# La c.d. “Direttiva NIS II” e la riforma europea in materia di *cybersecurity*

15/03/2021

DIRITTO EUROPEO E DELLA CONCORRENZA, IT&TMT, PROTEZIONE DEI DATI E CYBERSECURITY

Roberto A. Jacchia
Marco Stillo

In data 16 dicembre 2020, la Commissione ha proposto[1] una revisione completa delle norme contenute nella c.d. “Direttiva NIS”[2] al fine di adeguare l’attuale quadro giuridico europeo alla crescente digitalizzazione del mercato interno dotandolo degli strumenti necessari per far fronte all’evoluzione delle minacce alla cibersicurezza, la cui attualità è testimoniata dal recente attacco informatico[3] subito dell’Agenzia Europea per i Medicinali (*European Medicines Agency*, EMA) che ha causato l’esposizione di informazioni sensibili legate al vaccino contro il *coronavirus* prodotto dalla *BionNTech-Pfizer*[4].

Introdotta nel 2016 per assicurare un elevato livello di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti gli Stati Membri, la Direttiva NIS stabilisce i requisiti minimi di sicurezza informatica che debbono venire adottati da parte degli operatori delle infrastrutture critiche, imponendo anche dei livelli minimi di sicurezza delle tecnologie, delle reti e dei servizi digitali[5]. Nel corso degli anni, tuttavia, la Direttiva

[1] Com. Comm. COM(2020) 823 final del 16.12.2020, *Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la Direttiva UE 2016/1148*.
[2] Direttiva UE 2016/1148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell’Unione, GUUE L 194 del 19.07.2016.
[3] Per ulteriori informazioni, si veda il seguente LINK.
[4] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.
[5] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.

ha mostrato diversi limiti quali, tra gli altri, un basso livello di cyber-resilienza delle imprese dell'Unione, livelli di resilienza asimmetrici tra Stati Membri e tra settori, basso livello di consapevolezza situazionale comune e *deficit* nella risposta comune alle crisi.

A fronte di questo scenario, la proposta di "Direttiva NIS II", concepita nell'ambito della nuova strategia europea per la *cybersecurity*[6], mira ad eliminare le divergenze e le disparità tra gli Stati Membri, stabilendo norme minime riguardanti il funzionamento di un quadro normativo coordinato, meccanismi per una cooperazione efficace tra le autorità nazionali responsabili, aggiornamento dell'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza e mezzi di ricorso e sanzioni effettivi.

Più particolarmente, la proposta amplia l'ambito di applicazione della precedente Direttiva NIS, che si incentrava sulla distinzione tra, da un lato, gli operatori di servizi essenziali (OSE), ossia quei soggetti pubblici o privati che erogano servizi nei settori dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, sanitario, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali[7] e, dall'altro, i fornitori di servizi digitali (FSD), ossia le persone giuridiche che forniscono servizi di *e-commerce*, *cloud computing* e motori di ricerca, che dispongono di uno stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale e che non rientrano nella definizione di piccola o micro impresa[8]. La Direttiva NIS II, invece, abolirà la distinzione tra OSE e FSD, introducendo quella tra entità essenziali[9] ed entità importanti[10].

Questa nuova distinzione comporta diverse conseguenze.

In primo luogo, al fine di rimediare alle discrepanze all'interno del mercato unico causate dalla Direttiva NIS, non spetterà più agli Stati Membri il compito di identificare i destinatari delle norme[11], che saranno individuati dalla Direttiva NIS II[12] attraverso la regola della soglia di dimensione. In base ad essa, rientrano

---

[6] Com. Comm. JOIN(2020) 18 final del 16.12.2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*.

[7] L'articolo 5 della Direttiva UE 2016/1148, intitolato "Identificazione degli operatori di servizi essenziali", al paragrafo 2 dispone: "*... I criteri per l'identificazione degli operatori di servizi essenziali di cui all'articolo 4, punto 4, sono i seguenti:*
*a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;*
*b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; e*
*c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio...*".

[8] Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese, GUUE L 124 del 20.05.2003. L'articolo 2 della Raccomandazione, intitolato "Effettivi e soglie finanziarie che definiscono le categorie di imprese", ai paragrafi 2-3 dispone: "*... Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR.*
*Nella categoria delle PMI si definisce microimpresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR...*".

[9] Quali, tra gli altri, i settori dell'energia, dei trasporti, delle banche, delle infrastrutture del mercato finanziario, della salute e della pubblica amministrazione. Per ulteriori informazioni si veda l'Allegato I della proposta.

[10] Quali, tra gli altri, i servizi postali, la gestione dei rifiuti, l'industria chimica nonché quella alimentare. Per ulteriori informazioni si veda l'Allegato II della proposta.

[11] L'articolo 5 della Direttiva UE 2016/1148, intitolato "Identificazione degli operatori di servizi essenziali", al paragrafo 1 dispone: "*… Entro il 9 novembre 2018, gli Stati membri identificano, per ciascun settore e sottosettore di cui all'allegato II, gli operatori di servizi essenziali con una sede nel loro territorio…*".

[12] L'articolo 2 della Proposta, intitolato "Ambito di applicazione", al paragrafo 1 dispone: "*… La presente direttiva si applica ai tipi di soggetti pubblici e privati definiti soggetti essenziali di cui*

nel suo ambito di applicazione tutte le medie e le grandi imprese, quali definite nella Raccomandazione 2003/361/CE, che operano nei settori o forniscono il tipo di servizi contemplati dalla direttiva stessa. Le micro e piccole imprese, pertanto, continueranno in linea di principio a rimanere al di fuori del perimetro della direttiva, a meno che rientrino in una delle ipotesi previste dall'articolo 2, comma 2[13], nel qual caso le nuove norme si applicheranno indipendentemente dalle dimensioni dell'impresa.

In secondo luogo, pur rimanendo entrambe le categorie soggette alla medesima disciplina in materia di gestione del rischio[14] e di segnalazione delle violazioni[15], le entità essenziali saranno sottoposte ad un regime di vigilanza completo (*ex ante* ed *ex post*)[16],

---

*all'allegato I e soggetti importanti di cui all'allegato II. La presente direttiva non si applica ai soggetti che si qualificano come microimprese e piccole imprese ai sensi della raccomandazione 2003/361/CE della Commissione…*".

[13] L'articolo 2 della Proposta, intitolato "Ambito di applicazione", al paragrafo 2 dispone: "*... La presente direttiva si applica tuttavia anche ai soggetti di cui agli allegati I e II, indipendentemente dalle loro dimensioni, qualora:*
*a) i servizi siano forniti da uno dei soggetti seguenti:*
*i) reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico di cui all'allegato I, punto 8;*
*ii) prestatori di servizi fiduciari di cui all'allegato I, punto 8;*
*iii) registri di nomi di dominio di primo livello e fornitori di servizi DNS (domain name system, sistema dei nomi di dominio) di cui all'allegato I, punto 8;*
*b) il soggetto sia un ente della pubblica amministrazione quale definito all'articolo 4, punto 23;*
*c) il soggetto sia l'unico fornitore di un servizio in uno Stato membro;*
*d) una possibile perturbazione del servizio fornito dal soggetto potrebbe avere un impatto sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;*
*e) una possibile perturbazione del servizio fornito dal soggetto potrebbe comportare rischi sistemici, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;*
*f) il soggetto sia critico in ragione della sua particolare importanza a livello regionale o nazionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;*
*g) il soggetto sia identificato come soggetto critico a norma della direttiva (UE) XXXX/XXXX del Parlamento europeo e del Consiglio 29 [direttiva sulla resilienza dei soggetti critici] o come soggetto equivalente a un soggetto critico a norma dell'articolo 7 di tale direttiva.*
*Gli Stati membri redigono un elenco di soggetti identificati a norma delle lettere da b) a f) e lo trasmettono alla Commissione entro [6 mesi dopo il termine di recepimento]. Gli Stati membri riesaminano l'elenco periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano...*".

[14] L'articolo 18 della Proposta, intitolato "Misure di gestione dei rischi di cibersicurezza", al paragrafo 1 dispone: "… *Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nella fornitura dei loro servizi. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio esistente…*".

[15] L'articolo 20 della Proposta, intitolato "Obblighi di segnalazione", al paragrafo 1 dispone: "… *Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino senza indebito ritardo alle autorità competenti o al CSIRT, conformemente ai paragrafi 3 e 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi. Se opportuno, tali soggetti notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti che possono ripercuotersi negativamente sulla fornitura di tali servizi. Gli Stati membri provvedono affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta alle autorità competenti o al CSIRT di determinare l'eventuale impatto transfrontaliero dell'incidente…*".

[16] L'articolo 29 della Proposta, intitolato "Vigilanza ed esecuzione per i soggetti essenziali", al paragrafo 2 dispone: "… *Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti essenziali, abbiano il potere di sottoporre tali soggetti a:*
*a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali;*
*b) audit periodici;*
*c)audit sulla sicurezza mirati, basati su valutazioni dei rischi o sulle informazioni disponibili relative ai rischi;*

mentre quelle importanti saranno sottoposte solamente ad un regime *ex post*[17].

Per quanto riguarda la gestione del rischio, ferma restando la possibilità, da parte degli operatori che non rientrano nel campo di applicazione della Direttiva NIS II, di notificare volontariamente gli incidenti significativi[18], la proposta riprende la disciplina vigente[19] stabilendo che i soggetti interessati dovranno adottare misure tecniche e organizzative adeguate e proporzionate per gestire le minacce poste alla sicurezza delle reti e dei sistemi informativi minimizzando l'impatto di eventuali incidenti informatici. La proposta, tuttavia, identifica anche un livello minimo di misure che dovranno essere in ogni caso garantite quali, tra le altre, l'uso della crittografia e della cifratura, l'analisi dei rischi e politiche di sicurezza dei sistemi informatici nonché strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di *cybersecurity*[20]. La proposta, inoltre, introduce un'ulteriore novità rispetto alla precedente Direttiva NIS prevedendo per la prima volta che i componenti degli organi di amministrazione delle entità essenziali ed importanti potranno essere ritenuti personalmente responsabili per il mancato rispetto dei rispettivi obblighi nel

*d)scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti;*
*e) richieste di informazioni necessarie a valutare le misure di cibersicurezza adottate dal soggetto, comprese le politiche di cibersicurezza documentate, nonché il rispetto degli obblighi di notifica all'ENISA a norma dell'articolo 25, paragrafi 1 e 2;*
*f) richieste di accesso a dati, documenti o altre informazioni necessari allo svolgimento dei compiti di vigilanza;*
*g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova…*".

[17] L'articolo 30 della Proposta, intitolato "Vigilanza ed esecuzione per i soggetti importanti", al paragrafo 1 dispone: "… *Se ricevono elementi di prova o indicazioni che un soggetto importante non rispetta gli obblighi stabiliti dalla presente direttiva, in particolare dagli articoli 18 e 20, gli Stati membri provvedono affinché le autorità competenti intervengano, se necessario, mediante misure di vigilanza ex post …*".

[18] L'articolo 27 della Proposta, intitolato "Notifica volontaria di informazioni pertinenti", dispone: "… *Gli Stati membri provvedono affinché, fatto salvo l'articolo 3, i soggetti che non rientrano nell'ambito di applicazione della presente direttiva possano trasmettere, su base volontaria, notifiche di incidenti significativi, minacce informatiche o quasi incidenti. Nel trattamento delle notifiche gli Stati membri agiscono secondo la procedura di cui all'articolo 20. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie. La segnalazione volontaria non ha l'effetto di imporre al soggetto che la effettua alcun obbligo aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica…*".

[19] L'articolo 14 della Direttiva UE 2016/1148, intitolato "Obblighi in materia di sicurezza e notifica degli incidenti", al paragrafo 1 dispone: "… *Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. 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…*".

[20] L'articolo 18 della Proposta al paragrafo 2 dispone: "… *Le misure di cui al paragrafo 1 comprendono almeno i seguenti elementi:*
*a) analisi dei rischi e politiche di sicurezza dei sistemi informatici;*
*b) gestione degli incidenti (prevenzione e rilevamento degli incidenti e risposta agli stessi);*
*c) continuità operativa e gestione delle crisi;*
*d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi fornitori o fornitori di servizi, quali i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti;*
*e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;*
*f) strategie e procedure (test e audit) per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;*
*g) uso della crittografia e della cifratura…*".

garantire l'ottemperanza alle misure di sicurezza[21].

Pur ribadendo l'obbligo, per i soggetti interessati, di segnalare gli incidenti, la proposta introduce delle novità rispetto alla Direttiva NIS. Mentre quest'ultima, infatti, assoggetta all'obbligo di notifica gli "incidenti di impatto rilevante" sui servizi prestati, definiti tenendo conto, tra le altre cose, del numero di utenti interessati dalla perturbazione, della durata dell'incidente e della sua diffusione geografica[22], la nuova proposta si incentra sulla nozione di "incidente con impatto significativo", ossia che ha causato o può potenzialmente causare notevoli turbative operative o perdite finanziarie per l'entità interessata o che ha colpito, o può potenzialmente colpire, altre persone fisiche o giuridiche causando considerevoli danni materiali o non materiali[23]. Gli incidenti andranno notificati al massimo entro 24 ore dalla loro scoperta alle autorità competenti o al *team* di risposta agli incidenti di sicurezza informatica (*Computer Security Incident Response Team*, CSIRT)[24], con la possibilità di integrare successivamente tale notifica e presentando in ogni caso una relazione finale entro il mese successivo contenente la descrizione dettagliata dell'incidente, della sua gravità e del suo impatto, il tipo di minaccia o la causa che lo ha probabilmente provocato nonché le misure di mitigazione previste[25].

La proposta mira anche a rafforzare la cooperazione tra gli Stati Membri, risolvendo così una delle maggiori lacune della Direttiva NIS. Oltre a ribadire l'importanza del gruppo per la cooperazione strategica e lo scambio di informazioni tra gli Stati Membri (c.d. "*Cooperation Group*")[26], la proposta incoraggia questi ultimi a designare un CSIRT che, al fine di facilitare la divulgazione coordinata delle vulnerabilità, agisca da intermediario di fiducia tra i soggetti segnalanti e i fornitori di prodotti o di servizi delle tecnologie dell'informazione e della comunicazione (*information and*

[21] L'articolo 17 della Proposta, intitolato "Governance", al paragrafo 1 dispone: "… *Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti al fine di conformarsi all'articolo 18, ne vigilino l'attuazione e siano ritenuti responsabili in caso di mancato rispetto, da parte dei soggetti, degli obblighi di cui al presente articolo…*".

[22] Si vedano gli articoli 14, paragrafo 4, e 16, paragrafo 4, della Direttiva 2016/1148.

[23] L'articolo 20 della Proposta al paragrafo 3 dispone: "*… Un incidente è considerato significativo se:*
*a) ha causato o può causare una perturbazione operativa o perdite finanziarie sostanziali per il soggetto interessato;*
*b) si è ripercosso o può ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli…*".

[24] Il CSRT è la struttura, istituita in ogni Stato Membro, che ha la responsabilità di monitorare, intercettare, analizzare e rispondere alle minacce relative alla cibersicurezza.

[25] L'articolo 20 della Proposta al paragrafo 4 dispone: "… *Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano alle autorità competenti o al CSIRT:*
*a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente, una notifica iniziale che, se opportuno, indichi se l'incidente sia presumibilmente il risultato di un'azione illegittima o malevola;*
*b) su richiesta di un'autorità competente o di un CSIRT, una relazione intermedia sui pertinenti aggiornamenti della situazione;*
*c) una relazione finale entro un mese dalla trasmissione della notifica di cui alla lettera a), che comprenda almeno:*
*i) una descrizione dettagliata dell'incidente, della sua gravità e del suo impatto;*
*ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;*
*iii) le misure di attenuazione adottate e in corso.*
*Gli Stati membri dispongono che, in casi debitamente giustificati e con l'accordo delle autorità competenti o del CSIRT, il soggetto interessato possa derogare alle scadenze di cui alle lettere a) e c)…*".

[26] L'articolo 12 della Proposta, intitolato "Gruppo di cooperazione", al paragrafo 1 dispone: "*… Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri nell'ambito di applicazione della direttiva, è istituito un gruppo di cooperazione…*".

*communication technology*, ICT)[27], affidando il compito di mantenere un registro europeo delle vulnerabilità all'Agenzia dell'Unione Europea per la Cibersicurezza (*European Union Agency for Cybersecurity*, ENISA)[28]. La proposta altresì istituisce la Rete Europea delle Organizzazioni di Collegamento per le Crisi Informatiche (*European Cyber Crises Liaison Organisation Network*, EU-CyCLONe) allo scopo di coordinare la gestione degli incidenti su larga scala e garantire lo scambio regolare di informazioni tra gli Stati Membri e le istituzioni europee[29].

La proposta, infine, rafforza il quadro vigente in materia sanzionatoria. Mentre, infatti, la Direttiva NIS attribuisce agli Stati Membri la facoltà di determinare le sanzioni per il mancato rispetto delle misure di gestione del rischio e degli obblighi di notifica, limitandosi a richiedere che esse siano effettive, proporzionate e dissuasive[30], la Direttiva NIS II impone agli Stati Membri di prevedere ammende fino a 10 milioni di euro o al 2% del fatturato totale mondiale annuo dell'operatore interessato[31].

La palla passa ora al Parlamento e al Consiglio, chiamati a valutare l'efficacia e l'opportunità della proposta che, una volta adottata con direttiva, dovrà essere recepita ed implementata dagli Stati Membri entro 18 mesi dalla sua entrata in vigore.

---

[27] L'articolo 6 della Proposta, intitolato "Divulgazione coordinata delle vulnerabilità e registro europeo delle vulnerabilità", dispone: "*... Ogni Stato membro designa uno dei propri CSIRT di cui all'articolo 9 come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato agisce da intermediario di fiducia agevolando, se necessario, l'interazione tra il soggetto che effettua la segnalazione e il fabbricante o fornitore di servizi TIC o prodotti TIC. Se la vulnerabilità segnalata riguarda più fabbricanti o fornitori di servizi TIC o prodotti TIC nell'Unione, il CSIRT designato di ciascuno Stato membro interessato coopera con la rete di CSIRT.*
*L'ENISA elabora e mantiene un registro europeo delle vulnerabilità. A tal fine l'ENISA istituisce e gestisce i sistemi informatici, le misure strategiche e le procedure adeguati, volti in particolare a consentire ai soggetti essenziali e importanti e ai relativi fornitori di sistemi informatici e di rete di divulgare e registrare le vulnerabilità presenti nei prodotti TIC o nei servizi TIC, nonché a fornire a tutte le parti interessate l'accesso alle informazioni sulle vulnerabilità contenute nel registro. Il registro contiene, in particolare, informazioni che illustrano la vulnerabilità, i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata, la disponibilità di relative patch e, qualora queste non fossero disponibili, orientamenti rivolti agli utenti dei prodotti e dei servizi vulnerabili sulle possibili modalità di attenuazione dei rischi derivanti dalle vulnerabilità divulgate...*".

[28] L'ENISA è un centro di competenze in materia di sicurezza informatica che aiuta l'Unione e gli Stati Membri ad essere meglio attrezzati e preparati a prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione.

[29] L'articolo 14 della Proposta, intitolato "Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)", al paragrafo 1 dispone: "… *Al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE, è istituita la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)*…".

[30] L'articolo 21 della Direttiva 2016/1148, intitolato "Sanzioni", dispone: "*... Gli Stati membri stabiliscono le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e adottano tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono effettive, proporzionate e dissuasive. Gli Stati membri notificano tali norme e provvedimenti alla Commissione entro il 9 maggio 2018 e provvedono a darle immediata notifica di ogni successiva modifica...*".

[31] L'articolo 31 della Proposta, intitolato "Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti", al paragrafo 4 dispone: "… *Gli Stati membri provvedono affinché le violazioni degli obblighi di cui all'articolo 18 o all'articolo 20 siano, conformemente ai paragrafi 2 e 3 del presente articolo, soggette a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000 EUR o fino al 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale o importante appartiene, se tale importo è superiore*…".


Roberto A. Jacchia

**PARTNER**

r.jacchia@dejalex.com

+39 02 72554.1

Via San Paolo 7
20121 - Milano



Marco Stillo

**ASSOCIATE**

m.stillo@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles



MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com