La direttiva NIS e gli scenari futuri per gli operatori di Infrastrutture Critiche

Dr. Ing. Luisa Franchina

Presidente AIIC

Indice dei Contenuti

Introduzione

Lo scorso 6 luglio 2016 l'Unione Europea ha approvato una **Direttiva comunitaria per la sicurezza delle reti e dell'informazione**, nota anche come **Direttiva NIS** (Network and Information Security), che stabilisce i requisiti minimi per la sicurezza informatica per gli operatori di servizi essenziali e servizi digitali.

- Le reti, i sistemi ed i servizi informativi svolgono un **ruolo vitale nella società**. È essenziale che essi siano **affidabili e sicuri** per le attività economiche, sociali ed in particolare ai fini del funzionamento del mercato interno.

- Eventuali **incidenti a carico della sicurezza** rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi.

- Le reti e i sistemi informativi, e in prima linea internet, svolgono un **ruolo essenziale nell'agevolare i movimenti transfrontalieri** di beni, servizi e persone. Gravi perturbazioni di tali sistemi, intenzionali o meno e indipendentemente dal luogo in cui si verificano, possono ripercuotersi su singoli Stati membri e avere conseguenze in tutta l'Unione.

- Per una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi è **necessario un approccio globale a livello di Unione**, che contempli disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali.

- La presente direttiva **si applica sia agli operatori di servizi essenziali che ai fornitori di servizi digitali** in modo da coprire tutti i relativi rischi e incidenti.

- È opportuno tuttavia che **gli obblighi imposti agli operatori di servizi essenziali e ai fornitori di servizi digitali non si applichino alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico**, poiché tali imprese sono soggette a specifici obblighi di sicurezza e integrità previsti dalla direttiva *2002/21/CE* del Parlamento europeo e del Consiglio.

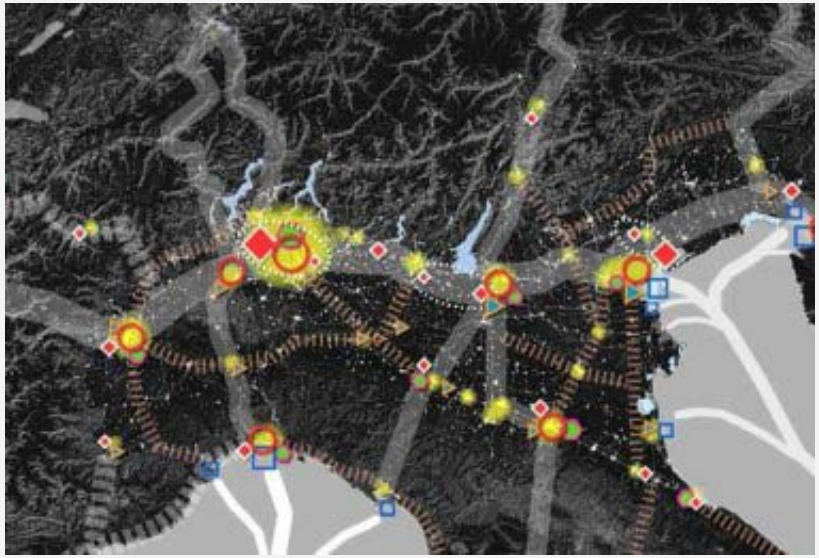
- Nelle slide successive saranno prese in esame le **definizioni e gli obblighi** degli operatori delle seguenti categorie di Servizi:

1. **Servizi Essenziali**
2. **Servizi Digitali**
3. **Servizi di Comunicazione Elettronica**

Categoria 1/ Servizi essenziali – Definizioni 1/2

- Si definisce **«operatore di servizi essenziali»** un soggetto pubblico o privato che soddisfa i seguenti criteri:

- Un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
- La fornitura di tale servizio dipende dalla rete e dai sistemi informativi;
- Un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.



Categoria 1/ Servizi essenziali – Definizioni 2/2

❑ Gli effetti negativi rilevanti verranno valutati secondo i seguenti indicatori:

- il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;
- la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;
- l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;
- la quota di mercato di detto soggetto;
- la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;
- l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

Operatori di servizi essenziali – Criteri di identificazione (1 di 2)

- elenco dei servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali.
- **consultazioni reciproche**.
- **riesame** almeno ogni due anni.
- **favorire un approccio coerente**.

Operatori di servizi essenziali – Criteri di identificazione (2 di 2)

❑ Trasmissione alla Commissione.

Tali informazioni comprendono, come minimo:

a) **Le misure nazionali** che rendono possibile l'identificazione degli operatori di servizi essenziali.

b) **L'elenco dei servizi**;

c) **Il numero degli operatori** di servizi essenziali identificati per ciascun settore e un'indicazione della loro importanza in relazione a tale settore;

d) **Le soglie**, ove esistono.

Operatori di Servizi essenziali – Settori e sottosettori

❑ **operatori di servizi essenziali** :

- **Settore Energia**
- **Settore Trasporti**
- **Settore bancario**
- **Infrastrutture dei mercati finanziari**
- **Settore sanitario**
- **Fornitura e distribuzione di acqua potabile**

Operatori di Servizi essenziali - Settore Energia

a) Energia elettrica

- **Impresa elettrica**;
- **Gestori del sistema di distribuzione**;
- **Gestori del sistema di trasmissione**;

b) Petrolio

- **Gestori di oleodotti**;
- **Gestori di impianti** di produzione, raffinazione, trattamento, deposito e trasporto di petrolio;

c) Gas

- **Imprese fornitrici**;
- **Gestori del sistema di distribuzione**;
- **Gestori del sistema di trasmissione**;
- **Gestori dell'impianto di stoccaggio**;
- **Gestori del sistema GNL**;
- **Imprese di gas naturale**;
- **Gestori di impianti di raffinazione** e trattamento di gas naturale.

Operatori di Servizi essenziali - Settore Trasporti (1 di 2)

a) Trasporto aereo

- **Vettori aerei**;
- **Gestori aeroportuali**;
- **Operatori** attivi nel controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo.

b) Trasporto ferroviario

- **Gestori dell'infrastruttura**;
- **Imprese ferroviarie**;

Operatori di Servizi essenziali - Settore Trasporti (2 di 2)

c) Trasporto per vie d'acqua

- **Compagnie di navigazione** per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci;

- **Organi di gestione dei porti**, compresi i relativi impianti portuali, e soggetti che gestiscono opere e attrezzature all'interno di porti;

- **Gestori di servizi di assistenza** al traffico marittimo.

d) Trasporto su strada

- **Autorità stradali**;

- **Gestori di sistemi di trasporto** intelligenti;

Operatori di Servizi essenziali - Settore bancario

- **Enti creditizi**.

Operatori di Servizi essenziali - Infrastrutture dei mercati finanziari

- **Gestori delle sedi di negoziazione**
- **Controparte centrale**.

Operatori di Servizi essenziali - Settore sanitario

- Istituti sanitari (compresi ospedali e cliniche private)
- **Prestatori di assistenza sanitaria**

Operatori di Servizi essenziali - Fornitura e distribuzione di acqua potabile

Fornitori e distributori di acque destinate al consumo umano, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è solo una parte della loro attività generale di distribuzione di altri prodotti e beni che non sono considerati servizi essenziali

Operatori di servizi essenziali - Obblighi in materia di sicurezza

- Gli obblighi in materia di sicurezza e notifica degli incidenti per gli **operatori di servizi essenziali** prevedono che questi:

1) adottino misure tecniche e organizzative adeguate e proporzionate alla **gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi** che usano nelle loro operazioni;

2) adottino misure adeguate per **prevenire e minimizzare l'impatto di incidenti** a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurarne la continuità;

3) **notifichino** all'autorità competente o al CSIRT **gli incidenti aventi un impatto rilevante** sulla continuità dei servizi essenziali prestati;

- **L'autorità competente o il CSIRT:**

1) **informa l'altro o gli altri stati membri interessati** se l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali in quello Stato membro;

2) **può informare il pubblico** in merito ai singoli incidenti, dopo aver consultato l'operatore notificante dei servizi essenziali;

- Le autorità competenti possono elaborare e adottare orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti.

Operatori di servizi essenziali - Parametri per determinare la rilevanza di un incidente

- Per determinare la rilevanza dell'impatto di un incidente si tiene conto dei seguenti parametri:

1) **Il numero di utenti** interessati dalla perturbazione del servizio essenziale;
2) **La durata dell'incidente**;
3) **La diffusione geografica** relativamente all'area interessata dall'incidente.

Categoria 2/ Servizi digitali - Definizioni

❑ Si definisce **«servizio digitale»** qualsiasi servizio, vale a dire qualsiasi servizio della società dell'informazione prestato normalmente dietro retribuzione, ovvero qualsiasi servizio a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi, di uno dei seguenti tipi:

- **Mercato online,** servizio digitale che consente ai consumatori e/o ai professionisti, di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online;
- **Motore di ricerca online,** servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto;
- **Servizi nella nuvola (cloud computing),** servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.

❑ Si definisce **«fornitore di servizio digitale»**, qualsiasi persona giuridica che fornisce un servizio digitale.

Fornitori di servizi digitali - Obblighi in materia di sicurezza (1 di 2)

- **Gli obblighi** in materia di sicurezza e notifica degli incidenti per i **fornitori di servizi digitali** prevedono che questi:

1) **identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano**

Tali misure tengono conto dei seguenti elementi:

a) la sicurezza dei sistemi e degli impianti,

b) il trattamento degli incidenti,

c) la gestione della continuità operativa,

d) la funzione di monitoraggio, audit e test,

e) la conformità con le norme internazionali.

1) **adottino misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali**, al fine di assicurare la continuità di tali servizi;

2) **notifichino senza indebito ritardo all'autorità competente o al CSIRT qualsiasi incidente avente un impatto rilevante sulla fornitura di un servizio** che essi offrono all'interno dell'Unione;

Fornitori di servizi digitali - Obblighi in materia di sicurezza (2 di 2)

- **L'autorità competente o il CSIRT**:

1) **tutelano**, **la sicurezza e gli interessi commerciali del fornitore del servizio digitale nonché la riservatezza delle informazioni fornite;**

2) **possono informare il pubblico riguardo ai singoli incidenti** o chiedere al fornitore di servizi digitali di provvedervi.

- L'operatore stesso notifica qualsiasi impatto rilevante per la continuità di servizi essenziali dovuto ad un incidente a carico di una eventuale terza parte.

Servizi digitali - Parametri per determinare la rilevanza di un incidente

- Nella **determinazione della rilevanza degli effetti negativi di un incidente sulla fornitura dei servizi**, gli Stati membri tengono conto almeno dei seguenti fattori intersettoriali:

1. **il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi;**
2. **la durata dell'incidente;**
3. **la diffusione geografica relativamente all'area interessata dall'incidente;**
4. **la portata della perturbazione del funzionamento del servizio;**
5. **la portata dell'impatto sulle attività economiche e sociali.**

- Al fine di determinare se un incidente avrebbe effetti negativi rilevanti, gli Stati membri tengono altresì conto, ove opportuno, di fattori settoriali.

- Le autorità competenti o i gruppi di intervento per la sicurezza informatica in caso di incidente e/o **Data Breach** (violazioni di dati personali) dovrebbero ricevere le notifiche di incidenti. I punti di contatto unici non dovrebbero ricevere direttamente le notifiche di incidenti, a meno che non fungano anche da autorità competente o da un **CSIRT** (**Computer Security Incident Response Team**). Un'autorità competente o un CSIRT dovrebbe tuttavia poter incaricare il punto di contatto unico di trasmettere notifiche di incidenti ai punti di contatto unici degli altri Stati membri interessati.

Categoria 3/ Servizi di Comunicazione Elettronica

La **direttiva *2009/140/CE*** del Parlamento Europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva *2002/21/CE* che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, «**istituisce un quadro normativo armonizzato per la disciplina dei servizi di comunicazione elettronica**, delle reti di comunicazione elettronica, delle risorse e dei servizi correlati e per taluni aspetti delle apparecchiature terminali onde facilitare l'accesso agli utenti disabili; definisce le funzioni delle autorità nazionali di regolamentazione ed istituisce le procedure atte a garantire l'applicazione armonizzata del quadro normativo nella Comunità».

Rif: Articolo 1, paragrafo 1, della direttiva 2009/140/CE del Parlamento Europeo e del Consiglio del 25 novembre 2009.

Servizi di Comunicazione Elettronica – Definizioni (1 di 2)

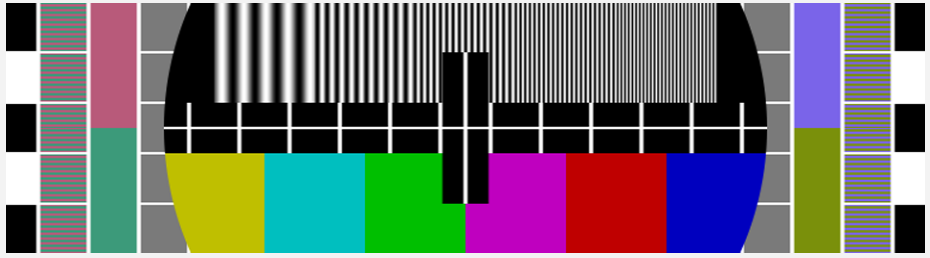
- Si definiscono **«servizi di comunicazione elettroniche»**, i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica;

- Si definisce «**operatore»** un'impresa che è autorizzata a fornire una rete pubblica di comunicazioni, o una risorsa correlata;

Rif: Direttiva 2009/140/CE del Parlamento Europeo e del Consiglio del 25 novembre 2009 (recante modifica della Direttiva 2002/21/CE) e dlgs n. 70 del 28 maggio 2012 (recante codice delle comunicazioni elettroniche in attuazione delle direttive 2009/140/CE in materia di reti e servizi di comunicazione elettronica, e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata).

- Si definiscono **«fornitori di servizi di comunicazione elettronica accessibili al pubblico»** quei soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione.

Rif: Garante per la protezione dei dati personali nel provvedimento – Sicurezza dei dati di traffico telefonico e telematico del 17 gennaio 2008, in riferimento al termine «fornitore» contenuto nell'articolo 132 del d.lgs 196/2003.



Servizi di Comunicazione Elettronica – Definizioni (2 di 2)

- **Mercati transnazionali**: mercati situati in piu' di uno Stato membro, che comprendono l'Unione Europea o una parte considerevole dei suoi Stati membri.
- **Reti di comunicazione elettronica**, i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- **Reti pubbliche di comunicazioni:** una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti.
- ***Risorse correlate:*** *i servizi correlati, le infrastrutture fisiche e le altre risorse o elementi correlati ad una rete di comunicazione elettronica o ad un servizio di comunicazione elettronica che permettono o supportano la fornitura di servizi attraverso tale rete o servizio, ovvero sono potenzialmente in grado di farlo, ivi compresi tra l'altro gli edifici o gli accessi agli edifici, il cablaggio degli edifici, le antenne, le torri e le altre strutture di supporto, le guaine, i piloni, i pozzetti e gli armadi di distribuzione-*

Fornitori di servizi di comunicazione elettronica accessibile al pubblico Obblighi in materia di sicurezza (1 di 3)

- Gli obblighi in materia di sicurezza e notifica degli incidenti per i **fornitori di servizi di comunicazione elettronica** prevedono che questi:

1) **adottino misure tecniche e organizzative adeguate al rischio esistente**, per salvaguardare la sicurezza dei propri servizi;
2) **garantiscano che i dati personali siano accessibili solamente al personale autorizzato** per fini legalmente autorizzati;
3) **garantiscano la protezione dei dati relativi al traffico e all'ubicazione e degli altri dati personali archiviati o trasmessi dalla distruzione accidentale, da perdita o alterazione anche accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati, illeciti,** nonché assicurino l'attuazione di una politica di sicurezza;
4) **adottino**, congiuntamente con il fornitore della rete pubblica di comunicazioni, **le misure riguardanti la sicurezza della rete**, quando la sicurezza del servizio o dei dati personali richiedano anche l'adozione di misure che riguardano la rete stessa;
5) **informino i contraenti e, ove possibile, gli utenti, se sussiste un rischio di violazione della sicurezza della rete**, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure, che il fornitore della rete stesso è tenuto ad adottare tutti i possibili rimedi ed i costi presumibili.

Fornitori di servizi di comunicazione elettronica accessibile al pubblico Obblighi in materia di sicurezza (2 di 3)

- Gli adempimenti per i **fornitori di servizi di comunicazione elettronica** conseguenti ad una violazione di dati personali prevedono che questi:

1) **comunichino** senza indebiti ritardi **detta violazione all'Autorità Garante**.
2) **comunichino, quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona, agli stessi, senza ritardo, l'avvenuta violazione.** Tale comunicazione non è obbligatoria unicamente nel caso venga dimostrato all'Autorità Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione.
3) **tengano un aggiornato inventario delle violazioni di dati personali,** ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in modo da consentire all'Autorità Garante di verificare il rispetto delle disposizioni del presente articolo. Nell'inventario figurano unicamente le informazioni necessarie a tal fine.

- Nel caso in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico affidi l'erogazione del predetto servizio ad altri soggetti, gli stessi **sono tenuti a comunicare al fornitore** senza indebito ritardo tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti sopra elencati.

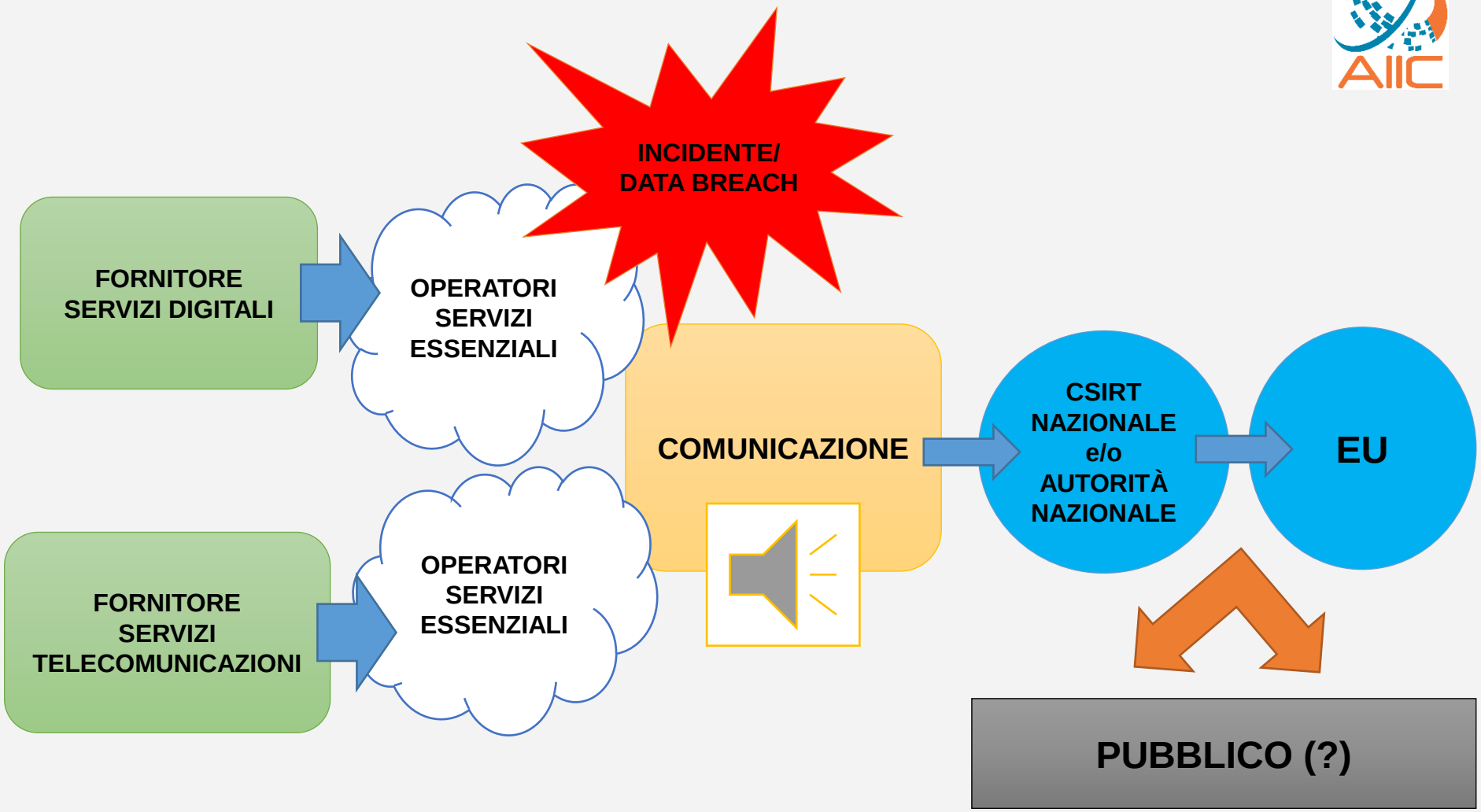
Fornitori di servizi di comunicazione elettronica accessibile al pubblico Obblighi in materia di sicurezza (3 di 3)

- Gli adempimenti per **l'Autorità Garante** conseguenti ad una violazione di dati personali prevedono che questa:

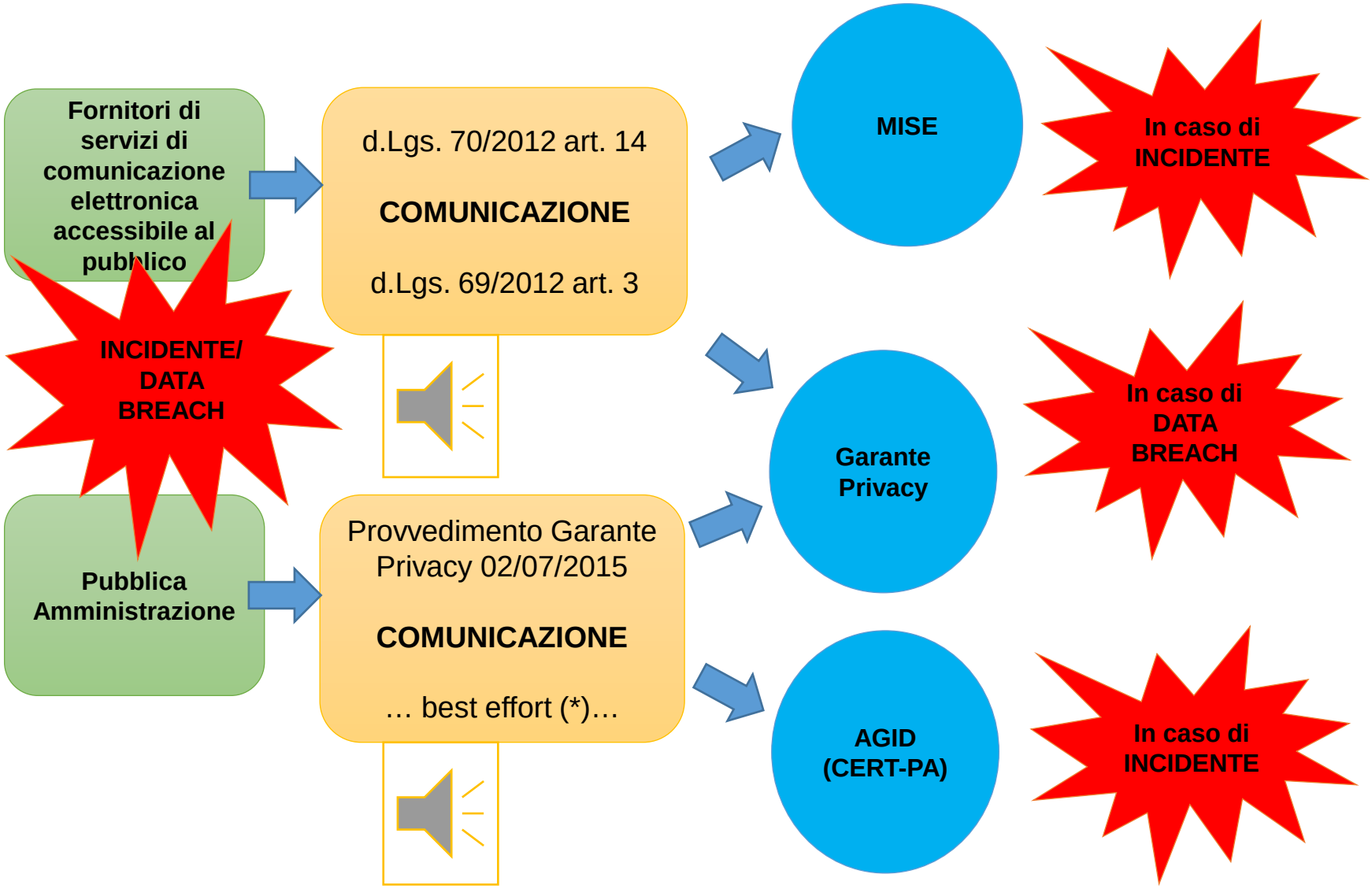
1) **obblighi il fornitore,** nel caso non vi abbia già provveduto lo stesso e considerate le presumibili ripercussioni negative della violazione, **a comunicare al contraente o ad altra persona l'avvenuta violazione.** Tale comunicazione contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione al Garante descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio.

2) **possa emanare, con proprio provvedimento, orientamenti e istruzioni in relazione circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di daalle ti personali,** al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione**.**

Schema del flusso informativo NIS



Schema del flusso informativo



(*) A differenza delle altre notifiche che sono OBBLIGATORIE, in questo caso, l'obbligo dovrebbe essere inserito all'interno delle Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni dell'Agid che sono in corso di emanazione (in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015).

Futuri…?

1. Chi realizza la NIS?
2. Stiamo affrontando il tema ICN?
3. Stiamo proteggendo le ICN?
4. Stiamo proteggendo il cittadino?
5. Abbiamo costruito le fondamenta dell'information sharing?
6. Stiamo pensando a uno standard? O a uno schema certificativo?
7. …?

blustarcacina@gmail.com