli tecnici che impedivano di*

Lord Hoffmann. But producing something more accessible and clear has to be possible" (cfr. G. Monti, The General Court's Google Shopping Judgment and the scope of Article 102 TFEU, 14 novembre 2021, p. 15, disponibile al link https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3963336).

[15] Cfr. il par. 176 della sentenza.

[16] Cfr. la sentenza della Corte di Giustizia europea resa nella causa C-7/97 il 26 novembre 1998.

[17] Cfr. i par. 212-249 della sentenza.

[18] Cfr. i par. 456-459 della sentenza.

garantire lo stesso trattamento ai servizi dei terzi. Il Tribunale ha respinto dette argomentazioni sottolineando che il trattamento discriminatorio non poteva giustificarsi in virtù di presunti caratteri pro-concorrenziali della condotta quali la capacità di migliorare la qualità del servizio. Google inoltre non avrebbe fornito prove sufficienti a dimostrare che la sua condotta avesse determinato incrementi di efficienza che controbilanciassero gli effetti anticoncorrenziali[19]. Con riguardo ai vincoli tecnici, egualmente secondo il Tribunale Google non ha dimostrato che gli stessi avrebbero impedito di utilizzare dei processi e metodi ai risultati di ricerca atti ad assicurare un trattamento non discriminatorio, in termini di posizionamento ed esibizione, dei servizi di comparazione degli acquisti di Google e dei terzi.[20]

Il Tribunale ha infine affermato la legittimità sia dell'irrogazione della sanzione che della relativa quantificazione effettuata dalla Commissione. Circa il primo aspetto[21], il Tribunale ha ritenuto che Google abbia tenuto una condotta intenzionalmente anticoncorrenziale. La Commissione, inoltre, aveva piena discrezionalità nel decidere se seguire una procedura standard o una procedura con impegni, come pure di passare dall'una all'altra in corso d'opera. Il fatto poi che il ricorrente avesse offerto rimedi durante la procedura non rendeva illegittima l'irrogazione della sanzione. Per quanto riguarda l'ammontare della sanzione, il Tribunale ha confermato la legittimità di quanto deciso dalla Commissione, rimarcando la particolare gravità della violazione, dovuta tra l'altro all'intenzionalità della condotta tenuta da Google[22].

Un altro sviluppo degno di nota è costituito dall'*Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations*, pubblicato il **4 ottobre**[23]. L'intento del documento, come pure degli *Statements* che l'hanno preceduto, è quello di individuare regole e principi di diritto internazionale applicabili in subiecta materia e sollecitare tutti gli Stati e gli altri attori internazionali a conformarvisi[24]. Come il precedente, quest'ultimo Statement concerne una tipologia specifica di operazioni cibernetiche.

Il termine *ransomware*, derivante dalla crasi di *ransom* (riscatto) e *malware* (programma malevolo), fa riferimento ad un virus attraverso il quale viene realizzata un'estorsione informatica. Il recente proliferare degli attacchi *ransomware* anche contro infrastrutture essenziali degli Stati, uno fra tutti l'attacco all'azienda USA specializzata in oleodotti Colonial Pipeline del maggio 2021, non fa che confermare la necessità di un chiarimento del quadro giuridico applicabile a livello internazionale.

Lo *Statement*, partendo dalla premessa che le condotte realizzate attraverso le tecnologie dell'informazione e delle comunicazioni sono disciplinate dal diritto internazionale, identifica una serie di obblighi posti dal diritto internazionale sugli Stati. Questi ultimi devono anzitutto astenersi dal condurre, dirigere, autorizzare o aiutare e assistere operazioni di *ransomware* che

[19] Cfr. il par. 572 della sentenza.
[20] Cfr. i par. 576, 578-9 della sentenza.
[21] Cfr. i par. 605-639 della sentenza.
[22] V. in particolare i par. 680 e 704 della sentenza.
[23] Il testo é disponibile al seguente link: https://www.ejiltalk.org/the-oxford-process-on-international-law-protections-in-cyberspace-the-regulation-of-ransomware-operations/.
[24] Sul terzo e quarto Statement sia permesso rinviare alle precedenti rassegne (qui https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2021/01/Cronache-dal-cyberspazio-3-2020.pdf e qui https://www.nomos-leattualitaneldiritto.it/nomos/cronache-dal-cyber-spazio/la-normalizzazione-della-sorveglianza-di-massa/).

violano i principi di sovranità e non ingerenza negli affari interni di uno Stato o che costituiscono una minaccia o un uso proibito della forza ai sensi della Carta ONU. Più in particolare, gli Stati devono astenersi da quelle operazioni che mirano o comportano un'interruzione dei sistemi elettorali, dell'assistenza sanitaria, delle reti elettriche, dei sistemi di distribuzione dell'acqua e delle centrali nucleari[25]. Egualmente gli Stati devono astenersi dal condurre, dirigere, autorizzare o aiutare e assistere operazioni di *ransomware* che comportino violazioni dei diritti umani delle persone che rientrano nella loro giurisdizione, come il diritto alla vita, alla salute, alla vita privata, all'istruzione, alla proprietà, alla libertà di pensiero e di opinione, alla libertà di espressione, compresa la libertà di cercare, ricevere e diffondere informazioni e idee di ogni tipo[26].

Gli Stati non devono poi permettere, allorquando ne hanno o dovrebbero averne conoscenza, che il loro territorio o le infrastrutture poste sotto la loro giurisdizione o controllo siano utilizzate per operazioni *ransomware* contrarie ai diritti di altri Stati[27]. A tal fine gli Stati devono adottare misure appropriate quali lo svolgimento di indagini, l'adozione di misure legali e tecniche, nonché la cooperazione con altri Stati. Tali misure devono essere comunque conformi al diritto internazionale applicabile, compreso il diritto internazionale dei diritti umani[28].

Gli Stati devono altresì prendere misure per proteggere i diritti umani delle persone che si trovano nella loro giurisdizione da operazioni *ransomware*, ad esempio vietandole per legge, indagando e punendo i responsabili, nonché prevenendo e annullando nella misura del possibile il pagamento di riscatti. Laddove tali misure di protezione interferiscano con altri diritti, le stesse devono essere conformi ai requisiti legali applicabili quali scopo legittimo, legalità, necessità, proporzionalità e non discriminazione[29].

Lo *Statement* conferma poi l'applicabilità del diritto internazionale umanitario allorché il *ransomware* sia utilizzato durante un conflitto armato[30]. Infine, stabilisce che l'applicazione delle regole in esso enunciate non pregiudica l'applicazione di qualsiasi altra norma internazionale che protegga da *ransomware* e attività connesse[31].

[25] Cfr. il punto 2 dello *Statement*.
[26] Cfr. il punto 3 dello *Statement*.
[27] Cfr. il punto 4 a) dello *Statement*.
[28] Cfr. il punto 4 b) dello *Statement*.
[29] Cfr. il punto 5 dello *Statement*.
[30] Cfr. il punto 6 dello *Statement*.
[31] Cfr. il punto 8 dello *Statement*.