lAUR Vulnerabilità e tutela dei diritti fondamentali alla prova della guerra cibernetica

di Alessandro Lauro

Abstract: *Vulnerability and fundamental rights protection at the test of cyberwarfare* - The contribution attempts to highlight the correlation that has arisen, in particular in European legislation on cybersecurity, between network vulnerability and rights vulnerability. The aim is to critically question whether eliminating the former is really a tool for eliminating the latter.

Keywords: Vulnerability – ICT – Cybersecurity – Cyberwarfare – Fundamental rights

1. L'interrogativo della ricerca: dalla vulnerabilità delle reti alla vulnerabilità dei diritti

Questo contributo parte da un termine che fa ormai parte del lessico contemporaneo "globalizzato": vulnerabilità. Con esso si intende un particolare stato di fragilità, di delicatezza, che impone un'attività di protezione preventiva rispetto ai rischi che possono prodursi.

In ambito giuridico, essa è un concetto particolarmente caro al diritto sovranazionale europeo, tanto per la giurisprudenza della Corte europea dei diritti dell'uomo, quanto per la legislazione dell'Unione europea[1].

[1] Si v., senza alcuna presunzione di esaustività: J.Y. Carlier, *Des droits de l'homme vulnérable à la vulnérabilité des droits de l'homme, la fragilité des* équilibres, in *Revue interdisciplinaire d'études juridiques*, n. 2/2017; A. Catherine, S. Etoa, *Vulnerabilité et droit public*, in *Cahier des recherches sur les droits fondamentaux*, n. 18, 2020; F. Cohet Cordey (a cura di), *Vulnérabilité et droit. Le développement de la vulnérabilité et ses enjeux en droit*, Grenoble, 2000; E. Paillet, P. Richard (a cura di), *Effectivité des droits et vulnérabilité de la personne*, Bruxelles, 2014; D. Roman, *Vulnerabilité et droits fondamentaux*, in *Revue des droits et libertés fondamentaux*, n. 19, 2019; S. Rossi, *Forme della vulnerabilità e attuazione del programma costituzionale*, in *Rivista AIC*, n. 2/2017, 1 ss.: F.X. Roux-Demare, *La notion de vulnérabilité, approche juridique d'un concept polymorphe*, in *Cahiers de la Justice*, n. 4/2019, 619 ss.; F. Rouviere, *Le droit à l'épreuve de la vulnérabilité. Études de droit français et de droit comparé*, Bruxelles, 2010; P. Scarlatti, *I diritti delle persone vulnerabili*, Napoli, 2022; A. Timmer, *A Quiet Revolution: Vulnerability in the European Court of Human Rights*, in M.A. Fineman, A. Grear (a cura di), *Vulnerability. Reflections on a New Ethical Foundation for Law and Politics*, Londra-New York, 2013, 147. Si v. anche la ricerca comparatistica realizzata per il *Conseil constitutionnel* francese AA.VV., *La QPC, outil efficace de protection des personnes en situation de vulnérabilité ?*, in *Titre VII*, ottobre 2020.

DPCE online
ISSN: 2037-6677

Vulnerabilità è un termine che – pur non variando nel suo significato – si presta ad applicazioni multiple e varie. L'uso che qui rileva concerne, in particolare, le infrastrutture informatiche.

Il *corpus* normativo dell'Unione europea dedicato alla sicurezza cibernetica (sia di diritto vincolante, che di *soft law*) fa sempre più di frequente riferimento alla "vulnerabilità" delle reti, dei sistemi, di tutto quel supporto materiale o digitale che regge l'intero universo cibernetico.

Per dare l'idea di alcuni di questi atti, basta citare i più recenti e rilevanti: l'ultima Strategia per la sicurezza cibernetica in Europa (adottata nel 2020); la c.d. Direttiva "NIS 2" (n. 2022/2555); il regolamento DORA (2022/2554 relativo alla "resilienza operativa digitale per il settore finanziario"); il Regolamento 2021/784 sul contrasto alla diffusione di contenuti terroristici online.

Fra questi, la direttiva NIS 2 contiene una definizione di vulnerabilità (art. 6, n. 15), identificata come «un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica».

L'idea di fondo è che per preservare l'ordine democratico europeo, il suo spazio giuridico di libertà e (soprattutto) il mercato unico (base giuridica, ai sensi dell'art. 114 TFUE dei vari atti normativi citati) occorre approntare un elevatissimo livello di protezione tecnica delle reti, identificando ed eliminando le vulnerabilità (tecniche) in queste presenti.

Non può essere trascurato che questa evoluzione fa da sempre *pendant* con i documenti e le linee-guida diffuse dalla NATO, da ultimo il manuale *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency*[2].

L'equazione sarebbe quindi esprimibile secondo una formula proporzionale: diminuire la vulnerabilità delle reti concorre a diminuire la vulnerabilità dei diritti. L'aumento della "superficie di attacco", non più solo fisica e geografica, che uno Stato deve sorvegliare, rende gli stessi diritti più esposti agli attacchi del nemico[3].

Questo processo – stando proprio alla Strategia per la sicurezza cibernetica – avviene in un contesto mondiale di "guerra cibernetica" latente, di tensioni multilaterali crescenti da ultimo sfociate nel conflitto russo-ucraino. Se è vero – come insegna autorevole magistero[4] – che nel mondo si combatte una "terza guerra mondiale a pezzi", un frammento consistente è proprio quello che corre sulle reti di internet[5].

Il concetto di guerra è ampio, sfaccettato e – già ben prima della rivoluzione digitale – di difficile qualificazione in termini giuridici esaustivi[6]: in realtà, si può forse dire che la dimensione cibernetica ha

[2] C.V. Evans (a cura di), *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency NATO COE-DAT Handbook 1*, Carlisle (Pennsylvania), 2022.

[3] Cfr. S. Biçakci, *Cyber Threats to Critical Infrastructure*, in C.V. Evans, *Enabling NATO's Collective Defense*, cit., 41 ss.

[4] Ci si riferisce, come è noto, agli accorati appelli di Papa Francesco, fra i quali v. il suo *Discorso al Consiglio di sicurezza delle Nazioni Unite*, 14 giugno 2023.

[5] Cfr. Commissione Europea, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale (Comunicazione congiunta al Parlamento europeo e al Consiglio)*, 16 dicembre 2020, 1 ss.

[6] La letteratura sul tema della guerra e delle sue trasformazioni è vasta, ma si v.

definitivamente consacrato l'impossibilità di una sua definizione precisa[7]. Però, da questo punto di vista, si incontra il vantaggio di poter ragionare in termini forzatamente più sfocati, ma anche più ampi. Non è un caso che gli atti sopra citati trattino diverse forme di belligeranza nell'ambiente digitale: conflitti interstatali "classici" (attinenti cioè alla difesa internazionale), ma spostati in un ambiente diverso; ma anche guerra commerciali e finanziarie (si veda il regolamento DORA[8]) o la (ormai anche questa classica) "guerra al terrorismo"[9]. Per non parlare di tutte quelle attività "interne" di contrasto alla criminalità (anche transnazionale) che generalmente si riportano sotto l'ombrello della sicurezza.

Questo contributo vorrebbe problematizzare l'equazione di proporzionalità sopra riportata: è proprio vero che contrastare la vulnerabilità delle reti significa rafforzare i diritti? Non si corre parallelamente il rischio di instaurare – in nome di una belligeranza latente – uno Stato (o meglio un super-Stato) di polizia cibernetica, secondo il più classico dei paradigmi autoritari?

2. La guerra cibernetica nell'ordinamento internazionale e lo sviluppo della disciplina europea in materia di cibersicurezza: una panoramica

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 Manuale di Tallin – 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[10].

Il Manuale, la cui ultima edizione risale al 2017, nasce dal bisogno di

almeno N. Bobbio, *Il problema della guerra e le vie della pace*, Bologna, 2009; A. Calore (a cura di), *Guerra giusta? : le metamorfosi di un concetto antico*, Milano, 2003; G. de Vergottini, *Guerra e Costituzione: nuovi conflitti e sfide alla democrazia*, Bologna, 2004; H. Dinnis, *Cyberwarfare and the laws of war*, Cambridge-New York, 2014; A. Vedaschi, À la guerre comme à la guerre? *La disciplina della guerra nel diritto costituzionale comparato*, Torino, 2007.

[7] Cfr. G. de Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e dell'emergenza normalizzata*, in *Rivista AIC*, n. 4/2019, 67 ss.

[8] Cfr. il *Considerando n. 1* del Regolamento DORA: «Il crescente grado di digitalizzazione e interconnessione amplifica d'altra parte i rischi informatici, rendendo l'intera società, e in particolare il sistema finanziario, più *vulnerabile* alle minacce informatiche o alle perturbazioni delle TIC. L'uso onnipresente dei sistemi di TIC e l'elevata digitalizzazione e connettività sono oggi caratteristiche fondamentali delle attività delle entità finanziarie dell'Unione» (enfasi aggiunta rispetto all'utilizzo dell'aggettivo vulnerabile).

[9] V. sul tema P. Bonetti, *Terrorismo, emergenza e costituzioni democratiche*, Bologna, 2006; M. Frau, E. Tira (a cura di), *Il contrasto al terrorismo negli ordinamenti democratici*, Brescia, 2022.

[10] M.N. Schmitt (a cura di), *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge-New York, 2017.

DPCE online
ISSN: 2037-6677

riorganizzare e razionalizzare gli indirizzi e le prassi sorti all'interno di alcuni Paesi della Nato[11].

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.

L'attenzione europea al tema della sicurezza informatica si sviluppa sostanzialmente in due macrofasi[12].

Una prima, agli inizi degli anni 2000, 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 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 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 in seno al mercato unico.

Una seconda fase (attualmente in via di ulteriore sviluppo) segue invece la crisi economico-finanziaria del 2008-2010, e prende le mosse dalla Strategia europea elaborata dalla Commissione e presentata nel febbraio 2013[13]. 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 l'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

[11] Fra i vari documenti v.: 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).

[12] Per una descrizione più analitica sia consentito rinviare a A. Lauro, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Gruppo di Pisa. Quaderno*, n. 3/2021, 529 ss.

[13] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico sociale ed al Comitato delle regioni, 7 febbraio 2013.

sviluppo economico.

Nei confronti degli Stati membri – e per l'ordinamento "multilivello" dell'Unione – il passaggio fondamentale avviene infine 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 misura 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.

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 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).

La direttiva NIS 2 del 2022 ha consolidato questo assetto, estendo ulteriormente l'ambito di applicazione del regime a varie attività private. È interessante notare che tale atto ha creato una Banca dati europea delle vulnerabilità (art. 12).

Nell'aprile 2023, infine, la Commissione Europea ha proposto un nuovo atto regolatorio, il c.d. *Cyber Solidarity Act*, al fine di installare un *European Cyber Shield* ed un *Cyber Emergency Mechanism* di livello europeo a supporto dei già esistenti meccanismi di cooperazione interstatale nella materia[14]. Mette conto evidenziare che questa novità intende adottare una base giuridica diversa: la nuova regolamentazione si fonderà precipuamente sull'art. 173, comma 3, TFUE, dedicato alle politiche industriali all'interno dell'Unione.

3. Guerra, sicurezza cibernetica e tutela dei "nuovi" diritti digitali nel costituzionalismo multilivello

Gli scopi del legislatore sovranazionale sono certamente nobili: mediante la protezione delle reti e dei sistemi, si prefigge di tutelare vari diritti di diversa caratura. È interessante osservare la sintesi operata dalla

[14] Proposta n. COM(2023) 209 della Commissione Europea, presentata il 18 aprile 2023.

DPCE online
ISSN: 2037-6677

Commissione europea nella proposta sulla solidarietà cibernetica sopra richiamata, secondo cui tale normativa partecipa alla tutela di molteplici diritti fondamentali previsti dalla Carta di Nizza: il diritto alla libertà e alla sicurezza (art. 6), il diritto alla riservatezza e alla vita familiare (art. 7), il diritto alla proprietà privata e alla libertà di impresa (artt. 16 e 17), nonché, proteggendo le infrastrutture pubbliche, il diritto alle cure sanitarie (art. 35) e il diritto all'accesso a servizi di interesse economico generale (art. 36). La sicurezza cibernetica diventerebbe insomma uno "scudo" intromesso fra le potenziali minacce ed il piano degli individui, con i loro diritti[15].

Il connubio fra tutela della sicurezza collettiva, garanzia della sicurezza individuale[16] e libertà si presenta da sempre complesso, a partire dal mondo fisico[17]. 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.

Tuttavia, non va dimenticato che, 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 sposano perfettamente con un regime da Stato di polizia, che subordina l'esistenza e la garanzia della libertà alla dimensione della sicurezza[18]. 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, dettando le loro regole[19].

Vi è poi un altro problema, assai significativo, che merita di essere evidenziato: nella realtà fisica degli ordinamenti limitazioni pesanti ai diritti fondamentali in nome della sicurezza e della difesa possono avvenire solo con procedure canoniche, con proclami di stati di grave emergenza (al di là dell'effettiva denominazione nei singoli ordinamenti) che impongono la compartecipazione di diversi organi costituzionali, secondo la migliore interpretazione del principio di separazione dei poteri. Viceversa, ciò non sembra accadere nel momento in cui ci si sposta nello spazio cibernetico[20].

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

---

[15] A.M. Gambino, *Diritti fondamentali e* cybersecurity, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Firenze, 2017, 93 ss.

[16] Sulla configurazione di un vero e proprio diritto soggettivo alla sicurezza, distinto dall'esigenza di protezione della collettività, v. le argomentazioni di N. Zanon, *Un diritto fondamentale alla sicurezza?*, in *Diritto penale e processo*, n. 11/2019, 1555 ss.

[17] Cfr. in particolare T.F. Giupponi, *Le dimensioni costituzionali della sicurezza*, Bologna, 2010; A. Torre (a cura di), *Costituzioni e sicurezza*, Santarcangelo di Romagna, 2013

[18] B. Warusfel, *La cyberdéfense, dimension numérique de la sécurité nationale*, in S.Y. Laurent (a cura di), *Conflits, crimes et régulations dans le cyberespace*, Londra, 2021, 105 ss.

[19] Sul fenomeno v. *ex multis* A. Iannuzzi, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Napoli, 2018, 29 ss.

[20] G. de Vergottini, *Una rilettura del concetto di sicurezza*, cit., 75.

3.1 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 regolare 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[21].

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 sopra, la tutela della sicurezza nel mondo cibernetico, da un lato, passa necessariamente per la responsabilizzazione dei privati che ne gestiscono le infrastrutture. Dall'altro, è ancor meno agevole, rispetto al mondo fisico, ritagliare esattamente gli ambiti di applicazione della disciplina di garanzia della "sicurezza" intesa in 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. 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 contromisure necessarie.

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

[21] Si v., per tutti, il volume a cura di L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017; sul tema del rapporto fra normativa sulla tutela dei dati personali e sicurezza v. in particolare nel volume citato P. Milazzo, *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, 709 ss.).

DPCE online
ISSN: 2037-6677

opera, la Corte di Giustizia 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 C-203/15 e C-698/15)[22], 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 dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante 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 dei dati 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* (C-311/18, 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[23].

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 a accesso ed utilizzo dei dati da parte delle autorità pubbliche a scopo di sicurezza nazionale, di amministrazione della giustizia o di interesse pubblico.

3.2 La cibersicurezza e la Convenzione europea dei diritti

[22] A commento v. D. Marrani, 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, 442 ss.; O. Pollicino, *Enforcement of the Right to Digital Privacy*, in G. De Minico, O. Pollicino (a cura di), *Virtual Freedoms, Terrorism and the Law*, Torino, 2021, 37 ss.

[23] 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.

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.

In particolare, di recente la più autorevole formazione della Corte – la Grande Camera – ha avuto modo di esprimersi sulla necessità delle intercettazioni globali di dati (c.d. *bulk inteceptions*) 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*)[24], 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 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 circostanza 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

[24] Sulle quali v. C. Cinelli, *Sorveglianza digitale, sicurezza nazionale e tutela dei diritti umani*, in *Ordine internazionale e diritti umani*, 2020, 588 ss.

DPCE online
ISSN: 2037-6677

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 individualmente bersagliati. Ma esiste poi anche il livello special-preventivo, che comporta l'applicazione di misure di controllo e sorveglianza elettronica ad individui determinati, in ragione di una loro qualche potenziale attitudine a commettere reati.

Ora, secondo i canoni del costituzionalismo classico, le misure individuali dovrebbero sempre ricadere sotto un controllo del giudice terzo e imparziale, allorché le misure generali possono essere applicate dall'autorità amministrativa *erga omnes*.

Ebbene, nel mondo cibernetico diventa in realtà ancora più complesso distinguere – dato che ciò deve avvenire a posteriori – quanto le misure considerate "generali" mirino in realtà soggetti o gruppi molto specifici, all'infuori delle garanzie che dovrebbero essere normalmente previste.

4. "Guerra" al terrorismo e polizia cibernetica: dal caso francese dei siti islamisti sino al regolamento europeo contro i contenuti terroristici

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 "belligeranti".

È in questo contesto che, oltre ad applicare e ad 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 giudicare 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.*)[25], il Consiglio ritiene che non

[25] Si tratta di due decisioni molto commentate dalla dottrina francese, per le quali v. D.

si sia effettivamente operata una conciliazione ragionevole fra la tutela dell'ordine pubblico e la prevenzione di reati da un lato 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 gli stessi 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.

L'esempio francese ha fatto scuola a livello europeo, dove si è prima adottata una Direttiva generale (n. 2017/541) per la lotta al terrorismo, che sostituiva precedenti decisioni del Consiglio nella materia della cooperazione penale, e poi un apposito regolamento espressamente dedicato alla lotta ai contenuti terroristici online, in cui si richiede una forte cooperazione fra pubblico e privato in questa "guerra". Nel marzo 2021 il Consiglio ha approvato in via definitiva il Regolamento relativo al contrasto della diffusione di contenuti terroristici online, entrato 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[26] potranno

Baranger, *Consultation de sites djihadistes : il ne faut pas réduire le Parlement au silence*, in *JusPoliticum Blog*, 16 febbraio 2017; V. Goesel-Le Bihan, *Une grande décision : la décision n° 2016-611 QPC*, in *Actualité juridique. Droit administratif*, n. 8/2017, 433 ss.; B. de Lamy, *La lutte contre le terrorisme à l'épreuve du contrôle de constitutionnalité : utiles précisions sur la nécessité d'une incrimination*, in *Revue de science criminelle et de droit pénal comparé*, n. 2/2017, 385 ss.; X. Latour, *La lutte contre les sites djihadistes et la liberté de communication*, in *La Semaine juridique. Administrations et collectivités territoriales*, n. 7/2018, 38 ss.; T. Hochmann, *Consultation habituelle, censure habituelle (À propos de la décision QPC rendue le 15 décembre 2017 par le Conseil constitutionnel)*, in *Jus Politicum Blog*, 11 gennaio 2018; N. Catelan, *Consultation de sites terroristes : quel dialogue entre le legislateur et ses juges ?*, in *Revue française de droit constitutionnel*, n. 115/2018, 645 ss.

[26] Nel caso italiano, con il d. lgs. 24 luglio 2023, n. 107, si è adeguata – in ritardo – la normativa nazionale al regolamento individuando nell'autorità giudiziaria, ed in particolare nell'ufficio del Pubblico ministero (art. 3), l'autorità interna titolare del potere di ingiunzione. Si tratta di un approccio "giurisdizionale" che appare minoritario in Europa (cfr. la lista delle autorità competenti pubblicata nel Giornale ufficiale dell'Unione Europea del 27 giugno 2023). Da segnalare, in particolare quanto

DPCE online
ISSN: 2037-6677

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).

Si tratta di un elemento per nulla irrilevante, poiché si arriva quasi ad una forma di "partenariato" (altra parola magica del vocabolario sovranazionale) a fini securitari. Tuttavia non si può dimenticare che, proprio nelle radici francesi del costituzionalismo moderno, 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)[27].

Tutto ciò alla luce della persistente difficoltà di definire cosa sia il terrorismo (a prescindere dalle definizioni della direttiva del 2017): un esempio abbastanza significativo è l'uso che se ne è fatto, in risoluzioni ufficiali del Parlamento europeo, nei confronti della Russia, definita Stato *sponsor* di attività terroristiche (risoluzione del 23 novembre 2022). Pur trattandosi di un pronunciamento non vincolante, ciò getta un'ombra su come la stessa libertà di espressione potrebbe trovarsi imbrigliata alla luce di queste definizioni.

5. Un tentativo di conclusione

I vari spunti emersi sembrano confermare che lo spazio cibernetico – celebrato come spazio di libertà, talvolta quasi di anarchia, se ricordiamo la Dichiarazione di indipendenza del cyberspazio scritta da John Perry Barlow nel 1996 – in realtà si è ben curvato (riprendendo un'immagine della fisica) attorno al potere degli Stati e delle potenze mondiali.

Oggi, le esigenze della sicurezza (che passa dalla prevenzione delle vulnerabilità) si sono imposte pure nella dimensione cibernetica e, forse più che nella realtà materiale, anche i tentativi di bilanciamento portati avanti

è avvenuto in Francia, dove le autorità nazionali sono competenti sono le "autorità amministrative", sotto la vigilanza dell'Autorità di regolazione delle comunicazioni (cfr. *loi n° 2022-1159 du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne*). Questa scelta è stata oggetto di una decisione del *Conseil constitutionnel* adito in via preventiva dalla minoranza parlamentare. Nella sua decisione n. n° 2022-841 DC del 13 agosto 2022 il Consiglio ha ritenuto che la scelta del legislatore non violasse la libertà di espressione e comunicazione, poiché le ingiunzioni emesse dall'autorità amministrativa sono sempre suscettibili di ricorso davanti al giudice amministrativo secondo la procedura d'urgenza del *référé-liberté* previsto agli artt. L. 521-1 et L. 521-2 del codice di giustizia amministrativa.

[27] È da ricordare la significativa pronuncia del *Conseil constitutionnel* francese n.2021-940 QPC del 15 ottobre 2021, con la quale si è riconosciuto come principio inerente all'identità costituzionale francese (quindi come "controlimite" al diritto europeo ed internazionale) il divieto di delegazione della forza pubblica ad entità private. Sulla decisione v. M. Verpeaux, *Les résistances de la Constitution française*, in *La Semaine juridique. Édition générale*, 15 novembre 2021, n. 46, 2100 ss.

dalle Corti sovranazionali, così come dal legislatore europeo, sembrano tutto sommato poco soddisfacenti, perché spesso imponderabili come imponderabile è Internet.

Il problema reale che pare affiorare è la scomparsa delle forme. Può sembrare paradossale, perché si è detto – e non a torto – che il costituzionalismo digitale predilige la procedimentalizzazione, i diritti procedurali, la previsione di obblighi di rendicontazione ecc[28]. Ciò è piuttosto vero a carico dei privati.

Tuttavia, a meglio guardare, sono scomparse le forme più rilevanti.

Scompaiono le procedure costituzionali solenni, pubbliche, controllate, dominate dal dibattito, talvolta anche lente, ma che erano volte ad evitare decisioni affrettate a salvaguardia dei diritti fondamentali.

È moribonda la riserva di legge e con lei il principio di uguaglianza formale (nel suo significato politico-ideologico primo, cioè il necessario coinvolgimento della rappresentanza politica della nazione nella definizione di una volontà generale, valida per tutti)[29]. Al posto della legge ci sono gli atti di *soft-law*, le indicazioni tecniche, il "buon senso" del caso concreto, talvolta anche le decisioni casistiche di Corti sovranazionali[30].

Ma si appanna anche la riserva di giurisdizione: il giudice, ammesso che arrivi, arriverà sempre dopo. E talvolta al posto del giudice-magistrato in senso tecnico, compaiono "arbitri" la cui natura non è di semplice identificazione (pensiamo a organismi di *audit* delle piattaforme)[31].

Occorre però non dimenticare che – come scriveva Benjamin Constant – le forme preservano dall'arbitrario[32] e lo spazio cibernetico non può restare "informe" se non vuole trasformarsi in uno spazio di arbitrio.

Alessandro Lauro
Diritto pubblico e comparato
Università Ca' Foscari di Venezia
Université Paris Panthéon Assas
alessandro.lauro@unive.it

[28] O. Pollicino, G. De Gregorio, *Constitutional Law in the Algorithmic Society*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*. Cambridge, 2021, 20 ss.

[29] Cfr. per questa considerazione N. Zanon, F. Biondi, *Il sistema costituzionale della magistratura*, Bologna, 2019, 135.

[30] Sulla produzione normativa di stampo tecnico v. A. Iannuzzi, *Le forme di produzione delle fonti a contenuto tecnico-scientifico nell'epoca del diritto transnazionale*, in *DPCE online*, n. 3/2020, 3277 ss.

[31] V. per una sintesi M.E. Bucalo, *I volti della libertà di manifestazione del pensiero nell'era digitale. Content moderation e regolazione di un diritto in evoluzione*, Torino, 2023, 95 ss.

[32] B. Constant, *Principes de politique*, Parigi, 1872, cap. XVIII: «*Ce qui préserve de l'arbitraire, c'est l'observance des formes. Les formes sont les divinités tutélaires des associations humaines; les formes sont les seules protectrices de l'innocence, les formes sont les seules relations des hommes entre eux*».

DPCE online
ISSN: 2037-6677