diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La Direttiva UE n. 1148/2016 sulla sicurezza delle reti e dei sistemi informativi dell'Unione

Autore: Muia' Pier Paolo
In: Diritto civile e commerciale

Parlamento e Consiglio Europeo: Direttiva n. 1148 del 6 luglio 2016

Premessa

Nel 2016 (così come tutt'ora) le reti informatiche e i relativi sistemi svolgevano di già un ruolo fondamentale, sia dal punto di vista economico che dal punto di vista informativo e di relazione. Per tali motivi, l'unione europea ha ritenuto che dette reti e servizi dovessero essere affidabili e sicuri per tutte le attività economiche e sociali, in modo da garantire un corretto funzionamento del mercato interno.

La verificazione di incidenti rispetto alla sicurezza delle reti di servizi informatici, quindi, poteva e può determinare delle limitazioni allo svolgimento dell'attività economiche e conseguentemente minare la fiducia degli utenti in tali servizi, con conseguenti notevoli perdite di carattere finanziario e danni in generale all'economia dei paesi dell'unione europea.

Il Parlamento e il Consiglio dell'Unione Europea, quindi, hanno ritenuto necessario costituire un gruppo di cooperazione tra gli Stati membri all'interno del quale vi fossero dei rappresentanti degli Stati medesimi nonché della commissione europea e dell'agenzia dell'unione europea per la sicurezza delle reti (ENISA), in modo che detto gruppo potesse agevolare la cooperazione degli Stati in materia di sicurezza delle reti informatiche. Inoltre, il Parlamento il consiglio europeo hanno valutato che, per poter permettere a tale gruppo di cooperazione di svolgere i propri compiti e raggiungere la suddetta finalità, fosse essenziale che tutti gli Stati membri avessero un livello minimo di capacità e di strategia in materia di sicurezza delle reti e dei sistemi informatici, in modo che vi fosse armonia in tutti gli Stati a livello di protezione delle reti medesime.

Infatti, nel 2016, i livelli di conoscenza in materia di protezione e sicurezza delle reti degli Stati membri erano molto diversi tra di loro e non garantivano un livello omogeneo di protezione delle imprese e dei consumatori. Secondo il Parlamento e il Consiglio, invece, per poter garantire la sicurezza delle reti e dei sistemi informativi, era necessario un approccio generale da parte di tutta l'unione europea, in modo che tutti gli Stati avessero un livello adeguato di protezione così da evitare incidenti e rischi per la sicurezza delle reti.

Diritto & Diritti ISSN 1127-8579

In considerazione di tali valutazioni, nel 2016, l'unione europea ha quindi approvato la direttiva numero 1148 del Parlamento e del consiglio avente proprio ad oggetto delle misure per la sicurezza delle reti e dei sistemi informatici, imponendo agli stati membri l'adozione di normative interne che recepissero tali misure.

La Direttiva UE

Il primo articolo della direttiva stabilisce l'oggetto e l'ambito di applicazione, precisando che la Direttiva individua le misure che servono per raggiungere un livello elevato, comune in tutti gli Stati membri, di sicurezza della rete e dei sistemi informativi dell'Unione, in modo da migliorare il funzionamento del mercato interno. In particolare, **la Direttiva obbliga tutti gli Stati membri ad adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi** e in generale **stabilisce degli obblighi di sicurezza a carico degli operatori e fornitori dei servizi digitali** nonché **crea un gruppo di cooperazione tra gli Stati per garantire lo scambio di informazioni** e **una rete di gruppi di intervento per la sicurezza informatica (CSIRT), con il compito di intervenire in caso di incidenti informatici, obbligando altresì gli Stati membri a designare un'autorità nazionale che si occupi della sicurezza della rete**.

La Direttiva impone, poi, agli Stati membri di adottare delle normative idonee a raggiungere un livello di sicurezza più elevato della rete e dei sistemi informativi.

L'articolo 4 è dedicato alle definizioni e stabilisce, tra le altre, cosa debba intendersi per **rete e sistema informativo** (cioè una rete di comunicazione elettronica oppure un qualsiasi dispositivo o gruppi di dispositivi interconnessi che esegue, attraverso un programma, un trattamento automatico di dati digitali oppure comunque un insieme di dati digitali trattati o trasmessi per messo delle reti o dei dispositivi di comunicazione alettronica), per **sicurezza della rete e dei sistemi informativi** (cioè la capacità di una rete di comunicazione elettronica o dei suddetti dispositivi di resistere ad attacchi che mirano a compromettere l'autenticità, la disponibilità, l'integrità o la riservatezza dei dati che vengono trattati), per **fornitore di servizio digitale** (inteso come qualsiasi persona giuridica che fornisca un servizio digitale) e per **incidente** (cioè ogni evento che pregiudichi la sicurezza della rete e dei sistemi informativi).

La direttiva individua i criteri per identificare gli operatori dei servizi essenziali, indicandoli in coloro i quali forniscono un servizio che è essenziale per mantenere le attività sociali e/o economiche fondamentali nei paesi dell'Unione oppure che forniscono un servizio che dipende dalla rete e dai sistemi informativi o comunque che forniscono un servizio rispetto al quale un "incidente" avrebbe effetti negativi sulla sua fornitura.

La **Direttiva, inoltre, impone ad ogni Stato membro**:

Diritto & Diritti ISSN 1127-8579

- di **adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi** con cui vengano individuate le misure per raggiungere e garantire un livello elevato di sicurezza della rete;

- di **designare una o più autorità nazionali** (Autorità competente), che si occupino della sicurezza delle reti e dei sistemi informativi e vigilino sull'applicazione della Direttiva all'interno dello Stato;

- di **designare un punto di contatto unico nazionale** in materia di sicurezza delle reti e dei sistemi informativi, che si occupi di garantire e mantenere i collegamenti tra l'Autorità competente nazionale dello Stato membro e quelle degli altri stati membri nonché con i CSIRT;

- di **designare uno o più CSIRT**, che si occupino di gestire gli incidenti e i rischi per la rete e i sistemi informativi.

La Direttiva, inoltre, **crea un gruppo di cooperazione** con il compito di raggiungere una strategia di cooperazione e di scambio di informazioni fra gli Stati membri in materia di sicurezza della rete (in modo da aumentare la sicurezza stessa all'interno dell'Unione e quindi far crescere la fiducia dei cittadini). I membri di tale gruppo di cooperazione vengono individuati nei rappresentanti di tutti gli Stati membri, della Commissione europea e dell'ENISA e il gruppo ha il compito di dare un orientamento strategico per le attività dei CSIRT, di scambiare buone pratiche in ordine allo scambio di informazioni sugli incidenti e sulla relativa formazione, di discutere del livello di preparazione degli Stati membri in materia di sicurezza delle reti e individuare le migliori pratiche, di discutere delle norme da adottare insieme con i rappresentanti degli organi legiferanti europei.

La Direttiva **crea altresì una rete di CSIRT**, con l'obiettivo di promuovere una cooperazione rapida ed efficace fra gli Stati e così far crescere la fiducia tra i medesimi. A tale rete la Direttiva affida il compito di scambiare informazioni sui servizi e sulle attività dei CSIRT, di scambiare e discutere informazioni (non commerciali) connesse ad un "incidente" e ai correlati rischi, di scambiare e mettere a disposizione le informazioni non riservate relative a singoli "incidenti", sostenere gli Stati membri nell'affrontare "incidenti" transfrontalieri e infine discutere e e individuare ulteriori forme di cooperazione fra gli Stati in ordine a categorie di "incidenti" e assistenza reciproca.

La Direttiva, inoltre, impone agli Stati membri di provvedere (con la normativa interna) affinchè gli operatori dei servizi essenziali adottino delle misure tecniche e organizzative idonee a gestire i rischi alla sicurezza delle reti e dei sistemi informatici, che detti operatori usano per svolgere la loro attività, nonché **affinchè prevengano e minimizzino le conseguenze degli "incidenti" sulla sicurezza della rete e notifichino senza ritardo all'autorità competente o al CSIRT gli "incidenti"** che incidano sulla continuità dei servizi essenziali che detti operatori forniscono.

Diritto & Diritti ISSN 1127-8579

Naturalmente, la Direttiva impone altresì agli Stati membri di fare in modo che le Autorità competenti siano dotate dei poteri e dei mezzi necessari per verificare se gli operatori dei servizi essenziali rispettino gli obblighi di cui sopra.

La Direttiva, inoltre, impone agli Stati membri di provvedere (sempre attraverso la normativa interna) affinchè anche i fornitori dei servizi digitali adottino delle misure tecniche e organizzative idonee a gestire i rischi alla sicurezza delle reti e dei sistemi informatici, che detti operatori usano per fornire i servizi digitali, nonché **affinchè prevengano e minimizzino le conseguenze degli "incidenti" sulla sicurezza della rete che usano per fornire i propri servizi e notifichino senza ritardo all'autorità competente o al CSIRT gli "incidenti"** che incidano sulla fornitura dei servizi forniti da tali soggetti.

Anche in questo caso, la Direttiva impone agli Stati membri di fare in modo che le autorità competenti vigilino sul rispetto degli obblighi di cui sopra da parte dei fornitori dei servizi digitali e intervengano in caso di mancato rispetto degli obblighi.

Infine, la Direttiva stabilisce l'assoggettamento del fornitore dei servizi digitali alla giurisdizione dello Stato membro in cui lo stesso ha il proprio stabilimento principale oppure (in caso in cui non abbia tale stabilimento) nello stato in cui sia stabilito il rappresentante del fornitore e impone agli Stati membri di individuare le sanzioni da applicare nel caso in cui venissero violate le disposizioni nazionali applicative della Direttiva.

Volume consigliato

https://www.diritto.it/la-direttiva-ue-n-1148-2016-sulla-sicurezza-delle-reti-e-dei-sistemi-informativi-delluni one/

Diritto & Diritti ISSN 1127-8579