Cristina Vicarelli
Avvocato

La direttiva NIS: il primo passo della strategia europea per la cybersecurity

Il 6 Luglio 2016 il Parlamento Europeo ha adottato la DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIOdel 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS). La direttiva si colloca all'interno di una strategia europea che mira a rafforzare la cybersecurity e la resilienza informatica dell'Unione Europea e muove dalla considerazione che le reti, i sistemi e i servizi informativi svolgono un ruolo vitale nella società e, pertanto, è essenziale che essi siano affidabili e sicuri per le attività economiche e sociali, in particolare ai fini del funzionamento del mercato interno.

Per fare ciò, e per fornire una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi, si è reputato necessario un approccio globale a livello di Unione, che contemplasse la creazione di una capacità minima comune e disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali. Nulla impedisce, però, che gli operatori di servizi essenziali e i fornitori di servizi digitali applichino misure di sicurezza più rigorose di quelle previste dalla direttiva.

La Direttiva è entrata in vigore nell'Agosto del 2016 e gli stati membri da allora hanno tempo sino al 9 maggio 2018 per trasporla -attraverso la normativa nazionale- nei rispettivi ordinamenti e altri 6 mesi per identificare gli "operatori dei servizi essenziali". Fermo il livello di armonizzazione minimo posto dalla direttiva, gli Stati membri sono liberi di adottare norme che garantiscono un livello di protezione più elevato.

Chi sono gli operatori di servizi essenziali?

La Direttiva NIS non identifica direttamente gli "operatori di servizi essenziali" ma detta alcuni criteri per la loro individuazione.

In particolare è tale il soggetto pubblico o privato, che appartiene alle categorie elencate nell'allegato 2 della medesima direttiva (energia, trasporti, settore bancario, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, infrastrutture dei mercati finanziari), che soddisfa i seguenti criteri:

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

La Direttiva NIS e i fornitori di servizi digitali

La Direttiva NIS non si applica solo ai fornitori di servizi essenziali, ma si applica anche ai cd. "fornitori di servizi digitali". E' tale qualsiasi persona giuridica che offra un servizio digitale. Anche i servizi digitali non vengono individuati direttamente ma attraverso un duplice richiamo: il primo alla Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, il secondo all'elenco contenuto nell'allegato III della direttiva stessa che riporta :

1. Mercato online (online marketplace)

2. Motore di ricerca online

3. Cloud computing.

Che cosa prevede la direttiva NIS in sintesi

La direttiva NIS è volta ad assicurare un elevato livello comune di sicurezza delle reti e dei sistemi informativi in tutta l'UE.

La direttiva NIS mira a incrementare il livello complessivo di sicurezza informatica assicurando:

1. che gli Stati Membri si muniscano di strumenti appropriati, ad esempio designando un gruppo di intervento per la sicurezza informatica in caso di incidente («CSIRT») e un'autorità nazionale competente in materia di sicurezza delle reti e dei sistemi informativi;
2. che gli stati membri cooperino tra loro, istituendo un gruppo di cooperazione – composto da rappresentanti degli Stati membri, dalla Commissione e dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)- al fine di sostenere e agevolare la cooperazione strategica fra gli Stati membri in relazione alla sicurezza delle reti e dei sistemi informativi e facilitare lo scambio di informazioni tra gli stati membri, in modo da accrescere la fiducia. Essi dovranno anche creare una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (rete CSIRT) allo scopo di promuovere una cooperazione operativa rapida ed efficace su specifici incidenti e condividere le informazioni relative ai rischi;
3. che si sviluppi la cultura della sicurezza nei settori che sono vitali per l'economia e la società, e che si basano profondamente sulle tecnologie dell'informazione e della comunicazione, come ad esempio i trasporti, l'energia, le banche, le infrastrutture dei mercati finanziari, la salute e le infrastrutture digitali. I soggetti pubblici e privati che operino in questi settori e che saranno individuati dagli stati membri come operatori di servizi essenziali dovranno prendere appropriate misure di sicurezza per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi e notificare gli incidenti rilevanti all'autorità nazionale competente. Anche i fornitori di servizi digitali (motori di ricerca, cloud computing e online marketplaces) dovranno

conformarsi ai requisiti di sicurezza e al regime delle notifiche previsti dalla direttiva.

Requisiti di sicurezza

Gli Stati membri dovranno provvedere affinché gli operatori di servizi essenziali adottino misure tecniche e organizzative adeguatee proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

Più dettagliate le regole per i fornitori di servizi digitali: gli Stati membri dovranno provvedere affinché questi ultimi identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano.

Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e tengono conto dei seguenti elementi:

1. la sicurezza dei sistemi e degli impianti;
2. trattamento degli incidenti;
3. gestione della continuità operativa;
4. monitoraggio, audit e test;
5. conformità con le norme internazionali.

La Commissione potrà ulteriormente specificare questi parametri.

Obblighi in materia di sicurezza e notifica degli incidenti

La direttiva NIS definisce incidente "ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi".

Gli operatori di servizi essenziali e i fornitori di servizi digitali devono notificare all'autorità competente o al CSIRT (non, quindi, alle persone che usufruiscono del servizio) ogni incidente che abbia:

1. un impatto rilevante sulla continuità dei servizi essenziali prestati (se sono operatori di servizi essenziali) oppure
2. un impatto sostanziale sulla fornitura di un servizio digitale (nel caso di fornitori di servizi digitali).

La direttiva distingue gli impatti rilevati riferiti ai servizi essenziali, da quelli sostanziali, riferiti, invece, ai servizi digitali.

In particolare per stabilire se un incidente sia rilevante occorrerà tenere conto dei seguenti criteri:

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

Per determinare se un incidente sia sostanziale occorrerà tenere conto:

a) del numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi;

b) della durata dell'incidente;

c) della diffusione geografica relativamente all'area interessata dall'incidente;

d) della portata della perturbazione del funzionamento del servizio;

e) della portata dell'impatto sulle attività economiche e sociali.

Questi parametri possono essere ulteriormente specificati dalla Commissione.

Solo nell'ultimo caso (notifica di incidenti che riguardano servizi digitali) è prevista la possibilità di informare il pubblico: dopo aver consultato il fornitore di servizi digitali

interessato, infatti, l'autorità competente o il CSIRT e, se del caso, le autorità o i CSIRT degli altri Stati membri interessati, possono informare il pubblico riguardo ai singoli incidenti o chiedere al fornitore di servizi digitali di provvedervi, qualora sia necessaria la sensibilizzazione del pubblico per evitare un incidente o gestirne uno in corso, o qualora la divulgazione dell'incidente sia altrimenti nell'interesse pubblico.

Nella pratica, nella valutazione operata in ordine alla comunicazione al pubblico, le Autorità o i CSIRT dovranno valutare attentamente i danni commerciali, anche in termini reputazionali, che la diffusione della comunicazione è potenzialmente in grado di arrecare non solo al fornitore ma anche a eventuali soggetti che si basano sul servizio compromesso per fornire i loro servizi.

In ordine alle tempistiche previste per la notifica, questa, in entrambe le ipotesi dovrà avvenire senza ingiustificato ritardo.

E' altresì prevista una modalità di notifica volontaria che possono effettuare i soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali; costoro, ferma restando la possibilità degli Stati nazionali di adottare nome che garantiscano un livello di protezione più elevato di quello della direttiva, possono notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati.

Le notifiche volontarie sono trattate soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo per gli Stati membri interessati.

In ogni caso la direttiva stabilisce che la notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

Integrazione con la normativa sulla protezione dei dati personali

La legislazione degli Stati membri individua le Autorità competenti, ma la direttiva NIS, dato che in molti casi gli incidenti compromettono dati personali, dispone anche che

l'autorità competente debba operare in stretta cooperazione con le autorità che vigilano sulla protezione dei dati, nei casi di incidenti che comportano violazioni di dati personali.

Al riguardo è opportuno che le autorità competenti e le autorità che vigilano sulla protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti.

E' importante segnalare come la normativa sulla protezione dei dati personali menzionata nella direttiva NIS e il cui rispetto la medesima direttiva richiama più volte, è destinata ad essere abrogata e sostituita dal Regolamento Generale sulla protezione dei dati.

Ebbene, detto Regolamento, già adottato e pubblicato, diventerà pienamente efficace nel maggio del 2018, dispiegando anche il suo effetto abrogativo sulla disciplina previgente.

A differenza della normativa attuale (Direttiva 965/46/CE) il Regolamento prevede un'autonoma disciplina sulla violazione dei dati personali (data breach), che si compone di peculiari procedure ed è diretta a differenti autorità.

Le due discipline non vanno confuse, e non vanno considerate un unicum: il regolamento sulla protezione dei dati e la direttiva NIS hanno diverso oggetto e diverso ambito di applicazione; tuttavia le due normative possono sovrapporsi quando un incidente di sicurezza implichi anche una violazione di dati personali: in questo caso i soggetti pubblici o privati che erogano il servizio interessato dall'incidente (e dalla contestuale violazione di dati personali) dovranno adempiere agli obblighi di notifica previsti da entrambe le normative, ossia dovranno effettuare sia la notifica per gli incidenti di cui alla direttiva NIS, sia la notifica per la violazione dei dati personali prevista dal RGPD (o GDPR).

È auspicabile pertanto che le Autorità responsabili della protezione dei dati (DPA) e le autorità nazionali competenti ai sensi della direttiva NIS emanino delle linee guida su come le imprese (o comunque i soggetti obbligati) possano far fronte agli incidenti di sicurezza in modo da assicurare la compliance a entrambe le normative e che comunque

i soggetti obbligati adottino idonee policy e misure organizzative interne in modo da poter svolgere tutti gli incombenti nei tempi brevissimi imposti dal RGPD.

Un'ultima annotazione: la direttiva NIS non esaurisce gli obblighi di sicurezza informatica, anche i soggetti che non sono obbligati agli adempimenti imposti dalla direttiva, infatti, possono essere destinatari di altre norme che impongono obblighi paralleli; in particolare, in ordine al trattamento dei dati personali, ho già parlato degli obblighi attinenti alla sicurezza informatica ai quali saranno tenuti tutti i titolari in attuazione dei principi di integrità e riservatezza.