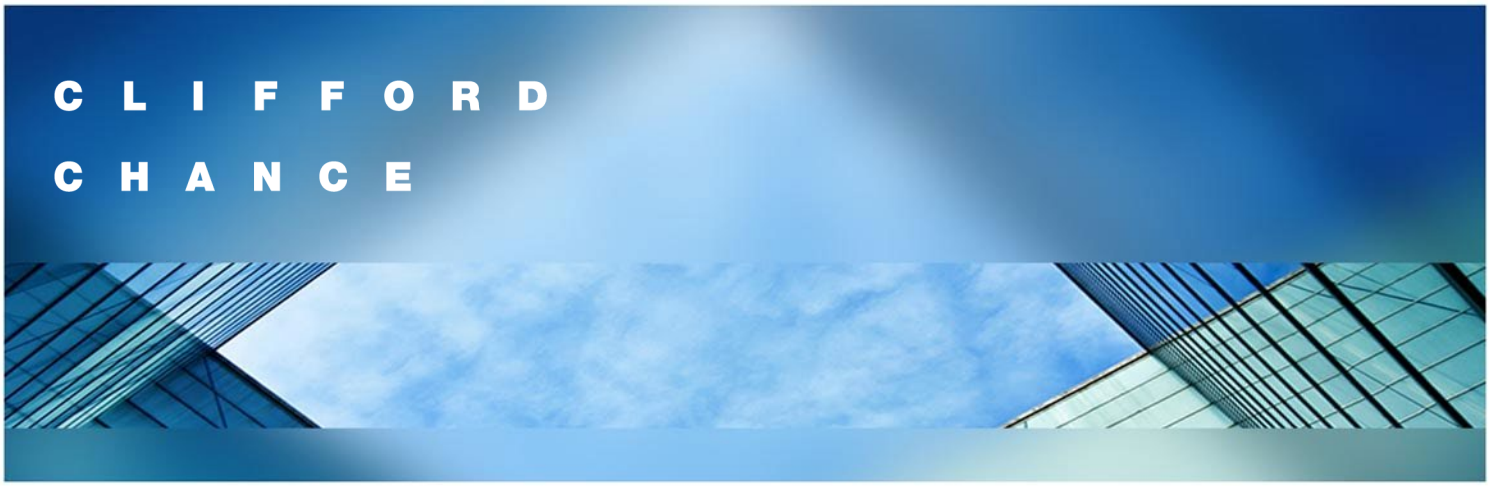

CYBERSICUREZZA: ULTERIORE RAFFORZAMENTO DEGLI STRUMENTI DI PREVENZIONE, REAZIONE E REPRESSIONE DEGLI INCIDENTI INFORMATICI E DEL CYBERCRIME

È stata pubblicata nella Gazzetta Ufficiale del 2 luglio 2024 la Legge contenente "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" (Legge n. 90 del 28 giugno 2024, di seguito la "**Legge Cybersicurezza**"). L'entrata in vigore è prevista per il prossimo 17 luglio 2024, con numerose novità sia sul versante *data protection* che su quello della tutela penale.

"*ITALIA SOTTO ASSEDIO*"

Così viene titolato uno dei paragrafi di apertura del Rapporto CLUSIT[1] 2024, che fornisce una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale, Italia inclusa, nel 2023.

La lettura dell'intero documento restituisce un quadro certamente non rasserenante: secondo i dati raccolti ed esaminati, nel 2023 gli attacchi informatici in Italia risultano essere aumentati del 65% rispetto al 2019; peraltro, gli attacchi ricevuti dall'Italia paiono rappresentare ben l'11% degli attacchi registrati a livello globale, a conferma di come il nostro Paese rappresenti uno dei bersagli preferiti dai criminali informatici.

L'incremento di tipo quantitativo degli incidenti informatici è stato, inoltre, accompagnato da un incremento di tipo qualitativo, con un generale e diffuso peggioramento dell'indice di gravità (c.d. *severity* media) degli attacchi informatici del 2023.

La Legge Cybersicurezza rappresenta, dunque, lo strumento mediante il quale il Legislatore italiano ha cercato di fornire risposta ad un fenomeno, quello del crimine informatico, non solo oramai sempre più dilagante, ma soprattutto dagli impatti sempre più significativi (e dannosi) a tutti i livelli (pubblica amministrazione, aziende pubbliche ed aziende private).

Quali, dunque, le principali novità introdotte dalla nuova Legge Cybersicurezza?

[1] Associazione Italiana per la Sicurezza Informatica.

La Legge Cybersicurezza in pillole

- Aumento della cornice edittale per i reati informatici già previsti nel Codice Penale
- Introduzione nel Codice Penale di nuove ipotesi di reato, in particolare la c.d. estorsione *cyber* e la c.d. truffa *cyber*
- Inasprimento delle sanzioni pecuniarie per gli Enti previste dal D.Lgs. n. 231/2001 per gli illeciti amministrativi dipendenti da reati informatici
- Inclusione della fattispecie di estorsione *cyber* nell'elenco dei reati presupposto di cui all'art. 24-*bis* del D.Lgs. n. 231/2001
- Introduzione di ulteriori obblighi di segnalazione e notificazione di incidenti *cyber* per amministrazioni pubbliche e soggetti nel perimetro di cybersecurity
- Previsione di tempi ristretti entro i quali effettuare segnalazioni e notificazioni all'ACN, applicabili anche ai soggetti già ricompresi nel perimetro di Cybersecurity
- Previsione di criteri premiali nelle procedure di approvvigionamento di beni e servizi informatici utilizzati in contesti relativi alla tutela della sicurezza nazionale, con riferimento alle proposte o offerte che prevedano l'uso di tecnologie di cybersicurezza italiane o di Paesi UE o appartenenti alla NATO o con paesi terzi appositamente individuati

LE NOVITÀ SUL VERSANTE *DATA PROTECTION*

Il Capo I della Legge Cybersicurezza contiene una serie di disposizioni finalizzate, in modo particolare, al rafforzamento della cybersicurezza a livello nazionale, anche attraverso l'attribuzione di un ruolo sempre più centrale all'Agenzia per la Cybersicurezza Nazionale ("**ACN**"), nonché al rafforzamento della resilienza delle pubbliche amministrazioni e degli operatori del settore finanziario.

Dove siamo oggi

La Legge Cybersicurezza si inserisce nel quadro di previsioni (nazionali e di derivazione comunitaria) volte ad assicurare un elevato livello di cybersicurezza nel nostro ordinamento. Ad oggi, rilevano in primo luogo le norme in materia di trattamento dei dati personali, ossia il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (il "**GDPR**") e il D. Lgs. 30 giugno 2003, n. 196 (il "**Codice Privacy**"), i quali prevedono l'obbligo di adozione di misure di sicurezza e di segnalazione con riferimento al trattamento dei dati personali. Inoltre, la cybersecurity è regolata dai seguenti atti normativi:

- D. Lgs. 18 maggio 2018, n. 65 (il "**Decreto NIS**"), che ha recepito la Direttiva (UE) del Parlamento europeo e del consiglio del 6 luglio 2016;
- D.L. 21 settembre 2019, n. 105 (il "**Decreto Perimetro Cybersecurity**"), che ha istituito il c.d. perimetro di sicurezza cybernetica, volto ad assicurare "*un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici*" degli operatori pubblici e privati, da cui dipende l'esercizio di una funzione essenziale o la prestazione di un servizio essenziale per gli interessi dello Stato e dal cui malfunzionamento e/o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. In particolare, il Decreto Perimetro Cybersecurity regola:
  - le procedure di notifica di incidenti aventi impatto su reti, sistemi informativi e servizi informatici; e
  - l'adozione di misure volte a garantire elevati livelli di sicurezza delle reti, sistemi informativi e servizi informatici, ivi inclusi specifici obblighi di comunicazione con riferimento all'affidamento di forniture.
- D.L. 14 giugno 2021, n. 82, che ha istituito l'ACN e ad essa ha attribuito poteri e funzioni in questo settore, oltre a nominarla Autorità Nazionale competente NIS.

Di fatto, il legislatore, dopo aver recepito gli obblighi di derivazione comunitaria con il Decreto NIS, ha introdotto ulteriori misure ed obblighi (oggetto di specifico coordinamento con quelli già previsti dal Decreto NIS) applicabili ai soggetti pubblici e privati che esercitano funzioni o forniscono servizi ritenuti essenziali, con il Decreto Perimetro Cybersecurity, successivamente integrato dalla Legge Cybersicurezza.

La nuova disciplina degli obblighi di notifica degli incidenti informatici

La Legge Cybersicurezza introduce una nuova disciplina in materia di obblighi di segnalazione e notifica con riferimento a specifici incidenti informatici, individuati con apposita determina dell'ACN.

- *Pubbliche Amministrazioni*

  La Legge Cybersicurezza in primo luogo prevede l'obbligo per gli enti locali, per le società di trasporto pubblico locale e per le aziende sanitarie locali, nonché per le rispettive società *in house* che forniscono servizi informativi, di trasporto, di raccolta, smaltimento o trattamento di acque reflue o di gestione rifiuti, che superino determinati requisiti dimensionali, l'obbligo di (i) segnalare e di (ii) effettuare la notifica completa con riferimento agli incidenti informatici individuati dall'ACN.

  La segnalazione dovrà essere effettuata entro il termine massimo di 24 ore e la notifica completa entro 72 ore dalla conoscenza effettiva dell'incidente, mediante le procedure disponibili sul sito internet di ACN.

  Nel caso di inosservanza, l'ACN ammonisce il soggetto e può esercitare poteri ispettivi. Nel caso di reiterazione, l'ACN potrà irrogare una pena amministrativa pecuniaria tra Euro 25.000 ed Euro 125.000.

- *Soggetti già ricompresi nel perimetro*

  La Legge Cybersicurezza è intervenuta anche con riferimento agli obblighi di segnalazione già previsti dal Decreto Perimetro Cybersicurezza, ossia relativi a incidenti aventi impatto su reti, sistemi informativi e servizi informatici, ove ha previsto le medesime stringenti tempistiche per la segnalazione (entro 24 ore) e per l'effettuazione della notifica completa (72 ore).

Rafforzamento degli obblighi di *governance* in tema di cybersicurezza

La Legge Cybersicurezza introduce inoltre obblighi volti a prevenire il verificarsi di incidenti informatici, nonché ad assicurare la resilienza (i) dei soggetti pubblici ai quali si applicano gli obblighi di segnalazione e notificazione, nonchè (ii) dei soggetti ricompresi nel perimetro di Cybersecurity e (iii) degli intermediari finanziari.

- *Pubbliche Amministrazioni e soggetti nel perimetro di Cybersicurezza*

  È previsto che le Pubbliche Amministrazioni soggette agli obblighi di segnalazione e notifica istituiscano strutture interne che:

  - sviluppino politiche e procedure volte a garantire la sicurezza delle informazioni, nonché di dati, sistemi e infrastrutture dell'amministrazione;
  - adottino piani per la gestione del rischio informatico, con la previsione di interventi di potenziamento; e
  - assicurino il costante monitoraggio delle minacce *cyber* e delle vulnerabilità dei sistemi.

  Inoltre, sia le Pubbliche Amministrazioni sia i soggetti inclusi nel perimetro di cybersicurezza devono assicurare che i programmi e le applicazioni informatiche che utilizzano soluzioni crittografiche rispettino le linee guida sulla crittografia e sulla conservazione delle password adottate dall'ACN.

- *Fornitura di servizi informatici alle Pubbliche Amministrazioni e ai soggetti nel perimetro di Cybersicurezza*

  Con riferimento all'approvvigionamento di beni e servizi informatici utilizzati in contesti relativi alla tutela della sicurezza nazionale da parte di pubbliche amministrazioni e soggetti che rientrano nel perimetro di

cybersicurezza, con decreto del Presidente del Consiglio dei Ministri saranno individuati:

- gli elementi di cybersicurezza che dovranno essere considerati ai fini dell'individuazione del contraente; e
- i criteri di premialità per le proposte o per le offerte che prevedano l'uso di tecnologie di cybersicurezza italiane o di Paesi UE o appartenenti alla NATO o con paesi terzi appositamente individuati.

❖ *Intermediari finanziari*

La Legge Cybersicurezza interviene anche rispetto al sistema di *governance* richiesto agli intermediari finanziari.

In particolare, l'art. 15 della Legge in commento stabilisce cha la disciplina applicabile agli intermediari finanziari iscritti nell'albo *ex* art. 106 del Testo Unico in materia bancaria e creditizia nonché a Poste italiane per l'attività del Patrimonio Bancoposta sia modificata al fine di conseguire un livello **elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso**:

- definendo presidi in materia di resilienza operativa digitale equivalenti a quelli stabiliti a livello europeo dal Regolamento DORA[2];
- tenendo conto, nella definizione dei predetti presidi, del principio di proporzionalità e delle attività svolte dagli intermediari finanziari e dal Patrimonio Bancoposta;
- attribuendo a Banca d'Italia l'esercizio dei poteri di vigilanza, di indagine e sanzionatori nei confronti dei soggetti interessati.

Potenziamento del ruolo di ACN

L'ACN ha un ruolo sempre più centrale nella gestione di questioni relative a temi di cybersicurezza, in quanto:

- diventa destinataria delle segnalazioni previste dalle diverse normative cybersecurity; e
- le sono attribuiti poteri ispettivi e di segnalazione con riferimento ad eventuali vulnerabilità cyber.

[2] Regolamento (UE)2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

LE NOVITÀ SUL VERSANTE PENALE

Il Capo II della Legge Cybersicurezza è dedicato, invece, al rafforzamento degli strumenti di prevenzione e di repressione dei reati informatici e prevede interventi di modifica sia al Codice Penale – tanto mediante l'aumento delle cornici edittali per le fattispecie già esistenti e l'ampliamento dell'ambito applicativo delle stesse quanto mediante l'introduzione di vere e proprie nuove ipotesi di reati informatici – che al Codice di Procedura Penale, al fine di adattare talune delle disposizioni ivi contenute alle peculiarità dei reati informatici.

Dall'aumento delle pene…

Anzi tutto, per effetto dell'art. 16 della Legge Cybersicurezza, si assiste ad un generale **inasprimento delle pene per i reati informatici già esistenti, soprattutto rispetto alle ipotesi aggravate**, le cui cornici edittali, in molti casi, vengono quasi raddoppiate.

Per fornire alcuni esempi, tra le principali fattispecie di reati informatici: l'attuale cornice edittale prevista per il delitto di accesso abusivo ad un sistema informatico nella forma aggravata (art. 615-*ter*, comma 2, c.p.) viene sostanzialmente raddoppiata, passando da una forbice di 1-5 anni di reclusione ad una forbice di 2-10 anni di reclusione; il delitto di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche nella forma aggravata (art. 617-*quater*, comma 4, c.p.) passa da una cornice edittale di 3-8 anni di reclusione ad una cornice edittale di 4-10 anni di reclusione; ancora, il delitto di danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.), sino ad oggi punito con la reclusione da 1 a 5 anni, sarà ora sanzionato con la reclusione da 2 a 6 anni.

…all'introduzione di nuove ipotesi di reato

La Legge Cybersicurezza, poi, amplia il ventaglio delle condotte penalmente rilevanti riconducibili a talune delle fattispecie già esistenti. Per esempio, il perimetro del già citato delitto di accesso abusivo ad un sistema informatico viene esteso a ricomprendere anche chi "minaccia" di usare violenza su cose o persone per commettere il fatto.

Di particolare interesse l'introduzione delle due seguenti nuove ipotesi di reato.

- *L'estorsione mediante reati informatici*

  La Legge Cybersicurezza introduce all'art. 629 c.p. l'ipotesi di estorsione commessa mediante la realizzazione di reati informatici (c.d. "**estorsione cyber**"); novità evidentemente finalizzata a colpire i casi, oramai sempre più numerosi (e dannosi, soprattutto per le società), di attacchi *ransomware* con connessa richiesta di riscatto.

  Più in particolare, la nuova disposizione sanziona penalmente chiunque costringa taluno a fare od omettere qualche cosa, procurando sé o altri un ingiusto profitto con altrui danno, con una delle seguenti condotte:

  - accesso abusivo ad un sistema informatico o telematico;
  - intercettazione, impedimento o interruzione illecita di comunicazioni telematiche o informatiche;
  - falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche;

- danneggiamento di informazioni, dati e programmi informatici, e di sistemi informatici o telematici.

La condotta è punita con la reclusione da sei a dodici anni e con la multa da 5mila a 10mila Euro; cornice edittale che aumenta da otto a ventidue anni di reclusione e da 6mila a 18mila Euro di multa qualora sia contestata una delle aggravanti previste per l'estorsione ordinaria (solo per fare un esempio, l'aver agito in quanto parte di una associazione per delinquere) oppure qualora il reato sia commesso nei confronti di persona incapace per età o per infermità.

❖ *La nuova truffa mediante strumenti informatici o telematici*

La Legge Cybersicurezza introduce una nuova aggravante al reato di truffa (art. 640, comma 2-*ter*, c.p.), integrata allorquando il fatto sia stato commesso **a distanza attraverso strumenti informatici o telematici idonei ad ostacolare la propria o l'altrui identificazione** (c.d. "**truffa *cyber***").

Nella predetta ipotesi, il reato è punito con la reclusione da uno a cinque anni e con la multa da 309 a 1.549 Euro e risulta procedibile d'ufficio.

In caso di condanna o patteggiamento trova applicazione la confisca obbligatoria, anche per equivalente, del profitto o del prezzo del reato oltre alla confisca dei beni e strumenti informatici o telematici che sono stati utilizzati, in tutto o in parte, per la commissione del reato nonché di quelli che ne costituiscono il prodotto o il profitto (anche per equivalente).

…ma anche di nuove attenuanti

Vengono, infine, introdotte anche due nuove **circostanze attenuanti** applicabili a talune specifiche fattispecie di reati informatici (nuovi artt. 623-*quater* e 639-*ter* c.p.):

- per i fatti di **lieve entità** in ragione della natura, della specie, dei mezzi, delle modalità o delle circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, sarà prevista una diminuzione della pena fino ad un terzo;
- per coloro i quali si adoperino per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando gli inquirenti nella raccolta degli elementi di prova o nel recupero dei proventi dei criminali o degli strumenti utilizzati per commetterli, una diminuzione della pena dalla metà a due terzi (**attenuante della c.d. "collaborazione"**); detta aggravante potrà persino essere ritenuta prevalente sulla recidiva reiterata, in deroga dell'art. 69, ultimo comma, c.p.; ne viene, tuttavia, esclusa l'applicazione ai casi di truffa *cyber* sopra descritta.

E quali conseguenze per gli Enti?

La Legge Cybersicurezza incide, poi, anche sulla responsabilità amministrativa da reato delle persone giuridiche. Due le principali novità introdotte dall'art. 20 della Legge Cybersicurezza all'art. 24-*bis* D.Lgs. n. 231/2001:

- anzi tutto, in linea con l'approccio adottato per i reati di cui al Codice Penale, è previsto un generale **inasprimento delle sanzioni pecuniarie** applicabili all'Ente nelle ipotesi in cui il reato presupposto sia un reato informatico commesso nell'interesse o a vantaggio dell'Ente medesimo;

- viene, poi, prevista l'inclusione nell'elenco dei reati presupposto di cui al citato art. 24-*bis* D.Lgs. n. 231/2001 della fattispecie di **estorsione cyber**, con una sanzione pecuniaria che può arrivare sino a 1.239.200 Euro, nonché, in caso di condanna dell'Ente per il relativo illecito amministrativo, la possibilità di applicare le sanzioni interdittive previste dall'art. 9, comma 2, D.Lgs. n. 231/2001 per un periodo non inferiore a due anni.

Rafforzamento degli strumenti a disposizione delle Procure

Pare qui utile segnalare, in ultimo, come la Legge Cybersicurezza abbia esteso il termine di conclusione delle indagini a **due anni** (invece del termine ordinario di 18 mesi) nelle ipotesi di reati informatici commessi in danno di sistemi informatici o telematici di interesse militare o comunque di interesse pubblico.

Inoltre, viene estesa ai reati informatici rimessi al coordinamento del Procuratore nazionale antimafia e antiterrorismo la speciale disciplina delle **intercettazioni** prevista per i fatti di criminalità organizzata, che consente un utilizzo più ampio del predetto strumento investigativo.

L'IMPORTANZA DI UN APPROCCIO PROATTIVO ED A 360°

L'impianto della Legge Cybersicurezza conferma come la materia degli incidenti informatici e, più in generale, della sicurezza e resilienza informatica richieda da parte delle società un **approccio sempre di più proattivo ed a 360°**, che attribuisca pari importanza tanto alla **prospettiva *ex ante* della prevenzione** quanto alla **prospettiva *ex post* della gestione e della reazione all'eventuale incidente informatico**.

La prevenzione, in una dimensione *ex ante*, richiede, anzi tutto, di implementare una ***governance* aziendale** quanto più **integrata** possibile: l'organizzazione deve avere una piena conoscenza degli *asset* aziendali e dei processi operativi, così da poter valutare in maniera adeguata i rischi associati alla propria realtà; egualmente, il *management* deve avere visibilità a trecentosessanta gradi di quello che avviene all'interno del perimetro aziendale, fisico e virtuale.

In particolare, sono quattro le direttrici essenziali che devono guidare l'attività di prevenzione:

- anzi tutto, l'identificazione e l'analisi dei rischi di *cyber security* ai quali l'azienda è esposta alla luce della tipicità dei propri processi operativi;
- in secondo luogo, l'implementazione di **adeguati presidi di sicurezza e mitigazione dei rischi**, non soltanto a livello informatico, ma anche a livello di funzioni di controllo e nella scelta dei fornitori;
- in terzo luogo, la predisposizione, l'effettiva implementazione ed il monitoraggio sul rispetto di ***policy*, procedure e linee guida adeguate**;
- in quarto luogo, assicurare un'adeguata **sensibilizzazione** degli utenti aziendali a tutti i livelli mediante l'erogazione di specifiche sessioni di **formazione**, posto che, è sempre opportuno tenerlo a mente, il fattore umano rimane la principale incognita nel costruire la linea di difesa contro gli attacchi informatici.

Qualora, nonostante i plurimi presidi adottati, l'azienda cada comunque vittima di un attacco informatico, in questo scenario, oltre alla gestione dei profili

tecnico-informatici, diviene essenziale la gestione dei profili giuridici connessi al fenomeno.

L'azienda, infatti, si trova a dover gestire i rapporti con una pluralità di Autorità Pubbliche.

In primis, certamente il Garante Privacy, laddove l'incidente informatico dia origine ad un *data breach* per il quale è necessario procedere con le notifiche e le connesse attività stabilite dal GDPR.

Inoltre, la vittima di un cyberattacco dovrà valutare se sia soggetta ad obblighi di segnalazione e notifica all'ACN.

L'azienda dovrà, altresì, valutare attentamente anche la presentazione di un esposto o di una denuncia-querela, a seconda delle circostanze, all'Autorità Giudiziaria (Procura della Repubblica o Polizia Postale), in un'ottica di maggior tutela nonché di collaborazione con le Autorità.

Anche sotto il profilo della gestione *ex post* di un incidente informatico diviene, perciò, essenziale per ogni azienda l'adozione di un sistema di *policy*, procedure e linee guida che definiscano in modo chiaro ruoli e responsabilità, nonché le azioni da intraprendere nei vari scenari, così da assicurare una risposta tempestiva, efficace ed efficiente.

CLIFFORD
CHANCE

CONTATTI

Antonio Golino

Partner

T +39 02 8063 4509
M +39 3478611889
E antonio.golino
@cliffordchance.com

Giuseppe Principato

Counsel

T +39 02 8063 4214
M +39 3371140405
E giuseppe.principato
@cliffordchance.com

Andrea Tuninetti-Ferrari
Counsel

T +39 02 8063 4435
M +39 366 6340549
E andrea.tuninettiferrari
@cliffordchance.com

Stella Magistro

Senior Associate

T +39 02 8063 4033
M +39 334 6930668
E stella.magistro
@cliffordchance.com

Laura Scaramellini

Senior Associate

T +39 02 8063 6297
M +39 337 1402082
E laura.scaramellini
@cliffordchance.com

Greta Negro

Associate

T +39 02 8063 44351
M +39 331 6934411
E greta.negro
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, Via Broletto, 16, 20121 Milano, Italia

Clifford Chance Studio Legale Associato