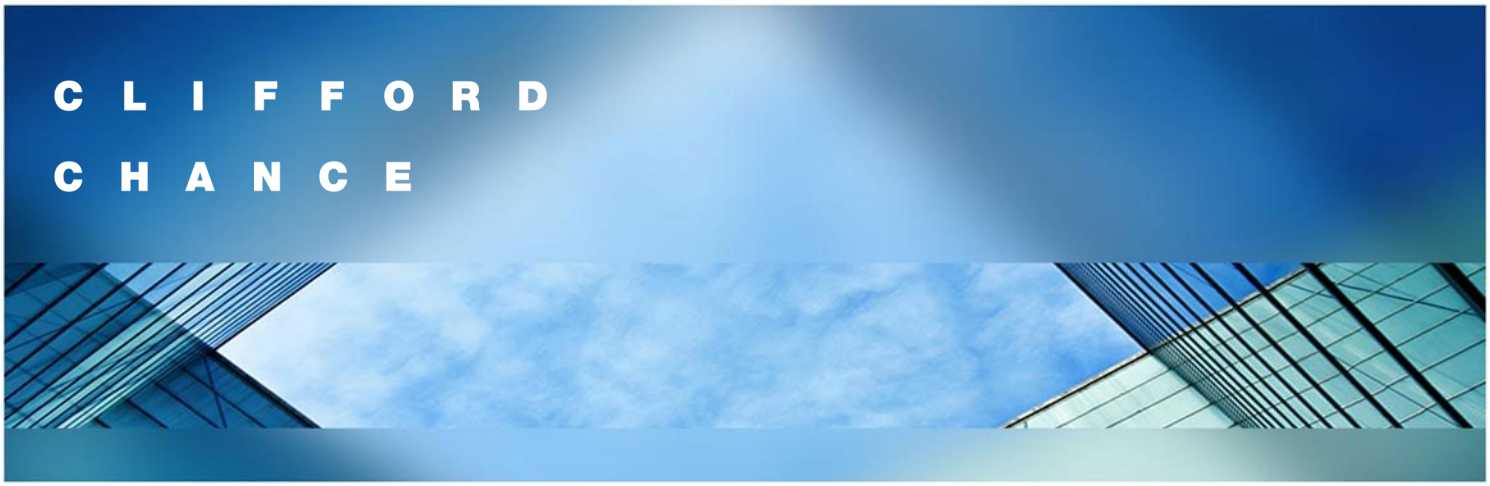

NUOVE FRONTIERE NELLA LOTTA AI *CYBERCRIMES*: IL SECONDO PROTOCOLLO ADDIZIONALE ALLA CONVEZIONE DI BUDAPEST

Lo scorso 12 maggio, 22 Paesi membri del Consiglio d'Europa, tra i quali l'Italia, hanno ratificato a Strasburgo il **Secondo Protocollo addizionale alla Convenzione sulla criminalità informatica** (la "**Convenzione di Budapest**") **concernente la cooperazione rafforzata e la divulgazione delle prove elettroniche** (il "**Secondo Protocollo**").

Key issues

- Canali di cooperazione diretta ed immediata tra Stati e *service provider* per l'ottenimento di informazioni sui titolari dei nomi di dominio, sugli abbonati e sui dati relativi al traffico
- Procedura specifica per i casi di emergenza
- Strumenti di assistenza reciproca
- Garanzie in materia di protezione dei dati personali

Atteso il crescente proliferare dei fenomeni di criminalità informatica, sempre più complessi e "senza frontiere", l'Autorità Giudiziaria si trova costantemente di fronte alla necessità (ed alle connesse difficoltà) di dover acquisire prove elettroniche – già di per sé estremamente volatili – dislocate in giurisdizioni estere. A questo riguardo, i "tradizionali" strumenti di cooperazione, quali, per esempio, la rogatoria internazionale, si sono dimostrati non di rado inefficaci o, in ogni caso, estremamente laboriosi.

L'obiettivo del Secondo Protocollo è, dunque, quello di stabilire **norme comuni** a livello internazionale per **rafforzare la cooperazione** in materia di criminalità informatica e **la raccolta di prove in formato elettronico** ai fini di indagini o procedimenti penali.

In particolare, il Secondo Protocollo impone ai Paesi firmatari la creazione di canali di comunicazione specifici, rapidi e diretti, non solo tra le Autorità statali preposte, ma, soprattutto, tra queste ultime ed i soggetti privati, quali, in particolare, i prestatori di servizi *online*, collocati in giurisdizioni straniere, al fine di consentire la raccolta e la divulgazione in modo agile ed in tempi brevi di informazioni relative, per esempio, alla registrazione dei nomi di dominio, agli abbonati ed ai dati del traffico telematico.

LE NUOVE PROCEDURE PREVISTE DAL SECONDO PROTOCOLLO

Più nel dettaglio, il Secondo Protocollo prevede che, in relazione a specifiche indagini o procedimenti penali pendenti avanti l'Autorità Giudiziaria di un Paese firmatario, il medesimo, per il tramite dei competenti organi, possa:

- inviare direttamente ad un **ente che fornisce servizi di registrazione di nomi di dominio** sul territorio di un altro Paese una **richiesta** relativa ad informazioni, in possesso o sotto il controllo del predetto ente, necessarie al

fine di identificare o contattare il titolare di un nome di dominio (art. 6 del Secondo Protocollo);

- inviare direttamente ad un **prestatore di servizi *online*** sul territorio di un altro Paese firmatario un **ordine** al fine di ottenere la divulgazione di specifiche informazioni memorizzate relative agli abbonati, in possesso o sotto il controllo del suddetto prestatore di servizi, qualora tali informazioni siano necessarie ai fini di un procedimento penale pendente avanti l'Autorità Giudiziaria del Paese richiedente (art. 7 del Secondo Protocollo).

  Qualora l'*internet provider* non risponda nei termini o rifiuti di fornire riscontro, il Secondo Protocollo prevede che le Autorità competenti dello Stato presso il quale si trova il prestatore di servizi "inadempiente" possano emettere un ordine al fine di imporre a quest'ultimo la divulgazione delle informazioni relative agli abbonati e dei dati relativi al traffico in suo possesso di cui necessita il Paese richiedente (art. 8 del Secondo Protocollo).

Il Secondo Protocollo introduce, altresì, una **procedura accelerata per i casi di emergenza**, che opererà attraverso il "Punto di Contatto" identificato da ciascuno Stato (già previsto dall'art. 35 della Convenzione di Budapest), attivo 7 giorni su 7 e 24 ore su 24, che si occuperà di ricevere e trasmettere le richieste di assistenza immediata per ottenere da un prestatore di servizi la trasmissione rapida di specifici dati informatici di cui è in possesso (art. 9 del Secondo Protocollo).

Infine, il Secondo Protocollo contempla, in chiusura, specifiche **garanzie per la tutela dei dati personali**. Con riferimento quantomeno ai Paesi dell'Unione Europea, si renderà, dunque, necessaria una armonizzazione della disciplina in considerazione dei principi già esistenti in materia (si pensi per esempio alla Direttiva Europea sulla Protezione dei Dati Personali nelle attività di Polizia e Giudiziarie).

A seguito della ratifica, i Paesi firmatari dovranno adottare adeguate misure, onde rendere effettive le procedure di cooperazione previste dal Secondo Protocollo che, si precisa all'art. 5, opereranno a prescindere dalla presenza o meno di singoli trattati di mutua assistenza giudiziaria tra gli Stati.

VERSO QUALE DIREZIONE SI MUOVE L'EUROPA?

La firma del Secondo Protocollo si inserisce nella scia delle importanti novità che negli ultimi anni, soprattutto a livello europeo, hanno portato ad un complessivo rafforzamento degli strumenti di cooperazione tra Stati, così da fornire una risposta quanto più efficace possibile ai fenomeni criminali. Basti pensare, a titolo d'esempio, all'introduzione di istituti quali il Mandato di Arresto Europeo, l'Ordine di Indagine Europeo, fino alla recente istituzione di una vera e propria Procura Europea.

Non solo. La ratifica del Secondo Protocollo costituisce anche un importante passo in avanti sia in termini di stretta **prevenzione del crimine informatico**, sia, ancor più, in termini di **evoluzione delle indagini digitali**; entrambi temi prioritari nell'agenda dell'Unione Europea.

La prova digitale ha, difatti, acquisito una sempre maggiore centralità, non soltanto in quei procedimenti riguardanti reati informatici in senso stretto, ma anche in relazione ad altre fattispecie criminose (un esempio può essere il reato

di riciclaggio, che non rientra nel novero dei canonici "reati informatici", ma che sta acquisendo sempre di più una dimensione digitale). In questo contesto, il ricorso ai "tradizionali" strumenti di cooperazione fra gli Stati, come la rogatoria internazionale, ovvero il mero affidarsi alle scelte dei *service provider*, attraverso la stipulazione di accordi, non permette più di garantire una risposta adeguata, rapida ed efficace su larga scala. Non bisogna, infatti, dimenticare che il mondo della rete è una realtà senza frontiere, sovrastatale.

Alla luce delle continue evoluzione che contraddistinguono, dunque, il panorama europeo – da intendersi in senso ampio, posto che la Convenzione di Budapest ed il Secondo Protocollo incidono su tutti i Paesi Membri del Consiglio D'Europa e non solo su quelli facenti parte dell'Unione Europea (tra i Paesi che hanno ratificato il Secondo Protocollo vi è, per esempio, il Regno Unito) – a diviene fondamentale affidarsi ad un *team* legale altamente specializzato e con una solida esperienza *cross-boarder*:

- da un lato, laddove vittime di reati informatici (e non), al fine di richiedere tempestivamente ed in maniera efficace l'attivazione da parte dell'Autorità Giudiziaria di tutti i canali e di tutti gli strumenti di cooperazione a livello europeo e transfrontaliero previsti dalle nuove normative, onde, in particolare, ottenere l'acquisizione di quegli elementi di prova essenziali nell'ambito di indagini e procedimenti penali, anche qualora situati in giurisdizioni straniere;
- dall'altro lato, qualora destinatari di richieste da parte di Autorità straniere, inviate alla stregua delle nuove normative europee e transfrontaliere, al fine gestire al meglio le suddette richieste, fornendo un riscontro adeguato nei tempi più rapidi possibili. Questo scenario, alla luce delle procedure introdotte dal Secondo Protocollo, diventerà sempre più frequente soprattutto per i gestori di piattaforme informatiche.

Più in generale, il Secondo Protocollo si colloca all'interno di un contesto più ampio di iniziative volte ad assicurare la legalità delle attività *online*. Si consideri, ad esempio, la bozza di 'Digital Services Act' ("**DSA**"), che ci si aspetta diventerà applicabile a partire dal 2024. Il DSA mira a rendere più sicuro lo spazio digitale europeo, prevedendo obblighi stringenti per i cc.dd. intermediari dei servizi dell'informazione – quali, ad esempio, *online marketplace*, *app store* e *social network* – nel tentativo di combattere fenomeni come *fake news* e disinformazione, commercializzazione di prodotti contraffatti, diffusione di contenuti illeciti. Sul modello del GDPR, il DSA prevede sanzioni che possono raggiungere il 6% del fatturato annuo globale del trasgressore.

CONTATTI

Giuseppe Principato
Counsel

T +39 02 8063 4214
M +39 337 1140405
E giuseppe.principato@cliffordchance.com

Laura Scaramellini
Senior Associate

T +39 02 8063 4297
M +39 337 1402082
E laura.scaramellini@cliffordchance.com

Giovanni Minucci
Associate

T +39 02 8063 4027
M +39 331 6672450
E Giovanni.Minucci@cliffordchance.com

Giada Scarnera
Associate

T +39 02 8063 4224
M +39 360 1012788
E giada.scarnera@cliffordchance.com