DE BERTI ■ JACCHIA

De Berti Jacchia Franchini Forlani
studio legale

LA *CYBERSECURITY* IN EUROPA. FONTI, LEGISLAZIONE E VISIONE

Roberto A. Jacchia e Cyber Team

1. Scopo

Scopo del presente lavoro è quello di individuare le azioni e le politiche intraprese dall'Unione Europea ed il ruolo svolto dalle Istituzioni nel settore della *cybersecurity* che, con velocità esponenziale, sempre più impatta sulla sicurezza nazionale e sulla crescita economica degli Stati Membri.

La natura eccezionalmente ampia e le caratteristiche uniche delle aggressioni informatiche (compressione spazio–temporale, trasversalità, a–simmetricità, a-territorialità e mutevolezza) comporta la necessità di una visione politica di lungo periodo, che travalichi i confini nazionali e risulti in una gestione condivisa, altrimenti impossibile da realizzare. Le relative azioni debbono necessariamente inscriversi nel sistema delle fonti, unionali e internazionali, e collocarsi in una visione globale.

Nel presente lavoro, si fornirà un'introduzione generale del tema (paragrafo 2); si ripercorreranno le azioni intraprese dall'Unione in materia di *cybersecurity*, fino al 2013 ed a partire dal 2013 rispettivamente (paragrafi 3 e 4); ci si soffermerà specificamente sul nuovo modello introdotto dalla Direttiva c.d. NIS, appunto del 2013, destinato ad entrare pienamente a regime nel 2018 (paragrafo 5); si discuteranno sommariamente le inter-relazioni fra la materia della *cybersecurity* e quelle, per diversi riguardi connesse ed interferenti, della tutela dei dati personali e dei controlli sui prodotti a duplice uso, in particolare, delle tecnologie di cyber-sorveglianza (paragrafo 6); si individueranno gli organi e le autorità rilevanti in materia istituiti a livello dell'Unione ed in taluni Stati Membri (paragrafi 7 e 8); ed infine, si farà cenno a taluni casi di recente attualità (paragrafo 9) ed all'impatto futuro della Brexit (paragrafo 10), con qualche considerazione conclusiva di sintesi (paragrafo 11).

2. Introduzione

Negli ultimi venti anni, la diffusione delle nuove tecnologie dell'informazione e della comunicazione (ICT) ha trasportato il centro di gravità delle attività sociali, politiche ed economiche in una nuova dimensione cibernetica, in cui prolifera un numero crescente di servizi irrinunciabili dipendenti dai sistemi digitali (i.e. commercio, salute, sicurezza, ed altri che contribuiscono al *well-being* generale).

Ancorché lo spazio cibernetico abbia reso possibile uno sviluppo accelerato nei Paesi più avanzati, la digitalizzazione dei servizi e dei flussi informativi ha accresciuto l'esposizione al rischio dei cosiddetti attacchi cibernetici – aumentati del 38% nel solo 2015 – che potrebbero, da un lato, causare danni economici e sociali di dimensione incalcolabile e, dall'altro, minare la fiducia degli utenti nella sicurezza dei servizi *online* e nella protezione della loro *privacy*.

Per prendere cura di tali problematiche, le istituzioni e i poteri pubblici che amministrano l'infrastruttura giuridica digitale riguardante i cittadini sono chiamati a garantire la disponibilità, integrità e riservatezza dei dati e delle informazioni, così come le imprese sono chiamate ad assicurare la continuità dei servizi erogati, proteggendoli da possibili attacchi cibernetici.

Si comprende, allora, la necessità di un'azione coordinata degli Stati Membri, che persegua il contrasto del crimine informatico, la protezione delle infrastrutture critiche e la tutela delle informazioni personali digitali.

La Commissione ha individuato come priorità della propria azione la sicurezza informatica e la *privacy* digitale, che sono alla base della Strategia del Mercato Unico Digitale[1], oltreché la lotta contro il *cybercrime* che, a sua volta, rappresenta uno dei tre pilastri dell'Agenda Europea sulla Sicurezza[2]. Quest'ultima enuncia i principi che guideranno l'azione europea in questo campo secondo due *driver* altrettanto vitali, ma non sempre di agevole coordinamento: l'universalità dell'accesso alle reti e la protezione *online* dei diritti fondamentali.

3. Le azioni dell'Unione in materia di cybersecurity fino al 2013

La Commissione ha da tempo intrapreso azioni (sia legislative, sia di *soft-law*) per garantire una sempre maggiore protezione dei mercati *online,* incentivare gli investimenti in ricerca e innovazione ed assicurare uno sviluppo costante e rapido delle reti e dei servizi di comunicazione elettronica.

Le prime azioni risalgono all'inizio di questo secolo con la pubblicazione della Comunicazione sul *Cybercrime*[3] del 2001, relativa alla sicurezza delle infrastrutture dell'informazione ed alla lotta al crimine informatico.

Questa Comunicazione è stata successivamente integrata da quella sulla *Network Information Security*[4] sempre del 2001 (NIS) che, al paragrafo 2.1, viene definita come

"*… la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema …*".

La definizione offerta dalla NIS è corredata da un inquadramento generale che illustra le tipologie di minacce che possono impattare sulla sicurezza delle reti, tipizzate in base alla loro natura, e consistenti nell'intercettazione delle comunicazioni, nell'accesso non autorizzato a computer e reti informatiche, nelle c.d. cadute di rete[5], nell'esecuzione di *software* c.d. "maligni"

---

1 Com. Comm., COM(2015) 192 final del 06.05.2015, *Strategia per il mercato unico digitale in Europa*.

2 Com. Comm., COM(2015) 185 final del 28.04.2015, *Agenda europea sulla sicurezza*.

3 Com. Comm., COM(2000) 890 del 26.01.2001, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informativa. eEurope 2002*.

4 Com. Comm., COM(2001) 298 del 06.06.2001, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*.

5 I c.d. *"disruptive attack"* che comportano l'interruzione delle funzioni di un'infrastruttura critica e che colpiscono gli utenti del servizio (ovvero, in taluni casi, il sistema Paese nel suo complesso) con possibilità di danni economici gravi.

che modificano o distruggono i dati[6], nell'usurpazione delle identità personali e negli incidenti ambientali ed eventi imprevisti[7].

Sempre nei primi anni 2000, la Commissione ha adottato altre due Comunicazioni (*eEurope*[8] ed *eEurope 2005*[9]), che hanno confermato l'interesse primario dell'Unione alle dinamiche del processo di digitalizzazione. Entrambe si inscrivono nella visione di Lisbona 2000[10], che auspicava di fare dell'Europa un'economia basata sulla conoscenza *"più competitiva e più dinamica del mondo"*[11] entro il 2010. Esse mostravano, inoltre, la necessità per l'Europa di ammodernare i servizi pubblici essenziali offerti sulla rete e di dotarsi di un'affidabile infrastruttura capace di proteggere le informazioni.

In tale contesto, nel 2002 sono state adottate le tre Direttive – di cui la 2002/21/CE c.d. Quadro – relative all'accesso e alle autorizzazioni per le reti e i servizi di comunicazione elettronica (vale a dire, la Direttiva 2002/21/CE[12] che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, la Direttiva 2002/19/CE[13] relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime, e la Direttiva 2002/20/CE[14] relativa alle autorizzazioni per le reti ed i servizi di comunicazione elettronica). Queste tre direttive sono state abrogate nel 2009 dalla nuova Direttiva Quadro 2009/140/CE per le reti ed i servizi di comunicazione elettronica[15], che impone agli Stati Membri di predisporre misure interne che garantiscano la sicurezza delle reti e la costituzione di un'apposita autorità nazionale di regolamentazione.

---

6 Sono *software* maligni ("*malware*") quelli che consentono di usurpare l'identità altrui oppure di infettare i computer minacciando la sicurezza e l'integrità dei dati da essi contenuti.

7 La categoria degli incidenti ambientali comprende sia i casi provocati da eventi naturali e catastrofi, sia quelli che si configurano quale conseguenza diretta dell'errore umano. *David Omand*, *Visiting Professor* del *King's College* di Londra e segretario permanente dell'*Home Office* del Regno Unito, ha affermato che è più alta la probabilità che l'interruzione di un servizio sia dovuta ad un incidente ambientale piuttosto che ad un attacco vero e proprio; quindi, la distinzione tra minacce volute ed eventi accidentali si rivelerebbe, in realtà, meno critica rispetto alla definizione dei tempi massimi di recupero del servizio.

8 Com. Comm., COM(2000) 130 del 08.03.2000, *eEurope. Una società dell'informazione per tutti*.

9 Com. Comm., COM(2002) 263 del 28.05.2002, *eEurope 2005: una società dell'informazione per tutti*.

10 Programma di riforme economiche approvato a Lisbona dai Capi di Stato e di Governo dell'Unione europea durante il Consiglio Europeo del 23-24 marzo del 2000.

11 Ibidem, p.7.

12 Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro), GU L 108 del 24.04.2002.

13 Direttiva 2002/19/CE del Parlamento europeo e del Consiglio, del 24 aprile 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime (direttiva accesso), GU L 108 del 24.04.2002.

14 Direttiva 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica (direttiva autorizzazioni), GU L 108 del 24.04.2002.

15 Direttiva 2009/140/CE del 25 novembre 2009 recante modifiche alle direttive 2002/21/CE, 2002/19/CE e 2002/20/CE, GU L 260 del 03.10.2009.

Nel 2003, l'Unione ha predisposto la propria strategia in materia di sicurezza informatica nel cui ambito, pur non venendo utilizzato il termine *"cybersecurity"*, viene per la prima volta fatto esplicito riferimento ad una

"*… dipendenza europea da un'infrastruttura interconnessa nel settore dei trasporti, dell'energia, dell'informazione ed altri, e la conseguente vulnerabilità dell'Europa sotto questo profilo…*"[16].

Infatti, l'espressione *cybersecurity* comparirà per la prima volta nella Relazione del 2008 sull'attuazione della Strategia europea in materia di sicurezza[17] del 2003, in cui la sicurezza informatica viene presentata come uno degli aspetti critici per combattere il terrorismo e la criminalità organizzata:

"*… Le economie moderne dipendono fortemente da infrastrutture critiche quali i trasporti, le comunicazioni e l'approvvigionamento energetico, ma anche Internet. La strategia europea per una società dell'informazione sicura, adottato nel 2006, mira a combattere la criminalità attraverso Internet. Tuttavia, gli attacchi contro sistemi informatici privati o governativi negli Stati membri dell'UE hanno dato a tale questione una nuova dimensione, quella di una nuova arma potenziale di tipo economico, politico e militare. È necessario lavorare ulteriormente in questo settore, al fine di ricercare un approccio globale dell'UE, prestare opera di sensibilizzazione e rafforzare la cooperazione internazionale …*"[18].

La Comunicazione del 2006 relativa ad una strategia per una *"società dell'informazione sicura"*[19], richiamata nel passaggio precedente, ha nuovamente ribadito l'esigenza di promuovere l'impegno europeo a realizzare una sempre più elevata sicurezza delle reti e delle informazioni e di una cultura orizzontale della sicurezza informatica.

A riprova dell'importanza centrale riconosciuta a questo tema, la Commissione ha, sempre nel 2006, pubblicato la Comunicazione relativa ad un programma europeo per la protezione delle infrastrutture critiche[20], con cui è stato istituito il gruppo di contatto c.d. PIC (Protezione Infrastrutture Critiche) che, riunendo tutti i punti di contatto PIC nazionali, coadiuva gli Stati Membri nell'individuare le infrastrutture critiche (*European Critical Infrastructures*; le c.d. ECI[21]) attraverso l'analisi della loro portata e della loro gravità[22].

---

16 Consiglio UE, *Un'Europa sicura in un mondo migliore. Strategia europea in materia di sicurezza*, 12.12.2003, p. 2.

17 Consiglio UE, S407/08 del 11.12.2008, *Relazione sull'attuazione della strategia europea in materia di sicurezza*.

18 *Relazione sull'attuazione della strategia europea in materia di sicurezza*, *cit.*, p. 5.

19 Com. Comm., COM(2006) 251 del 31.05.2006, *Una strategia per una società dell'informazione sicura. "Dialogo, partenariato e responsabilizzazione"*.

20 Com. Comm., COM(2006) 786 del 12.12.2006, *Comunicazione relativa a un programma europeo per la protezione delle infrastrutture critiche*.

21 L'articolo 2, lettera b), della Direttiva 2008/114/CE dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (GU L 345 del 23.12.2008) definisce ECI: "*… un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri …*".

22 *Cybersecurity: Unione europea e Italia Prospettive a confronto*, p. 29: "*… 1) portata: perturbazione o distruzione di una particolare infrastruttura critica, misurata in base all'ampiezza dell'area geografica che potrebbe essere danneggiata, dalla sua perdita od indisponibilità; 2) gravità: conseguenze della perturbazione o distruzione di una particolare infrastruttura,*

Poco dopo, il Consiglio ha adottato la Direttiva 2008/114/CE[23] relativa all'individuazione delle infrastrutture critiche europee ed alla necessità di migliorarne la protezione, altresì designando le ECI di rilevanza europea attraverso l'utilizzo di criteri omogenei per valutarne il peso e l'importanza.

Ad oggi, questa Direttiva non è stata modificata e rappresenta un elemento centrale nell'impianto della sicurezza ICT in Europa.

La Commissione ha poi elaborato la Comunicazione relativa alla protezione delle infrastrutture critiche informatizzate[24] del 2009, che delinea un piano d'azione specifico inteso a rafforzare la sicurezza e la resilienza di tutte le infrastrutture ICT.

Questa Comunicazione ha inoltre contribuito ad accrescere il ruolo dell'Agenzia Europea di Sicurezza delle Reti e dell'Informazione (ENISA), per il coordinamento delle politiche nazionali di protezione delle infrastrutture critiche. L'impegno europeo è stato riconfermato dalla Comunicazione del 2011 (sempre relativa alla protezione delle infrastrutture critiche informatizzate)[25] e dalle relative Conclusioni del Consiglio UE del 2011[26] sul ruolo dell'ENISA e l'impegno di ogni Stato Membro a realizzare un proprio *Computer Emergency Response Team* (CERT) nazionale.

Infine, nel 2010, sono state pubblicate la Comunicazione *Un'agenda digitale europea*[27] che persegue lo scopo di *"… ottenere vantaggi socioeconomici sostenibili grazie a un mercato digitale unico basato su internet veloce e superveloce e su applicazioni interoperabili…"*[28] e la Comunicazione sulla strategia di sicurezza interna[29] che delinea, invece, le principali minacce a cui è esposto il complesso europeo, individuando cinque grandi direttrici verso un'Europa informaticamente sicura

a) smantellare le reti criminali internazionali

b) prevenire il terrorismo e contrastare la radicalizzazione e il reclutamento

c) aumentare i livelli di sicurezza per i cittadini e le imprese nel cyberspazio

---

valutate in base ai seguenti elementi: conseguenze per i cittadini (numero di persone colpite); conseguenze economiche (entità delle perdite economiche e/o del deterioramento di prodotti o servizi); conseguenze ambientali; conseguenze politiche; conseguenze psicologiche; conseguenze a livello di salute pubblica …".

23 Direttiva 2008/114/CE, *cit.*.

24 Com. Comm., COM(2009) 149 del 30.03. 2009, *Proteggere le infrastrutture critiche informatizzate. "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberpertibazioni"*.

25 Com. Comm., COM(2011) 163 del 31.03.2011, *Comunicazione relativa alla protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale"*.

26 Consiglio UE, 10299/11 del 19.05.2011, *Protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale" (CIIP) – Adozione delle conclusioni del Consiglio*.

27 Com. Comm, COM(2010) 245 def. del 19.05.2010, *"Un'agenda digitale europea"*.

28 Com. Comm., COM(2010) 245 f/2 del 26.08.2010, *Un'agenda digitale europea*, p. 3.

29 Com. Comm., *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura.*

d) rafforzare la sicurezza attraverso la gestione delle frontiere

e) aumentare la resilienza dell'Europa alle crisi e alle calamità.

Il terzo punto, che costituisce una priorità assoluta, riconosce l'importanza strategica della protezione dai rischi derivanti dal crimine informatico di tutti gli utenti finali che usufruiscono di Internet e dei servizi *online*.

Viene altresì sottolineata la centralità della collaborazione con il settore privato e del progresso tecnologico, per garantire una risposta efficace agli attacchi cibernetici. Per fare ció, la strategia stabilisce tre linee d'azione, individuando per ciascuna sia autorità incaricate ed il termine previsto per l'implementazione.

La prima azione riguarda l'istituzione di un Centro Europeo per il *Cybercrime*, realizzato nel 2012 e operativo dal 2013, in sostituzione dell'*Hi-Tech Crime Centre* presso l'*Europol*. La seconda mira alla creazione di un meccanismo avanzato di *incident reporting*, attraverso il quale cittadini e imprese possano riferire sui crimini informatici subiti. La terza, infine, consiste nella messa in atto di un network di CERT nazionali, di un *Computer Emergency Response Team of the European Union* (CERT–EU) e di un sistema europeo di condivisione delle informazioni e di allarme (EISAS).

Il perseguimento di tali azioni è stato ulteriormente rafforzato dall'adozione nel 2013 della Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, che persegue l'obiettivo di introdurre

"*… norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione. Essa mira inoltre a facilitare la prevenzione di tali reati e a migliorare la cooperazione tra autorità giudiziarie e altre autorità competenti ..."* [30].

4. Le nuove strategie dell'Unione per la cybersicurezza post 2013

Sebbene le minacce alla sicurezza siano in continua evoluzione e la questione *cyber* abbia negli ultimi anni acquisito sempre maggior peso a livello globale, per quasi dieci anni (cioè dal 2003 – anno di adozione della prima strategia – al 2013) la politica comune in materia non è stata interamente attuata. Infatti, pur a seguito della Relazione del 2008 sull'implementazione della strategia europea in materia di sicurezza del 2003, non sono state realmente poste in essere delle azioni concrete e specifiche fino all'adozione nel 2013 della nuova *Strategia dell'Unione Europea per la Cybersicurezza*[31].

La Strategia del 2013 esprime la nuova visione dell'Unione sulla *cybersecurity* e sulle azioni da intraprendere al fine di garantire la sicurezza dei cittadini e degli Stati. Introduce, inoltre, la

---

30 Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, GU L 218 del 14.08.2013.

31 Com. Comm., JOIN(2013)1) del 07.02.2013, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*,.

nozione specifica di *cybersecurity*, che ricomprende l'insieme delle precauzioni e degli interventi che, al fine di preservare la disponibilità e l'integrità delle reti e delle infrastrutture e la riservatezza delle informazioni ivi contenute,

"*… si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti …*"[32].

Questa Strategia sottolinea, inoltre, il peso delle ICT, in quanto componente fondamentale della vita sociale e della crescita degli Stati Membri, oltreché risorsa critica sulla quale si basa gran parte del settore industriale. Considerato che la dipendenza di quest'ultimo e di molte infrastrutture critiche nazionali dai sistemi digitalizzati e da Internet in generale cresce esponenzialmente, è comprensibile che l'Europa debba dotarsi degli strumenti necessari per prevenire ed eventualmente contrastare gli attacchi cibernetici.

Compito dell'Unione è principalmente quello di promuovere l'applicazione di principi, norme comuni e valori validi nella dimensione sia fisica che digitale, in grado di

a) proteggere i diritti fondamentali, la libertà di espressione, i dati personali e la *privacy*

b) garantire l'accesso alla rete per tutti

c) costituire una *multi-stakeholder governance* democratica ed efficiente

d) prevedere responsabilità condivise tra tutti gli attori coinvolti.

Il rispetto di questi *"core values"* si presenta indispensabile per raggiungere le seguenti cinque priorità che la Strategia del 2013 si prefigge

"… (1) *conseguire la resilienza informatica*

(2) *ridurre drasticamente la criminalità informatica*

(3) *sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune*

(4) *sviluppare le risorse industriali e tecnologiche per la sicurezza informatica*

(5) *istituire una coerente politica internazionale del ciberspazio per l'Unione europea e sostenere i valori fondamentali dell'UE …*".

La resilienza consiste nella capacità di una rete o di un sistema di preservare le proprie capacità ed i servizi erogati anche sotto *stress* ed in caso di attacco. Una capacità di resilienza ottimale assicura l'intervento tempestivo delle autorità e, nello stesso tempo, il contenimento dei danni provocati dall'attacco attraverso il ripristino delle funzioni allo stadio iniziale (la c.d. attività di *recovery*).

---

32 *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, *cit.*, p. 3, nota 4.

La seconda priorità (la lotta al *cybercrime*) rappresenta l'obiettivo più urgente ed ambizioso, in quanto costituisce la causa più importante di perdite di danno economico, anche e soprattutto a carico del settore privato. Ridurre il *cybercrime* è necessario per garantire la protezione dei cittadini europei, di cui nel 2012 il 40% si é dichiarato preoccupato per una possibile manipolazione dei propri dati personali e il 30% per la sicurezza dei pagamenti *online*[33].

La terza priorità getta le basi della creazione di una politica di *cyberdefence* inscritta nella Politica di Sicurezza e Difesa Comune (PSDC).

La quarta sottolinea l'importanza di far progredire la tecnologia, così da gestire più agevolmente le situazioni di crisi, mentre la quinta proietta la *cybersecurity* sul piano internazionale, in considerazione del fatto che solo una proficua collaborazione a livello globale può produrre risultati concreti nella sfida contro le minacce asimmetriche provenienti dal cyber-spazio.

5. Direttiva NIS

Se fino alla Strategia del 2013 la sicurezza delle reti e delle informazioni era ancora materia di *work in progress,* la sua approvazione ha rappresentato un *turning point* che ha consentito l'elaborazione di strumenti più specifici dal punto di vista operativo.

Questo percorso ha condotto all'adozione della Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione[34] (anche conosciuta come Direttiva NIS), che rappresenta il primo insieme di regole positive dell'Unione sulla sicurezza informatica.

Al fine di raggiungere un elevato livello di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti gli Stati Membri, la Direttiva NIS stabilisce i requisiti minimi di sicurezza informatica che debbono venire adottati da parte degli operatori di infrastrutture critiche, imponendo anche dei livelli minimi di sicurezza delle tecnologie, delle reti e dei servizi digitali.

Garantendo parità di condizioni tramite norme armonizzate, la Direttiva obbligherà gli Stati Membri ad introdurre regole che impongano alle società di Internet, alle piattaforme di *e-commerce*, ai *social network* e ai servizi in materia di trasporti, banche e assistenza sanitaria, oltre agli operatori delle principali infrastrutture critiche, di promuovere un ambiente digitale sicuro e affidabile e di dotarsi di misure di sicurezza appropriate che comprendano la prevenzione dei rischi, la garanzia della sicurezza dei sistemi, delle reti e delle informazioni e la capacità di gestire gli incidenti.

Questi obiettivi verranno identificati direttamente da ogni Stato Membro, tenendo in considerazione l'essenzialità del servizio offerto per il funzionamento delle attività economiche

---

33 Commissione, *Special Eurobarometer 390: Cyber Security Report*, Luglio 2012, p. 25, consultabile al seguente LINK.

34 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, GU L 194 del 19.07.2016.

e sociali critiche, la circostanza che il servizio dipenda da sistemi informatici e se l'incidente di sicurezza rischi di produrre effetti gravi sulla fornitura di un servizio essenziale.

I tre punti chiave della Direttiva NIS sono

a) il miglioramento delle capacità di *cybersecurity* dei singoli Stati Membri

b) l'aumento del livello di cooperazione tra gli Stati Membri in materia di *cybersecurity*

c) l'obbligo di gestione dei rischi e di denuncia degli incidenti di una certa entità da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali.

La Direttiva inciderà, quindi, in maniera significativa su tutte le imprese che forniscono servizi essenziali e gestiscono le infrastrutture critiche in diversi settori, tra cui l'energia, i trasporti, le banche, la sanità e i servizi digitali. Le misure di sicurezza relative a questi soggetti prevedono alcuni elementi specifici, come la sicurezza dei sistemi e degli impianti, la gestione della continuità operativa, il monitoraggio, i test e la conformità alle norme internazionali[35].

A tutte queste entità sarà richiesta l'implementazione di *standard* minimi di sicurezza informatica.

Relativamente al miglioramento delle capacità dei singoli Stati Membri, la Direttiva prevede che ogni Stato dovrà dotarsi, qualora ne fosse sprovvisto, di una strategia nazionale di *cybersecurity* che definisca gli obiettivi, le politiche e le misure di regolamentazione. La Direttiva richiede agli Stati di designare una o più autorità competenti per il controllo della sua applicazione a livello nazionale. Un singolo punto di contatto dovrà essere designato da ognuno degli Stati Membri, con il compito di assicurare la cooperazione internazionale e quello di collegarsi con gli altri Stati attraverso i meccanismi identificati dalla Direttiva.

Ogni Stato Membro dovrà istituire uno o più CSIRT (*Computer Security Incident Response Team*) i quali si occuperanno del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci allo scopo di favorire lo scambio di informazioni.

L'*information sharing* tra gli Stati Membri è un altro pilastro della Direttiva. Infatti, le organizzazioni interessate avranno l'obbligo di segnalare tutti gli incidenti informatici gravi che subiscono ai CSIRT nazionali. In aggiunta, è stato istituito un Gruppo di Lavoro volto a facilitare i rapporti tra gli Stati Membri, composto da rappresentanti degli stessi, della Commissione e dell'ENISA. Le quattro aree di lavoro del gruppo saranno: pianificazione, guida, segnalazione e condivisione.

La Direttiva è entrata in vigore nell'agosto 2016, con inizio nel febbraio 2017 delle attività del Gruppo di Lavoro, per arrivare entro un anno ad un programma di lavoro definitivo. Entro agosto 2017 i fornitori di servizi digitali dovranno presentare i requisiti minimi di sicurezza e dotarsi di meccanismi di notifica degli incidenti. Poiché entro maggio 2018 la Direttiva dovrà essere

---

35 Nel comunicato stampa del Parlamento europeo si legge quanto segue: "*… il 6 luglio i deputati hanno approvato la Direttiva per la sicurezza delle reti e dell'informazione, che definisce un approccio comune dell'UE in materia di sicurezza informatica. Essa elenca i settori critici come l'energia, i trasporti e il settore bancario in cui le imprese dovranno assicurare di essere in grado di resistere ad un attacco informatico. Esse saranno obbligate a segnalare gravi incidenti di sicurezza alle Autorità nazionali, mentre i fornitori di servizi digitali come Amazon e Google dovranno inoltre notificare loro eventuali attacchi importanti. Inoltre, la direttiva mira a rafforzare la cooperazione in materia di sicurezza informatica tra i Paesi dell'UE …*".

implementata negli ordinamenti nazionali, gli Stati Membri hanno, quindi, a disposizione 21 mesi di tempo per adeguarsi e 6 mesi ulteriori per identificare gli operatori delle infrastrutture critiche nazionali.

6. L'interconnessione con la normativa in materia di trattamento dei dati personali e di controllo all'esportazione dei prodotti a duplice uso

Le azioni intraprese per garantire la cybersicurezza a livello unionale si integrano con le normative settoriali in materia di trattamento dei dati personali e di controllo all'esportazione dei prodotti a duplice uso. Vengono qui in gioco aspetti particolarmente sensibili, che investono la tutela nel cyberspazio dei diritti fondamentali (quali il diritto alla riservatezza, all'identità personale e alla protezione dei dati personali), consacrati nella Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (CEDU) e nella Carta dei Diritti Fondamentali dell'Unione Europea[36] (Carta UE).

6.1 La tutela dei dati personali attraverso la crittografia. Dalla Direttiva 95/46/CE al nuovo Regolamento 2016/679

In forza del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati[37], che sarà direttamente applicabile negli Stati Membri a partire dal 25 maggio 2018, il trattamento dei dati personali dovrà, da un lato, svolgersi nel rispetto dei diritti, delle libertà e della dignità dell'interessato, e, dall'altro, tutelarne la riservatezza, l'identità personale e il diritto alla protezione.

La nuova disciplina introdotta dal Regolamento (UE) 2016/679 garantisce ai cittadini un maggiore controllo sui propri dati personali, prevedendo esplicite misure sul consenso chiaro ed informato, sul trasferimento dei dati ad un altro fornitore di servizi e sul diritto di essere avvisati in caso di violazioni e incidenti.

Lo stesso Regolamento impone alle imprese l'adozione di determinate misure organizzative quali, ad esempio, la nomina in certe circostanze di un responsabile della protezione dei dati (il c.d. *Data Protection Officer*) con compiti di informazione, sorveglianza e controllo.

---

36 GU C 326 del 26.10.2012.

37 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, GU L 119 del 04.05.2016.

In tale contesto, il Regolamento assicura la cybersicurezza dei dati personali attraverso la crittografia, uno strumento di cui il titolare e il responsabile del trattamento possono avvalersi per mitigare i rischi[38].

Nello specifico, alla luce di quanto previsto dall'articolo 32, comma 1[39], il titolare e il responsabile del trattamento dovranno tenere in considerazione le metodiche della pseudonimizzazione e della cifratura nella valutazione dei concreti rischi ai quali sono esposti i dati trattati in modo da poter predisporre un livello di sicurezza adeguato.

La creazione di strutture di cifratura o pseudonimizzazione consentirà al titolare e al responsabile del trattamento, da un lato, di vedersi esonerati dal comunicare all'interessato l'eventuale violazione dei propri dati personali[40], dall'altro, di trattare dati per finalità anche differenti da quelle per cui erano stati originariamente raccolti, qualora non sia stato altresì raccolto il consenso dell'interessato o il diverso trattamento non sia di per sé consentito, sempreché la finalità perseguita sia compatibile con la prima[41].

Ad ogni modo, la crittografia non potrà costituire l'unico presidio di sicurezza informatica nella sfera di protezione dei dati personali. Tra le ulteriori misure di protezione che il titolare e il responsabile saranno chiamati ad adottare, il Regolamento menziona anche la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento e l'adozione di procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (il c.d. *penetration test*)[42].

Le criticità che recano con sé queste nuove pratiche in ordine alle esigenze di riservatezza, ai rischi connessi al danneggiamento dei dati, all'allocazione delle responsabilità e alle

---

38 In merito si veda il considerando no. 83: "*… Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale …*".

39 L'articolo 32, comma 1, statuisce quanto segue: "*… Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento ...*".

40 Si veda l'articolo 34, paragrafo 3, lett. a), del Regolamento (UE) 2016/679: "*... Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura…*".

41 Articolo 6, comma 4, lettera e) del Regolamento (UE) 2016/679.

42 Si veda in tal senso l'articolo 28 del Regolamento (UE) 2016/679.

implicazioni rispetto alla disciplina generale dei dati personali, costituiscono altrettanti fattori rilevanti in caso di esternalizzazione dei trattamenti, comportando l'obbligo positivo di nominare un responsabile del trattamento idoneo[43].

Peraltro, ove si operi in ambiti innovativi, questi aspetti andranno contemperati con il principio *privacy by design*, vale a dire, con l'implementazione della protezione dei dati personali sin dalla loro progettazione[44]. Se la protezione dei dati include risorse ascrivibili all'ambito della sicurezza informatica, come crittografia e *penetration test*, occorrerà intendere la *privacy by design* anche come *security by design*.

Fin quando il nuovo Regolamento non sarà operativo, continuerà a trovare applicazione la Direttiva 95/46/CE[45] che però non contiene riferimenti alle tecniche di cifratura per la protezione dei dati personali. Infatti, l'articolo 17 di questa si limita ad imporre al titolare l'attuazione di misure adeguate a garantire la protezione dei dati personali dalla distruzione e dalla perdita accidentali o illecite e dall'alterazione e dall'accesso non autorizzati al fine di "*… garantire un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere …*".

Quindi, nella vigenza della sola Direttiva, il diritto alla protezione dei dati personali nello spazio cibernetico viene garantito da altri strumenti giuridici dell'UE e del Consiglio d'Europa, quali la Carta UE che, con l'entrata in vigore del Trattato sul Funzionamento dell'Unione Europea (TFUE), è divenuta giuridicamente vincolante, e alla Convenzione no. 108 [46] del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione CdE) oppure a strumenti di *soft law*, quali il "Manuale sul diritto europeo in materia di protezione dei dati"[47], predisposto dall'Agenzia Europea per i Diritti Fondamentali, e il Parere no. 6/2013 reso dal Gruppo di Lavoro istituito in virtù dell'art. 29 della Direttiva 95/46/CE (Gruppo di Lavoro Art. 29)[48].

Più particolarmente, il Manuale considera la crittografia una misura utile alla pseudonimizzazione. Sebbene i dati pseudonimizzati non siano esplicitamente menzionati nella Convenzione CdE o nella Direttiva 95/46/CE, il Manuale sottolinea come la pseudonimizzazione debba essere ritenuta uno degli strumenti principali per l'ottenimento di una protezione dei dati su larga scala, soprattutto nei casi in cui evitare il loro uso risulti impossibile.

---

43 Si veda in merito il considerando 81 del Regolamento (UE) 2016/679.

44 Si veda l'articolo 25 del Regolamento (UE) 2016/679.

45 Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995.

46 "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale" del Consiglio d'Europa, Strasburgo, 28 gennaio 1981.

47 "Manuale sul diritto europeo in materia di protezione dei dati", elaborato nell'aprile 2014 dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA).

48 Parere 6/2013 sui dati aperti e sul riutilizzo delle informazioni del settore pubblico ("ISP"), adottato il 5 giugno 2013, WP207, disponiblile al seguente LINK .

Invece, nel proprio Parere, il Gruppo di Lavoro Art. 29 evidenzia come, in ordine alle procedure di pseudonimizzazione e anonimizzazione, sia necessario evitare i rischi di reidentificazione.

Poiché la determinazione del rischio può essere difficile, si ricorre al *penetration test* per rilevare le vulnerabilità esistenti. Dal momento che, però, il rischio può variare nel tempo, in base agli strumenti e alle tecniche di analisi dei dati che si hanno a disposizione, occorre rivedere periodicamente le politiche adottate, basandosi anche sulle minacce future e prevedibili.

6.2 Controlli sui prodotti a duplice uso e tecnologie di cyber-sorveglianza

Nel settembre del 2016, la Commissione ha presentato una articolata proposta[49] di modifica del Regolamento (CE) no. 428/2009 del Consiglio del 5 maggio 2009, che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso civile e militare[50], al fine di incrementare i controlli all'esportazione delle tecnologie di cyber-sorveglianza.

Più particolarmente, la proposta di modifica estende la definizione di "prodotti a duplice uso"[51] alle tecnologie di cyber-sorveglianza, in casi di gravi violazioni dei diritti umani o del diritto umanitario internazionale, o in presenza di minacce per la sicurezza internazionale o per gli interessi essenziali di sicurezza dell'Unione e dei suoi Stati Membri. Inoltre, la proposta mira a semplificare i controlli sui trasferimenti tecnologici, assicurando un alto livello di sicurezza e trasparenza per prevenire un utilizzo deviato delle esportazioni.

L'utilizzo di tecnologie di sorveglianza di origine europea ha infatti costituito un crescente problema di sicurezza nell'Unione negli ultimi anni, riflettendo la preoccupazione che tali strumenti possano formare oggetto di abuso da parte di regimi repressivi in violazione dei diritti umani o contro gli interessi della sicurezza dell'Unione.

---

49 Proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce un regime dell'Unione di controllo delle esportazioni, del trasferimento, dell'intermediazione, dell'assistenza tecnica e del transito di prodotti a duplice uso (rifusione), COM(2016) 616 final del 28.09.2016.

50 GU L 134 del 29.05.2009.

51 L'articolo 2 della proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce un regime dell'Unione di controllo delle esportazioni, del trasferimento, dell'intermediazione, dell'assistenza tecnica e del transito di prodotti a duplice uso, recita: "*... 1) "prodotti a duplice uso" sono i prodotti, inclusi il software e le tecnologie, che possono avere un utilizzo sia civile sia militare; essi comprendono: a) prodotti che possono essere impiegati per la progettazione, lo sviluppo, la produzione o l'uso di armi nucleari, chimiche e biologiche e dei loro vettori, compresi tutti i prodotti che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari; b) tecnologia di sorveglianza informatica che può essere impiegata per commettere gravi violazioni dei diritti umani o del diritto umanitario internazionale, o che può rappresentare una minaccia per la sicurezza internazionale o gli interessi essenziali in materia di sicurezza dell'Unione e dei suoi Stati membri ...*".

Per far fronte a tale minaccia, nel dicembre 2014, la Commissione aveva adottato un regolamento delegato[52] che aggiornava la legislazione europea sui prodotti a duplice uso, includendovi anche i cosiddetti "software di intrusione", che consentono l'accesso "segreto" ai sistemi di informazione e di telecomunicazione.

Quando verranno attuate, le nuove misure richiederanno alle aziende di passare attraverso processi di autorizzazione protratti e complessi per l'esportazione di tecnologie come i dispositivi di rilevamento della posizione e le apparecchiature biometriche e di sorveglianza. I produttori e i distributori di *smartphone* e di dispositivi GPS saranno tra coloro che risentiranno con maggiore probabilità di tali cambiamenti a causa della capacità dei loro prodotti di tracciare la posizione dell'utente.

7. Organi e agenzie dell'Unione

L'Unione ha progressivamente attribuito a propri organi ed agenzie specifiche competenze in materia di *cybersecurity*.

La Commissione e, più di recente, l'Alto Rappresentante per gli Affari Esteri e la Politica di Sicurezza, svolgono un ruolo di rilievo nell'elaborazione di proposte e nella preparazione di documenti riguardanti la *cybersecurity* (come ad esempio la strategia di sicurezza cibernetica del 2013). La Commissione ha inoltre promosso i primi documenti ufficiali dell'Unione in ambito *cyber.*

Una Direzione Generale della Commissione – quella per le Reti di Comunicazione, Contenuti e Tecnologia (CNET; detta DG CONNECT) – è stata dedicata allo sviluppo delle ICT, al fine di aumentare i posti di lavoro e favorire la crescita economica dell'Unione nel settore.

Un ruolo di particolare rilievo è quello svolto dall'ENISA, punto di riferimento principale per il coordinamento delle politiche *cyber* nazionali e promotore continuativo del dialogo in materia tra l'Unione e gli Stati Membri.

L'Agenzia è stata istituita dal Regolamento (CE) 460/2004[53] "*…* (a)*l fine di assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione …*"[54]. Il suo mandato, inizialmente previsto per un periodo di nove anni e sei mesi, è stato rafforzato ed esteso fino al 2020 con il Regolamento (UE) 526/2013[55].

---

52 Regolamento delegato (UE) no. 1382/2014 della Commissione, del 22 ottobre 2014, che modifica il Regolamento (CE) no. 428/2009 del Consiglio che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso, GU L 371 del 30.12.2014.

53 Regolamento (CE) 460/2004 del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, GU L 77 del 13.03.2004.

54 Ibidem, art. 1.1.

55 Regolamento (UE) 526/2013 del 21 maggio 2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004, GU L 165 del 18.06.2013.

Operativa da marzo 2004, l'Agenzia

"*… assiste la Commissione e gli Stati membri, e di conseguenza collabora con la comunità degli operatori economici, al fine di aiutarli a soddisfare i requisiti di sicurezza delle reti e dell'informazione, assicurando in tal modo il buon funzionamento del mercato interno, compresi quelli previsti dalla normativa comunitaria attuale e futura, quale la direttiva 2002/21/CE …*"[56].

Dunque, l'Agenzia ha per missione di potenziare le capacità della Commissione e degli Stati Membri di prevenire e affrontare i problemi di sicurezza delle reti e dell'informazione, dando loro assistenza e consulenza e contribuendo allo sviluppo di un alto livello di competenze settoriali. Inoltre, l'Agenzia promuove e diffonde una nuova cultura della sicurezza, affinché la *cybersecurity* venga adeguatamente trattata a livello europeo e nazionale.

Le attività principali dell'Agenzia sono quelle di coordinare l'operato degli Stati Membri nella direzione di un dialogo continuo intra-europeo, e di elaborare *best practice* e documenti finalizzati all'aggiornamento costante della *cybersecurity* in Europa con l'obiettivo di stimolare il confronto tra gli Stati Membri e consentire il consolidamento delle pratiche più avanzate[57].

L'operato dell'Agenzia è significativo anche per quanto riguarda la cooperazione in ambito *cybersecurity*. A tal fine è stato istituito un meccanismo di *incident reporting*, per incentivare gli *Internet Service Provider* (ISP) a rendere pubblici gli attacchi cibernetici subiti, coinvolgendo così tutte le autorità nazionali competenti e le Istituzioni europee interessate.

In tale contesto, la Commissione e l'ENISA adottano, congiuntamente e sulla base degli incidenti denunciati, le misure di sicurezza opportune indirizzandole alle autorità nazionali e agli ISP. Le Istituzioni europee sono al vertice della struttura operativa e dovrebbero garantire una guida sovranazionale efficiente per fronteggiare i casi specifici.

La realtà lascia, però, ancora a desiderare. Solo pochi incidenti informatici vengono infatti comunicati e, nella maggior parte dei casi, con ritardi rilevanti, perché le imprese preferiscono non rendere pubblici gli attacchi subiti per non mettere in discussione la propria reputazione. L'ENISA è anche impegnata a promuovere un cambio di mentalità, nella direzione di un modello di sicurezza informatica i cui *core values* siano fiducia, trasparenza e *information sharing*.

Nel 2012 la Commissione ha richiesto ad *Europol* di creare l'*European Cyber Crime Centre* (EC3) (di cui si è accennato in precedenza), per farne lo snodo centrale della lotta contro il crimine informatico in Europa. Il Centro è divenuto operativo da gennaio 2013 e svolge un ruolo di coordinamento delle indagini a livello europeo, offrendo supporto agli Stati Membri e alle Istituzioni nello sviluppo delle capacità operative ed analitiche relative alle attività di investigazione e alla promozione della cooperazione con i partner internazionali.

---

56 Ibidem, art. 2.1.

57 Ad esempio, di grande interesse è il Manuale *National Cyber Security Strategies*, pubblicato nel 2012, che mira a migliorare la sicurezza e la resilienza delle infrastrutture e dei servizi nazionali. Rivolto soprattutto agli Stati Membri che non si sono ancora dotati degli strumenti necessari per gestire la *cybersecurity* in modo efficace, il manuale, che si rivolge sia al settore pubblico che a quello privato, propone un modello semplificato del tipo *life-cycle* per lo sviluppo, la valutazione ed il mantenimento delle strategie nazionali. Il modello si distingue secondo due fasi: la prima di sviluppo ed esecuzione e la seconda di valutazione ed aggiustamento, nell'ambito di una struttura del tipo *"Plan-Do-Check-Act"* (PDCA).

Inoltre, l'Unione ha creato il CERT–EU (di cui si è pure accennato in precedenza), l'organo europeo deputato al monitoraggio delle minacce nel *cyber* spazio e alla risposta ad attacchi di natura cibernetica. Il CERT-EU è composto da esperti nel campo della sicurezza informatica provenienti da alcune delle maggiori Istituzioni e collabora sia con i CERT nazionali che con alcune grandi compagnie di sicurezza ICT.

Dal 2012 l'Unione si è dunque dotata di strumenti operativi per affrontare i rischi provenienti dal mondo digitale e per coordinare le attività dei singoli Stati Membri. È necessario che questi ultimi si adeguino, impegnandosi a realizzare proprie strutture coerenti e consentendo un'attività di dialogo e scambio efficiente a livello dell'Unione.

8. L'implementazione della legislazione unionale e le autorità di controllo istituite in taluni Stati Membri

Taluni Stati Membri[58] hanno implementato gli strumenti adottati dal legislatore europeo nel settore della cybersicurezza, non soltanto modificando od adottando discipline di settore, ma anche istituendo autorità specializzate, con l'obiettivo di garantire che tali normative siano effettivamente rispettate.

Come auspicato dalla Commissione, gli Stati Membri hanno adottato delle strategie nazionali di cybersicurezza, che definiscono gli obiettivi e lo *status* delle azioni intraprese a livello nazionale.

Inoltre, Germania, Regno Unito ed Italia hanno previsto specifici orientamenti per attuare le Comunicazioni del 2009 e del 2011 relative alla protezione delle infrastrutture critiche informatizzate, e per rafforzare la sicurezza e la resilienza delle infrastrutture ICT e la costituzione dei CERT. In merito, la Francia non ha ancora legiferato, mentre il Belgio non ha adottato un documento omnicomprensivo.

In particolare, la Germania ha adottato nel 2015 la *IT-Sicherheitsgesetz*[59], con annessi Regolamenti di attuazione, che stabiliscono i livelli minimi di cybersicurezza delle infrastrutture critiche e gli obblighi di conformità che gli operatori sono chiamati a rispettare. Inoltre, è previsto dalla Legge sull'Ufficio Federale per la Sicurezza delle Informazioni del 2009[60] che le autorità riportino obbligatoriamente gli incidenti di cybersicurezza all'Ufficio Federale stesso nel momento in cui sono individuati.

Ad ogni modo, tutti gli Stati Membri hanno costituito i CERT.

In attesa dell'implementazione entro il 2018 della Direttiva NIS, taluni Stati Membri hanno anche adottato misure nazionali di protezione delle informazioni segrete, tramite simulazioni di

---

58 Con l'espressione "Stati Membri" si fa qui riferimento ai Paesi che sono stati oggetto di analisi, cioé Belgio, Francia, Germania, Italia e Regno Unito.

59 Disponibile al seguente LINK.

60 La versione originale del documento è disponibile al seguente LINK, una traduzione in inglese del medesimo documento è disponibile al seguente LINK.

sicurezza e la previsione di requisiti da monitorare in caso di raggiungimento di determinati livelli di rischio.

Ancora, Italia e Regno Unito hanno istituito delle *National Incident Management Structures* (NIMS), che si occupano di notificare gli incidenti di cybersicurezza. In Italia, la struttura è controllata dalla Presidenza del Consiglio dei Ministri che, in caso di incidenti rilevanti per la sicurezza nazionale, deve attivare l'Unità di Cyber Crisi, che a sua volta mette in allerta Ministri e Governo.

Invece, con l'eccezione del Regno Unito, gli Stati Membri non hanno ancora previsto piani di coordinamento tra il settore pubblico e il settore privato per lo scambio delle informazioni relative agli incidenti di cybersicurezza e la previsione di misure di prevenzione comuni.

In merito, nel Regno Unito è stato istituito il *Centre for the Protection of National Infrastructure* (CPNI), che organizza scambi di informazioni tra il pubblico e il privato e ricerca, in partenariato con il Governo, la polizia, l'industria ed il mondo accademico, per individuare i rischi strutturali e le relative soluzioni.

La futura implementazione in tutti gli Stati Membri della Direttiva NIS condurrà ad una maggiore omogeneità, capacità di scambio di informazioni e sicurezza all'interno dei confini dell'Unione.

8.1 Regno Unito

L'autorità britannica responsabile per la sicurezza cybernetica nazionale è il *National Cyber Security Centre* (NCSC) che persegue gli obiettivi delineati nel 2015 dalla *National Security Strategy*[61], e approfonditi nella *National Cyber Security Strategy* per gli anni 2016–2021[62].

Grazie alla disponibilità di capacità sofisticate ed alla collaborazione con le altre agenzie governative, con le forze dell'ordine, con la difesa, con l'intelligence nazionale ed i servizi di sicurezza dei *partner* internazionali, l'NCSC opera per ridurre i rischi di incidenti informatici e migliorare la sicurezza e la resilienza cibernetica della nazione.

L'NCSC collabora con le organizzazioni nazionali, con i settori economici interessati e con i cittadini al fine di fornire indicazioni coerenti e autorevoli sulla cybersicurezza e per fornire sostegno nella gestione degli incidenti informatici. E' responsabile del coordinamento della risposta governativa e delle forze dell'ordine in caso di incidente informatico. Inoltre, in caso di incidenti informatici di particolare gravità, l'NCSC può effettuare comunicazioni pubbliche e fornire a cittadini e imprese raccomandazioni su come proteggersi dalla minaccia informatica.

---

61 La "*National Security Strategy and Strategic Defence and Security Review 2015*" (disponibile al seguente LINK), identifica gli attacchi cibernetici come uno dei principali rischi agli interessi nazionali e stabilisce l'intenzione del Governo di affrontare tali rischi e introdurre nuove e vigorose misure per ribadire il ruolo ledear del Regno Unito nella sicurezza cybernetica.

62 "*National Cyber Security Strategy 2016 to 2021*", disponibile al seguente link: LINK.

8.2 Italia

In Italia, la sicurezza cibernetica è monitorata dal Sistema di Informazione per la Sicurezza della Repubblica che raggruppa diversi organi e autorità responsabili di garantire la sicurezza nazionale. Nello specifico, la sicurezza cibernetica è assicurata dal Dipartimento delle Informazioni per la Sicurezza (DIS) al quale, con l'entrata in vigore della Legge 133/2012[63], è attribuita la responsabilità di coordinare le attività informative indirizzate alla protezione delle infrastrutture critiche e dello spazio cibernetico del Paese.

Il DIS raccoglie le informazioni prodotte dall'Agenzia Informazioni e Sicurezza Esterna (AISE) e dall'Agenzia Informazioni e Sicurezza Interna (AISI), e le elabora per fornire informative e risposte al Presidente del Consiglio dei Ministri. Il DIS si occupa anche della comunicazione istituzionale in materia di promozione della cultura della sicurezza.

8.3 Francia

In Francia, l'*Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) si occupa di sicurezza informatica, attuando le politiche governative in materia di sicurezza cibernetica definite dal Primo Ministro.

Fin dal 2011, anno di nascita della *Stratégie de la France en matière de défense et de sécurité des systèmes d'information*[64], l'ANSSI persegue quattro obiettivi principali

a) rendere la Francia una potenza mondiale nell'ambito della difesa cibernetica pur conservando la propria autonomia

b) garantire la libertà decisionale della Francia attraverso la protezione delle informazioni rilevanti a livello statale

c) rinforzare la cybersicurezza delle infrastrutture nazionali di importanza vitale

d) assicurare la sicurezza dello spazio cibernetico.

In seguito alla presentazione della nuova *Stratégie nationale pour la sécurité du numérique*, dal 2015 sono stati identificati ulteriori obiettivi che l'ANSSI deve assicurare come la protezione della sovranità nazionale, la fornitura di risposte adeguate agli attacchi cibernetici, informare i cittadini dei rischi informatici, rendere la sicurezza cibernetica un vantaggio concorrenziale per le imprese francesi e rafforzare anche in tal modo il ruolo internazionale della Francia.

---

63 Legge 7 agosto 2012, no. 133, Modifiche alla legge 3 agosto 2007, no. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto, GU no.186 del 10.08.2012.

64 Disponibile al seguente LINK

8.4 Germania

Il *Bundesamt für Sicherheit in der Informationstechnik* (BSI) è l'autorità federale che si occupa della cybersicurezza nazionale. Anche il BSI, come le autorità degli altri Stati Membri, investiga i rischi associati all'uso della tecnologia informatica ricercando le opportune soluzioni.

Il BSI si occupa altresì di analizzare l'evolversi dei *trend* del settore informatico e digitale e di testare, valutare e sviluppare i sistemi IT con l'eventuale collaborazione delle imprese interessate.

Consapevole del fatto che anche i sistemi informatici e di telecomunicazione sicuri sono soggetti a rischi, l'autorità tedesca si propone di contenerli anche attraverso attività di informazione rivolte ai produttori, ai distributori e ai consumatori finali dei servizi informatici.

8.5 Belgio

In Belgio l'autorità responsabile per la cybersicurezza è il *Centre pour la Cybersécurité Belgique* (CBB) istituito a norma dell'*Arrêté Royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique*[65]. Il CBB opera sotto l'autorità del Primo Ministro e con il supporto logistico e amministrativo della sua Cancelleria.

Tra gli obiettivi perseguiti dal CBB, i principali sono la supervisione, il coordinamento e il controllo dell'implementazione delle misure relative alla *cybersecurity* in Belgio, la gestione dei diversi progetti in tale ambito con modalità integrate e centralizzate, il coordinamentro tra i diversi dipartimenti governativi e tra le autorità pubbliche, il settore privato e quello scientifico, la formulazione di proposte per l'adattamento delle normative nel campo della *cybersecurity*, la gestione dell'emergenza in caso di incidenti informatici e il coordinamento delle valutazioni e certificazioni sulla sicurezza dei sistemi informatici e di telecomunicazione.

Infine, anche il CCB si occupa di informare gli utilizzatori sui rischi cibernetici connessi all'utilizzo dei sistemi informatici e di telecomunicazione.

9. Casi recenti[66]

Il tema della cybersicurezza è tornato di particolare attualità in seguito all'eclatante decisione dell'allora Presidente degli Stati Uniti, *Barack Obama*, di espellere 35 diplomatici russi dagli Stati

---

65 Disponibile al seguente LINK.

66 Per una panoramica più completa dei casi di violazione di dati verificatisi negli ultimi 10 anni si veda il seguente LINK.

Uniti, come risposta agli attacchi *hacker* subiti dal partito democratico durante la campagna elettorale che ha portato all'elezione di *Donald Trump* l'8 novembre 2016.

Fonti di *intelligence* americane avrebbero infatti ricondotto alla Russia l'origine degli attacchi informatici subiti dal partito democratico. Nello specifico, attraverso l'uso di *software* e *malware* sofisticati, presunti *hacker* russi sarebbero riusciti a sottrarre informazioni riservate dai *server* del partito per poi diffonderle *online* con grande risonanza mediatica, così influenzando indirettamente l'opinione pubblica americana e gli elettori che si apprestavano a recarsi alle urne per votare il Presidente che avrebbe sostituito Barack Obama al termine dei suoi due mandati.

Ricondurre un attacco informatico ad una fonte certa è un'operazione molto complessa. Inoltre, per tutelare le fonti e i mezzi utilizzati dall'*intelligence* per ricostruire l'incidente informatico e le sue origini, è spesso necessario non rivelare il metodo o le prove che permettono di formulare un'accusa specifica contro una nazione, un soggetto o un'organizzazione indicata come responsabile di un attacco informatico.

Una risposta dura come quella adottata dall'ex Presidente Obama con l'espulsione dei diplomatici russi lascia supporre che le prove dell'intenzione di influenzare le elezioni fossero notevoli. A sostegno di questa ipotesi vi sono anche le risultanze dell'indagine interna aperta dal partito democratico ed affidata ad un'azienda specializzata in cybersicurezza, che sembrerebbe aver ricondotto la sottrazione dei dati riservati e la successiva pubblicazione *online* degli stessi a due diversi *hacker* soprannominati "*Cozy Bear"* e "*Fancy Bear*" asseritamente legati ai servizi e all'*intelligence* militare russa.

Recentemente si è tornato a parlare molto di cyberspionaggio anche in Italia, a seguito della vicenda che ha portato all'arresto dei fratelli Giulio e Francesca Maria Occhionero, con accuse di intrusione nelle comunicazioni di numerosi personaggi, politici e non solo.

Gli Occhionero avrebbero utilizzato un *malware* per insinuarsi negli account email di politici come l'*ex* Presidente del Consiglio dei Ministri, Matteo Renzi, parlamentari come Ignazio La Russa e Fabrizio Cicchito, il Presidente della Banca Centrale Europea, Mario Draghi, o esponenti illustri del mondo cattolico e le sue istituzioni come il Cardinale Gianfranco Ravasi e l'Università Cattolica del Sacro Cuore.

Nel caso italiano, a far notizia sono stati più i nomi eccellenti delle persone vittime delle intrusioni che non le tecniche utilizzate. Diversi esperti, sulla base delle informazioni a disposizione, mettono in dubbio la capacità effettiva dei fratelli Occhionero di sottrarre informazioni riservate di alto livello e di gestire azioni di *hackeraggio* complesse, come dimostrato dal fatto che taluni account email violati sono risultati obsoleti e non più utilizzati dai loro possessori.

Tuttavia, il caso Occhionero dimostra come la prevenzione sia fondamentale per la cybersicurezza, affinché informazioni riservate non vengano sottratte, anche da criminali comuni in cerca di ingiusti guadagni rivendendo le informazioni sottratte o utilizzandole per avvantaggiarsene personalmente.

10. L'impatto della Brexit

L'approccio europeo alla *cybersecurity* ha proceduto a passi relativamente lenti, se paragonati a quelli compiuti da Stati Uniti e Regno Unito. L'Unione ha infatti registrato un notevole ritardo nella formulazione di una strategia propria, e la mancanza di una definizione di *cybersecurity* universalmente accettata ha contribuito a rendere più complessa non solo l'attività di raccordo politico, ma anche quella di ricerca.

La Brexit rischia di aumentare questo divario, oltre all'incertezza in merito alla legislazione applicabile al Regno Unito, una volta che la sua uscita dall'Unione diventerà effettiva.

Ad ogni modo, l'impatto della Brexit potrebbe essere lenito dalla circostanza che, in tale settore, le principali azioni intraprese dall'Unione sono state di *soft-law* (attraverso l'adozione di Comunicazioni), quindi non vincolanti, e relativamente ridotte.

La questione più rilevante sarà se, in attesa della Brexit, il Regno Unito implementerà nel proprio ordinamento la Direttiva NIS il cui termine di recepimento scadrà sostanzialmente nel tempo (maggio 2018) in cui l'uscita potrebbe essere già divenuta effettiva, sulla base di quanto dichiarato dalla Premier britannica *Theresa May* (secondo cui la clausola di recesso dovrebbe essere attivata entro marzo 2017) e dal capo negoziatore della Commissione *Michel Barnier* (secondo cui le negoziazioni dovrebbero concludersi entro marzo 2018).

Questa, come altre tematiche, saranno verosimilmente definite dagli accordi di uscita previsti dall'articolo 50 del Trattato sull'Unione Europea e dipenderanno dal modello di relazioni che il Regno Unito e l'Unione intenderanno costituire tra di loro in futuro. A tal proposito, la decisione della Premier britannica di imboccare la strada della *Hard Brexit* [67] rende ancora più problematica ed incerta la previsione delle future relazioni tra il Regno Unito e l'UE in questo settore.

Va da sé che, in considerazione della natura ampia e delle caratteristiche uniche delle minacce informatiche, sarebbe auspicabile un accordo che consenta al Regno Unito di continuare a partecipare alla definizione di politiche europee e strumenti comuni idonei a tutelare gli interessi dei cittadini in quel settore. In particolare, sarebbe auspicabile un accordo che consenta ai rappresentanti del Regno Unito di essere in qualche forma ancora parte degli organi dell'Unione che assicurano a livello europeo il coordinamento dell'operato degli Stati Membri nella direzione di un dialogo intra-europeo e della cooperazione in ambito *cybersecurity*, oltre che delle indagini e del monitoraggio delle minacce nel *cyber spazio*.

11. Considerazioni di sintesi

Al netto del ritardo accumulato dall'Unione di cui si è già accennato, l'approvazione di una strategia europea nel 2013 costituisce la base dell'evoluzione normativa e dell'elaborazione di

---

67 Per *Hard Brexit* si intende che il Regno Unito non adotterà alcuno dei modelli già esistenti per regolare i futuri rapporti con l'Unione e cercherà di ottenere il migliore compromesso possibile in ciascun settore, in maniera tale da continuare a rimanere un alleato strategico dell'Unione sia in termini commerciali che politici e di difesa.

strumenti operativi settoriali. La strategia, infatti, ha stabilito le linee essenziali della *cybersecurity* segnando anche una svolta dal punto di vista normativo, in quanto primo e unico documento a tutto campo predisposto dall'Unione in materia, destinato a proiettarsi nel lungo periodo.

Nonostante taluni Stati Membri abbiano adottato delle strategie nazionali, l'Unione continua a perseguire regole comuni e meccanismi di effettiva comunicazione ed azione intra-europea.

Un significativo passo avanti in tal senso è certamente costituito dall'approvazione della Direttiva NIS.

* * *

GLOSSARIO

AISE: Agenzia informazioni e sicurezza esterna

AISI: Agenzia informazioni e sicurezza interna

ANSSI: Agence nationale de la sécurité des systèmes d'information

BSI: Bundesamt für Sicherheit in der Informationstechnik

Carta UE: Carta dei diritti fondamentali dell'Unione europea

CBB: Centre pour la Cybersécurité Belgique

CEDU: Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali

CERT: Computer Emergency Response Team

CERT–EU: Computer Emergency Response Team of the European Union

CSIRT: Computer Security Incident Response Team

Convenzione: Convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale

CPNI: Centre for the Protection of National Infrastructure

DG CONNECT: Direzione Generale della Commissione per le Reti di Comunicazione, Contenuti e Tecnologia

DIS: Dipartimento delle informazioni per la sicurezza

EC3: European Cyber Crime Centre

ECI: European Critical Infrastructures

EISAS: Sistema europeo di condivisione delle informazioni e di allarme

ENISA: Agenzia Europea di Sicurezza delle Reti e dell'Informazione

FRA: Agenzia dell'Unione europea per i diritti fondamentali

Gruppo di lavoro art. 29: Gruppo di lavoro istituito in virtù dell'art. 29 della Direttiva 95/46/CE

ICT: Tecnologie dell'informazione e della comunicazione

ISP: Internet and service provider

NCSC: National Cyber Security Centre

NIMS: National Incident Management Structures

NIS: Network Information Security

PDCA: Plan-Do-Check-Act

PIC: Protezione Infrastrutture Critiche

PSDC: Politica di Sicurezza e Difesa Comune

TFUE: Trattato sul funzionamento dell'Unione europea