



Golden power e reti di quinta generazione. L'Italia adotta nuove disposizioni in ottica di sicurezza nazionale

📅 05/06/2019

📖 PROSPETTIVE, IT & TMT, PROTEZIONE DEI DATI E CYBERSECURITY

Roberto A. Jacchia
Sara Capruzzi

In data 25 marzo 2019 il Governo italiano ha approvato il Decreto Legge 25 marzo 2019, n. 22, che include nelle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G¹.

Le reti di quinta generazione (5G) sono reti le cui prestazioni e velocità sono

assimilabili a quelle della rete fissa senza però che siano presenti i cavi. Grazie ad esse, il volume dei dati comunicati, la velocità, la sicurezza e la disponibilità di banda sono incrementati, consentendo di collegare miliardi di oggetti e sistemi, in campi che vanno dalla manifattura alla gestione delle aree urbane, dai trasporti alla sanità, dai media alla distribuzione più efficiente dell'energia².

¹ Decreto Legge 25 marzo 2019, n. 22, Misure urgenti per assicurare sicurezza, stabilità finanziaria e integrità dei mercati, nonché tutela della salute e della libertà di soggiorno dei cittadini italiani e di quelli del Regno Unito, in caso di recesso di quest'ultimo dall'Unione europea, GU Serie Generale n.71 del 25-03-2019.

² Secondo un recente studio presentato dalla *European Telecommunications Network Operators' Association* (Etno), l'associazione che rappresenta le grandi aziende di telecomunicazioni europee,



Il Decreto aggiorna la normativa in materia di poteri speciali (c.d. *golden power*)³ in conseguenza dell'evoluzione tecnologica intercorsa, con particolare riferimento alla tecnologia 5G e ai connessi rischi di un uso improprio dei dati con implicazioni sulla sicurezza nazionale⁴.

La disciplina del *golden power* deriva da quella del precedente istituto comunemente noto come *golden share*.

La *golden share* era stata introdotta in Italia tramite il Decreto Legge 31 maggio 1994, n. 332, convertito con la Legge n. 474 del 30 luglio 1994⁵. Il Decreto attribuiva allo Stato alcune partecipazioni azionarie munite di poteri speciali⁶ che permettevano di influenzare le decisioni del *management* quali l'opposizione all'acquisizione di partecipazioni rilevanti, il veto su alcune delibere societarie oppure il diritto di nomina di membri degli organi amministrativi.

nel 2025 saranno 138 milioni le connessioni 5G nei Paesi dell'Unione Europea. Per ulteriori informazioni, si veda il seguente [LINK](#).

³ Decreto-legge 16 ottobre 2017, n. 148, coordinato con la legge di conversione 4 dicembre 2017, n. 172 recante: "Disposizioni urgenti in materia finanziaria e per esigenze indifferibili. Modifica alla disciplina dell'estinzione del reato per condotte riparatorie", GU Serie n.284 del 05-12-2017; Decreto legge 15 marzo 2012, no. 21, Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, GU Serie Generale n.63 del 15-03-2012.

⁴ L'articolo 1 del D. L. 22/2019, denominato "Modifiche al decreto-legge 15 marzo 2012, no 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, recante "Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni", così dispone: "... Al fine di un aggiornamento della normativa in materia di poteri speciali in conseguenza dell'evoluzione tecnologica intercorsa, con particolare riferimento alla tecnologia 5G e ai connessi rischi di un uso improprio dei dati con implicazioni sulla sicurezza nazionale, al decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, dopo l'articolo 1 è inserito il seguente: «Art. 1-bis (Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G). - 1. Costituiscono, ai fini dell'esercizio dei poteri di cui al comma 2, attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G. La stipula di contratti o accordi aventi ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di cui al comma 1, ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, quando posti in essere con soggetti esterni all'Unione europea, sono soggetti alla notifica di cui all'articolo 1, comma 4, al fine dell'eventuale esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni. A tal fine, sono oggetto di valutazione anche gli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano.

Per le finalità di cui al comma 2, per soggetto esterno all'Unione europea si intende:

- 1) qualsiasi persona fisica o persona giuridica, che non abbia la residenza, la dimora abituale, la sede legale o dell'amministrazione ovvero il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che non sia comunque ivi stabilito;
- 2) qualsiasi persona giuridica che abbia stabilito la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che sia comunque ivi stabilito, e che risulti controllato direttamente o indirettamente da una persona fisica o da una persona giuridica di cui al n. 1);
- 3) qualsiasi persona fisica o persona giuridica che abbia stabilito la residenza, la dimora abituale, la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che sia comunque ivi stabilito, al fine di eludere l'applicazione della disciplina di cui al presente articolo.

Con decreto del Presidente del Consiglio dei ministri, sentito il Gruppo di coordinamento costituito ai sensi dell'articolo 3 del decreto del Presidente del Consiglio dei ministri del 6 agosto 2014, possono essere individuate misure di semplificazione delle modalità di notifica, dei termini e delle procedure relativi all'istruttoria ai fini dell'eventuale esercizio dei poteri di cui al comma 2.»...

⁵ Conversione in legge, con modificazioni, del decreto-legge 31 maggio 1994, no. 332, recante norme per l'accelerazione delle procedure di dismissione di partecipazioni dello Stato e degli enti pubblici in società per azioni, GU n. 177 del 30.07.1994.

⁶ Si veda l'articolo 2 della Legge di conversione.

Tale meccanismo, tuttavia, era stato oggetto di critica in quanto comportava una deroga ai principi di diritto societario, determinando una discriminazione tra operatori, tant'è vero che la Corte di Giustizia era intervenuta per individuare i requisiti necessari affinché l'esercizio dei poteri speciali fosse conforme alle libertà fondamentali dell'Unione, in particolare la libertà di circolazione dei capitali ed il diritto di stabilimento⁷, rafforzando quanto già stabilito dalla Commissione nella Comunicazione del 1997 relativa ad alcuni aspetti giuridici attinenti agli investimenti intracomunitari⁸. In tale occasione, la Commissione aveva affermato che l'esercizio dei poteri speciali avrebbe dovuto essere attuato senza discriminazioni e sarebbe stato ammissibile solo se fondato "... *su una serie di criteri obiettivi, stabili e resi pubblici e... giustificati da motivi imperiosi di interesse generale...*".

Inoltre, la Commissione aveva ribadito l'importanza del rispetto del principio di proporzionalità, da tradursi nell'attribuire allo Stato solo i poteri strettamente necessari per il conseguimento dell'obiettivo perseguito.

Di conseguenza, era stato successivamente emanato il Decreto 10 giugno 2004, con il quale venivano specificati i criteri di esercizio dei poteri speciali⁹. Nonostante ciò, nel luglio del 2007 la Commissione aveva deciso di adire la Corte di Giustizia ritenendo che tali criteri non fossero stati sufficientemente specificati, non permettendo agli investitori di conoscere anticipatamente e con certezza le modalità del loro utilizzo. Accogliendo le richieste della Commissione, nel 2009 la Corte di Giustizia aveva dichiarato incompatibili con il diritto europeo i poteri speciali detenuti dallo Stato italiano in *Enel, Eni, Finmeccanica e Tim*¹⁰.

⁷ CGUE 23.05.2000, causa C-58/99, *Commissione delle Comunità europee contro Repubblica italiana*, punto 13.

⁸ Com. Comm. relativa ad alcuni aspetti giuridici attinenti agli investimenti intracomunitari, GUUE C 220 del 19.07.1997.

⁹ Decreto del Presidente del Consiglio dei Ministri, del 10 giugno 2004, Definizione dei criteri di esercizio dei poteri speciali, di cui all'art. 2 del decreto-legge 31 maggio 1994, n. 332, convertito, con modificazioni, dalla legge 30 luglio 1994, n. 474, GU n. 139 del 16.06.2004. L'articolo 1 del Decreto così stabilisce: "... *I poteri speciali di cui all'art. 2 del decreto-legge n. 332 del 1994, sono esercitati esclusivamente ove ricorrano rilevanti e imprescindibili motivi di interesse generale, in particolare con riferimento all'ordine pubblico, alla sicurezza pubblica, alla sanità pubblica e alla difesa, in forma e misura idonee e proporzionali alla tutela di detti interessi, anche mediante l'eventuale previsione di opportuni limiti temporali, fermo restando il rispetto dei principi dell'ordinamento interno e comunitario, e tra questi in primo luogo del principio di non discriminazione. I poteri speciali di cui alle lettere a), b) e c) dell'art. 2, comma 1, del decreto-legge n. 332 del 1994, ferme restando le finalità indicate allo stesso comma 1, sono esercitati in relazione al verificarsi delle seguenti circostanze:*

a) *grave ed effettivo pericolo di una carenza di approvvigionamento nazionale minimo di prodotti petroliferi ed energetici, nonché' di erogazione dei servizi connessi e conseguenti e, in generale, di materie prime e di beni essenziali alla collettività, nonché' di un livello minimo di servizi di telecomunicazione e di trasporto;*

b) *grave ed effettivo pericolo in merito alla continuità di svolgimento degli obblighi verso la collettività nell'ambito dell'esercizio di un servizio pubblico, nonché' al perseguimento della missione affidata alla società nel campo delle finalità di interesse pubblico;*

c) *grave ed effettivo pericolo per la sicurezza degli impianti e delle reti nei servizi pubblici essenziali;*

d) *grave ed effettivo pericolo per la difesa nazionale, la sicurezza militare, l'ordine pubblico e la sicurezza pubblica;*

e) *emergenze sanitarie.*

Al fine di garantire la proporzionalità delle misure adottate, i poteri speciali di cui alle lettere a), b) e c) dell'art. 2, comma 1, del decreto-legge n. 332 del 1994, potranno essere esercitati anche in forma condizionata. Il potere speciale di cui alla lettera c) potrà essere esercitato sia in relazione alle delibere assunte dall'assemblea degli azionisti che in relazione alle delibere degli organi di amministrazione..."

¹⁰ CGUE 26.03.2009, causa C-326-07, *Commissione delle Comunità europee contro Repubblica italiana*, punti 50-55.

A seguito di questa sentenza, in Italia si era provveduto alla modifica dei meccanismi precedentemente approntati o alla loro abrogazione, sostituendo l'istituto della *golden share* con quello del *golden power*¹¹, introdotto con il Decreto Legge 15 marzo 2012, n. 21¹². La principale differenza rispetto alla normativa precedente si rinviene nell'ambito operativo della nuova disciplina, che consente al Governo l'esercizio dei poteri speciali rispetto a tutte le società, pubbliche o private, che svolgono attività considerate di rilevanza strategica per il sistema di difesa e sicurezza nazionali¹³ oppure nei settori dell'energia, dei trasporti e delle comunicazioni¹⁴, e non più soltanto rispetto alle società privatizzate o in mano pubblica. I poteri attribuiti al Governo trovano applicazione sia nei confronti dei soggetti appartenenti all'Unione Europea che ai soggetti riconducibili a Paesi terzi c.d. esterni, e variano in funzione della possibilità di imporre determinate condizioni alle imprese interessate, fino a misure di intensità maggiore come il potere di opporsi all'acquisto di imprese strategiche¹⁵.

La materia aveva formato oggetto di una nuova riforma nel 2017¹⁶, che aveva ulteriormente ampliato l'ambito di applicazione del *golden power* qualora siano coinvolti soggetti esterni all'Unione Europea, i quali già ai sensi della normativa del 2012 erano tenuti a notificare entro 10 giorni alla Presidenza del Consiglio dei Ministri l'acquisto a

qualsiasi titolo di partecipazioni comportanti l'assunzione del controllo di società che detengono attivi strategici. Con la riforma del 2017 era stato specificato che la sussistenza di un pericolo per la sicurezza e l'ordine pubblico che permette l'esercizio dei poteri speciali nei settori ad alta intensità tecnologica va valutata prendendo in considerazione le infrastrutture critiche o sensibili, come l'immagazzinamento e la gestione dei dati, le infrastrutture finanziarie, l'intelligenza artificiale e la robotica, la tecnologia a potenziale doppio uso, la sicurezza in rete, la tecnologia spaziale e nucleare, l'accesso a input critici o informazioni sensibili e la capacità di controllare informazioni sensibili¹⁷.

La riforma del 2019 prevede ora che la stipula di un contratto avente ad oggetto materia 5G con un soggetto estraneo all'Unione Europea deve essere preventivamente comunicata al Governo, e che la mancanza di tale comunicazione comporta una sanzione amministrativa pari ad un massimo pari al doppio del valore del contratto ma, in ogni caso, non inferiore all'1% del fatturato complessivo delle società coinvolte. Inoltre, qualora i contratti 5G fossero implementati in violazione del veto o delle condizioni imposte dal Governo, essi sarebbero nulli e privi di effetti, ed il Governo potrebbe obbligare le parti a ripristinare lo *status quo ante* a proprie spese. Una volta ricevuta la comunicazione, il Governo disporrà di 15 giorni lavorativi (più ulteriori 10 qualora fossero necessari chiarimenti) per verificare se i contratti

¹¹ La nuova configurazione si caratterizza per il fatto che l'intervento dello Stato si sposta da un piano privatistico, in cui venivano inseriti elementi pubblicistici, ad un piano meramente pubblicistico: lo Stato, infatti, resta un soggetto estraneo alla compagine sociale ed interviene in maniera eccezionale, preservando la concorrenzialità dell'impresa in situazioni ordinarie.

¹² Decreto Legge 15 marzo 2012, n. 21, Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, GU Serie Generale n.63 del 15-03-2012.

¹³ Si veda l'articolo 1 del D. L. 21/2012.

¹⁴ Si veda l'articolo 2 del D. L. 21/2012.

¹⁵ Per ulteriori informazioni, si veda il nostro precedente contributo, disponibile al seguente [LINK](#).

¹⁶ Decreto Legge 16 ottobre 2017, n. 148, coordinato con la legge di conversione 4 dicembre 2017, n. 172 recante: "Disposizioni urgenti in materia finanziaria e per esigenze indifferibili. Modifica alla disciplina dell'estinzione del reato per condotte riparatorie", GU Serie n.284 del 05-12-2017.

¹⁷ Si veda l'articolo 14 del D.L. 148/2017. Per maggiori informazioni, si veda il nostro precedente contributo, disponibile al seguente [LINK](#).

5G possano costituire un pericolo per la sicurezza nazionale o per l'ordine pubblico, tenuto conto anche delle eventuali vulnerabilità tecniche che potrebbero mettere a repentaglio la solidità e la sicurezza delle reti e dei dati. Ad esito di tale valutazione, il Governo potrà porre il veto o imporre condizioni ai contratti 5G; altrimenti, qualora i suddetti termini decorrano senza alcuna obiezione, i relativi contratti saranno validi e potranno entrare regolarmente in vigore.

A livello europeo, la Commissione è da tempo consapevole delle potenzialità delle reti 5G, ed è per questo che nel 2013 ha istituito un partenariato pubblico-privato (*5G Infrastructure Public Private Partnership, 5G PPP*)¹⁸ stanziando un finanziamento pubblico di 700 milioni di euro tramite il programma Orizzonte 2020¹⁹ per sostenere questa attività, includendo gli *standard* 5G tra i settori prioritari dell'iniziativa *Digitizing European Industry* lanciata nel 2016²⁰. Per garantire una rapida diffusione dell'infrastruttura 5G, inoltre, nel 2016 la Commissione ha adottato un piano d'azione 5G per l'Europa con l'obiettivo di avviare il lancio dei servizi 5G in tutti gli

Stati Membri dell'UE entro la fine del 2020²¹ e, allo scopo di monitorarne i progressi, ha lanciato l'Osservatorio europeo 5G due anni più tardi²².

Sulla base delle conclusioni del Consiglio Europeo²³ e della risoluzione del Parlamento Europeo sulle minacce alla sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione²⁴, in data 26 marzo 2019 la Commissione ha raccomandato una serie di iniziative e misure operative per valutare i rischi per la cibersicurezza delle reti 5G e per rafforzare le misure preventive, consistenti in una combinazione di strumenti legislativi e di azioni pensati per proteggere le economie, le società ed i sistemi democratici europei²⁵ da attuarsi sia a livello nazionale che a livello UE.

Per quanto riguarda le prime, in particolare, ogni Stato Membro dovrebbe completare la valutazione nazionale dei rischi delle infrastrutture di rete 5G entro fine giugno 2019, aggiornando su tale base i requisiti di sicurezza vigenti a carico dei fornitori di servizi di rete e fissando condizioni per garantire la sicurezza delle reti pubbliche, soprattutto

¹⁸ Il 5G PPP è un'iniziativa congiunta tra la Commissione e le industrie europee nel campo delle Tecnologie dell'Informazione e della Comunicazione il cui compito è fornire soluzioni, architetture, tecnologie e standard per le infrastrutture di comunicazione di prossima generazione, con l'obiettivo di assicurare la *leadership* europea nelle aree in cui esiste la possibilità di creare nuovi mercati come città intelligenti, sanità elettronica, trasporto intelligente, istruzione o intrattenimento e media. Per ulteriori informazioni, si veda il seguente [LINK](#).

¹⁹ Orizzonte 2020 è il Programma Quadro dell'Unione Europea per la ricerca e l'innovazione relativo al periodo 2014-2020. Introdotto con l'intento di unificare in un unico strumento finanziario tre programmi precedenti finalizzati a supportare la ricerca, l'innovazione e lo sviluppo tecnologico (il Settimo Programma Quadro, il Programma Quadro per la Competitività e l'Innovazione e l'Istituto Europeo di Innovazione e Tecnologia), si prefigge di contribuire, alla realizzazione di una società basata sulla conoscenza e sull'innovazione, orientata verso le grandi priorità indicate dall'Agenda europea per il 2020, ossia crescita intelligente, sostenibile e inclusiva. Per ulteriori informazioni, si veda il seguente [LINK](#).

²⁰ Com. Comm. del 19.04.2016, Digitalizzazione dell'industria europea Cogliere appieno i vantaggi di un mercato unico digitale, COM(2016) 18 final.

²¹ Com. Comm. del 19.04.2016, Il 5G per l'Europa: un piano d'azione, COM(2016) 588 final.

²² L'Osservatorio europeo 5G monitora gli sviluppi del mercato e le azioni preparatorie intraprese dalle parti interessate del settore e dagli Stati membri nel contesto del lancio del 5G in Europa e oltre, fornendo i relativi sviluppi. Per ulteriori informazioni, si veda il seguente [LINK](#).

²³ Conclusioni del Consiglio Europeo, del 22 marzo 2019, EUCO 1/19.

²⁴ Risoluzione del Parlamento Europeo, del 12 marzo 2019, sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione a livello di Unione per ridurre tali minacce, 2019/2575(RSP).

²⁵ Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G, GUUE L 188 del 29.03.2019.

in merito alla concessione dei diritti di uso delle frequenze radio nelle bande 5G. Tali valutazioni, che dovrebbero tener conto di diversi fattori di rischio quali i rischi tecnici e i rischi connessi al comportamento dei fornitori e degli operatori, compresi quelli dei Paesi terzi, costituiranno un elemento centrale per una valutazione coordinata dei rischi a livello europeo.

Per quanto riguarda le seconde, invece, gli Stati Membri dovrebbero scambiare informazioni tra di loro e, con il sostegno della Commissione e dell'Agenzia dell'Unione Europea per la cibersicurezza (*European Union Agency for Network and Information Security*, ENISA)²⁶, completare la valutazione dei rischi coordinata entro il 1° ottobre 2019, concordando un insieme di misure di attenuazione utilizzabili a livello nazionale. Di tale compito sarà incaricato un gruppo di cooperazione delle autorità competenti, istituito nel quadro della direttiva sulla sicurezza delle reti e dei sistemi informativi, con l'ausilio della Commissione e dell'ENISA.

Queste misure si inseriscono nell'insieme degli strumenti di cui l'Unione già dispone per proteggere le reti di comunicazione elettronica, come ad esempio la Direttiva sulla sicurezza delle reti e dei sistemi informativi²⁷, che mira a raggiungere un livello comune elevato di sicurezza delle reti e dei sistemi di informazione in tutta l'UE, il recente Regolamento sulla cibersicurezza²⁸, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico

della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali, e le nuove norme sulle telecomunicazioni²⁹, che impongono agli Stati Membri di garantire l'integrità e la sicurezza delle reti pubbliche di comunicazione, stabilendo obblighi volti ad assicurare che gli operatori in effetti adottino misure tecniche e organizzative per gestire adeguatamente i rischi per la sicurezza delle reti e dei servizi.

Vi è, infine, da dire che nell'attuale clima di contrapposizione geopolitica globale e di rivalorizzazione degli interessi nazionali, ci si trova di fronte ad una continua *escalation* delle misure di controllo e limitazione degli investimenti diretti. Il ruolo effettivo dell'Unione al momento non va al di là di un sistema di informazione reciproca e di coordinamento *soft*. Ben difficilmente questo *retrenchment* nella direzione degli interessi nazionali vedrà sorgere e proseguire grandi progetti multilaterali di innovazione nei settori di punta di lungo termine, quali, ad esempio, le tecnologie spaziali, l'intelligenza artificiale e le tecnologie quantiche. Se è vero che l'Unione Europea è nel suo complesso già un *player* primario nella maggior parte di queste aree, è altrettanto vero che gli Stati Membri privi di *national champion* di dimensione planetaria a motivo di questa tendenza in atto ad erigere nuove barriere, rischieranno di ritrovarsi ancora più deboli e più marginali.

²⁶ L'ENISA è un centro di competenze in materia di sicurezza informatica in Europa, il cui compito consiste nell'aiutare l'UE e i Paesi membri ad essere meglio attrezzati e preparati a prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione. A tale incarico essa assolve fornendo consigli pratici e soluzioni per il settore pubblico e privato negli Stati membri e per le istituzioni dell'UE e pubblicando relazioni e studi sulle questioni di sicurezza informatica. Per ulteriori informazioni, si veda il seguente [LINK](#).

²⁷ 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 nell'Unione, *GUUE L 194 del 19.7.2016*.

²⁸ Risoluzione legislativa del Parlamento Europeo, del 12 marzo 2019, sulla proposta di Regolamento del Parlamento Europeo e del Consiglio relativo all'ENISA l'agenzia dell'Unione europea per la cibersicurezza, che abroga il Regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.


²⁹ Risoluzione legislativa del Parlamento Europeo, del 14 novembre 2018, sulla proposta di Direttiva del Parlamento Europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche.



Roberto A. Jacchia
PARTNER

 r.jacchia@dejalex.com


 +39 02 72554.1

 Via San Paolo 7
20121 - Milano



Sara Capruzzi
ASSOCIATE

 s.capruzzi@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