ANNO XVI - Bari, aprile 2013

ISBN 1825-6112

sud in europa

DIPARTIMENTO DI
SCIENZE POLITICHE
DELL'UNIVERSITÀ DEGLI STUDI
DI BARI ALDO MORO

www.sudineuropa.net
info@sudineuropa.net

EUROPA
più unita e democratica
contro la crisi

L'editoriale di GIANNI PITTELLA*

* Vicepresidente vicario del Parlamento europeo

Nel 2010 abbiamo "celebrato" un anno dall'approvazione del Trattato di Lisbona. E già dal momento della ratifica era chiaro che la vera sfida sarebbe stata quella di verificare nella pratica che i singoli governi accettassero pienamente, e non solo a parole, la parziale cessione di sovranità a favore dell'autonomia europea che il Trattato prevede, nel rispetto del principio di sussidiarietà.

L'obiettivo politico principale che le forze progressiste avevano posto nel nuovo Trattato era quello di colmare un *deficit* di rappresentanza che aveva reso la burocrazia dell'UE sempre più distante e addirittura ostile nella percezione comune dei suoi cittadini, con pericolose ricadute sulla tenuta democratica complessiva dell'intero continente. Il pericolo maggiore per il processo di integrazione europea era individuabile proprio nella diffidenza verso le istituzioni di Bruxelles, alimentata e cavalcata in questi anni da schieramenti populisti e xenofobi, fautori della supremazia della nazione su ogni organismo sovranazionale e addirittura della reclusione rassicurante delle aspirazioni delle comunità locali nelle cosiddette "piccole patrie", celebrate nel nostalgico e mitico ricordo di un presunto, idilliaco e antistorico passato.

Oggi questo pericoloso processo di disgregazione dell'Unione europea si è ripresentato sotto nuove forme sull'onda dello tsunami che ha investito l'economia e i mercati finanziari pubblici e privati, a partire dalla crisi dei *sub-prime* statunitensi nel 2008 che ne ha costituito l'innesco.

Il ripiegamento su logiche strettamente nazionali, che hanno pesato quando bisognava prendere decisioni importanti e rapide in favore di Paesi in difficoltà come Grecia ed Irlanda, è un comportamento che non

Presidenza del Consiglio Regione Puglia

Provincia di Bari

Comune di Bari

europe direct puglia

europe direct
Centro di Documentazione Europea di Bari

Il piano dell'Unione europea in materia di **sicurezza informatica**

di GIUSEPPE MORGESE

1. Com'è noto, la strategia "Europa 2020", inaugurata nel 2010, ha fissato gli obiettivi di crescita dell'Unione europea e dei suoi Stati membri da raggiungere, appunto, entro il 2020. Nel quadro di tale strategia, l'Unione sta portando avanti tra l'altro una "Agenda digitale europea", che ha lo scopo di utilizzare le potenzialità delle tecnologie dell'informazione e della comunicazione per promuovere l'innovazione, la crescita economica e il progresso. Nella comunicazione del 19 maggio 2010 sull'agenda digitale europea, COM(2010)245 def., la Commissione si era posta come obiettivo la creazione di sette "pilastri" concernenti la realizzazione del mercato digitale unico; l'aumento dell'interoperabilità e degli standard; il consolidamento della fiducia e della sicurezza *online*; la promozione dell'accesso a Internet veloce e superveloce per tutti; maggiori investimenti in ricerca e sviluppo; il miglioramento dell'alfabetizzazione, delle competenze e dell'inclusione nel mondo digitale; e infine la promozione di un utilizzo intelligente della tecnologia.

Il Consiglio europeo del 28 e 29 giugno 2012 ha chiesto che venisse ulteriormente rafforzata la *leadership* europea del digitale e si completasse il mercato unico digitale entro il 2015, anche in considerazione delle perduranti significative differenze tra Stati membri. A tal fine, nel dicembre 2012 la Commissione ha operato una revisione dell'agenda digitale, elencando sette nuove priorità dirette ad aumentare gli investimenti nella banda larga e ottimizzare il contributo del settore digitale per la più generale ripresa economica dell'Europa. Queste priorità riguardano la creazione di un nuovo contesto normativo stabile per la banda larga; la predisposizione di nuove infrastrutture per servizi digitali pubblici; l'avvio di una grande coalizione sulle competenze e i posti di lavoro in ambito digitale; la proposizione di una strategia e una direttiva in materia di sicurezza informatica; l'aggiornamento del quadro relativo ai diritti d'autore; l'accelerazione delle questioni connesse al c.d. "*cloud computing*"; e l'avvio di una nuova strategia industriale per l'elettronica.

2. Per quel che interessa la sicurezza informatica, nel biennio 2010-2012 l'Unione ha intrapreso azioni di tutela dei cittadini dalla c.d. *cibercriminalità* attraverso la previsione del Centro europeo per la lotta alla criminalità informatica (EC3), la proposta di atti normativi sugli attacchi ai sistemi d'informazione e l'instaurazione di un'alleanza mondiale contro l'abuso sessuale di minori *online*.

L'EC3, istituito presso Europol (Ufficio europeo di polizia con sede a L'Aia, nei Paesi Bassi) e divenuto pienamente operativo dall'11 gennaio 2013, è un centro di sostegno operativo, investigativo e forense, con l'obiettivo di fornire precise competenze in materia di lotta alla criminalità informatica e di contrastare le minacce provenienti dai criminali informatici, minacce cui non si può porre rimedio in maniera efficace al solo livello nazionale. Il Centro intende occuparsi, per un verso, della prevenzione e repressione delle attività illegali *online* della criminalità organizzata (quelle cioè che generano notevoli profitti, quali ad es. le frodi *online* me-

diante l'abuso di carte di credito e coordinate bancarie); per altro verso, della protezione dei profili dei *social networks* e del contrasto ai furti di identità *online*; per altro verso ancora, dei reati informatici che causano gravi danni alle vittime, quali lo sfruttamento sessuale dei minori *online* e gli attacchi informatici contro infrastrutture e sistemi d'informazione dell'Unione.

Quanto alla normativa in materia di attacchi ai sistemi informatici, il 30 settembre 2010 la Commissione ha proposto di adottare una direttiva e un regolamento. La proposta di direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione, COM(2010)517 def., si basa sulle disposizioni già previste nell'omonima decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, e introduce nuove circostanze aggravanti e sanzioni penali più rigide avverso gli attacchi su larga scala contro i sistemi di informazione. Questa proposta, attualmente al vaglio delle istituzioni legislative dell'Unione, contempla inoltre un miglioramento della cooperazione fra le autorità giudiziarie e di polizia degli Stati membri e la creazione di un sistema di registrazione e tracciabilità degli attacchi informatici.

Con la proposta di regolamento del Parlamento europeo e del Consiglio, relativo all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), COM(2010)521 def., la Commissione intende rafforzare e modernizzare quest'ultima Agenzia (creata con il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004) per migliorare la cooperazione fra gli Stati membri, le autorità di contrasto e il settore industriale di riferimento. Le nuove norme – qualora approvate – consentirebbero all'ENISA di coinvolgere con maggiore flessibilità gli Stati membri e il settore privato in attività congiunte su scala europea (esercitazioni di sicurezza informatica, partenariati pubblico-privati per la resilienza delle reti, analisi economiche, valutazioni del rischio e campagne di sensibilizzazione). La proposta inoltre estende il mandato dell'Agenzia per cinque anni, ne aumenta le risorse finanziarie e umane, e prevede un ruolo di maggiore supervisione da parte del suo consiglio di amministrazione (composto da rappresentanti della Commissione e degli Stati membri).

La Commissione si è inoltre attivata per creare un fronte comune tra Paesi europei ed extraeuropei contro la pedopornografia *online*. Nel dicembre 2012, infatti, è nata l'Alleanza mondiale contro l'abuso sessuale di minori *online*, iniziativa avente l'obiettivo di individuare e assistere le vittime nonché di punire i colpevoli di tali gravi abusi. Ne fanno parte i 27 Paesi membri dell'Unione e altri 21 Stati (Albania, Australia, Cambogia, Croazia, Georgia, Ghana, Giappone, Moldova, Montenegro, Nuova Zelanda, Nigeria, Norvegia, Filippine, Serbia, Repubblica di Corea, Svizzera, Tailandia, Turchia, Ucraina, Stati Uniti d'America e Vietnam). In seno all'Alleanza, detti Stati si sono impegnati a mettere in pratica alcuni obiettivi strategici e a contrastare in maniera più incisiva gli abusi sessuali di minori *online* mediante una migliore cooperazione internazionale. In specie, quei Paesi si adopereranno – scegliendo i mezzi ritenuti più adeguati e presentando regolari rapporti – nel senso di potenziare gli sforzi diretti a individuare le vittime e garantire loro l'assistenza, il sostegno e la protezione necessari; a investigare i casi di pedopornografia *online* e punire i relativi autori; a informare i giovani sui rischi della Rete legati all'autoproduzione di immagini e ai metodi di adescamento; a intercettare il materiale pedopornografico *online* e evitare la rivittimizzazione dei minori.

Cittadinanza europea: i cittadini europei sono sempre più consapevoli dei diritti che l'UE garantisce ma ne vogliono sapere di più

Secondo una nuova indagine Eurobarometro pubblicata dalla Commissione europea, a vent'anni dall'introduzione della cittadinanza dell'UE gli europei sono largamente consapevoli dell'esistenza dei diritti ad essa legati, ma non sempre sanno cosa implicano. In Italia la consapevolezza di questi diritti appare ben superiore alla media europea, se il 93% degli intervistati (rispetto all'81% della media UE) afferma di sapere di essere cittadino dell'UE, oltre ad esserlo del proprio Paese. Tuttavia solo il 35% (36% la media europea) ritiene di essere ben informato sui diritti che derivano da questa condizione. La maggioranza degli europei conosce i propri diritti in fatto di libera circolazione (88% - 84% in Italia) e petizione presso le istituzioni dell'UE (89% - solo l'80% in Italia), mentre i due terzi degli europei (67%) pensano che la libera circolazione delle persone all'interno dell'UE sia vantaggiosa per il proprio Paese dal punto di visto economico. Nell'indagine Eurobarometro sulla cittadinanza dell'Unione europea veniva chiesto agli europei di esprimersi sulla loro condizione di cittadini dell'UE e sui diritti ad essa associati. Nel complesso, gli intervistati erano a conoscenza della maggior parte di questi diritti, compreso il diritto di petizione presso le istituzioni UE (89%), libera circolazione (88%), non-discriminazione fondata sulla nazionalità (82%), protezione consolare (79%) e partecipazione a un'iniziativa dei cittadini (73%). Se più di un terzo degli intervistati (36%) si reputa ben informato su questi diritti (il che costituisce un aumento di 5 punti percentuali rispetto al 2007), solo il 24% ritiene di sapere come procedere nel caso i suoi diritti UE non siano rispettati. Per quanto riguarda il diritto di libera circolazione, l'idea che apporti vantaggi economici per il proprio paese è condivisa dalla netta maggioranza degli intervistati in tutti i 27 Stati membri.

3. Nel febbraio 2013, la Commissione ha pubblicato un'ampia strategia sulla sicurezza informatica, proponendo anche una direttiva in materia di sicurezza delle reti e dell'informazione.
La comunicazione congiunta della Commissione e dell'Alto rappresentante per gli affari esteri e la politica di sicurezza, del 7 febbraio 2013, dedicata alla strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, JOIN(2013)1 def., muove dalla considerazione secondo cui il ciberspazio presenta aspetti sia positivi sia negativi. Da un lato, infatti, esso è idoneo a promuovere l'inclusione politica e sociale, ad abbattere le barriere nazionali in vista di un migliore scambio di informazioni e di idee, e a creare un luogo di libertà di espressione ed esercizio dei diritti fondamentali, favorendo la partecipazione democratica dei cittadini. Dall'altro lato, però, si fa sempre più pressante l'esigenza che nel ciberspazio si applichino le stesse norme, gli stessi principi e gli stessi valori applicabili negli spazi fisici. In altri termini, la comunicazione in esame chiarisce la necessità che nell'ambiente digitale *online* siano contemperate le esigenze della libertà con quelle della sicurezza. L'esperienza degli ultimi anni ha peraltro dimostrato che il ciberspazio procura vantaggi ma presenta anche vulnerabilità, con particolare riferimento alle minacce derivanti da attacchi criminali, di natura politica o terroristica o commissionati da uno Stato, oppure causate da calamità naturali ed errori non intenzionali.
La strategia in esame mette in luce gli obiettivi ai quali dovrebbe tendere un'efficace politica in materia di cibersicurezza a livello sia internazionale sia dell'Unione. In particolare, si propone che i valori costitutivi dell'Unione valgano sia nel mondo digitale sia in quello fisico; che siano rispettate nel ciberspazio le norme dell'Unione in materia di protezione della libertà di espressione, dei dati personali e della vita privata; che sia garantito a tutti un accesso sicuro a Internet; che sia mantenuto e rafforzato l'attuale approccio diffuso e partecipativo alla *governance* di Internet; che vi sia una precisa responsabilità condivisa per garantire la cibersicurezza. Per il raggiungimento di questi obiettivi, la strategia del febbraio 2013, pur riconoscendo la primaria competenza degli Stati membri in materia, propone interventi specifici che possano rafforzare l'efficienza complessiva dell'Unione. Le cinque priorità strategiche consistono, in specie, nel raggiungimento della ciberresilienza; nella drastica riduzione del cibercrimine; nello sviluppo di una politica e capacità di ciberdifesa connesse al quadro normativo della Politica di sicurezza e di difesa comune; nello sviluppo delle risorse industriali e tecnologiche per la cibersicurezza; e, infine, nella creazione di una politica internazionale coerente dell'Unione sul ciberspazio che promuova i valori costitutivi dell'Unione. La strategia propone inoltre un coordinamento tra le diverse autorità nazionali ed europee, nonché meccanismi di sostegno dell'Unione in caso di ciberincidente o ciberattacco grave.
La proposta di direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione, COM(2013)48 def., rappresenta la principale misura diretta a concretizzare la strategia appena descritta. Essa muove dalla constatazione per cui la proposta di direttiva del 2010 ricordata agli attacchi contro i sistemi di informazione, sopra descritta, contempla la punibilità di comportamenti specifici ma nulla dice in merito alla prevenzione di rischi e incidenti di sicurezza delle reti e dell'informazione né all'attenuazione delle loro conseguenze. La proposta del 2013 invece si propone di garantire un elevato livello comune di sicurezza delle reti e dell'informazione nel territorio dell'Unione, e richiede che tutti gli Stati membri, gli operatori Internet e di infrastrutture critiche (piattaforme per l'*e-commerce* e di *social networks*), nonché gli imprenditori nei settori dell'energia, dei trasporti, dei servizi bancari e dell'assistenza sanitaria garantiscano un ambiente digitale sicuro e affidabile nell'intera Unione.
A tal fine si stabiliscono misure concernenti, per un verso, l'elaborazione da parte degli Stati membri di una strategia per la sicurezza delle reti e dell'informazione (insieme alla designazione di un'autorità nazionale in materia, che abbia risorse finanziarie e umane idonee a prevenire, far fronte e rispondere ai rischi e agli incidenti connessi alla cibersicurezza). Per altro verso, un meccanismo di cooperazione tra gli Stati membri e la Commissione diretto soprattutto a migliorare i sistemi nazionali di preallarme relativi ai suddetti rischi e incidenti. Per altro verso ancora, l'adozione, da parte di una serie di soggetti privati (operatori di infrastrutture critiche e di servizi della società d'informazione) e pubblici, di efficaci prassi sulla gestione dei rischi e sulla notifica dei gravi incidenti concernenti la sicurezza dei servizi offerti da ognuno di loro.
Si ricorda che nel settore della cibersicurezza risulta applicabile il vigente quadro normativo dell'Unione per le comunicazioni elettroniche (composto da numerosi regolamenti, direttive, decisioni e raccomandazioni), in vigore dal novembre 2009, che – per quanto interessa ai nostri fini – impone precisi obblighi di sicurezza ai fornitori di comunicazioni elettroniche. Rilevano infine altre disposizioni normative UE sulla protezione dei dati personali e sull'individuazione e designazione delle infrastrutture critiche europee, oltre alle pertinenti norme e raccomandazioni elaborate nel quadro di alcune organizzazioni (anche non governative) internazionali quali l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), l'Assemblea generale delle Nazioni Unite, l'Unione internazionale delle telecomunicazioni (UIT), l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), il Vertice mondiale sulla società dell'informazione (WSIS) e il Forum sulla *governance* di Internet (IGF).