DIDATTICA

1

Brixia University Press
Piazza del Mercato 15, 25121 Brescia
Tel. (+39) 030 29881
www.unibs.it

ISBN
ISBN online

Prima edizione: xxxxxx 2022

Il contrasto al terrorismo negli ordinamenti democratici

a cura di
Matteo Frau ed Elisa Tira

Brixia University Press

Indice

PARTE III

ULTERIORI SFIDE DEL COSTITUZIONALISMO NEL CONTRASTO AL FENOMENO TERRORISTICO

2. La *cybersecurity*

Alessandro Lauro

Sommario: 1. La ricerca della sicurezza nel ciberspazio: polizia cibernetica e *cyberwarfare.* – 2. La guerra cibernetica nell'ordinamento internazionale. – 3. L'evoluzione europea della disciplina. – 4. Sicurezza cibernetica e tutela dei "nuovi" diritti digitali nel costituzionalismo multilivello. – 4.1. La normativa europea sui dati personali e la giurisprudenza della Corte di Giustizia. – 4.2. La cibersicurezza e la Convenzione europea dei diritti dell'Uomo. – 5. Lotta al terrorismo e polizia cibernetica: il caso del delitto di consultazione di siti islamisti in Francia. – 6. *Cybersecurity* e organizzazione dei poteri. – 6.1. Il caso italiano: il Presidente del Consiglio al vertice.

1. *La ricerca della sicurezza nel ciberspazio: polizia cibernetica e* cyberwarfare

La tutela dell'integrità fisica delle persone e delle cose è attività che storicamente risiede in capo ai pubblici poteri. Agli albori del costituzionalismo, l'art. XV della Dichiarazione francese dei diritti dell'uomo e del cittadino del 1789 stabiliva la necessità di creare una "forza pubblica" per la garanzia dei diritti fondamentali (all'epoca: la libertà, la proprietà, la sicurezza e la resistenza all'oppressione, come sancisce l'art. II della stessa Dichiarazione).

La tutela della sicurezza da parte dello Stato si è sempre esercitata su due versanti: la *sicurezza interna*, affidata alle forze di polizia e volta a prevenire e a reprimere sul territorio statale i crimini e le minacce all'ordine pubblico, e la *sicurezza esterna* – che assume il termine di *difesa* allorché siano previsti interventi militari – diretta a proteggere la comunità statale da aggressioni provenienti dal di fuori dei confini nazionali e, in particolare, da altri Stati o organizzazioni.

Persino nel mondo fisico questa distinzione è andata via via assottigliandosi, ad esempio con la dottrina della c.d. *guerra preventiva*, che ammette l'uso della forza da parte di uno Stato all'estero al fine di proteggere i suoi interessi nazionali da possibili attacchi (v. *supra*, parte II).

Con l'evoluzione delle nuove tecnologie e la creazione della rete Internet, si è posta la necessità di riprodurre queste attività di sicurezza nel mondo virtuale, mondo nel quale le minacce a persone e cose non sono meno concrete che in quello fisico. Ciò, però, con una differenza di non poco rilievo: nel ciberspazio è difficile individuare dei confini. Lo Stato ha difficoltà a comprendere se le minacce provengono dall'interno o dall'esterno della sua giurisdizione.

È per questa ragione che – nel momento in cui parliamo di *cybersecurity* o cibersicurezza – è opportuno ricomprendere all'interno del concetto tanto le attività di vera e propria

belligeranza cibernetica (*cyberwarfare*) quanto le operazioni di polizia cibernetica che lo Stato mette all'opera per tutelarsi dall'interno. La sostanziale impossibilità di individuare chiaramente l'origine territoriale delle minacce e di differenziare le contromisure in base a questa impone di conseguenza l'adozione di accorgimenti generali per proteggere gli interessi dello Stato e dei suoi cittadini nel loro complesso.

2. *La guerra cibernetica nell'ordinamento internazionale*

Nel diritto internazionale, il fenomeno della guerra cibernetica non è regolato né da norme di *jus cogens*, né da trattati o convenzioni internazionali (c.d. *hard law*).

L'unico documento nella materia è un atto di *soft law* adottato da un organismo di studi strategici, il centro NATO per la ciberdifesa. Si tratta del c.d. "Manuale di Tallinn" – dal nome della città dove tale centro ha sede –, il quale si occupa di attualizzare alcuni temi specifici del diritto bellico rispetto al mutato quadro tecnologico.

Il Manuale, la cui ultima edizione risale al 2017, nasce dal bisogno di riorganizzare e razionalizzare gli indirizzi e le prassi sorti all'interno di alcuni Paesi della NATO[1].

Il tema della cibersicurezza presenta tuttavia rilevanti difficoltà rispetto al suo inquadramento da parte dello *jus gentium*, prima fra tutte la possibilità di riferire gli atti ostili di natura cibernetica (come hackeraggi; attacchi all'integrità delle reti; interruzione di servizi informatici) ad organi dello Stato per farne discendere la responsabilità di questo. Tali difficoltà di natura pratica rendono conseguentemente complesso uno sviluppo del diritto internazionale, di natura pattizia o consuetudinaria, sul punto.

È per questa ragione che è invece più opportuno soffermarsi sugli ordinamenti c.d. "regionali" che hanno adottato atti di natura vincolante nella materia, come avvenuto nel caso dell'Unione europea.

3. *L'evoluzione europea della disciplina*

L'attenzione europea al tema della sicurezza informatica si sviluppa sostanzialmente in due macrofasi.

Una prima, agli inizi degli anni Duemila, consegue alla più estesa disciplina del mercato unico digitale.

In questa fase vengono adottate, fra le altre, le direttive 2002/21/CE, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica, e 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata. Nel giugno 2004 il Consiglio europeo chiede peraltro la preparazione di una Strategia globale per le infrastrutture critiche, culminata nella direttiva 2008/114/CE. Sempre in questi anni, con

[1] Fra i vari documenti si vedano: nel Regno Unito *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digitalized World* (2011); negli Stati Uniti la *Strategy for Operating in Cyberspace* del *Department of Defense* (2011); in Canada la *Canada's Cyber Security Strategy* (2010).

il regolamento CE n. 460/2004, viene istituita un'apposita Agenzia dedicata alla sicurezza delle reti. Ciò avviene sul fondamento dell'art. 95 del trattato sulla Comunità europea (oggi art. 114 del Trattato sul funzionamento dell'Unione europea o TFUE): la base giuridica è dunque l'instaurazione e il funzionamento del mercato interno. Coerentemente con la missione originaria della Comunità europea, la sicurezza cibernetica è considerata una precondizione per un ordinato svolgersi degli scambi economici interni agli Stati membri.

Una seconda fase (attualmente in via di ulteriore sviluppo) segue invece la crisi economico-finanziaria del 2008-10, e prende le mosse dalla Strategia europea elaborata dalla Commissione e presentata nel febbraio 2013. Tale atto richiede espressamente agli Stati membri di elaborare una propria strategia nazionale in accordo con le linee guida comuni.

Di lì a poco, l'atto di indirizzo sarà seguito dal regolamento UE n. 526/2013 che, innovando il precedente regolamento, istituisce l'ENISA – l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione – riplasmando la precedente Agenzia secondo più avvedute esigenze di coordinamento delle attività in materia di sicurezza informatica e con una maggiore consapevolezza circa la natura strategica di tale materia nello sviluppo economico.

Ma nei confronti degli Stati membri – e per l'ordinamento "multilivello" dell'Unione – il passaggio fondamentale avviene con la direttiva europea 2016/1148 (c.d. Direttiva "NIS", *Network and Information Security*), destinata a fissare un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.

Tale atto non è peraltro restato isolato, inserendosi in una più ampia cornice di misure dettate dal legislatore europeo per rafforzare la difesa di interessi, reti e beni strategici per gli Stati membri e per l'Unione nel suo complesso, concretizzatasi di recente con l'adozione del regolamento 2019/881 sul potenziamento dell'ENISA e la creazione di un sistema di certificazione della cibersicurezza, che sostituisce il precedente regolamento del 2013. Tali indirizzi sono peraltro ancora in fase di evoluzione[2].

Accanto all'emanazione di questi atti, la stessa ENISA ha fornito un volume non indifferente di linee guida e raccolta di buone prassi in materia di sicurezza cibernetica.

Il risultato ultimo della legislazione unionale segue un andamento tipico del diritto europeo: attorno all'autorità europea (l'ENISA, in questo caso) si crea una rete di autorità nazionali[3] che debbono coordinarsi con questa e sono dotate di poteri di vigilanza, di sanzione e di natura talvolta mista, autorizzatoria e certificatoria. All'interno degli ordinamenti statali è possibile poi individuare delle autorità settoriali, cui è devoluta la competenza per i segmenti di attività economiche e sociali da loro presieduti. Accanto alla rete propriamente amministrativa, si costituisce anche una rete "tecnica" composta dai CSIRT nazionali (i Gruppi di intervento per la sicurezza informatica in caso di incidente, previsti dall'art. 9 della direttiva NIS).

---

[2] Il 16 dicembre 2020 è stata infatti presentata una nuova proposta di direttiva detta NIS-2, volta ad ampliare i settori di intervento della precedente regolazione. Essa è stata contestualmente accompagnata da un nuovo documento programmatico europeo per la cibersicurezza intitolato *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*.

[3] L'art. 8 della direttiva NIS prevede, da un lato, le autorità nazionali e, dall'altro, i «punti di contatto unici», vale a dire gli organismi di collegamento con l'Agenzia e gli altri Stati.

Nel marzo 2021 il Consiglio ha approvato in via definitiva il *Regolamento relativo al contrasto della diffusione di contenuti terroristici online*, destinato ad entrare in vigore nel 2022 dopo aver ricevuto il visto dei Parlamenti nazionali consultati. Lo scopo di questo atto – come si legge nel considerando n. 1 – è «garantire il buon funzionamento del mercato unico digitale in una società aperta e democratica contrastando l'uso improprio dei servizi di hosting a fini terroristici e contribuendo alla sicurezza pubblica in tutta l'Unione». Destinatari di questa norma sono tanto gli Stati (dunque, i poteri pubblici), quanto i prestatori di servizi di *hosting*, grandi soggetti privati che offrono servizi di memorizzazione di informazioni su richiesta di un fornitore di contenuti (art. 2, n. 1). Le autorità competenti di ciascuno Stato potranno dirigere ordini di rimozione direttamente agli *hosting providers* (art. 3). Costoro sono peraltro tenuti a particolari obblighi di trasparenza (art. 7), dovendo fornire nelle condizioni contrattuali i termini della loro politica in materia di lotta ai contenuti terroristici e possono anche essere soggetti alle sanzioni previste (art. 18).

4. *Sicurezza cibernetica e tutela dei "nuovi" diritti digitali nel costituzionalismo multilivello*

Il connubio fra tutela della sicurezza e garanzia dei diritti e delle libertà individuali si presenta da sempre complesso, a partire dal mondo fisico. L'esigenza di garantire l'esistenza pacifica e tranquilla delle comunità è stata spesso utilizzata come "grimaldello" per forzare l'assetto dei diritti individuali e conculcarli.

Nello spazio cibernetico, si riproducono gli stessi fenomeni e gli stessi rischi: l'attuazione di misure "cibersecuritarie" (si pensi ad attività di sorveglianza di massa, di analisi dei dati di connessione, di divieti dell'anonimato) si sposa perfettamente con un regime da Stato di polizia, che subordina l'esistenza e la garanzia della libertà alla dimensione della sicurezza. Ma vi è di più: queste misure possono essere messe in atto non da autorità pubbliche, ma da entità private che controllano le infrastrutture tecnologiche della comunicazione, senza limiti spaziali.

Anche per questa ragione è nel livello sovranazionale che vanno ricercati gli strumenti più idonei per bilanciare le legittime esigenze collettive di sicurezza con il godimento pieno dei diritti e delle libertà fondamentali.

4.1. *La normativa europea sui dati personali e la giurisprudenza della Corte di Giustizia*

Nel 2016, l'Unione europea adotta il regolamento generale sulla protezione dei dati personali n. 2016/679 (conosciuto anche come GDPR dal suo nome in inglese: *General Data Protection Regulation*). Scopo precipuo del regolamento è dettare un quadro normativo per controllare il fenomeno dei c.d. *big data*, vale a dire la raccolta massiva di dati degli utenti da parte dei grandi colossi del web a fini di profilazione.

Ora, il regolamento in teoria non si applica a questioni riguardanti la sicurezza nazionale (considerando n. 16 e n. 19). Tuttavia, come si è messo in luce nel paragrafo iniziale, da un lato, la tutela della sicurezza nel mondo cibernetico passa necessariamente per la responsabilizzazione dei privati che ne gestiscono le infrastrutture e, dall'altro, in tale con-

testo è ancor meno agevole che nel mondo fisico ritagliare esattamente gli ambiti di applicazione della disciplina di garanzia della "sicurezza" intesa nel senso di attività di polizia generale dei pubblici poteri.

Viceversa, il regolamento consacra la sua sezione seconda (artt. 32 e seguenti) alla "sicurezza dei dati personali", intesa come insieme di procedure e accorgimenti tecnici che devono essere posti in essere dai soggetti che realizzano i trattamenti dei dati. Di particolare importanza è l'art. 33 concernente le c.d. "*data breaches*", ovvero il furto di dati personali commesso a livello informatico tramite attività di hackeraggio. In questo caso, è richiesto che il titolare e il responsabile del trattamento comunichino all'autorità di controllo – in Italia, il Garante per la protezione dei dati personali – l'avvenuto incidente, di modo che possano essere condotte tutte le indagini necessarie e adottate le adeguate contromisure.

L'atto legislativo europeo fa comunque salva la possibilità che gli Stati adottino limitazioni agli obblighi e ai diritti previsti dal regolamento, purché esse rispettino i diritti fondamentali e costituiscano misure necessarie e proporzionate in una società democratica per salvaguardare una serie di beni fondamentali della collettività, quali la sicurezza pubblica, la difesa, la sicurezza nazionale, l'accertamento dei reati ecc. (art. 23 GDPR). Tale formula è tratta dall'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU), che tutela la vita privata e familiare.

La previsione del GDPR ricalca, peraltro, disposizioni già esistenti nel diritto dell'Unione, in particolare l'art. 15 della direttiva 2002/58/CE (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, non abrogata dal GDPR) e l'art. 13 della direttiva 95/46/CE (quest'ultima abrogata dall'entrata in vigore del regolamento del 2016).

Proprio in relazione a queste misure restrittive e alla loro messa in opera, la Corte di giustizia dell'Unione europea ha avuto modo di pronunciarsi sul bilanciamento possibile tra legittime attività di sicurezza e repressione criminale condotte dagli Stati e tutela dei dati personali degli utenti.

Con la sentenza *Tele2 Sverige e Watson* del 21 dicembre 2016 (cause riunite C203/15 e C698/15), la Corte stabilisce che non è conforme al diritto dell'Unione una normativa nazionale che, per finalità di lotta contro la criminalità, preveda una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e di quelli relativi all'ubicazione di tutti gli abbonati e utenti iscritti, con riguardo a tutti i mezzi di comunicazione elettronica. Allo stesso modo, non è possibile per gli Stati disciplinare la protezione e la sicurezza dei dati relativi al traffico e di quelli relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che tali dati siano conservati nel territorio dell'Unione.

L'attenzione per la tutela dei dati personali e per l'opportuno bilanciamento di questa con le esigenze di sicurezza pubblica è emersa anche nel caso *Schrems II* (C311/18, sentenza del 16 luglio 2020), che ben mette in luce come l'assenza di confini fisici renda assai fluida l'applicazione delle normative nel ciberspazio e si renda necessario regolare i rapporti fra lo

spazio giuridico europeo e l'esterno. Del resto, con un atto di *soft law*, il Parlamento europeo sin dal 2015 chiede alle istituzioni europee di vigilare a che nel mondo la tecnologia non si tramuti da strumento di libertà a mezzo di controllo ed oppressione da parte del potere nei confronti degli individui (Risoluzione del Parlamento europeo, *Diritti umani e tecnologia: impatto dei sistemi di sorveglianza e di individuazione delle intrusioni sui diritti umani nei paesi terzi*, 8 settembre 2015).

Nel caso *Schrems II*, si verteva sul trasferimento di dati dall'Unione europea agli Stati Uniti ad opera di Facebook. La società sosteneva di potersi sottrarre agli obblighi e alle garanzie del GDPR poiché i dati trasferiti oltre Atlantico erano trattati dalle autorità statunitensi a fini di sicurezza e difesa. La Corte rigetta questo argomento riconoscendo la piena applicabilità del GDPR e, tra le altre cose, annulla l'accordo esistente fra UE e USA (il c.d. "scudo UE-USA per la *privacy*") poiché tale regime non garantisce una protezione equivalente a quella del regolamento europeo quanto ad accesso ed utilizzo dei dati da parte delle autorità pubbliche a scopo di sicurezza nazionale, di amministrazione della giustizia o di interesse pubblico.

4.2. *La cibersicurezza e la Convenzione europea dei diritti dell'uomo*

Il rapporto fra attività di cibersicurezza e diritto alla vita privata consacrato dall'art. 8 CEDU è stato oggetto anche di alcune pronunce della Corte europea dei diritti dell'uomo, istituzione con sede a Strasburgo che ha il compito di verificare proprio il rispetto della CEDU da parte degli Stati.

In particolare, la più autorevole formazione della Corte di Strasburgo – la Grande Camera – ha avuto modo di recente di esprimersi sulla necessità delle intercettazioni globali di dati (c.d. *bulk interceptions*) al fine di garantire la sicurezza degli Stati.

In due decisioni del 25 maggio 2021 (*Big Brother Watch c. Regno Unito*; *Centrum För Rättvisa c. Svezia*), la Corte EDU traccia alcuni principi-guida sulla conciliazione del diritto alla *privacy* e le attività di pubblica sicurezza condotte con le nuove tecnologie. In particolare, la Corte sviluppa dei canoni che aveva già applicato alle intercettazioni individuali, dovendo però estenderli e precisarli in relazione alla dimensione massiva che tale fenomeno assume allorquando sia generalizzato, in assenza cioè di target specifici, ma con il solo scopo di scovare eventuali minacce per la sicurezza dello Stato. La Corte non nega che, allo stato della tecnica e nelle dinamiche internazionali attuali, le operazioni di vaste analisi di dati siano necessarie per assicurare la sicurezza interna ed esterna degli Stati. Tuttavia, ritiene che le leggi nazionali debbano inquadrare in maniera scrupolosa tali attività, affinché esse non sconfinino nell'arbitrio e rivelino intenti discriminatori o autoritari.

Questi, dunque, gli elementi che ogni ordinamento deve sufficientemente definire affinché l'intercettazione di massa possa considerarsi compatibile con l'art. 8 CEDU (par. 361, sentenza *Big Brother Watch*):

1) i motivi per i quali è possibile autorizzare un'intercettazione di massa;

2) le circostanze nelle quali le comunicazioni di un individuo possono essere intercettate;

3) la procedura da seguire per autorizzare tali attività;

4) le procedure per selezionare, esaminare ed utilizzare il materiale intercettato;

5) i limiti di durata dell'intercettazione, della conservazione dei materiali intercettati e le circostanze nelle quali tale materiale può essere cancellato o distrutto;

6) le procedure e le modalità di supervisione da parte di un'autorità indipendente sul rispetto degli elementi precedenti e i suoi poteri sanzionatori in caso di violazione;

7) le procedure per una verifica indipendente a posteriori di questo rispetto e i poteri di cui è investito l'organo competente per trattare i casi di violazione.

Quanto all'uso di dati personali in singoli casi da parte di forze di polizia, la Corte (caso *P.N. c. Germania*, 11 giugno 2020) ha ritenuto necessari e proporzionati la conservazione e il trattamento di dati personali di identificazione allo scopo di prevenire crimini particolarmente gravi o per evitare casi di recidive.

Riscontriamo qui due "livelli" di applicazione delle misure di *cibersecurity*: prendendo a prestito termini dal diritto penale, abbiamo anzitutto un livello *general-preventivo*, volto cioè a prevenire all'interno di tutta la collettività ed in maniera aspecifica minacce all'ordine pubblico, in assenza di soggetti specificamente bersagliati. Ma esiste poi anche il livello *special-preventivo*, che comporta l'applicazione di misure di controllo e sorveglianza elettronica ad individui specifici, in ragione di una loro qualche potenziale attitudine a commettere reati.

Ebbene, nel mondo cibernetico diventa in realtà molto complesso distinguere – dato che ciò deve avvenire a posteriori – quanto le misure considerate "generali" mirino in realtà soggetti o gruppi molto specifici, senza le garanzie che dovrebbero essere normalmente previste, secondo i canoni del costituzionalismo classico, per l'adozione di misure di "sorveglianza individuale".

5. *Lotta al terrorismo e polizia cibernetica: il caso del delitto di consultazione di siti islamisti in Francia*

Il bilanciamento fra i diritti esercitabili nel ciberspazio e le esigenze di sicurezza è un'opera complessa, che deve tenere conto tanto della gravità delle minacce che incombono concretamente sull'ordine pubblico di un dato Paese, quanto della garanzia di tutti i diritti fondamentali che si interfacciano nella rete.

La lotta al terrorismo rappresenta un evidente caso in cui il punto di equilibrio fra i due poli viene a spostarsi verso le esigenze securitarie, attratto dai gravi rischi all'integrità delle persone, dal sentimento di incertezza e paura che ingenera nella popolazione e dall'essere un fenomeno per definizione alieno da qualunque forma di regolazione fra i "belligeranti".

A scopo illustrativo, pare opportuno citare un caso tratto dal sistema francese. La Francia ha conosciuto fra il 2015 e il 2017 una serie di gravi attacchi terroristici ad opera di militanti del c.d. "Stato islamico", noto sotto il nome di *ISIS*: nel gennaio 2015 un commando fa strage nella redazione del giornale satirico *Charlie Hebdo*, reo di aver pubblicato

delle vignette sul profeta Maometto, e sequestra poi degli ostaggi, uccidendone alcuni, in un supermercato *kosher*. Nel novembre 2015, altri attacchi sono condotti in vari punti della città di Parigi e alle sue porte. Il 14 luglio 2016, sul lungomare di Nizza, un furgone si getta sulla folla uccidendo vari passanti che stavano assistendo allo spettacolo pirotecnico per la festa nazionale. Nel corso dello stesso mese, due fondamentalisti islamici uccidono un prete cattolico in una chiesa in Normandia. Nell'aprile 2017, un attacco terroristico sugli *Champs-Élysées* oppone la polizia e i terroristi in uno scontro a fuoco.

È in questo contesto che, oltre ad applicare e a irrigidire il regime dell'*état d'urgence* previsto dalla legge 55-385 del 3 aprile 1955, il legislatore francese crea varie fattispecie di "reati di pericolo" per perseguire tutti quegli atti considerati come un'adesione a finalità terroristiche o prodromi di attacchi concreti. Nel corso del 2017, per due volte il giudice costituzionale francese – il *Conseil constitutionnel* – si trova a dover decidere della legittimità costituzionale del delitto di «consultazione abituale di siti internet terroristici» (art. 421-2-5-2 del codice penale francese).

In particolare, si chiedeva al giudice di annullare questa ipotesi di reato poiché il legislatore aveva limitato, in maniera sproporzionata e non necessaria, la libertà di comunicazione degli utenti di Internet.

Nelle sue decisioni (n. 2016-611 QPC del 10 febbraio 2017; n. 2017-682 QPC del 15 dicembre 2017, *M. David P.*), il Consiglio ritiene che non si sia effettivamente operato un bilanciamento ragionevole fra, da un lato, la tutela dell'ordine pubblico e la prevenzione di reati e, dall'altro, la libertà di informazione e comunicazione cui Internet è strumentale. In particolare, rileva il giudice, nell'ordinamento già esistono molteplici possibilità per le autorità pubbliche di contrastare e prevenire il fenomeno terroristico.

Da una parte, l'autorità giudiziaria può mettere in atto misure di intercettazione della corrispondenza elettronica e di comunicazioni sonore e di immagini, nonché attività di raccolta dei dati di connessione e di altri dati informatici. Dall'altra, gli stessi organi amministrativi – in particolare, i servizi di informazione – possono compiere i medesimi atti di controllo e di captazione di dati, oltre a disporre del potere di ingiungere agli *hosting providers* la rimozione di contenuti potenzialmente pericolosi. Erano dunque presenti nell'ordinamento tanto strumenti di controllo general-preventivo che strumenti special-preventivi tali da rendere non necessarie ulteriori restrizioni nell'accesso a talune pagine ed informazioni in Internet.

6. Cybersecurity *e organizzazione dei poteri*

La sicurezza cibernetica, oltre ad avere un rilevante impatto in materia di diritti individuali, impone anche di approntare un'organizzazione istituzionale idonea a gestire le sfide poste dal mondo digitale.

Nel quadro dell'Unione europea, l'adozione della direttiva NIS ha obbligato gli Stati ad organizzare un'architettura istituzionale di poteri cibersecuritari. La natura tipicamente "trasversale" delle politiche di cibersicurezza e la loro conseguente difficile collocazione nel quadro ordinamentale emerge nitidamente allorché ci si focalizzi sulla natura delle diverse "autorità NIS" dei Paesi membri.

In effetti, possiamo verificare che l'attuazione è stata estremamente variegata, in ciò rilevandosi anche specifiche scelte di indirizzo politico-amministrativo interne agli Stati, riassumibili sostanzialmente in tre ipotesi.

La prima è consistita nell'affidamento del ruolo ad autorità amministrative indipendenti o, comunque, ad organismi tecnici di regolazione. Così, ad esempio, è successo in Lussemburgo, dove l'Autorità per le telecomunicazioni è stata investita del ruolo, affiancata dalla sola Autorità per i mercati finanziari per l'ambito di competenza[4]. Nel Regno Unito *ante Brexit* il ruolo di autorità nazionale era invece assegnato all'*Information Commissioner*[5], alle cui cure già erano affidati i compiti discendenti dalla normativa europea sulla *privacy*.

La seconda opzione ha invece innestato poteri, doveri e competenze derivanti dalla direttiva NIS direttamente su apparati ministeriali o su enti da questi dipendenti. Si tratta, in realtà, della scelta più frequente all'interno degli ordinamenti statali[6], sebbene poi l'identificazione del dicastero dipenda in buona parte dal numero di autorità settoriali individuate, ma – in fondo – anche dall'interpretazione che i legislatori nazionali danno alle politiche di cibersicurezza. Così facendo, in alcuni casi è l'aspetto infrastrutturale ad emergere (a Malta e in Irlanda il compito spetta al Ministero delle Comunicazioni), in altri è il profilo prettamente legato alla sicurezza (in Germania è il Ministero degli Interni), in altri ancora è l'idea della lotta all'illegalità informatica (nei Paesi Bassi è il ministro della Giustizia).

Da ultimo, alcuni Paesi hanno scelto di conferire direttamente al capo del Governo o ad un'agenzia a questi sottoposta le funzioni di autorità nazionale NIS (così in Belgio[7], Francia[8], Portogallo[9], Austria[10]).

Questa diversità di trasposizione rivela la natura ibrida della cibersicurezza: si tratta di una questione tecnica da lasciare ad entità esperte? È una funzione amministrativa di polizia che i pubblici poteri devono esercitare a livello virtuale come nel mondo fisico? Oppure è una questione più densamente politica, che attiene alle strategie di fondo dell'azione statuale, ponendosi quindi al cuore stesso dell'indirizzo politico?

---

[4] Secondo la *loi du 29 mai 2019*, le autorità competenti sono la *Commission de surveillance du secteur financier* e l'*Institut luxembourgeois de régulation*, ciascuno per il proprio settore di regolazione (i mercati finanziari e le telecomunicazioni).

[5] Cfr. *The Network and Information Systems Regulations 2018*, sez. 3.

[6] Questi alcuni dei Paesi che hanno individuato l'autorità nazionale NIS in un ministero o in un apparato alle dirette dipendenze di questo: Germania (Ministero dell'Interno); Spagna (Ministero dell'Interno, Ministero dell'Economia e Ministero della Difesa); Paesi Bassi (Ministero della Giustizia); Malta (Ministero delle Comunicazioni); Irlanda (Ministero per la Comunicazione, l'azione climatica e l'ambiente).

[7] La *loi du 7 avril 2019* ha rinviato ad un *arrêté royal* l'individuazione dell'autorità nazionale. Tale atto (adottato il 18 luglio 2019) ha conferito il ruolo al *Centre pour la Cybersécurité Belgique*, che è posto alle dirette dipendenze del Primo Ministro (*arrêté royal* del 10 ottobre 2014).

[8] In questo caso il tema della cibersicurezza è stato integrato direttamente nel *Code de la défense* dalla *loi* n. 2015-917 (*loi actualisant la programmation militaire 2015-2019*), che ha inserito l'articolo L. 1332-6-1, il quale attribuisce al Primo Ministro il potere di fissare le regole necessarie alla protezione dei sistemi informatici di interesse pubblico. L'autorità nazionale è rappresentata dall'*Agence Nationale de la sécurité des systèmes d'information*, che dipende dal Servizio generale della difesa e della sicurezza nazionale del Primo Ministro.

[9] Si tratta del *Centro Nacional de Cibersegurança* che, ai sensi dell'art. 7 della *lei* 46/2018, opera nell'ambito del *Gabinete Nacional de Segurança*, a sua volta sotto la direzione del Primo Ministro.

[10] I compiti del *Bundeskanzler* sono evidenziati dalla *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen* (§ 4). Egli è assistito dal *Büro für Strategische Netz- und Informationssystemsicherheit*.

I contenuti della direttiva NIS – a ben vedere – trattano tutti e tre gli aspetti, mettendo l'accento tanto sul versante tecnico (più precisamente individuato nella rete europea e nei punti di contatto: art. 9), quanto sul versante amministrativo (con i poteri riconosciuti alle autorità nazionali: art. 8) ed anche – seppure in maniera meno incisiva – sul lato politico, domandando l'adozione di specifiche strategie nazionali (art. 7).

Tuttavia, è chiaro che l'afflusso di nuovi, significativi poteri di derivazione europea, che attingono interessi fondamentali dello Stato (la sicurezza e la difesa), non potesse lasciare indifferenti le strutture di governo, né si sarebbe potuta realizzare silenziosamente la fuoriuscita di queste facoltà dall'orbita di una loro titolarità politica. Sicché non sorprende che, da un lato, il ricorso alle autorità indipendenti sia stato in definitiva ridotto e, dall'altro, i vertici del potere esecutivo siano stati direttamente coinvolti nella definizione delle architetture nazionali di cibersicurezza, soprattutto ove già detenessero competenze in materia di sicurezza e servizi segreti. A questo proposito è particolarmente significativo l'esempio dell'Italia.

6.1. *Il caso italiano: il Presidente del Consiglio al vertice*

La recezione da parte dell'ordinamento italiano delle novità maturate a livello europeo merita una menzione a parte, se non altro per l'andamento altalenante che l'ha caratterizzata.

In effetti, la prima fonte di attuazione (o, meglio, di anticipazione) degli orientamenti europei è stata la legge 7 agosto 2012 n. 133 che, intervenendo sulla legge 3 agosto 2007 n. 124 sulla sicurezza della Repubblica, ha posto il Presidente del Consiglio al vertice delle politiche nazionali di protezione cibernetica e sicurezza informatica. In questo modo il tema della cibersicurezza veniva concretamente introiettato nella dinamica della forma di governo nel nostro Paese. A seguito della novella, e sul fondamento delle nuove norme introdotte, il Presidente del Consiglio dettava una strategia nazionale sul modello di quanto da lì a poco avrebbe fatto formalmente anche l'Unione europea (DPCM 24 gennaio 2013: «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale»).

La direttiva NIS, invece, trova applicazione in Italia con il d.lgs. 18 maggio 2018 n. 65, adottato dal Governo Gentiloni, dimissionario a seguito delle elezioni del marzo 2018 (dunque limitato, nella sua attività, agli affari correnti): non a caso vi è stata una ricezione minimale della normativa, poi integrata nel 2019. In particolare, il decreto legislativo, pur riconoscendo al Presidente del Consiglio il potere di adozione della strategia nazionale (art. 6), delegava a vari Ministeri la competenza settoriale in materia cibernetica (art. 7). Tale scelta di *governance* è stata in parte rivista con il successivo d.l. 21 settembre 2019 n. 105, che ha attribuito al Presidente del Consiglio in Italia importanti poteri (sia normativi che preventivi, ma anche sanzionatori) al fine di garantire un livello elevato di sicurezza delle reti in conformità con la direttiva NIS. In particolare, il decreto da ultimo citato ha creato il "perimetro di sicurezza nazionale cibernetica", affidando al Capo del Governo la vigilanza degli operatori pubblici e privati ivi inclusi e fornendogli vari poteri di difesa in caso di crisi cibernetica[11].

[11] L'art. 5 prevede in particolare un potere di "spegnimento", con cui si ordina la disattivazione di prodotti, apparati o snodi infrastrutturali inseriti nel perimetro ed esposti a fragilità in caso di grave rischio nazionale: una sorta di virtuale "ponte levatoio" che si richiude per proteggere la rete nel suo complesso.

Nel 2021, il Governo Draghi ha adottato un nuovo decreto-legge (14 giugno 2021 n. 82) con cui – oltre a riaffermare l'architettura nazionale di sicurezza cibernetica con al vertice il Presidente del Consiglio – viene creata l'Agenzia Nazionale per la cibersicurezza nazionale (sotto l'egida del Capo del Governo), a cui si affidano le funzioni di Autorità nazionale ai fini della direttiva NIS, superando l'assetto stabilito nel 2018 e riportando coerenza fra i vari interventi succedutisi.

Bibliografia

Cinelli C., *Sorveglianza digitale, sicurezza nazionale e tutela dei diritti umani*, in «Ordine internazionale e diritti umani», 2020, pp. 588 ss.; Cocco G. (a cura di), *I diversi volti della sicurezza*, Giuffrè, Milano, 2012; De Vergottini G., *Guerra e Costituzione: nuovi conflitti e sfide alla democrazia*, il Mulino, Bologna, 2004; Id., *Una rilettura del concetto di sicurezza nell'era digitale e dell'emergenza normalizzata,* in «Rivista AIC», 2019 (4), pp. 67 ss.; Dinnis H., *Cyberwarfare and the laws of war*, Cambridge University Press, Cambridge-New York, 2014; Giupponi T., *Le dimensioni costituzionali della sicurezza*, Bonomo, Bologna, 2010; Laurent S.Y. (a cura di), *Conflits, crimes et régulations dans le cyberespace*, ISTE Editions, London, 2021; Lauro A., *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in «Gruppo di Pisa», 2021 (3), pp. 529 ss.; Marrani D., *Cybersicurezza e tutela della riservatezza dei dati personali: le decisioni Breyer e Tele2 Sverige c. Watson della Corte di Giustizia UE*, in «Il diritto dell'Unione Europea», 2017 (4), pp. 442 ss.; Montessoro P.L., *Cybersecurity: conoscenza e consapevolezza come prerequisiti dell'amministrazione digitale*, in «Istituzioni del federalismo», 2019 (3), pp. 783 ss.; Schmitt M.N. (a cura di), *Tallin Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, Cambridge-New York, 2016; Torre A. (a cura di), *Costituzioni e sicurezza*, Maggioli, Santarcangelo di Romagna, 2013; Turk P., Vallar C. (a cura di), *La souveraineté numérique. Le concept, les enjeux*, Mare&Martin, Paris, 2017; Vedaschi A., À la guerre comme à la guerre*? La disciplina della guerra nel diritto costituzionale comparato*, Giappichelli, Torino, 2007.