*i*com

Roma, 15 febbraio 2018

LA NUOVA STRATEGIA E LE REGOLE EUROPEE

Prof. Avv. Maurizio Mensi

Luiss Guido Carli - Responsabile @LawLab

SNA- Scuola nazionale dell'amministrazione

SOMMARIO

1. UE: un **quadro normativo in evoluzione**. Varie tappe. Gli strumenti giuridici
2. **Cybersicurezza e Privacy.** Strategia e regole
3. **Il «pacchetto» UE** – 2016 e 2017
4. La **Direttiva NIS** e la trasposizione
5. Il **GDPR**

PRIVACY E CYBERSICUREZZA

- Strettamente connessi, ***privacy* e sicurezza delle reti** costituiscono obiettivi codificati a livello europeo e nazionale. Per il **Codice delle comunicazioni elettroniche (d.lgs. n. 259/2003) e il Codice della *privacy* (d.lgs. n. 163/2003)** , la regolazione di settore deve garantire ***«un livello elevato di protezione dei dati personali"* e *"il mantenimento dell'integrità e della sicurezza delle reti pubbliche di comunicazione»* (CCE, Art. 13, comma 3).** Sono le stesse reti di comunicazione elettronica a dover garantire il rispetto della *privacy*.
- Le modifiche del 2012 al Codice delle comunicazioni elettroniche prevedono una nuova disposizione in tema di **sicurezza e integrità**, che affida la vigilanza al Ministero dello sviluppo economico e all'AGCom **(CCE, Art. 16 *ter*, Attuazione e controllo).**
- La **direttiva 2002/58/CE, *e-privacy***, si applica «[…] *al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione*» (art. 3, n.1) e prevede l'obbligo, per gli Stati membri, di assicurare la **riservatezza delle comunicazioni** effettuate tramite la rete pubblica di comunicazione ed i servizi di comunicazione accessibili al pubblico, vietando in particolar modo «*l'ascolto, la captazione, la memorizzazione ed altre forme di intercettazione o di sorveglianza delle comunicazioni e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di quest'ultimi* […]» **(CCE, Art. 16 *bis*, Sicurezza e integrità).**

A). STRATEGIA E REGOLE - CYBERSICUREZZA

Consiglio d'Europa

Convenzione sul *Cybercrime* (Budapest, 23 novembre 2001), in vigore dal il 1° luglio 2004 – ratif. legge 18 marzo 2008 n. 48 – coop. internaz

Unione europea

- 2001 Comunicazione sulla criminalità informatica

- 2006 Strategia per una società dell'informazione sicura

- 2013 Strategia in tema di Cybersecurity – *cyberreslience* EU (*security framework* mirato alla prevenzione dei rischi basato su cooperazione e condivisione delle informazioni / approccio USA

- Agenda Digitale 2010, Pilastro III: fiducia e sicurezza - una delle 7 iniziative faro della strategia **Europa 2020.** Contiene 101 azioni raggruppate intorno a 7 pilastri o aree prioritarie

Ec3 Europol, 11 gennaio 2013

- Comunicazione 20 giugno 2014 - strategia di sicurezza interna

Dir. 2008/114/CE *Network* fisico (energia e trasporti) – nozione di "*infrastruttura critica europea*"

Dir. 2013/40/UE Attacchi contro i sistemi di informazione
Standard minimi definizione dei reati / armonizzazione – giurisdiz.

Dir. NIS 2016/1148– ***Network and Information Security***
Settore pubblico e privato - strategia nazionale – rete di cooperazione - requisiti di sicurezza – standards – *enforcement*

IL PACCHETTO UE CYBERSICUREZZA 2017

2013 Strategia

- da allora, minaccia accresciuta e sempre più evoluta, richiede **interventi efficaci e coordinati**
- **EU** si trova nella posizione migliore per intervenire sul fronte della **cybersicurezza**, data l'ampiezza dei suoi poteri di intervento, la sua capacità d'azione, gli strumenti e le strutture di cui dispone – occorre disporre di un quadro **aggiornato**
- Gli Stati sono responsabili della **sicurezza nazionale** (rif. Art. 4, par. 2, TEU – Cons. 16 GDPR) ma la **cybersicurezza** ….

2017 "Pacchetto" UE – Pres. Juncker - **Stato dell'Unione**

IL «PACCHETTO» UE – 13 settembre 2017

1. **Comunicazione congiunta. Resilienza, deterrenza e difesa** JOIN (2017) 450 final
2. **Proposta di regolamento su ENISA** COM (2017) 477 final
3. **Comunicazione «Sfruttare al meglio la NIS»** COM (2017) 476 final e allegato
4. **Proposta di direttiva relativa alla lotta contro la frode e la falsificazione di mezzi di pagamento diversi dai contanti** COM (2017) 489 final
5. **Raccomandazione sulla risposta coordinata agli incidenti e alle crisi su larga scala della cybersicurezza (*The Blueprint*)** S (2017) 6100 final

I CONTENUTI DEL «PACCHETTO» DEL 13/9/2017

- Rafforzata l'Agenzia per la sicurezza delle reti e dell'informazione **(ENISA)**
- Creazione di un **sistema di certificazione** della sicurezza informatica a livello europeo
- Il **«Blueprint»**, un piano per rispondere rapidamente e operativamente quando si verifica un attacco informatico su larga scala
- Una rete di **centri di competenza** negli Stati membri e la proposta di un **Centro europeo di ricerca e competenza sulla cybersicurezza**
- **Un quadro per una risposta diplomatica dell'UE** comune alle attività informatiche dannose e misure per rafforzare la cooperazione internazionale sulla cybersicurezza, compreso l'approfondimento della cooperazione tra l'UE e la NATO
- Sviluppo di **competenze di alto livello per professionisti civili e militari** l'istituzione di una piattaforma di formazione e istruzione per la cyber difesa.

ENISA – L'AGENZIA DI CYBERSICUREZZA UE

Proposta di regolamento COM (2017) 477 final

A. più compiti e risorse per assistere gli Stati membri nella gestione degli attacchi informatici fornendo competenze e consulenza per gestire ***operativamente*** la cybersicurezza
B. Un **mandato rafforzato** (esteso dopo la scadenza di giugno 2020)
C. Uno **status permanente**
D. **Risorse adeguate**

Funzioni proposte

1. Sviluppo e attuazione delle politiche (rafforzare il sostegno alle istituzioni dell'UE e agli SM). Rif. Dir. NIS
2. **Cooperazione operativa** nella rete di CSIRT *(Computer Security Incident Response Team)*, di cui già fornisce il segretariato
3. Sviluppare conoscenza e diffondere informazioni (*one-stop shop* - *InfoHub*- per informazioni sulla cybersicurezza)
4. ***Capacity building*** (supporto agli Stati membri)
5. Attività correlate al mercato nell'ambito del quadro di **certificazione della cybersicurezza** (preparazione dei progetti di schemi di certificazione dell'UE)

B). STRATEGIA E REGOLE – DATA PRIVACY

Unione europea

- Direttiva 95/46/CE: obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

- Direttiva 2002/58 *e-privacy*, a breve sarà sostituita da un Regolamento, proposto il 10/1/2017

Entrambe trasposte in Italia dal **Codice privacy (d.lgs. 196 del 2003)**

Il «Pacchetto Privacy» del 2016

→ **Obiettivo: OVVIARE ALLA FRAMMENTAZIONE**

1. **Regolamento 2016/679**
2. **Direttiva *Enforcement* 2016/680** (trasp. 6 maggio 2018), che regola il trattamenti dei dati personali nei settori della prevenzione, contrasto e repressione dei crimini
3. **Direttiva PNR 2016/681** (trasp. 25 maggio 2018) sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi

Consiglio d'Europa

Convenzione COE n. 108/1981 (in corso di revisione) sul trattamento automatizzato dei dati personali - *standard* universale - meno prescrittiva e più focalizzata sui diritti umani (ratif. Legge 21 febbraio 1989, n. 98)

UN QUADRO ADEGUATO E TEMPESTIVO ?

La prima regola della cybersicurezza, per imprese, PA e cittadini / consumatori, é il rispetto delle regole

Quali ? Stabilite da chi ? Complete e aggiornate ? Rischi di sovrapposizione …

Cantiere normativo in corso, a livello internazionale, europeo e nazionale – singolare congiuntura

Codice Privacy (d.lgs. n. 196 del 2003), quali norme applicabili dopo l'entrata in vigore del Regolamento europeo

- **Sfera pubblica e privata**
- Concetto di **sicurezza nazionale** (tema di competenza nazionale - considerato 16 GDPR - Art. 4, par. 2, TEU).

LA DIRETTIVA NIS - PREMESSE

- **Riconoscimento di un insufficiente livello di protezione.**
- Rischio per il mercato interno– sistemi interconnessi –incidenti superano confini nazionali – interventi regolamentari degli SM non coordinati dannosi – alcuni settori chiave a supporto del mercato interno: **banche – borse valori – energia (generazione, trasmissione e distribuzione) - trasporti - salute**
- **Lacune nell'attuale assetto regolamentare – *Data controllers*** (banche, ospedali) sono costretti a porre in essere misure di sicurezza proporzionate al livello di rischio che fronteggiano, ma sono tenute a **notificare le violazioni di sicurezza** soltanto nel caso in cui siano compromessi dati personali.
- **La Dir. 2008/114 sulle Infrastrutture critiche europee** riguarda soltanto **trasporti ed energia** e non pone alcun obbligo agli operatori di segnalare danni ai sistemi di sicurezza o di cooperare.

ELEMENTI CHIAVE

Obiettivo della **Dir. 2016/1148:** un **livello elevato di sicurezza** per i sistemi, le reti e le informazioni comune a tutti i Paesi membri dell'UE, garantendo parità di condizioni tramite norme armonizzate e lo scambio regolare di informazioni tra **settore privato e pubblico.** Impone un livello minimo di sicurezza per le tecnologie, le reti e i servizi digitali in tutti gli Stati membri.

I **tre punti** chiave della direttiva NIS sono:

1. Migliorare le capacità di **cyber security** dei singoli Stati dell'Unione;
2. Aumentare il livello di **cooperazione tra gli Stati dell'Unione e promuovere una cultura della sicurezza e della gestione dei rischi**;
3. **Obbligo di gestione dei rischi** e di comunicare gli incidenti di una certa entità da parte degli **operatori di servizi essenziali e dei fornitori di servizi digitali.**

La direttiva lascia impregiudicata la possibilità, per ciascuno Stato membro, di adottare le misure necessarie per assicurare **la tutela degli interessi essenziali della sua sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati.**

CRONOLOGIA

- **6 luglio 2016**: adozione
- **8 agosto 2016:** entrata in vigore
- **9 maggio 2018**: trasposizione
- **9 novembre 2018**: identificazione degli OSE
- **2019:** la **Commissione europea** valuta la coerenza dell'identificazione degli operatori di servizi essenziali da parte degli Stati membri.
- **2021:** **la Commissione** riesamina il funzionamento della direttiva con particolare attenzione alla cooperazione strategica e operativa degli Stati e la sua applicazione.

LA TRASPOSIZIONE – I PUNTI CHIAVE

Comunicazione (CE COM (2017) 476 def) e allegato

Le strategie nazionali

Portata, contenuto, procedure per una strategia nazionale

Autorità nazionali competenti (approccio decentralizzato: Svezia, Austria, Finlandia / centralizzato: Francia) – Varie tappe per gli Stati membri - **CSIRT** - Punto di contatto unico - ***Best practice*** tratte dalla precedente esperienza in materia di protezione delle infrastrutture critiche informatizzate (CIIP) - **Studio ENISA 2016**

5 TAPPE

1. definizione dei principi guida e degli obiettivi strategici, che dovrebbero essere **specifici, misurabili, realizzabili, realistici e vincolanti nel tempo (SMART)**
2. elaborazione dei contenuti della strategia
3. sviluppo della ***governance***. Ruoli e responsabilità, processo decisionale
4. Predisposizione e revisione del progetto di strategia, mediante analisi dei punti di forza e debolezza, opportunità e minacce **(SWOT)**
5. Adozione formale

STRATEGIA NAZIONALE

La strategia nazionale deve:

1. definire obiettivi strategici, politiche adeguate, misure di regolamentazione.
2. comprendere, le priorità nazionali, la *governance*, l'individuazione di misure proattive, di risposta e di *recovery*; sensibilizzazione, formazione ed istruzione; incentivazione della **cooperazione tra settore pubblico e settore privato**; lista degli attori coinvolti nella attuazione della strategia.

Gli Stati devono designare **una o più autorità competenti** per il controllo dell'applicazione della direttiva stessa a livello nazionale **(Art. 8, par. 1).**

Un singolo punto di contatto per assicurare la **cooperazione internazionale** e di collegarsi con gli altri Stati attraverso meccanismi di cooperazione identificati della direttiva stessa.

Uno o più **CSIRT (Computer Security Incident Response Team)** responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti, fornire analisi sui rischi e incidenti e aumentare il grado di consapevolezza. Fondamentale è la **cooperazione internazionale e l'information sharing**

LA TRASPOSIZIONE – PUNTI CHIAVE

1. **Efficacia dell'attuazione e applicazione** - oltre i requisiti minimi ed i settori coperti (All. II e III) – PA ? – **Art. 3, Armonizzazione minima**
2. **Potenziamento delle capacità nazionali di CSIRTS -** Risorse umane e finanziarie adeguate
3. **Coerenza del processo di identificazione degli OSE** – 6 domande - Settori aggiuntivi - Giurisdizione - *Lex specialis*
4. **Approcci allineati relativi ai requisiti di sicurezza e di notifica degli incidenti per gli OSE**

I SOGGETTI RIGUARDATI

- La cooperazione tra i vari enti dei singoli Stati membri è un aspetto fondamentale della direttiva NIS. **Un gruppo di cooperazione** facilita i rapporti tra gli Stati membri e aumenta la fiducia, composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA.
- **GLI OPERATORI DI SERVIZI ESSENZIALI** sono aziende pubbliche o private che **hanno un ruolo importante per la società e l'economia**, identificati direttamente da ogni Stato membro, all'interno dei seguenti ambiti: **energia, trasporti, banche e società finanziarie, salute, acqua ed infrastrutture digitali.**
- **I criteri per l'inclusione nella lista** sono: **l'essenzialità del servizio offerto per il mantenimento di attività critiche in ambito economico e sociale; il servizio dipende da sistemi informatici; se l'incidente di sicurezza rischia di avere effetti gravi e significativi sulla fornitura di un servizio essenziale.**
- Queste entità devono dotarsi di **misure di sicurezza appropriate** e notificare all'autorità nazionale competente **gravi incidenti di sicurezza** secondo parametri di numero di utenti coinvolti, durata dell'incidente e diffusione geografica.
- **Le misure di sicurezza** richieste comprendono: prevenzione dei rischi; garanzia della sicurezza dei sistemi, delle reti e delle informazioni; capacità di gestire gli incidenti.
- **I FORNITORI DI SERVIZI DIGITALI** sono identificati nei motori di ricerca, gli operatori del mercato *on line* e di servizi *cloud*.

IL PROCESSO DI IDENTIFICAZIONE

La **direttiva NIS** non indica quali particolari entità sono considerate come OSE, ma fornisce i **criteri** che gli Stati membri dovranno applicare per effettuare il processo di identificazione.

Gli Stati membri devono garantire che entità che svolgono un ruolo analogo nel mercato interno siano **identificati in modo coerente** come operatori di servizi essenziali in altri Stati membri.

Nei casi in cui gli **operatori di servizi essenziali** forniscono servizi essenziali in due o più Stati membri, è essenziale sia raggiunto **un accordo tra Stati membri** per evitare una diversa regolamentazione e trattamento della stessa entità in giurisdizioni di diversi Stati membri.

Devono essere **stabiliti sul territorio nazionale** (effettivo e reale esercizio di un'attività in loco anche mediante accordi commerciali) a prescindere dalla loro veste giuridica.

INCLUSIONE DI SETTORI AGGIUNTIVI

Tenendo conto dei **requisiti di armonizzazione minima** (Art. 3 Dir. NIS), gli Stati membri sono liberi di estendere gli obblighi di sicurezza e di notifica (in termini di requisiti di sicurezza e obblighi di notifica), alle entità appartenenti ad altri settori. Vari Stati membri stanno valutando se includere alcuni dei seguenti settori aggiuntivi:

- **Pubbliche amministrazioni**
- **Settore postale**
- **Settore alimentare**
- **Industria chimica e nucleare**
- **Settore ambientale**
- **Protezione civile**

LA NOTIFICA DELL'INCIDENTE

Gli OSE devono **notificare ogni incidente** che abbia **un impatto "*rilevante*" sulla "*continuità dei servizi essenziali*"** prestati, da valutarsi in base a: **(i)** il numero di utenti interessati dalla perturbazione del servizio essenziale; **(ii)** la durata dell'incidente; **(iii)** la diffusione geografica relativamente all'area interessata dall'incidente) **(Art. 14, comma 4).**

I FSD devono sono chiamati a **notificare ogni incidente** che abbia **un impatto "*sostanziale*" sulla "*fornitura di un servizio digitale*",** da valutarsi in base a**: (i)** del numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi**; (ii)** della durata dell'incidente; **(iii)** della diffusione geografica relativamente all'area interessata dall'incidente; **(iv)** della portata della perturbazione del funzionamento del servizio; **(v)** della portata dell'impatto sulle attività economiche e sociali **(Art. 16, comma 4).**

La NIS prevede anche una **notifica su base volontaria** degli incidenti,che può essere effettuata dai **soggetti diversi dagli OSE e dai FSD.**

LEX SPECIALIS

Il rapporto tra la direttiva NIS e altre normative (Art. 1, par. 7)

Le disposizioni sugli obblighi di sicurezza e / o di notifica per i fornitori di servizi digitali o gli operatori di servizi essenziali ai sensi della NIS **non sono applicabili** se una **legislazione di settore** prevede requisiti di sicurezza e / o notifica, che sono equivalenti ai corrispondenti obblighi della direttiva NIS.

ESEMPIO - Provider di telecomunicazioni e fornitori di servizi fiduciari

I requisiti di sicurezza e di notifica previsti dalla dir. non si applicano ai fornitori che sono soggetti ai requisiti della **dir. 2002/21/CE**, i cui Artt. 13 bis e 13 ter si applicano alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico.

PRIVACY - L'INTERVENTO NORMATIVO UE

25 gennaio 2012: proposta della Commissione europea **in materia di protezione dei dati**

27 aprile 2016: approvato il ***Pacchetto Privacy***:

A. **Regolamento 2016/679** che stabilisce un quadro generale dell'Unione per la protezione dei dati, che sostituisce la **Dir. 95/46.**

B. **Direttiva 2016/680** sulla protezione delle persone fisiche con riguardo al trattamento dei dati ai fini di prevenzione, indagine, accertamento o perseguimento dei reati e nell'ambito delle connesse attività giudiziarie.

C. **Direttiva 2016/681** sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi

4 maggio 2016: pubblicazione in Gazzetta UE.

A partire dal ventesimo giorno dalla pubblicazione (24 maggio), **due anni di tempo** per allineare la normativa nazionale alle nuove prescrizioni introdotte dal Regolamento, che diventerà definitivamente **applicabile** dal **25 maggio 2018.**

Il **regolamento** è considerato "*lo strumento giuridico più appropriato per definire un livello comune di protezione dei dati in tutta l'Unione. L'applicabilità diretta di un regolamento* ***ridurrà la frammentazione giuridica*** *e fornirà* ***maggiore certezza del diritto*** *attraverso l'introduzione di un* ***insieme armonizzato di regole di base***".

PRINCIPALI ASPETTI DEL GDPR

A. Ambito di applicazione soggettivo
B. Nozione ampia di dati personali (es. genetici, biometrici) e di trattamento
C. Ambito di applicazione territoriale ampliato
D. Responsabilizzazione
E. Notifica di violazione dei dati
F. Registro dei trattamenti (titolari, responsabili, incaricati, interessati, finalità, ecc.) per documentare gli adempimenti e le procedure relative a ciascun trattamento
G. Informativa (dettagliata)
H. Responsabile della protezione dati (*Data Protection Officer*)
I. Diritto all'oblio
J. Portabilità dei dati
K. Valutazione di impatto sulla protezione dei dati
L. Misure di sicurezza
M. Responsabilità e *data governance*
N. Sanzioni rafforzate (fino a 20 milioni Euro o 4 % fatturato anno precedente)
O. Sportello unico
P. Margini di manovra per il legislatore nazionale

GDPR E CYBERSICUREZZA

Unica previsione in tema di cybersicurezza del GDPR

Sezione 2 - Sicurezza dei dati personali

Articolo 32, Sicurezza del trattamento

1. 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.**

[...] 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi presentati dal trattamento** che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

IL LEGISLATORE NAZIONALE

Il Reg. consente agli **Stati membri** di mantenere o introdurre **previsioni più specifiche** con riferimento al trattamento di **dati sensibili**, per il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un **compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento **(Cons. 10 e 19).**

In particolare gli Stati membri possono prevedere **deroghe** rispetto a quanto stabilito dal Reg. con riferimento ai trattamenti per **scopi giornalistici, all'accesso del pubblico ai documenti ufficiali, al trattamento dei dati nell'ambito del rapporto di lavoro**.

Il Reg. non si applica alle attività riguardanti **la sicurezza nazionale** né al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla **politica estera e di sicurezza comune dell'Unione** **(Cons. 16).**

ESEMPIO DI APPLICAZIONE GDPR - NIS

Sebbene il GDPR e la direttiva NIS abbiano un **diverso oggetto e ambito di applicazione**, le due normative trovano **contemporanea applicazione** qualora un **incidente relativo alla sicurezza informatica determini anche una violazione di dati personali.**

In tal caso, coloro che erogano il servizio interessato dall'incidente debbono soddisfare gli obblighi di notifica imposti da ambedue le normative e quindi procedere sia con una notifica per l'incidente ai sensi della NIS sia con una notifica per la violazione dei dati personali prevista dal RGPD (Artt, 33-34).