Giovedì 13 marzo 2014

P7_TA(2014)0244

Livello comune elevato di sicurezza delle reti e dell'informazione ***I

Risoluzione legislativa del Parlamento europeo del 13 marzo 2014 sulla proposta di direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione (COM(2013)0048 — C7-0035/2013 — 2013/0027(COD))

(Procedura legislativa ordinaria: prima lettura)

(2017/C 378/74)

Il Parlamento europeo,

— vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2013)0048),

— visti l'articolo 294, paragrafo 2, e l'articolo 114 del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C7-0035/2013),

— visto l'articolo 294, paragrafo 3, del trattato sul funzionamento dell'Unione europea,

— visto il parere motivato presentato, nel quadro del protocollo n. 2 sull'applicazione dei principi di sussidiarietà e di proporzionalità, dal Parlamento svedese, ove si afferma che il progetto di atto legislativo non è conforme al principio di sussidiarietà,

— visto il parere del Comitato economico e sociale europeo del 22 maggio 2013 ([1]),

— vista la sua risoluzione del 12 settembre 2013 sulla strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro ([2]),

— visto l'articolo 55 del suo regolamento,

— visti la relazione della commissione per il mercato interno e la protezione dei consumatori e i pareri della commissione per l'industria, la ricerca e l'energia, della commissione per le libertà civili, la giustizia e gli affari interni e della commissione per gli affari esteri (A7-0103/2014),

1. adotta la posizione in prima lettura figurante in appresso;

2. chiede alla Commissione di presentargli nuovamente la proposta qualora intenda modificarla sostanzialmente o sostituirla con un nuovo testo;

3. incarica il suo Presidente di trasmettere la posizione del Parlamento al Consiglio e alla Commissione nonché ai parlamenti nazionali.

P7_TC1-COD(2013)0027

Posizione del Parlamento europeo definita in prima lettura il 13 marzo 2014 in vista dell'adozione della direttiva 2014/…/UE del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

---

([1]) GU C 271 del 19.9.2013, pag. 133.
([2]) Testi approvati, P7_TA(2013)0376.

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) Le reti e i sistemi e servizi di informazione svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per ***la libertà e la sicurezza globale dei cittadini dell'Unione oltre che per*** l'attività economica e il benessere sociale e in particolare ai fini del funzionamento del mercato interno. **[Em. 1]**

(2) La portata ~~e~~, la frequenza ***e l'impatto*** degli incidenti ~~dolosi o accidentali~~ a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. ***Tali sistemi possono inoltre diventare un facile bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi.*** Tali incidenti possono impedire il proseguimento di attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e ***degli investitori e*** causare gravi danni all'economia dell'Unione ***e, infine, mettere in pericolo il benessere dei cittadini dell'Unione e la capacità degli Stati membri di proteggere se stessi e garantire la sicurezza delle infrastrutture critiche***. **[Em. 2]**

(3) In quanto strumenti di comunicazione non vincolati a frontiere, i sistemi informativi digitali — e in prima linea internet — svolgono un ruolo essenziale per agevolare i movimenti transnazionali di beni, servizi e persone. Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi in uno Stato membro possono ripercuotersi sugli altri Stati membri e avere conseguenze in tutta l'UE. La resilienza e la stabilità delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno.

(3 bis) Poiché comunemente le cause di guasto dei sistemi continuano a essere involontarie, come eventi naturali o errori umani, le infrastrutture dovrebbero essere resilienti sia alle perturbazioni intenzionali che a quelle involontarie e gli operatori delle infrastrutture critiche dovrebbero progettare sistemi basati sulla resilienza. **[Em. 3]**

(4) È opportuno istituire un meccanismo di cooperazione a livello dell'Unione che permetta lo scambio di informazioni e il coordinamento delle attività ***di prevenzione,*** di individuazione e di risposta attinenti alla sicurezza delle reti e dell'informazione (SRI). Perché tale meccanismo sia effettivo e inclusivo è importante che tutti gli Stati membri dispongano di un livello minimo di capacità e si dotino di una strategia per garantire un livello elevato di sicurezza delle reti e dell'informazione sul loro territorio. È opportuno che anche ~~alle pubbliche amministrazioni e agli~~ ***a determinati*** operatori di ***mercato di*** infrastrutture informatiche ~~critiche~~ si applichino obblighi minimi di sicurezza, per promuovere una cultura della gestione dei rischi e garantire la segnalazione degli incidenti più gravi. ***Le società quotate nei mercati azionari dovrebbero essere incoraggiate a pubblicare volontariamente i loro incidenti nei rendiconti finanziari. È opportuno che il quadro giuridico si basi sull'esigenza di tutelare la riservatezza e l'integrità dei cittadini. La rete informativa di allarme sulle infrastrutture critiche (CIWIN) dovrebbe essere estesa agli operatori di mercato coperti dalla presente direttiva.*** **[Em. 4]**

(4 bis) Sebbene le amministrazioni pubbliche, in virtù della loro missione pubblica, debbano esercitare la dovuta diligenza nella gestione e protezione delle proprie reti e dei rispettivi sistemi informatici, occorre che la presente direttiva sia incentrata sulle infrastrutture critiche che sono essenziali per il mantenimento di attività vitali per l'economia e la società nei campi dell'energia, dei trasporti, delle banche, delle infrastrutture dei mercati finanziari e della sanità. Gli sviluppatori di software e i produttori di hardware dovrebbero essere esclusi dall'ambito di applicazione della presente direttiva. **[Em. 5]**

([1]) GU C 271 del 19.9.2013, pag. 133.
([2]) Posizione del Parlamento europeo del 13 marzo 2014.

Giovedì 13 marzo 2014

(4 ter) ***La cooperazione e il coordinamento tra le competenti autorità dell'Unione con l'alto rappresentante/vicepresidente, il responsabile per la politica estera e di sicurezza comune e la politica di sicurezza e difesa comune, nonché con il coordinatore antiterrorismo dell'UE, dovrebbero essere garantiti nei casi in cui gli incidenti aventi un impatto significativo sono percepiti come rischi di natura esterna e terroristica.*** **[Em. 6]**

(5) È necessario che la presente direttiva si applichi a tutte le reti e a tutti i sistemi informativi in modo da coprire tutti i relativi rischi e incidenti. È opportuno tuttavia che gli obblighi fatti alle pubbliche amministrazioni e agli operatori del mercato non si applichino alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi della direttiva 2002/21/CE del Parlamento europeo e del Consiglio ([1]), perché tali imprese sono soggette a specifici obblighi di sicurezza e integrità previsti dall'articolo 13 bis di detta direttiva; i suddetti obblighi non devono inoltre applicarsi ai prestatori di servizi fiduciari.

(6) Le capacità esistenti non bastano a garantire un livello elevato di sicurezza delle reti e dell'informazione nell'Unione. I livelli di preparazione negli Stati membri sono molto diversi tra loro il che comporta una frammentazione degli approcci nell'Unione. Ne deriva un livello disomogeneo di protezione dei consumatori e delle imprese che compromette il livello globale di sicurezza delle reti e dell'informazione nell'Unione. La mancanza di obblighi minimi comuni imposti ~~alle pubbliche amministrazioni e~~ agli operatori del mercato rende inoltre impossibile la creazione di un meccanismo globale ed efficace di cooperazione a livello dell'Unione. ***Le università e i centri di ricerca svolgono un ruolo determinante nell'incentivare la ricerca, lo sviluppo e l'innovazione in tali settori e dovrebbero ricevere fondi adeguati.*** **[Em. 7]**

(7) Per una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi è pertanto necessario un approccio globale a livello di Unione, che contempli la creazione di una capacità minima comune e disposizioni minime in materia di pianificazione, ***lo sviluppo di competenze sufficienti in materia di sicurezza informatica, lo*** scambio di informazioni e ***il*** coordinamento delle azioni, nonché obblighi minimi comuni di sicurezza ~~per tutti gli operatori del mercato interessati e le pubbliche amministrazioni~~. ***È opportuno applicare norme comuni minime conformemente alle raccomandazioni pertinenti dei Cyber Security Coordination Group (CSGC).*** **[Em. 8]**

(8) Le disposizioni della presente direttiva lasciano impregiudicata la possibilità per ciascuno Stato membro di adottare le misure necessarie per assicurare la tutela dei suoi interessi essenziali in materia di sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati. Conformemente all'articolo 346 del trattato sul funzionamento dell'Unione (TFUE), nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza. ***Nessuno Stato membro è obbligato a divulgare le informazioni classificate UE ai sensi della decisione 2011/292/UE del Consiglio*** ([2])***, le informazioni soggette agli accordi di non divulgazione o agli accordi di non divulgazione informali, quale il Traffic Light Protocol (protocollo sui semafori).*** **[Em. 9]**

(9) Per conseguire e mantenere un livello comune elevato di sicurezza delle reti e dei sistemi informativi è opportuno che ogni Stato membro disponga di una strategia nazionale in materia di SRI che definisca gli obiettivi strategici e gli interventi strategici concreti da attuare. Per poter raggiungere una capacità di risposta tale da permettere un'efficiente collaborazione a livello nazionale e unionale in caso di incidenti è necessario che siano elaborati, a livello nazionale, ***sulla base di requisiti minimi stabiliti nella presente direttiva,*** piani di collaborazione in materia di sicurezza delle reti e dell'informazione, rispondenti a condizioni essenziali***, i quali rispettino e tutelino la vita privata e i dati personali. È pertanto opportuno che ogni Stato membro sia obbligato a rispettare norme minime comuni riguardo al formato e alla scambiabilità dei dati da condividere e valutare. Gli Stati membri dovrebbero poter richiedere l'assistenza dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ai fini dello sviluppo delle rispettive strategie nazionali in materia di SRI, sulla base di un programma strategico SRI minimo comune***. **[Em. 10]**

([1]) 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 24.4.2002, pag. 33).

([2]) ***Decisione 2011/292/UE del Consiglio, del 31 marzo 2011, sulle norme di sicurezza per la protezione delle informazioni classificate UE (GU L 141 del 27.5.2011, pag. 17).***

(10) Per permettere l'efficace attuazione delle disposizioni adottate a norma della presente direttiva è necessario che sia istituito o individuato in ogni Stato membro un organismo responsabile del coordinamento degli aspetti della SRI, che funga da perno della cooperazione transnazionale a livello unionale. Tali organismi devono essere dotati di risorse adeguate sul piano tecnico, finanziario e umano per permettere loro di eseguire in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva.

(10 bis) In considerazione delle differenze esistenti tra le strutture di governance nazionali e al fine di salvaguardare gli accordi settoriali preesistenti o gli organismi di vigilanza e di regolamentazione dell'Unione ed evitare duplicazioni, è opportuno che gli Stati membri abbiano la facoltà di designare più di un'autorità nazionale competente incaricata di soddisfare i compiti connessi alla sicurezza delle reti e dei sistemi informativi degli operatori di mercato di cui alla presente direttiva. Tuttavia, onde garantire che la cooperazione e la comunicazione transfrontaliere siano fluide, è necessario che ogni Stato membro, fatti salvi gli accordi settoriali in materia di regolamentazione, designi soltanto un unico punto di contatto nazionale incaricato della cooperazione transfrontaliera a livello di Unione. Qualora la sua struttura costituzionale o altre disposizioni lo richiedano, uno Stato membro dovrebbe poter designare soltanto un'autorità per svolgere i compiti dell'autorità competente e del punto di contatto unico. Le autorità competenti e i punti di contatto unici dovrebbero essere organismi di diritto civile, sottoposti al controllo democratico, e non svolgere compiti di intelligence, di applicazione o difesa della legge, o essere collegati dal punto di vista organizzativo, indipendentemente dalla forma, a organismi che operano in tali ambiti. **[Em. 11]**

(11) È necessario che tutti gli Stati membri ***e gli operatori di mercato*** siano dotati delle capacità tecniche e organizzative necessarie a prevenire, individuare, rispondere e attenuare ***in qualsiasi momento*** i rischi e gli incidenti a carico delle reti e dei sistemi informativi. ***I sistemi di sicurezza delle pubbliche amministrazioni dovrebbero essere sicuri e sottoposti al controllo democratico. Le attrezzature e le capacità normalmente richieste dovrebbero essere conformi a norme tecniche decise di comune accordo oltre che a procedure operative standard.*** Per questo è necessario che, in tutti gli Stati membri, siano costituite squadre di pronto intervento informatico ***(CERT)*** rispondenti a determinati requisiti essenziali, in modo da garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione. ***È opportuno che tali squadre CERT possano interagire sulla base di norme tecniche comuni e procedure operative standard. In considerazione delle diverse caratteristiche delle squadre CERT esistenti, che rispondono a diverse esigenze soggettive e a diversi attori, gli Stati membri dovrebbero garantire che a ciascuno dei settori elencati nella presente direttiva siano forniti servizi da almeno una squadra CERT. Relativamente alla cooperazione transfrontaliera delle squadre CERT, gli Stati membri dovrebbero garantire che esse dispongano di mezzi sufficienti per partecipare alle reti di cooperazione internazionali e unionali già esistenti.*** **[Em. 12]**

(12) Basandosi sui notevoli progressi compiuti all'interno del Forum europeo degli Stati membri (EFMS) nel promuovere le discussioni e gli scambi di buone pratiche, come l'elaborazione dei principi della collaborazione europea in caso di crisi cibernetica, è opportuno che la Commissione e gli Stati membri creino una rete che assicuri una comunicazione permanente tra loro e ne sostenga la collaborazione. Tale meccanismo di collaborazione sicuro ed effettivo***, compresa la partecipazione degli operatori di mercato, ove opportuno,*** è destinato a permettere di strutturare e coordinare lo scambio di informazioni e le attività di individuazione e risposta a livello dell'Unione. **[Em. 13]**

(13) ~~L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)~~ ***L'ENISA*** dovrebbe assistere gli Stati membri e la Commissione mettendo loro a disposizione le proprie competenze e consulenze e agevolando lo scambio di buone pratiche. In particolare è opportuno che la Commissione ~~consulti~~ ***e gli Stati membri consultino*** l'ENISA nell'applicazione della presente direttiva. Per garantire un'informazione effettiva e tempestiva degli Stati membri e della Commissione è necessario che gli incidenti e i rischi siano segnalati precocemente attraverso la rete di collaborazione. Per creare capacità e conoscenze tra gli Stati membri, la rete di collaborazione dovrebbe anche servire da strumento di scambio di buone pratiche, assistendo i propri membri a creare capacità e conducendo l'organizzazione di valutazioni tra pari e di esercitazioni in materia di SRI. **[Em. 14]**

(13 bis) Laddove opportuno, gli Stati membri dovrebbero poter utilizzare o adattare le strutture o strategie organizzative esistenti al momento di applicare le disposizioni della presente direttiva. **[Em. 15]**

Giovedì 13 marzo 2014

(14) Nella rete di collaborazione è opportuno creare un'infrastruttura di scambio sicuro di informazioni che consenta lo scambio di informazioni sensibili e riservate tra autorità competenti. ***A tale scopo è opportuno che le strutture esistenti nell'Unione siano utilizzate appieno.*** Fatto salvo il loro obbligo di segnalare gli incidenti e i rischi di dimensione unionale alla rete di collaborazione, è opportuno che l'accesso a informazioni riservate di altri Stati membri sia concesso soltanto agli Stati membri che dimostrano di possedere processi e risorse finanziarie, tecniche ed umane e un'infrastruttura di comunicazione tali da garantirne la partecipazione effettiva, efficiente e sicura alla rete***, utilizzando metodi trasparenti***. **[Em. 16]**

(15) La collaborazione tra il settore pubblico e il settore privato è essenziale visto che la maggioranza delle reti e dei sistemi informativi funziona per opera di operatori privati. Gli operatori del mercato devono essere incoraggiati a portare avanti propri meccanismi informali di collaborazione per garantire la sicurezza delle reti e dell'informazione. È necessario che essi collaborino anche con il settore pubblico e scambino ***reciprocamente*** informazioni e buone pratiche ~~in cambio~~***, tra cui lo scambio reciproco di informazioni pertinenti e*** di supporto operativo***, e informazioni analizzate in modo strategico*** in caso di incidenti. ***Per incoraggiare efficacemente la condivisione di informazioni e buone pratiche, è essenziale garantire che gli operatori del mercato, che partecipano a tali scambi, non siano svantaggiati in conseguenza della loro cooperazione. Occorrono tutele adeguate per garantire che tale cooperazione non esponga tali operatori a un più elevato rischio di conformità o a nuove responsabilità in materia, tra l'altro, di concorrenza, proprietà intellettuale, protezione dei dati o norme sulla cibercriminalità, né a rischi operativi o di sicurezza più elevati.*** **[Em. 17]**

(16) Per garantire la trasparenza e una corretta informazione dei cittadini e degli operatori del mercato dell'UE è necessario che ~~le competenti autorità~~ ***i punti di contatto unici*** allestiscano un sito comune ***a livello di Unione*** su cui pubblicare informazioni non riservate sui rischi ~~e~~, sugli incidenti ***e sui mezzi per attenuare i rischi, nonché, ove necessario, suggerimenti in merito alle opportune misure di manutenzione. È opportuno che le informazioni sul sito web siano accessibili indipendentemente dal dispositivo utilizzato. I dati personali pubblicati su questo sito web dovrebbero essere limitati esclusivamente a quanto necessario e dovrebbero essere quanto più possibile anonimi***. **[Em. 18]**

(17) Qualora le informazioni siano considerate riservate in virtù di norme unionali e nazionali sulla riservatezza degli affari, è necessario che tale riservatezza sia garantita nello svolgimento delle attività e nella realizzazione degli obiettivi stabiliti dalla presente direttiva.

(18) In base in particolare alle esperienze nazionali in materia di gestione delle crisi e in collaborazione con l'ENISA è opportuno che la Commissione e gli Stati membri elaborino un piano unionale di collaborazione in materia di SRI che definisce meccanismi di collaborazione ~~nella lotta contro~~***, buone prassi e modelli operativi per prevenire, individuare, segnalare e contrastare*** i rischi e gli incidenti. Occorre tenere debitamente conto di tale piano ai fini della segnalazione di preallarmi all'interno della rete di collaborazione. **[Em. 19]**

(19) È necessario notificare un preallarme nella rete solo se la portata e la gravità dell'incidente o del rischio di cui si tratta sono o potrebbero essere così significative da richiedere l'informazione o il coordinamento della risposta a livello dell'Unione. È quindi necessario che i preallarmi si limitino agli incidenti o ai rischi~~, effettivi o potenziali,~~ che presentano una crescita rapida, che superano le capacità nazionali di risposta o che colpiscono più di uno Stato membro. Per garantirne la corretta valutazione è necessario che siano comunicate alla rete di collaborazione tutte le informazioni pertinenti alla valutazione del rischio o dell'incidente. **[Em. 20]**

(20) Dopo aver ricevuto e valutato un preallarme, è opportuno che ~~le autorità competenti~~ ***i punti di contatto unici*** adottino una risposta coordinata nell'ambito del piano unionale di collaborazione materia di SRI. È necessario che ~~le autorità competenti~~ ***i punti di contatto unici, l'ENISA*** e la Commissione siano informate delle misure adottate a livello nazionale in esito alla risposta coordinata. **[Em. 21]**

Giovedì 13 marzo 2014

(21) Data la natura planetaria dei problemi che interessano la sicurezza delle reti e dell'informazione è necessaria una cooperazione internazionale più stretta per migliorare le norme di sicurezza e gli scambi di informazioni e promuovere un approccio globale comune agli aspetti della SRI. ***Qualsiasi quadro per tale cooperazione internazionale dovrebbe essere soggetto ala direttiva 95/46/CE del Parlamento europeo e del Consiglio*** ([1]) ***e del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio*** ([2])**. [Em. 22]**

(22) La responsabilità di garantire la sicurezza delle reti e dell'informazione incombe in larga misura ~~alle pubbliche amministrazioni e~~ agli operatori del mercato. È opportuno promuovere e sviluppare attraverso adeguati obblighi regolamentari e pratiche industriali volontarie una cultura della gestione del rischio, ***della stretta collaborazione e della fiducia,*** che comprende la valutazione del rischio e l'attuazione di misure di sicurezza commisurate ~~al rischio corso~~ ***ai rischi e agli incidenti, dolosi o accidentali***. È altresì fondamentale creare pari condizioni ***affidabili*** per l'efficace funzionamento della rete di collaborazione in modo da garantire la collaborazione effettiva di tutti gli Stati membri. **[Em. 23]**

(23) La direttiva 2002/21/CE fa obbligo alle imprese che forniscono reti pubbliche di comunicazioni elettroniche o servizi di comunicazione elettronica accessibili al pubblico di adottare misure adeguate per salvaguardarne l'integrità e la sicurezza e introduce obblighi di comunicazione delle violazioni di sicurezza o perdita dell'integrità. La direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([3]) obbliga i fornitori di servizi di comunicazione elettronica accessibili al pubblico ad adottare misure e procedure tecniche e organizzative adeguate a salvaguardare la sicurezza dei loro servizi.

(24) È opportuno che tali obblighi imposti al settore delle comunicazioni elettroniche siano estesi ***agli operatori di infrastrutture che dipendono pesantemente dalla tecnologia dell'informazione e delle comunicazioni e che sono essenziali per il mantenimento di funzioni vitali, in termini economici o societali, come l'elettricità e il gas, i trasporti, gli enti creditizi, le infrastrutture dei mercati finanziari e la sanità. Le perturbazioni a carico di tali reti e sistemi informativi avrebbero ripercussioni sul mercato interno. Anche se è opportuno non estendere gli obblighi stabiliti nella presente direttiva*** ai principali fornitori di servizi della società dell'informazione, quali definiti dalla direttiva 98/34/CE del Parlamento europeo e del Consiglio ([4]), che supportano i servizi della società dell'informazione a valle o attività online come le piattaforme del commercio elettronico, i portali di pagamento su internet, le reti sociali, i motori di ricerca, i servizi nella nuvola ~~e~~ ***in generale o*** i negozi online di applicazioni. ~~Le eventuali perturbazioni che colpiscono questi servizi essenziali della società dell'informazione impediscono la fornitura di altri servizi della società dell'informazione che si basano sui primi. Gli sviluppatori di programmi informatici e i costruttori di hardware non sono fornitori di servizi della società dell'informazione e sono pertanto esclusi. È necessario che i suddetti obblighi siano estesi anche alle pubbliche amministrazioni e agli operatori di infrastrutture critiche che dipendono pesantemente dalla tecnologia dell'informazione e delle comunicazioni e che sono essenziali per il mantenimento di funzioni vitali, in termini economici o societali, come l'elettricità e il gas, i trasporti, gli enti creditizi, le borse e la sanità. Le eventuali perturbazioni a carico di tali reti e sistemi informativi avrebbero ripercussioni sul mercato interno.~~ ***, tali fornitori potrebbero, su base volontaria, informare l'autorità competente o il punto di contatto unico in merito agli incidenti relativi alla sicurezza delle reti che essi reputano appropriati. È opportuno che l'autorità competente o il punto di contatto unico presentino, se del caso, agli operatori del mercato che hanno loro segnalato l'incidente, le informazioni analizzate in modo strategico che contribuiranno a superare la minaccia alla sicurezza***. **[Em. 24]**

([1]) ***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, pag. 31).***

([2]) ***Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).***

([3]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

([4]) Direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche (GU L 204 del 21.7.1998, pag. 37).

Giovedì 13 marzo 2014

(***24 bis***) ***Anche se i fornitori di hardware e software non sono operatori di mercato comparabili a quelli disciplinati dalla presente direttiva, i loro prodotti agevolano la sicurezza della rete e dei sistemi informativi. Essi svolgono pertanto un ruolo importante nel permettere agli operatori di mercato di mettere in sicurezza le loro reti e le loro strutture informative. Dato che i prodotti hardware e software sono già soggetti alle norme esistenti sulla garanzia dei prodotti, è opportuno che gli Stati membri provvedano a che tali norme vengano applicate.*** **[Em. 25]**

(25) Le misure tecniche e organizzative imposte ~~alle amministrazioni pubbliche e~~ agli operatori del mercato non devono richiedere che una particolare informazione commerciale o un particolare prodotto della tecnologia delle comunicazioni siano concepiti, sviluppati e fabbricati in una maniera particolare. **[Em. 26]**

(26) È necessario che ~~le amministrazioni pubbliche e~~ gli operatori di mercato garantiscano la sicurezza delle reti e dei sistemi di cui hanno il controllo. Si tratta in particolare di reti e sistemi privati gestiti dal loro personale IT interno, oppure la cui sicurezza sia stata esternalizzata. Gli obblighi di notifica e di sicurezza devono applicarsi agli operatori del mercato ~~e alle amministrazioni pubbliche~~ indipendentemente dal fatto che la manutenzione delle loro reti e dei loro sistemi informativi sia eseguita al loro interno o sia esternalizzata. **[Em. 27]**

(27) Per evitare di imporre un onere finanziario e amministrativo sproporzionato a piccoli operatori e piccoli utenti, è necessario che gli obblighi siano proporzionati al rischio corso dalla rete o dal sistema informativo di cui si tratta, tenendo conto dello stato dell'arte di tali misure. Tali obblighi non devono applicarsi alle microimprese.

(28) È opportuno che le autorità competenti ***e i punti di contatto unici*** procurino in particolare di salvaguardare l'esistenza di canali informali e affidabili di scambio di informazioni tra gli operatori del mercato e tra settore pubblico e privato. ***Le autorità competenti e i punti di contatto unici dovrebbero informare i produttori e i fornitori di servizi in merito agli incidenti di cui abbiano ricevuto notifica e riguardanti i prodotti e i servizi TIC che hanno un impatto significativo.*** La pubblicità degli incidenti segnalati alle autorità competenti ~~deve~~ ***e ai punti di contatto unici dovrebbe*** contemperare l'opportunità che il pubblico sia informato delle minacce esistenti con i possibili danni di immagine e commerciali per ~~le pubbliche amministrazioni e~~ gli operatori di mercato che segnalano gli incidenti. Nell'attuare gli obblighi di notifica è necessario che le autorità competenti ***e i punti di contatto unici*** tengano adeguatamente conto della necessità di mantenere strettamente riservate le informazioni sulle vulnerabilità del prodotto prima di ~~diffondere~~ ***impiegare*** i rimedi di sicurezza appropriati. ***Come regola generale, i punti di contatto unici non dovrebbero divulgare i dati personali delle persone fisiche coinvolte negli incidenti. I punti di contatto unici dovrebbero divulgare i dati personali soltanto se tale divulgazione è necessaria e proporzionata rispetto all'obiettivo perseguito.*** **[Em. 28]**

(29) È necessario che le autorità competenti possiedano i mezzi necessari all'assolvimento dei loro compiti, come la facoltà di ottenere informazioni sufficienti dagli operatori del mercato ~~e dalle amministrazioni pubbliche~~ per valutare il livello di sicurezza delle reti e dei sistemi informativi, ***constatare il numero, la portata e l'ambito degli incidenti,*** nonché dati attendibili e completi su incidenti reali che hanno avuto un impatto sul funzionamento delle reti e dei sistemi informativi. **[Em. 29]**

(30) In molti casi alla base di un incidente vi sono attività criminali. Si può sospettare la natura dolosa di incidenti anche se non vi sono prove sufficientemente chiare fin dall'inizio. Al riguardo, una risposta effettiva e esauriente alla minaccia di incidenti di sicurezza presuppone un'adeguata collaborazione tra autorità competenti***, punti di contatto unici*** e autorità di contrasto ***nonché una cooperazione con l'EC3 (Europol Cybercrime Centre) e l'ENISA***. In particolare, la promozione di un ambiente sicuro, affidabile e più resiliente richiede la segnalazione sistematica, alle autorità di contrasto, degli incidenti di cui si sospetta la natura dolosa grave. La natura dolosa grave degli incidenti va valutata alla luce delle norme dell'Unione sulla cibercriminalità. **[Em. 30]**

(31) I molti casi gli incidenti compromettono dati personali. ***È opportuno che gli Stati membri e gli operatori del mercato tutelino i dati personali archiviati, trattati o trasmessi, da distruzioni accidentali o illecite, perdite accidentali o alterazione, nonché archiviazione, accesso, divulgazione o diffusione non autorizzati o illeciti; è altresì opportuno assicurare l'attuazione di una strategia di sicurezza concernente il trattamento dei dati personali.*** Al riguardo è opportuno che le autorità competenti***, i punti di contatto unici*** e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni ~~su tutti gli aspetti pertinenti per~~, ***anche, se del caso, con gli operatori del mercato, al fine di*** affrontare le violazioni ai dati personali determinate dagli incidenti ***conformemente alla normativa applicabile in materia di protezione dei dati***. ~~Gli Stati membri devono adempiere~~ L'obbligo di segnalazione degli incidenti di sicurezza ***dovrebbe essere espletato*** in modo da minimizzare gli oneri amministrativi nel caso in cui l'incidente di sicurezza costituisca anche una violazione di dati personali~~, in conformità al regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati ([1]). Coordinandosi con le autorità competenti e le autorità responsabili della protezione dei dati, l'ENISA può~~ ***che va notificata a norma del diritto unionale sulla protezione dei dati. L'ENISA dovrebbe*** contribuire alla messa a punto di meccanismi e ~~modelli~~ per lo scambio di informazioni~~, evitando in questo modo che siano necessari due modelli~~ ***e*** di ~~notifica.~~ un modello di notifica unico ***il quale*** può facilitare la segnalazione di incidenti che compromettono dati personali, alleviando in questo modo gli oneri amministrativi per le imprese e le pubbliche amministrazioni. **[Em. 31]**

(32) La standardizzazione degli obblighi di sicurezza è un'esigenza che nasce dal mercato ***a carattere volontario che dovrebbe consentire agli operatori del mercato di utilizzare mezzi alternativi per ottenere almeno risultati simili***. Per garantire un'applicazione convergente delle norme di sicurezza è opportuno che gli Stati membri incoraggino il rispetto o la conformità a norme ***interoperabili*** specifiche volte a garantire un livello elevato di sicurezza in tutta l'Unione. A tal fine ~~potrebbe~~ ***è opportuno valutare l'applicazione di norme internazionali aperte in tema di sicurezza dell'informazione in rete oppure la definizione di strumenti in tal senso***. ***Potrebbe inoltre*** essere necessario elaborare norme armonizzate in conformità al regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([2]). ***In particolare, è opportuno conferire all'Istituto europeo per le norme di telecomunicazioni (ETSI), al Comitato europeo di normalizzazione (CEN) e al Comitato europeo di normalizzazione elettrotecnica (CENELEC) il mandato a proporre norme di sicurezza unionali aperte, efficienti ed efficaci, in cui le preferenze tecnologiche siano quanto più possibile evitate, e che siano facilmente gestibili da operatori del mercato di piccole e medie dimensioni. È opportuno che le norme internazionali in materia di cibersicurezza siano esaminate con cura per garantire che non siano compromesse e che offrano adeguati livelli di sicurezza, facendo sì che l'obbligo di conformità alle norme in materia di cibersicurezza migliori il livello generale di sicurezza informatica dell'Unione e non il contrario.*** **[Em. 32]**

(33) È opportuno che la Commissione riesamini le disposizioni della presente direttiva a scadenze regolari, in ***consultazione con tutte le parti interessate, in*** particolare per valutare la necessità di modificarle in funzione dell'evoluzione ~~delle tecnologie~~ ***sociale, politica e tecnologica*** o delle condizioni del mercato. **[Em. 33]**

(34) Per garantire il corretto funzionamento della rete di collaborazione deve essere conferito alla Commissione il potere di adottare atti a norma dell'articolo 290 TFUE per quanto riguarda ~~la definizione dei criteri che devono essere rispettati perché uno Stato membro sia autorizzato a partecipare al sistema sicuro di~~ ***l'insieme comune di norme concernenti l'interconnessione e la sicurezza per l'infrastruttura dello*** scambio di informazioni, ***e*** la specificazione più precisa degli eventi che richiedono l'invio di un preallarme ~~e la definizione delle circostanze alle quali gli operatori del mercato e le amministrazioni pubbliche sono tenuti a notificare gli incidenti~~. **[Em. 34]**

([1]) ~~SEC(2012) 72 definitivo.~~

([2]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

Giovedì 13 marzo 2014

(35) È particolarmente importante che la Commissione, nel corso del suo lavoro preparatorio, svolga consultazioni adeguate, anche a livello di esperti. Quando elabora e redige atti delegati la Commissione è tenuta a procedere alla trasmissione contestuale, tempestiva ed appropriata dei relativi documenti al Parlamento europeo e al Consiglio.

(36) Al fine di garantire condizioni uniformi di esecuzione della presente direttiva è opportuno attribuire alla Commissione competenze di esecuzione per quanto riguarda la collaborazione tra ~~le autorità competenti~~ ***i punti di contatto unici*** e la Commissione nel quadro della rete di collaborazione, ~~l'accesso all'infrastruttura sicura di scambio di informazioni~~, il piano unionale di collaborazione in materia di SRI, ***e*** il formato e le procedure applicabili ~~all'informazione del pubblico in merito agli~~ ***alla segnalazione degli*** incidenti ~~e le pertinenti norme e/o le specifiche tecniche in materia di SRI~~ ***che hanno un impatto significativo***. Tali competenze di esecuzione devono essere esercitate in conformità al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([1]). **[Em. 35]**

(37) Nell'applicazione della presente direttiva la Commissione ~~deve~~ ***dovrebbe*** coordinarsi adeguatamente con i comitati settoriali competenti e gli altri organi costituiti a livello dell'Unione in particolare nei settori ***dell'e-government,*** dell'energia, dei trasporti, ~~delle banche~~ e della sanità ***e della difesa***. **[Em. 36]**

(38) Le informazioni considerate riservate da un'autorità competente ***o da un punto di contatto unico***, in conformità con la normativa unionale e nazionale sulla riservatezza degli affari, possono essere scambiate con la Commissione ~~e~~, con ***le sue agenzie pertinenti, i punti di contatto unici e/o le*** altre autorità ***nazionali*** competenti solo nella misura in cui tale scambio sia strettamente necessario ai fini dell'applicazione della presente direttiva. Lo scambio ~~deve~~ ***dovrebbe*** limitarsi alle sole informazioni pertinenti ~~ed essere commisurato~~***, necessarie e commisurate*** allo scopo***, e rispettare i criteri di riservatezza e sicurezza prestabiliti, a norma della decisione 2011/292/UE, e delle informazioni soggette agli accordi di non divulgazione o agli accordi di non divulgazione informali, quale il Traffic Light Protocol (protocollo sui semafori)***. **[Em. 37]**

(39) Lo scambio di informazioni sui rischi e sugli incidenti all'interno della rete di collaborazione e il rispetto degli obblighi di notifica degli incidenti alle autorità nazionali competenti ***o al punto di contatto unico*** possono richiedere il trattamento di dati personali. Tale trattamento di dati personali è necessario per conseguire gli obiettivi di interesse pubblico perseguiti dalla presente direttiva ed è quindi legittimo in virtù dell'articolo 7 della direttiva 95/46/CE. In relazione a tali obiettivi legittimi esso non costituisce un intervento sproporzionato ed inammissibile che pregiudicherebbe la sostanza stessa del diritto di protezione dei dati personali sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. Nell'applicazione della presente direttiva si applica, per quanto di ragione, il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([2]). In caso di trattamento di dati da parte di istituzioni ed organismi dell'Unione, tale trattamento ai fini dell'attuazione della presente direttiva deve rispettare le disposizioni del regolamento (CE) n. 45/2001. **[Em. 38]**

(40) Poiché gli obiettivi della presente direttiva, ossia garantire un elevato livello di sicurezza delle reti e dell'informazione nell'Unione, non possono essere conseguiti in misura sufficiente dai soli Stati membri e possono dunque, a causa della portata e degli effetti dell'azione, essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(41) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata e delle comunicazioni, la protezione dei dati personali, la libertà di impresa, il diritto di proprietà, il diritto a un ricorso effettivo dinanzi a un giudice e il diritto al contraddittorio. La presente direttiva deve essere applicata nel rispetto di tali diritti e principi,

([1]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

([2]) Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

(41 bis) Conformemente alla dichiarazione politica congiunta degli Stati membri e della Commissione sui documenti esplicativi del 28 settembre 2011, gli Stati membri si sono impegnati ad accompagnare, ove ciò sia giustificato, la notifica delle loro misure di recepimento con uno o più documenti intesi a precisare il rapporto tra gli elementi di una direttiva e le parti corrispondenti delle misure nazionali di attuazione. In relazione alla presente direttiva il legislatore ritiene che la trasmissione di tali documenti sia giustificata. **[Em. 39]**

(41 ter) Conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001, il garante europeo della protezione dei dati è stato consultato e ha espresso un parere il 14 giugno 2013 ([1]),

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e campo di applicazione

1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di Sicurezza delle reti e dell'informazione (SRI) nell'Unione.

2. A tal fine la presente direttiva:

a) stabilisce obblighi per tutti gli Stati membri in materia di prevenzione, trattamento e risposta nei confronti dei rischi e degli incidenti a carico delle reti e dei sistemi informativi;

b) crea un meccanismo di collaborazione tra gli Stati membri per garantire un'applicazione uniforme della presente direttiva nell'Unione e, se necessario, una risposta e un trattamento coordinati ~~ed~~, efficienti ***ed efficaci*** dei rischi di incidenti a carico delle reti e dei sistemi informativi ***con la partecipazione delle parti interessate pertinenti***; **[Em. 40]**

c) stabilisce obblighi di sicurezza per gli operatori del mercato ~~e le amministrazioni pubbliche~~. **[Em. 41]**

3. Gli obblighi di sicurezza di cui all'articolo 14 della presente direttiva non si applicano né alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi della direttiva 2002/21/CE, le quali sono tenute a rispettare gli obblighi specifici di sicurezza e integrità stabiliti dagli articoli 13 bis e 13 ter della medesima direttiva, né ai prestatori di servizi fiduciari.

4. La presente direttiva lascia impregiudicate le disposizioni legislative dell'Unione in materia di cibercriminalità e la direttiva 2008/114/CE del Consiglio ([2]).

5. La presente direttiva lascia impregiudicate anche le disposizioni della direttiva 95/46/CE, della direttiva 2002/58/CE e del regolamento ***(CE) n. 45/2001*** . ***Eventuali usi dei dati personali devono limitarsi a quanto strettamente necessario ai fini della presente direttiva e tali dati devono essere quanto più anonimi possibili, se non completamente anonimi.*** **[Em. 42]**

6. Lo scambio di informazioni all'interno della rete di collaborazione in virtù delle disposizioni del capo III e le notifiche di incidenti a carico della SRI in virtù dell'articolo 14 possono comportare il trattamento di dati personali. Tale trattamento, necessario per conseguire gli obiettivi di pubblico interesse perseguiti dalla presente direttiva, è soggetto all'autorizzazione degli Stati membri a norma dell'articolo 7 della direttiva 95/46/CE e in virtù della direttiva 2002/58/CE quali recepite negli ordinamenti nazionali.

([1]) GU C 32 del 4.2.2014, pag. 19.
([2]) Direttiva 2008/114/CE del Consiglio, 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, pag. 75).

Articolo 1 bis

Protezione e trattamento dei dati personali

1. Il trattamento dei dati personali negli Stati membri a norma della presente direttiva è effettuato conformemente alle direttive 95/46/CE e 2002/58/CE.

2. Il trattamento dei dati personali da parte della Commissione e dell'ENISA a norma del presente regolamento è effettuato secondo il regolamento (CE) n. 45/2001.

3. Ai fini della presente direttiva il trattamento dei dati personali da parte del Centro europeo per la lotta alla criminalità informatica nell'ambito di Europol è effettuato conformemente alla decisione 2009/371/GAI del Consiglio ([1]).

4. Il trattamento dei dati personali è equo e conforme alla legge e strettamente limitato ai dati minimi necessari per le finalità di tale trattamento. I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

5. Le segnalazioni degli incidenti di cui all'articolo 14 della presente direttiva lasciano impregiudicate le disposizioni e gli obblighi riguardo alle notifiche di violazioni dei dati personali stabilite all'articolo 4 della direttiva 2002/58/CE e nel regolamento (UE) n. 611/2013 della Commissione ([2]). **[Em. 43]**

Articolo 2

Armonizzazione minima

Nulla osta a che gli Stati membri adottino o mantengano in vigore disposizioni atte a garantire un livello di sicurezza più elevato, fermi restando gli obblighi loro imposti dal diritto dell'Unione.

Articolo 3

Definizioni

Ai fini della presente direttiva si intende per:

1) «rete e sistema informativo»,

   a) una rete di comunicazioni elettroniche ai sensi della direttiva 2002/21/CE e

   b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati ~~elettronici~~ ***digitali*** e **[Em. 44]**

   c) i dati ~~elettronici~~ ***digitali*** conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione; **[Em. 45]**

2) «sicurezza», la capacità di una rete o di un sistema informativo di resistere, a un determinato livello di riservatezza, a eventi imprevisti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi offerti o accessibili tramite tale rete o sistema informativo; ***il concetto di «sicurezza» include i dispositivi tecnici nonché le soluzioni e le procedure operative idonei a garantire i requisiti di sicurezza di cui alla presente direttiva;*** **[Em. 46]**

([1]) ***Decisione 2009/371/GAI del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di polizia (Europol) (GU L 121 del 15.5.2009, pag. 37).***

([2]) ***Regolamento (UE) n. 611/2013 della Commissione, del 24 giugno 2013, sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche (GU L 173 del 26.6.2013, pag. 2).***

3) «rischio», ogni circostanza o evento ***ragionevolmente individuabile*** con potenziali effetti pregiudizievoli per la sicurezza; **[Em. 47]**

4) «incidente», ogni ~~circostanza o~~ evento con un reale effetto pregiudizievole per la sicurezza; **[Em. 48]**

~~5) «servizi della società dell'informazione», i servizi ai sensi dell'articolo 1, punto 2, della direttiva 98/34/CE;~~ **[Em. 49]**

6) «piano di collaborazione in materia di SRI», un piano che definisce il quadro dei ruoli organizzativi, delle responsabilità e delle procedure per il mantenimento o il ripristino dell'operatività delle reti e dei sistemi informativi qualora si verifichi un rischio o un incidente a loro carico;

7) «trattamento dell'incidente», tutte le procedure necessarie per ***l'identificazione, la prevenzione,*** l'analisi, il contenimento e la risposta a un incidente; **[Em. 50]**

8) «operatore del mercato»,

~~a) fornitore di servizi della società dell'informazione che consentono la fornitura di altri servizi della società dell'informazione; un elenco non esaustivo di tali operatori figura nell'allegato II;~~ **[Em. 51]**

b) operatore di infrastrutture ~~critiche~~ che sono essenziali per il mantenimento di attività vitali per l'economia e la società nei campi dell'energia, dei trasporti, delle banche, delle ~~borse~~ ***infrastrutture dei mercati finanziari, dei punti di scambio internet, della catena di approvvigionamento alimentare*** e della sanità***, la cui interruzione o distruzione avrebbe un impatto significativo in uno Stato membro in conseguenza dell'incapacità di mantenere tali funzioni***; un elenco non esaustivo di tali operatori figura nell'allegato II***, nella misura in cui la rete e i sistemi informativi interessati sono correlati ai suoi servizi principali***; **[Em. 52]**

8 bis) ***«incidente avente un impatto significativo», incidente che pregiudica la sicurezza e la continuità di una rete o di un sistema informativi provocando gravi perturbazioni di funzioni vitali per l'economia o la società;*** **[Em. 53]**

9) «norma», una norma ai sensi del regolamento (UE) n. 1025/2012;

10) «specifica», una specifica ai sensi del regolamento (UE) n. 1025/2012;

11) «prestatore di servizio fiduciario», una persona fisica o giuridica che presta un servizio elettronico consistente nella creazione, verifica, convalida, nel trattamento e nella conservazione di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, servizi elettronici di recapito, autenticazione di siti web e certificati elettronici, compresi i certificati di firma elettronica e di sigillo elettronico.

11 bis) ***«mercato regolamentato», mercato regolamentato ai sensi della definizione di cui all'articolo 4, punto 14, della direttiva 2004/39/CE del Parlamento europeo e del Consiglio*** ([1])**; [Em. 54]**

11 ter) ***«sistema multilaterale di negoziazione», sistema multilaterale di negoziazione così come definito all'articolo 4, punto 15, della direttiva 2004/39/CE;*** **[Em. 55]**

11 quater) ***«sistema organizzato di negoziazione», un sistema o un regime multilaterale diverso da un mercato regolamentato, da un sistema multilaterale di negoziazione o da una controparte centrale, gestito da una società di investimenti o da un operatore di mercato, che consente l'interazione tra interessi multipli di acquisto e di vendita di terzi relativi a obbligazioni, prodotti finanziari strutturati, quote di emissione o strumenti derivati, in modo da dare luogo a un contratto conformemente alle disposizioni del titolo II della direttiva 2004/39/CE;*** **[Em. 56]**

([1]) ***Direttiva 2004/39/CE del Parlamento europeo e del Consiglio, del 21 aprile 2004, relativa ai mercati degli strumenti finanziari (GU L 45 del 16.2.2005, pag. 18).***

Giovedì 13 marzo 2014

CAPO II

QUADRI NAZIONALI PER LA SICUREZZA DELLE RETI E DELL'INFORMAZIONE

Articolo 4

Principio

Gli Stati membri assicurano un livello elevato di sicurezza delle reti e dei sistemi informativi nel loro territorio in conformità alla presente direttiva.

Articolo 5

Strategia nazionale e piano nazionale di collaborazione in materia di SRI

1. Ogni Stato membro adotta una strategia nazionale in materia di SRI nella quale definisce gli obiettivi strategici e misure strategiche e regolamentari concrete per conseguire e conservare un livello elevato di sicurezza delle reti e dell'informazione. La strategia nazionale in materia di SRI affronta in particolare i seguenti aspetti:

a) la definizione degli obiettivi e delle priorità della strategia in base ad un'analisi aggiornata dei rischi e degli incidenti;

b) un quadro di governance per raggiungere obiettivi e priorità della strategia, con una definizione chiara dei ruoli e delle responsabilità degli organismi pubblici e degli altri attori implicati;

c) l'individuazione delle misure generali di preparazione, risposta e recupero, con meccanismi di collaborazione tra settore pubblico e settore privato;

d) l'indicazione di programmi di formazione, sensibilizzazione e istruzione;

e) i piani di ricerca e sviluppo e la descrizione di come essi rispecchino le priorità individuate.

e bis) gli Stati membri hanno la facoltà di chiedere l'assistenza dell'ENISA nell'elaborazione di strategie e piani nazionali di collaborazione in materia di SRI, sulla base di strategie minime comuni di SRI. **[Em. 57]**

2. La strategia nazionale comprende un piano nazionale di collaborazione in materia di SRI rispondente almeno alle seguenti prescrizioni:

a) un ~~piano di valutazione~~ ***quadro per la gestione*** dei rischi ***finalizzato all'elaborazione di una metodologia*** per ~~individuare i~~ ***l'identificazione, l'ordine di priorità, la valutazione e il trattamento dei*** rischi ~~e valutare le~~***, l'esame delle*** conseguenze di potenziali incidenti***, le scelte di prevenzione e di controllo, così come la definizione dei criteri per la selezione delle possibili contromisure***; **[Em. 58]**

b) la definizione dei ruoli e delle responsabilità ~~dei vari~~ ***delle varie autorità e degli altri*** attori implicati nell'attuazione del ~~piano~~ ***quadro***; **[Em. 59]**

c) la definizione dei processi di collaborazione e comunicazione che garantiscono la prevenzione, l'individuazione, la risposta, la riparazione e il recupero, con la relativa modulazione in funzione del livello di allerta;

d) una tabella di marcia per esercitazioni relative alla SRI e formazioni per rafforzare, convalidare e testare il piano; una documentazione degli insegnamenti tratti e il loro inserimento negli aggiornamenti del piano.

3. La strategia nazionale e il piano nazionale di collaborazione in materia di SRI sono comunicati alla Commissione entro ~~un mese~~ ***tre mesi*** dalla loro adozione. **[Em. 60]**

Articolo 6

Autorità ~~nazionale competente~~ ***nazionali competenti e punti di contatto unici*** in materia di sicurezza delle reti e dei sistemi informativi **[Em. 61]**

1. Ogni Stato membro designa ~~un'autorità nazionale competente~~ ***una o più autorità nazionali civili competenti*** in materia di sicurezza delle reti e dei sistemi informativi (~~la~~ ***in seguito la/le*** «autorità ~~competente~~ ***competente/i***»). **[Em. 62]**

2. Le autorità competenti controllano l'applicazione della presente direttiva a livello nazionale e contribuiscono alla coerenza di applicazione della medesima in tutta l'Unione.

2 bis. Se uno Stato membro designa più di una autorità competente, esso procede con la nomina di un'autorità nazionale civile, per esempio un'autorità competente, come punto di contatto unico nazionale per la sicurezza delle reti e dei sistemi informativi («punto di contatto unico»). Se uno Stato membro designa soltanto un'autorità competente, quest'ultima è anche il punto di contatto unico. **[Em. 63]**

2 ter. Le autorità competenti e il punto di contatto unico di uno stesso Stato membro collaborano a stretto contatto per quanto concerne gli obblighi di cui alla presente direttiva. **[Em. 64]**

2 quater. Il punto di contatto unico provvede alla collaborazione transfrontaliera con gli altri punti di contatto unici. **[Em. 65]**

3. Gli Stati membri garantiscono che le autorità competenti ***e i punti di contatto unici*** siano ~~dotate~~ ***dotati*** di risorse adeguate sul piano tecnico, finanziario e umano per eseguire in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva. Gli Stati membri provvedono a garantire la collaborazione effettiva, efficiente e sicura ~~delle autorità competenti~~ ***dei punti di contatto unici*** attraverso la rete di cui all'articolo 8. **[Em. 66]**

4. Gli Stati membri procurano che le autorità competenti ***e i punti di contatto unici, se del caso in conformità del paragrafo 2 bis del presente articolo,*** ricevano le notifiche degli incidenti da parte ~~delle amministrazioni pubbliche e~~ degli operatori del mercato come specificato all'articolo 14, paragrafo 2 e che siano loro attribuiti i poteri di attuazione e di controllo di cui all'articolo 15. **[Em. 67]**

4 bis. Qualora il diritto dell'Unione preveda un organismo di vigilanza o di regolamentazione settoriale dell'Unione, tra l'altro per la sicurezza delle reti e dei sistemi informativi, tale organismo riceve le notifiche degli incidenti in conformità dell'articolo 14, paragrafo 2, da parte degli operatori del mercato interessati in tale settore e gli sono attribuiti i poteri di attuazione e di controllo di cui all'articolo 15. L'organismo dell'Unione collabora a stretto contatto con le autorità competenti e il punto di contatto unico dello Stato membro ospitante per quanto concerne detti obblighi. Il punto di contatto unico dello Stato membro ospitante rappresenta l'organismo dell'Unione per quanto concerne gli obblighi di cui al capo III. **[Em. 68]**

5. Le autorità competenti ***e i punti di contatto unici*** consultano le competenti autorità nazionali di contrasto e le autorità nazionali competenti per la protezione dei dati e collaborano con le stesse come necessario. **[Em. 69]**

6. Ogni Stato membro comunica senza indugio alla Commissione ~~l'~~ ***le*** autorità ~~competente designata~~ ***competenti designate e il punto di contatto unico***, i ~~suoi~~ ***loro*** compiti e qualsiasi ulteriore modifica dei medesimi. Ogni Stato membro rende ~~pubblica l'~~ ***pubblica la designazione delle*** autorità ~~competente designata~~ ***competenti***. **[Em. 70]**

Articolo 7

Squadre di pronto intervento informatico

1. Ogni Stato membro costituisce ***almeno*** una squadra di pronto intervento informatico («CERT») ***per ciascuno dei settori elencati all'allegato II,*** col compito di trattare gli incidenti e i rischi secondo una procedura ben definita e conforme ai requisiti di cui all'allegato I, punto 1. È possibile creare una squadra CERT all'interno dell'autorità competente. **[Em. 71]**

2. Gli Stati membri procurano che le squadre CERT siano dotate di risorse umane, tecniche e finanziarie adeguate per l'adempimento dei loro compiti, precisati nell'allegato I, punto 2.

3. Gli Stati membri procurano che le squadre CERT possano contare su un'infrastruttura di informazione e comunicazione sicura e resiliente a livello nazionale, che sia compatibile e interoperabile con il sistema sicuro di scambio di informazioni di cui all'articolo 9.

4. Gli Stati membri comunicano alla Commissione le risorse e il mandato delle squadre CERT e la procedura di trattamento degli incidenti loro affidata.

5. ~~La squadra~~ ***Le squadre*** CERT ~~opera~~ ***operano*** sotto la supervisione dell'autorità competente ~~la~~ ***o del punto di contatto unico, il*** quale rivede periodicamente l'adeguatezza delle ~~sue~~ ***loro*** risorse, il mandato e l'efficacia della ***loro*** procedura di trattamento degli incidenti. **[Em. 72]**

5 bis. Gli Stati membri assicurano che le squadre CERT siano dotate di risorse umane e finanziarie adeguate per partecipare attivamente alle reti di collaborazione internazionali e, in particolare, dell'Unione. **[Em. 73]**

5 ter. Le squadre CERT hanno la facoltà, di cui sono incoraggiate ad avvalersi, di avviare esercitazioni congiunte con altre CERT, con squadre CERT che includano tutti gli Stati membri, con le opportune istituzioni di paesi terzi nonché con CERT di istituzioni multinazionali e internazionali come la NATO e le Nazioni Unite, con la possibilità di prendervi parte. **[Em. 74]**

5 quater. Gli Stati membri possono richiedere l'assistenza dell'ENISA o di altri Stati membri nello sviluppo delle rispettive squadre CERT nazionali. **[Em. 75]**

CAPO III

COOPERAZIONE FRA AUTORITÀ COMPETENTI

Articolo 8

Rete di collaborazione

1. ~~Le autorità competenti e~~ ***I punti di contatto unici,*** la Commissione ***e l'ENISA*** costituiscono una rete («rete di collaborazione») per collaborare in caso di rischi e incidenti a carico delle reti e dei sistemi informativi. **[Em. 76]**

2. La rete di collaborazione assicura la comunicazione permanente tra la Commissione e le autorità competenti. Se richiesta, l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) assiste la rete di collaborazione mettendole a disposizione le proprie competenze e consulenze. ***Se del caso, gli operatori del mercato e i fornitori di soluzioni di cibersicurezza possono essere inoltre invitati a partecipare alle attività della rete di collaborazione di cui al paragrafo 3, lettere g) e i).***

La rete di collaborazione, se del caso, coopera con le autorità competenti per la protezione dei dati.

La Commissione informa regolarmente la rete di collaborazione della ricerca nell'ambito della sicurezza e di altri programmi pertinenti di Orizzonte 2020. **[Em. 77]**

3. All'interno della rete di collaborazione ~~le autorità competenti~~ ***i punti di contatto unici***:

a) diffondono preallarmi in merito a rischi e a incidenti in conformità all'articolo 10;

b) garantiscono una risposta coordinata in conformità all'articolo 11;

c) pubblicano periodicamente informazioni non riservate sui preallarmi in corso e sulla risposta coordinata su un sito comune;

d) discutono e valutano insieme~~, su richiesta di uno Stato membro o della Commissione,~~ una o più strategie nazionali e uno o più piani nazionali di collaborazione in materia di SRI ai sensi dell'articolo 5, nell'ambito della presente direttiva;

e) discutono e valutano insieme~~, su richiesta di uno Stato membro o della Commissione,~~ l'efficacia delle squadre CERT, in particolare in occasione di esercitazioni in materia di SRI eseguite a livello di Unione;

f) collaborano e scambiano ~~informazioni su tutti gli~~ ***competenze sugli*** aspetti pertinenti ***in materia di sicurezza delle reti e dell'informazione*** col Centro europeo per la lotta alla criminalità informatica di Europol e con altri organismi europei competenti in particolare nei campi della protezione dei dati, dell'energia, dei trasporti, delle banche, ~~delle borse~~ ***dei mercati finanziari*** e della sanità;

f bis) informano, se del caso, il coordinatore antiterrorismo dell'UE, mediante segnalazione, e lo invitano a fornire assistenza per l'analisi, i lavori preparatori e l'azione della rete di cooperazione;

g) si scambiano reciprocamente e comunicano alla Commissione informazioni e buone pratiche e si assistono reciprocamente ai fini della creazione di capacità in materia di SRI;

~~h) organizzano periodicamente revisioni tra pari in materia di capacità e preparazione;~~

i) organizzano esercitazioni in materia di SRI al livello di Unione e partecipano, secondo il caso, a esercitazioni internazionali in materia di SRI.

i bis) interagiscono, si consultano e scambiano informazioni, se del caso, con gli operatori di mercato in merito ai rischi e agli incidenti a carico delle reti e dei sistemi informativi;

i ter) elaborano, in collaborazione con l'ENISA, orientamenti per i criteri settoriali per la notifica di incidenti rilevanti, oltre ai parametri di cui all'articolo 14, paragrafo 2, ai fini di un'interpretazione comune, un'applicazione coerente e un'attuazione coerente all'interno dell'Unione. **[Em. 78]**

3 bis. La rete di collaborazione pubblica una volta all'anno una relazione basata sulle attività della rete e sulla relazione sintetica presentata ai sensi dell'articolo 14, paragrafo 4, della presente direttiva, per i 12 mesi precedenti. **[Em. 79]**

4. La Commissione stabilisce, mediante atti di esecuzione, le modalità necessarie per agevolare la collaborazione di cui ai paragrafi 2 e 3 tra ~~le autorità competenti e con~~ ***i punti di contatto unici,*** la Commissione ***e l'ENISA***. Tali atti di esecuzione sono adottati secondo la procedura di ~~consultazione~~ ***esame***di cui all'articolo 19, paragrafo ~~2~~ ***3***. **[Em. 80]**

Articolo 9

Sistema sicuro di scambio di informazioni

1. Lo scambio di informazioni sensibili e riservate all'interno della rete di collaborazione avviene attraverso un'infrastruttura sicura.

1 bis. I partecipanti all'infrastruttura sicura rispettano, tra l'altro, adeguate misure in materia di riservatezza e di sicurezza conformemente alla direttiva 95/46/CE e al regolamento (CE) n. 45/2001 in tutte le fasi del trattamento. **[Em. 81]**

Giovedì 13 marzo 2014

~~2. Alla Commissione è conferito il potere di adottare atti delegati, conformemente all'articolo 18, relativi alla definizione dei criteri che devono essere rispettati perché uno Stato membro sia autorizzato a partecipare al sistema sicuro di scambio di informazioni, riguardanti:~~

~~a) la disponibilità di un'infrastruttura di informazione e comunicazione sicura e resiliente a livello nazionale, che sia compatibile e interoperabile con l'infrastruttura sicura della rete di collaborazione a norma dell'articolo 7, paragrafo 3, e~~

~~b) l'esistenza di processi e risorse umane, tecniche e finanziarie adeguate per le proprie autorità competenti e squadre CERT, che ne permettano la partecipazione effettiva, efficiente e sicura al sistema sicuro di scambio di informazioni a norma dell'articolo 6, paragrafo 3, articolo 7, paragrafo 2 e articolo 7, paragrafo 3.~~ **[Em. 82]**

3. La Commissione adotta, mediante atti ~~di esecuzione, decisioni sull'accesso degli Stati membri a tale infrastruttura sicura, in base ai criteri di cui ai paragrafi 2 e 3. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 19, paragrafo 3~~ ***delegati a norma dell'articolo 18, un insieme comune*** di ***norme di interconnessione e di sicurezza a cui i punti di contatto unici si conformano prima dello scambio di informazioni sensibili e riservate nella rete di collaborazione***. **[Em. 83]**

Articolo 10

Preallarmi

1. ~~Le autorità competenti~~ ***I punti di contatto unici*** o la Commissione trasmettono preallarmi all'interno della rete di collaborazione in merito ai rischi e agli incidenti che rispondono ad una o più delle seguenti condizioni:

~~a) la cui portata aumenta o è suscettibile di aumentare rapidamente;~~

b) ***il punto di contatto unico ritiene*** che ~~superano o sono suscettibili di superare~~ ***il rischio o l'incidente superi potenzialmente*** la capacità nazionale di risposta;

c) ***i punti di contatto unici o la Commissione ritengono*** che ~~colpiscono o sono suscettibili di colpire~~ ***il rischio o l'incidente colpisca*** più di uno Stato membro. **[Em. 84]**

2. Nei preallarmi ~~le autorità competenti~~ ***i punti di contatto unici*** e la Commissione comunicano ***senza indebito ritardo*** tutte le informazioni pertinenti in loro possesso che possono essere utili a valutare il rischio o l'incidente. **[Em. 85]**

~~3. Su richiesta di uno Stato membro o di propria iniziativa la Commissione può chiedere a uno Stato membro di fornire qualunque informazione pertinente su uno specifico rischio o incidente.~~ **[Em. 86]**

4. Qualora il preallarme riguardi un rischio o un incidente di sospetta natura dolosa~~, le autorità competenti o la Commissione ne informano~~ ***e qualora l'operatore del mercato interessato abbia segnalato incidenti di cui sospetta la natura dolosa grave a norma dell'articolo 15, paragrafo 4, gli Stati membri garantiscono che*** il Centro europeo per la lotta alla criminalità informatica di Europol ***sia informato, se del caso***.**[Em. 87]**

4 bis. I membri della rete di collaborazione non rendono pubbliche informazioni ricevute sui rischi e gli incidenti di cui al paragrafo 1 senza aver ricevuto previa approvazione del punto di contatto unico che ha effettuato la segnalazione.

Inoltre, prima della condivisione delle informazioni nella rete di collaborazione, il punto di contatto unico notificante informa l'operatore del mercato cui le informazioni fanno riferimento in merito alla sua intenzione, e laddove lo ritenga opportuno, rende anonime le informazioni in questione. **[Em. 88]**

4 ter. Qualora il preallarme riguardi un rischio o un incidente di sospetta natura tecnica grave a livello transfrontaliero, i punti di contatto unici o la Commissione ne informano l'ENISA. **[Em. 89]**

5. Alla Commissione è conferito il potere di adottare atti delegati, conformemente all'articolo 18, per precisare ulteriormente i rischi e gli incidenti per i quali è necessaria la trasmissione dei preallarmi di cui al paragrafo 1 del presente articolo.

Articolo 11

Risposta coordinata

1. In seguito ad un preallarme a norma dell'articolo 10 ~~le autorità competenti~~ ***i punti di contatto unici*** adottano ***senza indebito ritardo***, dopo aver valutato le informazioni pertinenti, una risposta coordinata in conformità al piano unionale di collaborazione in materia di SRI di cui all'articolo 12. **[Em. 90]**

2. Le varie misure adottate a livello nazionale in esito alla risposta coordinata sono comunicate alla rete di collaborazione.

Articolo 12

Piano unionale di collaborazione in materia di SRI

1. Alla Commissione è conferito il potere di adottare, mediante atti di esecuzione, un piano unionale di collaborazione in materia di SRI. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 19, paragrafo 3.

2. Il piano unionale di collaborazione in materia di SRI comporta:

a) ai fini dell'applicazione dell'articolo 10,

— una definizione del formato e delle procedure di raccolta e scambio di informazioni compatibili e comparabili sui rischi e sugli incidenti da parte ~~delle autorità competenti~~ ***dei punti di contatto unici***, **[Em. 91]**

— una definizione delle procedure e dei criteri di valutazione dei rischi e degli incidenti da parte della rete di collaborazione;

b) la procedura da seguire per le risposte coordinate di cui all'articolo 11, con l'individuazione dei ruoli e delle responsabilità e delle procedure di collaborazione;

c) una tabella di marcia di esercitazioni relative alla SRI e formazioni per rafforzare, convalidare e testare il piano;

d) un programma relativo al trasferimento di conoscenze tra gli Stati membri in materia di creazione di capacità e apprendimento tra pari;

e) un programma di sensibilizzazione e formazione tra gli Stati membri.

3. Il piano unionale di collaborazione in materia di SRI è adottato non oltre l'anno successivo all'entrata in vigore della presente direttiva ed è riveduto periodicamente. ***I risultati di ciascuna revisione sono comunicati al Parlamento europeo.*** **[Em. 92]**

3 bis. È assicurata la coerenza tra il piano unionale di collaborazione in materia di SRI e le strategie e i piani nazionali di collaborazione in materia di SRI, conformemente all'articolo 5. **[Em. 93]**

Articolo 13

Cooperazione internazionale

Ferma restando la possibilità, per la rete di collaborazione, di intrattenere una cooperazione informale a livello internazionale, l'Unione può concludere accordi internazionali con paesi terzi o organizzazioni internazionali che permettono o organizzano la loro partecipazione ad alcune delle attività della rete di collaborazione. Tali accordi tengono conto della necessità di garantire la protezione adeguata dei dati personali che circolano nella rete di collaborazione ***e specificano la procedura di controllo da seguire per garantire la protezione di tali dati personali. Il Parlamento europeo è informato in merito alla negoziazione degli accordi. Qualsiasi trasferimento di dati personali a destinatari ubicati in paesi al di fuori dell'Unione deve essere effettuato ai sensi degli articoli 25 e 26 della direttiva 95/46/CE e dell'articolo 9 del regolamento (CE) n. 45/2001***. **[Em. 94]**

Articolo 13 bis

Livello di criticità degli operatori del mercato

Gli Stati membri possono determinare il livello di criticità degli operatori del mercato, tenendo conto delle peculiarità dei settori, di parametri quali l'importanza per un determinato operatore del mercato di mantenere un livello sufficiente del servizio settoriale, il numero di parti fornite dall'operatore e il periodo di tempo fino a quando la discontinuità dei servizi principali dell'operatore del mercato non avrà un impatto negativo sul mantenimento di attività vitali per l'economia e la società. **[Em. 95]**

CAPO IV

SICUREZZA DELLE RETI E DEI SISTEMI INFORMATIVI DELLE PUBBLICHE AMMINISTRAZIONI E DEGLI OPERATORI DEL MERCATO

Articolo 14

Obblighi in materia di sicurezza e notifica degli incidenti

1. Gli Stati membri procurano che ~~le amministrazioni pubbliche e~~ gli operatori del mercato adottino misure tecniche e organizzative adeguate ***e proporzionate all'individuazione e*** alla gestione ***efficace*** dei rischi che corre la sicurezza delle reti e dei sistemi informativi di cui hanno il controllo e che usano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza adeguato al rischio in essere. In particolare sono adottate misure per prevenire e minimizzare l'impatto di incidenti a carico ***della sicurezza*** delle reti e dei sistemi informativi ~~relativi ai~~ ***sui*** servizi principali prestati, assicurando in questo modo la continuità dei servizi supportati da tali reti e sistemi informativi. **[Em. 96]**

2. Gli Stati membri procurano che ~~le amministrazioni pubbliche e~~ gli operatori del mercato notifichino ***senza indebito ritardo*** all'autorità competente ***o al punto di contatto unico*** gli incidenti aventi un impatto significativo sulla ~~sicurezza~~ ***continuità*** dei servizi principali prestati. ***La notifica non espone la parte che la effettua a una maggiore responsabilità.***

Per determinare l'entità dell'impatto di un incidente si tiene conto, tra le altre cose, dei seguenti parametri: **[Em. 97]**

a) il numero degli utenti i cui servizi essenziali sono stati colpiti; **[Em. 98]**

b) la durata dell'incidente; **[Em. 99]**

c) la diffusione geografica relativamente all'area interessata dall'incidente. **[Em. 100]**

Tali parametri sono ulteriormente specificati ai sensi dell'articolo 8, paragrafo 3, lettera i ter). **[Em. 101]**

2 bis. Gli operatori di mercato notificano gli incidenti di cui ai paragrafi 1 e 2 all'autorità competente o al punto unico di contatto dello Stato membro in cui si trova il servizio essenziale interessato. Qualora siano interessati i servizi essenziali di più di uno Stato membro, il punto di contatto unico che ha ricevuto la notifica allerta, sulla base delle informazioni fornite dall'operatore di mercato, gli altri punti di contatto unici interessati. L'operatore del mercato è informato quanto prima in merito agli altri punti di contatto informati dell'incidente nonché delle eventuali azioni intraprese, dei risultati o di qualsiasi informazione pertinente per l'incidente. **[Em.102]**

2 ter. Se la notifica contiene dati personali, questi sono divulgati unicamente ai destinatari dell'autorità competente notificata o del punto di contatto unico, che devono trattarli per lo svolgimento dei propri compiti, conformemente alla normativa in materia di protezione dei dati. La divulgazione dei dati si limita a quanto necessario per lo svolgimento di tali compiti. **[Em. 103]**

2 quater. Gli operatori di mercato che non rientrano nell'allegato II possono segnalare incidenti a norma dell'articolo 14, paragrafo 2, su base volontaria. **[Em. 104]**

3. Gli obblighi di cui ai paragrafi 1 e 2 si applicano a tutti gli operatori del mercato che prestano servizi all'interno dell'Unione europea.

4. ***Dopo essersi consultato con*** l'autorità competente ***notificata e l'operatore di mercato interessato, il punto di contatto unico*** può informare il pubblico~~, oppure richiedere alle amministrazioni pubbliche e agli operatori del mercato di informarlo, se ritiene che la divulgazione dell'incidente sia di pubblico interesse~~ ***sui singoli incidenti***, se ***determina che l'informazione al pubblico è necessaria per evitare un incidente o gestire un incidente in corso, o se l'operatore di mercato, in caso di incidente, si rifiuta di affrontare quanto prima una grave vulnerabilità strutturale connessa all'incidente***.

Prima di un'eventuale divulgazione pubblica, l'autorità competente notificata garantisce che l'operatore di mercato interessato abbia la possibilità di essere ascoltato e che la decisione in merito alla divulgazione pubblica sia debitamente controbilanciata dall'interesse pubblico.

Se sono rese pubbliche le informazioni sui singoli incidenti, l'autorità competente notificata o il punto di contatto unico garantiscono che siano quanto più anonime possibile.

L'autorità competente o il punto di contatto unico forniscono all'operatore di mercato interessato, se ragionevolmente possibile, le informazioni a sostegno del trattamento efficace dell'incidente notificato.

Una volta l'anno ~~l'autorità competente~~ ***il punto di contatto unico*** trasmette alla rete di collaborazione una relazione sintetica delle notifiche ricevute***, compreso il loro numero*** e ***i parametri degli incidenti di cui al paragrafo 2 del presente articolo, nonché*** delle misure adottate conformemente al presente paragrafo. **[Em. 105]**

4 bis. Gli Stati membri incoraggiano gli operatori di mercato a pubblicare nei rendiconti finanziari, su base volontaria, gli incidenti che coinvolgono le loro società. **[Em. 106]**

~~5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 18 riguardanti la definizione delle circostanze alle quali le amministrazioni pubbliche e gli operatori del mercato sono tenuti a notificare gli incidenti.~~ **[Em. 107]**

6. ~~Fatti salvi gli atti delegati adottati a norma del paragrafo 5,~~ Le autorità competenti ***o i punti di contatto unici*** possono adottare orientamenti ~~e, se necessario, emanare istruzioni~~ sulle circostanze alle quali ~~le amministrazioni pubbliche e~~ gli operatori del mercato sono tenuti a notificare gli incidenti. **[Em. 108]**

7. Alla Commissione è conferito il potere di definire, mediante atti di esecuzione, i formati e le procedure applicabili ai fini del paragrafo 2. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 19, paragrafo 3.

8. Il disposto dei paragrafi 1 e 2 non si applica alle microimprese quali definite nella raccomandazione 2003/361/CE ([1])***, a meno che le microimprese non fungano da affiliate per un operatore di mercato quale definito all'articolo 3, paragrafo 8, lettera b)***. **[Em. 109]**

8 bis. Gli Stati membri possono decidere di applicare, mutatis mutandis, il presente articolo e l'articolo 15 alle amministrazioni pubbliche. **[Em. 110]**

Articolo 15

Attuazione e controllo

1. Gli Stati membri procurano che le autorità competenti ***e i punti di contatto unici*** siano ~~dotate di tutti i~~ ***dotati dei*** poteri necessari per ~~indagare i casi di mancato~~ ***garantire il*** rispetto~~, da parte delle amministrazioni pubbliche o~~ degli ~~operatori del mercato, degli~~ obblighi ~~loro~~ imposti ***agli operatori di mercato*** dall'articolo 14 e ~~gli~~ ***degli*** effetti di tale mancato rispetto sulla sicurezza delle reti e dei sistemi informativi. **[Em. 111]**

([1]) Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

Giovedì 13 marzo 2014

2. Gli Stati membri procurano che le autorità competenti ***e i punti di contatto unici*** abbiano il potere di richiedere agli operatori del mercato ~~e alle amministrazioni pubbliche~~ di: **[Em. 112]**

a) fornire le informazioni necessarie per valutare la sicurezza delle loro reti e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;

b) ~~sottoporsi ad~~ ***comprovare l'efficace attuazione delle politiche di sicurezza, anche mediante i risultati di un*** audit ***sulla sicurezza*** audit ***sulla sicurezza*** condotto da un organismo qualificato indipendente o da un'autorità nazionale ~~e metterne i risultati~~***, mettendo i riscontri*** a disposizione dell'autorità competente ***o del punto di contatto unico***. **[Em. 113]**

Quando tale richiesta è presentata, le autorità competenti e i punti di contatto unici indicano lo scopo della stessa specificando adeguatamente il tipo di informazioni richieste. **[Em. 114]**

3. Gli Stati membri procurano che le autorità competenti ***e i punti di contatto unici*** abbiano il potere di emanare istruzioni vincolanti per gli operatori del mercato ~~e le amministrazioni pubbliche.~~ **[Em. 115]**

3 bis. In deroga al paragrafo 2, lettera b), del presente articolo, gli Stati membri possono decidere che le autorità competenti o i punti di contatto unici, se del caso, devono applicare una diversa procedura a determinati operatori del mercato, in base al loro livello di criticità stabilito ai sensi dell'articolo 13 bis. Nel caso in cui gli Stati membri decidano in tal senso:

a) le autorità competenti o i punti di contatto unici, se del caso, hanno il potere di inviare una richiesta sufficientemente specifica agli operatori del mercato in base alla quale si richiede loro di comprovare l'efficace attuazione delle politiche di sicurezza, anche mediante i risultati di un audit sulla sicurezza condotto da un revisore interno qualificato, mettendo i riscontri a disposizione dell'autorità competente o del punto di contatto unico;

b) laddove necessario, a seguito dell'invio da parte dell'operatore del mercato della richiesta di cui alla lettera a), l'autorità competente o il punto di contatto unico può richiedere ulteriori prove o lo svolgimento di un audit aggiuntivo da parte di un organismo qualificato indipendente o di un'autorità nazionale.

3 ter. Gli Stati membri possono decidere di ridurre il numero e l'intensità degli audit per un operatore di mercato interessato se il relativo audit sulla sicurezza indica il rispetto delle disposizioni del capo IV in modo coerente. **[Em. 116]**

4. Le autorità competenti ~~notificano~~ ***e i punti di contatto unici informano gli operatori del mercato interessati in merito alla possibilità di segnalare*** alle autorità di contrasto gli incidenti di cui sospettano la natura dolosa grave. **[Em. 117]**

5. ***Fatte salve*** le ***norme di legge applicabili in materia di protezione dei dati,*** le autorità competenti ***e i punti di contatto unici*** operano in stretta cooperazione con le autorità competenti della protezione dei dati personali nei casi di incidenti che comportano violazioni di dati personali. ***I punti di contatto unici e le autorità competenti della protezione dei dati mettono a punto, in collaborazione con l'ENISA, meccanismi per lo scambio di informazioni e un modello unico da utilizzare tanto per le notifiche di cui all'articolo 14, paragrafo 2, della presente direttiva quanto per altre norme dell'Unione in materia di protezione dei dati.*** **[Em. 118]**

6. Gli Stati membri garantiscono che gli obblighi imposti dal presente capo ~~alle pubbliche amministrazioni e~~ agli operatori del mercato possano essere soggetti a controllo giurisdizionale. **[Em. 119]**

6 bis. Gli Stati membri possono decidere di applicare, mutatis mutandis, l'articolo 14 e il presente articolo alle amministrazioni pubbliche. **[Em. 120]**

Articolo 16

Normazione

1. Per garantire l'attuazione convergente del disposto dell'articolo 14, paragrafo 1, gli Stati membri***, senza prescrivere l'uso di una particolare tecnologia,*** incoraggiano l'uso di norme e/o specifiche ***interoperabili europee o internazionali*** relative alla sicurezza delle reti e dell'informazione. **[Em. 121]**

2. ~~Mediante atti di esecuzione~~ la Commissione ~~redige~~ ***dà mandato a un pertinente organismo di normazione europeo di redigere, in consultazione con le parti interessate,*** un elenco delle norme ***e/o delle specifiche*** di cui al paragrafo 1. L'elenco è pubblicato nella *Gazzetta ufficiale dell'Unione europea*. **[Em. 122]**

CAPO V

DISPOSIZIONI FINALI

Articolo 17

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano tali disposizioni alla Commissione entro la data di attuazione della presente direttiva e provvedono a dare immediata notifica di ogni successiva modifica.

1 bis. Gli Stati membri garantiscono che le sanzioni di cui al paragrafo 1 del presente articolo vengano applicate solo se l'operatore del mercato è venuto meno intenzionalmente o per grave negligenza agli obblighi di cui al capo IV. **[Em. 123]**

2. Gli Stati membri assicurano che, se un incidente di sicurezza coinvolge dati personali, le sanzioni previste siano coerenti con le sanzioni contemplate dal regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati ([1]).

Articolo 18

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. È conferito alla Commissione il potere di adottare gli atti delegati di cui all'articolo 9, paragrafo 3, e all'articolo 10, paragrafo 5. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 9, paragrafo 3 e all'articolo 10, paragrafo 5, ~~e all'articolo 14, paragrafo 5,~~ può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla sua pubblicazione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore. **[Em. 124]**

4. Non appena adotta un atto delegato, la Commissione lo notifica simultaneamente al Parlamento europeo e al Consiglio.

([1]) SEC(2012) 72 definitivo.

5. L'atto delegato adottato ai sensi dell'articolo 9, paragrafo 3, e dell'articolo 10, paragrafo 5, ~~e dell'articolo 14, paragrafo 5,~~ entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio. **[Em. 125]**

Articolo 19

Procedura di comitato

1. La Commissione è assistita da un comitato (in prosieguo «il comitato per la sicurezza delle reti e dell'informazione»). Tale comitato è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 4 del regolamento (UE) n. 182/2011.

3. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

Articolo 20

Revisione

La Commissione riesamina periodicamente il funzionamento della presente direttiva***, in particolare l'elenco di cui all'allegato II,*** e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La prima relazione è presentata entro tre anni dalla data di attuazione di cui all'articolo 21. A tal fine la Commissione può chiedere agli Stati membri di fornire informazioni senza ritardi. **[Em. 126]**

Articolo 21

Attuazione

1. Gli Stati membri adottano e pubblicano, entro [un anno dalla data di adozione], le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

Essi applicano tali disposizioni a partire da [un anno e mezzo dalla data di adozione].

Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della loro pubblicazione ufficiale. Le modalità del riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni essenziali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

Articolo 22

Entrata in vigore

La presente direttiva entra in vigore il [ventesimo] giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 23

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a …,

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

ALLEGATO I

Requisiti e compiti delle squadre di pronto intervento informatico (CERT)

I requisiti e i compiti delle squadre CERT devono essere adeguatamente e chiaramente definiti nel quadro di una strategia e/o di una regolamentazione nazionale. Essi includono quanto segue:

1) Requisiti per le squadre CERT

a) ~~La squadra~~ ***Le squadre*** CERT ~~garantisce~~ ***garantiscono*** un'elevata disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e ~~dispone~~ ***dispongono*** di vari mezzi che ~~le~~ permettono ***loro*** di essere ~~contattata~~ ***contattate*** e di contattare altri ***in qualsiasi momento***. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla sua base di utenti e ai partner con cui collabora. **[Em. 128]**

b) La squadra CERT attua e gestisce misure di sicurezza che garantiscono la riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni che riceve e tratta.

c) Gli uffici ~~della squadra~~ ***delle squadre*** CERT e i sistemi informativi di supporto sono ubicati in siti sicuri***, con reti e sistemi informativi protetti***. **[Em. 129]**

d) È istituito un sistema di gestione della qualità del servizio per seguire le prestazioni della squadra CERT e garantire un costante processo di miglioramento. Tale sistema si basa su metriche chiaramente definite che includono livelli formali di servizio e indicatori principali di prestazione.

e) Continuità operativa:

— la squadra CERT è dotata di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi,

— la squadra CERT dispone di personale sufficiente per garantirne l'operatività 24 ore su 24,

— la squadra CERT opera in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario costituire sistemi ridondanti e spazi di lavoro di backup perché la squadra CERT possa garantire l'accesso permanente ai mezzi di comunicazione.

2) Compiti delle squadre CERT

a) I compiti delle squadre CERT comprendono almeno:

— ***identificazione e*** monitoraggio degli incidenti a livello nazionale, **[Em. 130]**

— emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti,

— risposta agli incidenti,

— informazioni sul rischio dinamico e analisi degli incidenti, nonché sensibilizzazione situazionale,

— massiccia sensibilizzazione del pubblico sui rischi connessi all'attività online,

— ***partecipazione attiva alle reti di collaborazione delle squadre CERT internazionali e dell'Unione,*** *[Em. 131]*

— organizzazione di campagne sulla sicurezza delle reti e dell'informazione (SRI).

b) Le squadre CERT stabiliscono relazioni di cooperazione con il settore privato.

c) Per facilitare la cooperazione, le squadre CERT promuovono l'adozione e l'uso di prassi comuni o standardizzate nei seguenti settori:

— procedure di trattamento degli incidenti e dei rischi,

— programmi di classificazione degli incidenti, dei rischi e delle informazioni,

— tassonomie delle metriche,

— modelli di scambi di informazione su rischi, incidenti e convenzioni di denominazione dei sistemi.

Giovedì 13 marzo 2014

ALLEGATO II

Elenco degli operatori del mercato

~~Operatori di cui all'articolo 3, paragrafo 8, lettera a):~~

~~1. Piattaforme di commercio elettronico~~

~~2. Portali di pagamento su internet~~

~~3. Reti sociali~~

~~4. Motori di ricerca~~

~~5. Servizi nella nuvola (cloud computing)~~

~~6. Negozi online di applicazioni~~

~~Operatori di cui all'articolo 3, paragrafo 8, lettera b):~~ **[Em. 132]**

1. Energia

a) Elettricità

— Fornitori ~~di elettricità e di gas~~ ***i***~~—~~

— Operatori dei sistemi di distribuzione ~~dell'elettricità e/o del gas e distributori~~ al dettaglio ai consumatori finali

~~— Gestori dei sistemi di trasporto, di impianti di stoccaggio o di impianti di GNL nel settore del gas naturale~~

— Operatori dei sistemi di trasmissione nel settore dell'energia elettrica

b) Petrolio

— Oleodotti e depositi di petrolio

— Operatori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio

c) Gas

~~— Operatori del mercato dell'energia elettrica e del gas~~

— Fornitori

— Operatori dei sistemi di distribuzione e distributori al dettaglio ai consumatori finali

— Operatori dei sistemi di trasporto, di impianti di stoccaggio e di GNL nel settore del gas naturale

— Operatori di impianti di produzione, raffinazione ~~e~~, trattamento ~~di petrolio e~~***, deposito e trasporto di*** gas naturale

— Operatori del mercato del gas *[Em. 133]*

2. Trasporti

~~— Vettori aerei (trasporto aereo di merci e passeggeri)~~

~~— Vettori marittimi (compagnie di navigazione per il trasporto marittimo e costiero di passeggeri e per il trasporto marittimo e costiero di merci)~~

~~— Trasporto ferroviario (gestori dell'infrastruttura, imprese integrate e operatori di trasporto ferroviario)~~

— ~~Aeroporti~~

— ~~Porti~~

— ~~Operatori attivi nel controllo della gestione del traffico~~

— ~~Servizi logistici ausiliari a) deposito e stoccaggio, b) movimentazione merci e c) altre attività di supporto ai trasporti)~~

a) Trasporti su strada

i) Operatori attivi nel controllo della gestione del traffico

ii) Servizi logistici ausiliari:

— deposito e stoccaggio,

— movimentazione merci, e

— altre attività di supporto ai trasporti

b) Trasporto ferroviario

i) Trasporto ferroviario (gestori dell'infrastruttura, imprese integrate e operatori di trasporto ferroviario)

ii) Operatori attivi nel controllo della gestione del traffico

iii) Servizi logistici ausiliari:

— deposito e stoccaggio,

— movimentazione merci, e

— altre attività di supporto ai trasporti

c) Trasporto aereo

i) Vettori aerei (trasporto aereo di merci e passeggeri)

ii) Aeroporti

iii) Operatori attivi nel controllo della gestione del traffico

iv) Servizi logistici ausiliari:

— depositi,

— movimentazione merci, e

— altre attività di supporto ai trasporti

d) Trasporti marittimi

i) Vettori marittimi (compagnie di navigazione per il trasporto terrestre, marittimo e costiero di passeggeri e per il trasporto terrestre, marittimo e costiero di merci) *[Em. 134]*

3. Settore bancario: enti creditizi ai sensi dell'articolo 4, punto 1, della direttiva 2006/48/CE del Parlamento europeo e del Consiglio ([1]).

([1]) Direttiva 2006/48/CE del Parlamento europeo e del Consiglio, del 14 giugno 2006, relativa all'accesso all'attività degli enti creditizi ed al suo esercizio (GU L 177 del 30.6.2006, pag. 1)

Giovedì 13 marzo 2014

4. Infrastrutture dei mercati finanziari: ~~Borse~~ ***mercati regolamentati, strutture multilaterali di negoziazione, strutture organizzate di negoziazione*** e stanze di compensazione di tipo controparte centrale **[Em. 135]**

5. Settore sanitario: istituti sanitari (compresi ospedali e cliniche private) e altri soggetti che forniscono assistenza sanitaria

5 bis. ***Produzione e approvvigionamento idrico*** **[Em. 136]**

5 ter. ***Catena di approvvigionamento alimentare*** **[Em. 137]**

5 quater. ***Punti di scambio Internet*** **[Em. 138]**