SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

EUROPOL

EUROJUST

Linee Guida Generali

SULL'ACCESSO TRANSFRONTALIERO ALLE PROVE ELETTRONICHE

Ultimo aggiornamento: 26/11/2020

Il progetto SIRIUS ha ricevuto finanziamenti dal servizio degli strumenti di politica estera (FPI) della Commissione europea in base alla convenzione di sovvenzione n. PI/2017/391-896

Il presente documento è stato realizzato con l'assistenza finanziaria dell'Unione europea. Le opinioni in esso espresse non possono in alcun modo essere considerate opinioni ufficiali dell'Unione europea.

Il presente documento è stato redatto con le informazioni disponibili al momento della stesura. Si raccomanda di consultare le linee guida più recenti dell'azienda durante la presentazione di una richiesta di divulgazione di dati.

- Questo documento contiene informazioni **Europol non classificate - Livello di protezione di base**. Deve essere protetto per garantirne la riservatezza e non deve essere divulgato a persone non autorizzate o al pubblico.
- Il presente documento può essere distribuito esclusivamente ad **autorità giudiziarie e di contrasto**. Non può essere divulgato senza previo consenso scritto di Europol.

INDICE

ACRONIMI

- BSI: informazioni di base sull'abbonato (Basic Subscriber Information)
- CD: dati relativi al contenuto (Content Data)
- CLOUD Act: Clarifying Lawful Overseas Use of Data Act
- DOJ: dipartimento di Giustizia (Department of Justice)
- DR: richiesta diretta (Direct Request)
- EDR: richiesta di divulgazione di emergenza (Emergency Disclosure Request)
- E-Evidence: prove elettroniche
- OEI: ordine europeo di indagine
- RGE: rete giudiziaria europea (European Judicial Network)
- EPE: Piattaforma Europol per esperti (Europol Platform for Experts)
- UE: Unione europea
- FBI: Federal Bureau of Investigation
- IP: Internet Protocol
- LEA: Agenzia di contrasto (Law Enforcement Agency)
- MLA: mutua assistenza giudiziaria (Mutual Legal Assistance)
- SM: Stati membri
- NDO: ordine di non divulgazione (Non-Disclosure Order)
- OIA: Ufficio per gli Affari internazionali - Dipartimento di giustizia statunitense (Office of International Affairs)
- OSINT: intelligence da fonti aperte (Open Source Intelligence)
- PSO: prestatori di servizi online
- P2P: cooperazione tra forze di polizia (Police-to-police)
- PR: richiesta di conservazione (Preservation Request)
- SCSI: Interfaccia di sistema per piccoli computer
- SIENA: applicazione di rete per lo scambio di informazioni protetta (Secure Information Exchange Network Application)
- SPoC: Punto di contatto unico (Single Point of Contact)
- TD: dati relativi al traffico (Traffic Data)
- USA: Stati Uniti d'America

La **Guida generale di SIRIUS sull'accesso transfrontaliero alle prove elettroniche** fornisce linee guida su come recuperare legalmente informazioni disponibili e non disponibili al pubblico conservate da prestatori di servizi nell'ambito di indagini penali. In base alla convenzione di Budapest sulla criminalità informatica[1] del 2001, la definizione di prestatore di servizi è la seguente: «qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico; qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio»[2].

La presente guida riguarda le procedure per richiedere dati ai soggetti giuridici e alle imprese titolari del trattamento dati stabiliti nel territorio dell'UE e in paesi terzi (ad esempio negli Stati Uniti). Indipendentemente dall'ubicazione dei prestatori di servizi online (PSO), è sempre consigliabile verificare le differenze nella procedura e le disposizioni specifiche del paese interessato.

RISORSE SUPPLEMENTARI DISPONIBILI SU SIRIUS

Per maggiori informazioni sulle procedure dei singoli prestatori di servizi online, sulle informazioni di contatto e sul tipo di dati che è possibile richiedere, cfr. la sezione sugli Orientamenti specifici di SIRIUS.

1. CATEGORIE DI DATI

I dati elettronici si possono classificare in due categorie principali: **dati archiviati** e **comunicazioni in tempo reale**.

Inoltre, esistono sottocategorie sia per i dati elettronici conservati che per quelli in tempo reale, in base al livello di sensibilità loro attribuito. A seconda del tipo di dati, la procedura e i requisiti per richiederli nel quadro di indagini penali variano considerevolmente.

Esistono strumenti giuridici che forniscono una definizione generale per ciascuna categoria, come la convenzione di Budapest sulla criminalità informatica, ma non solo: il «Clarifying Lawful Overseas Use of Data Act» (o «CLOUD Act»[3]) riconosce due definizioni di dati, distinguendo «i contenuti di una comunicazione cablata o elettronica»[4] da «qualsiasi registrazione o altra informazione concernenti il cliente o l'abbonato»[5].

In ogni caso, occorre ricordare che i prestatori di servizi online (PSO) acquisiscono dati diversi in modi diversi, in base alle esigenze e ai tipi di servizi aziendali. Pertanto, potrebbero esserci alcune differenze da un'azienda all'altra in merito a ciò che rientra in ciascuna categoria o sottocategoria. Per questo motivo, prima di effettuare richieste, è consigliabile consultare le linee guida aziendali o quelle specifiche di SIRIUS, ove possibile.

Cfr. l'annesso 1 per una panoramica visiva delle categorie di dati elettronici.

A- INFORMAZIONI ARCHIVIATE

I. DATI NON RELATIVI AL CONTENUTO

1 - INFORMAZIONI DI BASE SUGLI ABBONATI (BSI)

A. DEFINIZIONE DI BSI[6]

«Ogni informazione detenuta in forma di dato informatico o sotto altra forma da un fornitore di

[1] Tutti i dettagli relativi alla Convenzione di Budapest sulla criminalità informatica sono disponibili sul sito web del Consiglio d'Europa.
[2] Ai sensi dell'articolo 1, convenzione di Budapest sulla criminalità informatica.
[3] Il CLOUD Act statunitense è stato promulgata nel marzo 2018. Le sue disposizioni in materia di conservazione e richiesta di dati sono applicabili sulla base degli accordi esecutivi istituiti a norma di detto strumento e su base bilaterale.
[4] Articolo 3, paragrafo 2713, «Conservazione obbligatoria e divulgazione di comunicazioni e registrazioni». Il testo completo del CLOUD Act è disponibile qui.
[5] *Ibid.*
[6] Ai sensi dell'articolo 18, paragrafo 3, della convenzione di Budapest sulla criminalità informatica.

servizi e relativa agli abbonati ad un proprio servizio e diversa dai dati relativi al traffico o al contenuto e attraverso la quale è possibile stabilire:

a) il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche prese a tale riguardo e il periodo del servizio;
b) l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio;
c) ogni altra informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio».

B. TIPO DI INFORMAZIONI DISPONIBILI SULL'ABBONATO

- L'account dell'utente o il suo nome utente;
- il nome dell'utente o il suo vanity URL;
- il suo numero o i suoi numeri di telefono;
- il suo indirizzo di posta elettronica;
- l'indirizzo IP (Internet Protocol) utilizzato per la registrazione, l'arco temporale di attività (date e orari) e l'indirizzo MAC;
- informazioni di fatturazione;
- data e ora della modifica della password/dei dati di contatto;
- indirizzo IP utilizzato per la modifica della password/dei dati di contatto.

Qualsiasi altra informazione relativa all'identità dell'abbonato tra cui, ma non solo, le informazioni di fatturazione (ivi compresi il tipo e il numero di carte di credito o altre informazioni di identificazione).

Esistono vari modi di richiedere ai prestatori di servizi online (PSO) informazioni di base sull'abbonato, quali ad esempio:

- la cooperazione volontaria: richiesta diretta / richiesta di divulgazione di emergenza;
- la cooperazione obbligatoria: mutua assistenza giudiziaria / ordine europeo di indagine.

Questo argomento verrà spiegato ulteriormente nella sezione relativa a *Come recuperare informazioni non disponibili al pubblico*.

2- DATI RELATIVI AL TRAFFICO (TD)

A. DEFINIZIONE DI DATI RELATIVI AL TRAFFICO

Ai sensi della convenzione di Budapest sulla criminalità informatica, per dato relativo al traffico si intende «qualsiasi informazione computerizzata relativa ad un comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio»[7].

I dati relativi al traffico sono dunque le informazioni, comprese quelle registrate, che identificano le persone con cui un utente ha comunicato, i siti che ha visitato e informazioni analoghe sulla sua attività online, compresi tutti gli indirizzi IP utilizzati per collegarsi all'account, le date, le durate e i tempi di sessione.

B. TIPO DI DATI DISPONIBILI RELATIVI AL TRAFFICO

I tipi di set di dati specifici che vengono considerati dati relativi al traffico possono includere, ma non in modo esclusivo:

<u>Per gli account di posta elettronica o di web hosting:</u>

- destinazione o indirizzo sorgente della connessione, con marcatura temporale; orario e data di disconnessione; metodo di

[7] Articolo 1, lettera d, della convenzione di Budapest sulla criminalità informatica.

connessione al sistema; volume dei trasferimenti di dati e altre informazioni di routing;
- intestazione dei messaggi di posta elettronica, ivi comprese la sorgente e la destinazione, la data, l'orario e il volume dei dati;
- metadati di immagini o altri documenti caricati sull'account, nonché le dimensioni dei file (contenuto escluso);
- account con cui è stato effettuato l'accesso a un file o a un sito web specifico in un determinato periodo di tempo.

Per i social media e i servizi di messaggeria online:

- applicazioni;
- registri di connessione;
- impostazioni di notifica;
- impostazioni/blocchi sulla privacy;
- macchine/cookie;
- siti web;
- siti cui è stato effettuato l'abbonamento;
- poke;
- registro delle attività.

Esistono vari modi di richiedere dati relativi al traffico ai prestatori di servizi online (PSO), quali ad esempio:

- la cooperazione volontaria: richiesta diretta / richiesta di divulgazione di emergenza;
- la cooperazione obbligatoria: mutua assistenza giudiziaria / ordine europeo di indagine.

Questo argomento verrà spiegato ulteriormente nella sezione relativa a *Come recuperare informazioni non disponibili al pubblico*.

II. DATI RELATIVI AL CONTENUTO (CD)

A. DEFINIZIONE DI DATI RELATIVI AL CONTENUTO

L'articolo 209 della relazione della convenzione sulla criminalità informatica[8] afferma che quelli relativi al contenuto «*sono dati (diversi da quelli relativi al traffico) che si riferiscono al contenuto della comunicazione, ossia al significato o al senso di quest'ultima, oppure al messaggio o all'informazione trasmessa dalla comunicazione*».

Perciò i dati relativi al contenuto riguardano di norma le informazioni inviate dal mittente al destinatario in un'e-mail, tramite l'account di una rete sociale o un servizio di comunicazione, nonché i dati archiviati in un cloud o nell'ambito di servizi di informatica in remoto.

B. TIPO DI DATI DISPONIBILI RELATIVI AL CONTENUTO

La categoria dei dati relativi al contenuto comprende, in via non limitativa:

- messaggi scritti;
- fotografie o immagini incorporate;
- file video;
- file allegati;
- post;
- cronologia degli acquisti.

Per richiedere ai prestatori di servizi online (PSO) l'accesso transfrontaliero ai dati relativi al contenuto può rendersi necessario seguire canali di cooperazione obbligatoria attraverso la procedura della mutua assistenza giudiziaria o dell'ordine europeo di indagine. Questo argomento verrà spiegato ulteriormente nella sezione sull'Assistenza Giudiziaria (per eventuali eccezioni, fare riferimento alle sezioni relative a *Richiesta di divulgazione di emergenza* e *Cooperazione tra forze di polizia*).

B- COMUNICAZIONI IN TEMPO REALE

[8] La relazione della convenzione sulla criminalità informatica non costituisce uno strumento che fornisca un'interpretazione autorevole della convenzione. La relazione è disponibile qui.

La convenzione di Budapest sulla criminalità informatica prevede l'adozione di misure legislative e di altro tipo a livello nazionale per la raccolta in tempo reale dei dati sul traffico (articolo 20) e l'intercettazione dei dati relativi al contenuto (articolo 21) per le autorità competenti degli Stati firmatari, mediante l'applicazione diretta dei mezzi tecnici sul territorio dello Stato firmatario o imponendo obblighi a un prestatore di servizi.

L'articolo 30 della direttiva OEI prevede l'intercettazione di telecomunicazioni con l'assistenza tecnica di un altro Stato membro. L'articolo 31 di detta direttiva prevede una notifica (utilizzando il modulo di cui all'allegato C della direttiva) allo Stato membro nel quale si trova la persona soggetta a intercettazione e la cui assistenza tecnica non è necessaria.

In tutti i casi in cui la direttiva OEI non è applicabile, l'intercettazione delle telecomunicazioni è disciplinata esplicitamente dalla convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea (titolo III, articoli da 17 a 22).

Altrimenti, l'intercettazione delle telecomunicazioni e la raccolta in tempo reale dei dati in transito potrebbero essere effettuate sulla base di altri accordi internazionali, regionali o bilaterali.

In assenza di un accordo di mutua assistenza giudiziaria, la convenzione di Budapest sulla criminalità informatica prevede la fornitura di mutua assistenza giudiziaria agli Stati firmatari in entrambi i casi: raccolta in tempo reale dei dati sul traffico (articolo 33) e intercettazione dei dati relativi al contenuto (articolo 34). A norma dell'articolo 33, paragrafo 2, della convenzione di Budapest sulla criminalità informatica, la mutua assistenza giudiziaria in relazione alla raccolta in tempo reale dei dati sul traffico è fornita «*almeno per quanto riguarda i reati per i quali la raccolta in tempo reale dei dati sul traffico sarebbe disponibile in un caso nazionale analogo*». Conformemente all'articolo 34 della convenzione di Budapest sulla criminalità informatica, la mutua assistenza giudiziaria in relazione all'intercettazione dei dati relativi al contenuto è fornita «*nella misura consentita dai trattati e dalle legislazioni nazionali applicabili*».

Richieste per ottenere dati sul traffico in tempo reale e per intercettare dati relativi al contenuto dalle autorità statunitensi:

È possibile ottenere dati in tempo reale relativi al traffico da prestatori di servizi online (PSO) aventi sede negli Stati Uniti con una richiesta di mutua assistenza giudiziaria effettuata da autorità estere. In tal caso occorre spiegare nei dettagli quale attinenza abbiano con l'indagine i dati registrati. Ai sensi della legislazione nazionale, un tribunale statunitense può emanare un ordine che consenta a un'agenzia di contrasto degli Stati Uniti di acquisire e conservare le informazioni per un massimo di 60 giorni (termine potenzialmente prorogabile per altri 60 giorni).

Nel caso di aziende aventi sede negli Stati Uniti, attualmente la prassi giuridica nazionale vieta l'acquisizione prospettica in tempo reale di dati relativi al contenuto esclusivamente a nome di governi esteri. Gli Stati Uniti possono condividere l'acquisizione in tempo reale di dati relativi al contenuto solo se tali dati sono acquisiti nell'ambito di un'indagine statunitense.

Qualora il prestatore di servizi online (PSO) abbia sede negli Stati Uniti, l'unica modalità per acquisire dati in tempo reale relativi al contenuto consisterebbe nella *condivisione* con controparti statunitensi di informazioni investigative. Le autorità degli Stati Uniti potrebbero avviare la loro indagine parallela e richiedere informazioni in tempo reale sul contenuto delle comunicazioni.

2. COME RECUPERARE INFORMAZIONI DISPONIBILI AL PUBBLICO

Cfr. l'annesso 2 per un grafico delle seguenti informazioni.

A- DOWNLOAD DI CONTENUTI DISPONIBILI AL PUBBLICO

La prima fase di ogni indagine riguardante prove elettroniche consiste nel valutare la necessità di conservare le prove prima che vengano cancellate in modo permanente e adottare provvedimenti in merito. Il tempo è fondamentale.

Esistono soluzioni tecniche che permettono di scaricare informazioni disponibili al pubblico da un intero sito web al proprio computer, creando una «versione speculare». Ciò impedirebbe la perdita di informazioni che, in una fase successiva, potrebbero potenzialmente costituire prove elettroniche. Si osservi che alcuni PSO possono avere politiche specifiche volte a limitare la creazione di profili falsi, anche se vengono creati dalle autorità investigative a fine d'indagine.

Vi sono molti strumenti specializzati gratuiti e open source che possono agevolare il download da un sito web di informazioni disponibili al pubblico:

HTTRACK

HTTrack[9] è un programma di utilità browser gratuito, disponibile offline e facile da usare.

Permette di scaricare un sito web da Internet in una directory locale, con tutte le informazioni pubblicamente disponibili, creando in modo ricorsivo tutte le directory e trasferendo dal server al proprio computer il codice HTML, immagini e altri file. HTTrack riorganizza la struttura dei link interni del sito originale. Basta aprire una pagina del sito web «replicato» nel proprio browser ed è possibile navigare nel sito da un link all'altro, come se lo si stesse consultando online. HTTrack può inoltre aggiornare un sito replicato preesistente e ripristinare i download interrotti. È interamente configurabile e dispone di un sistema di assistenza integrato.

COMPONENTI AGGIUNTIVI

- **SaveAsMHT** è un'estensione Chrome che salva le pagine in formato .mht.
- **Fireshot** è un plugin molto utile per Chrome e Firefox che **può catturare interi siti web**, una loro selezione o solo la loro parte visibile.
  È possibile salvare rapidamente su disco in formato PDF, PNG, GIF, JPEG o BMP le parti di sito acquisite e caricarle per poi esportarle.

SALVARE IL SITO WEB IN FORMATO PDF

Una soluzione flessibile a questo problema consiste nel creare un file PDF che può essere visualizzato e condiviso. La procedura è diversa da un browser all'altro (Windows, Mozilla, Safari, ecc.)[10].

B- STRUMENTI DI SIRIUS

SIRIUS è un repertorio di strumenti analitici e di indagine sviluppati da Europol e da agenzie di contrasto negli Stati membri. Hanno la finalità di agevolare le indagini e l'analisi dei dati e sono incentrati sull'OSINT, nonché sull'elaborazione e sull'analisi di prove elettroniche.

IMPORTANTE: STRUMENTI DI TERZI

L'utilizzo di eventuali strumenti di terzi deve essere convalidato a livello interno affinché le prove (acquisite mediante gli strumenti) siano ammesse in tribunale in una fase successiva.

[9] Ulteriori informazioni tecniche su HTTrack sono disponibili qui.
[10] Spiegazione completa disponibile qui.

RISORSE SUPPLEMENTARI DISPONIBILI SU SIRIUS

Gli Strumenti di SIRIUS sono disponibili qui.

I professionisti troveranno inoltre informazioni supplementari relative agli strumenti di OSINT nelle linee guida specifiche di SIRIUS sui prestatori di servizi online (PSO), disponibili a questo indirizzo.

3. COME RECUPERARE INFORMAZIONI NON DISPONIBILI AL PUBBLICO

Nel corso di un'indagine le potenziali prove elettroniche sono detenute o controllate da un certo numero di parti diverse, quali l'autore del reato, la vittima, i prestatori di servizi online (PSO) e vari altri terzi.

La localizzazione, l'ottenimento e la conservazione di tali prove elettroniche nelle indagini sulla criminalità informatica richiedono tattiche, metodi e strumenti di contrasto diversi che possono essere differenti da quelli impiegati nel corso di indagini che coinvolgono esclusivamente prove fisiche.

Poiché la procedura di richiesta dei dati ai prestatori di servizi online (PSO) può essere dispendiosa in termini di tempo, si raccomanda di sondare anche i mezzi legali disponibili per la raccolta di prove, quali l'accesso diretto tramite atti coercitivi, l'assistenza volontaria del soggetto e/o l'analisi forense dei dispositivi.

RISORSE SUPPLEMENTARI DISPONIBILI SU SIRIUS

Conformemente alla legislazione nazionale, le autorità competenti dell'UE possono accedere direttamente ai dati elettronici all'interno di un sistema informatico se questo è ubicato nella stessa giurisdizione responsabile delle indagini o, in alcuni casi, unilateralmente attraverso un accesso transfrontaliero diretto ai dati che si ritiene siano ubicati in una giurisdizione diversa.

Un'ulteriore analisi delle disposizioni giuridiche che consentono l'accesso diretto ai dati è disponibile sul Cybercrime Judicial Monitor (edizione del 2 novembre 2016, pagg. 38-39).

Si osservi che i PSO possono chiedere il rimborso dei costi sostenuti per rispondere alle richieste di informazioni secondo quanto previsto dalla legge o dalle normative nazionali[11]. Questo meccanismo, inteso a compensare le spese sostenute per rispondere alle autorità che richiedono l'accesso ai dati, è anch'esso una parte standard delle politiche dei PSO, tuttavia, al momento della stesura della presente guida, non sembra applicabile alle richieste di dati provenienti dall'UE.

[11] Per quanto riguarda i PSO con sede negli Stati Uniti, tale aspetto è disciplinato dall'articolo 18, paragrafo 2706, del Codice degli Stati Uniti d'America. Anche alcuni Stati membri dell'UE (ad esempio Austria e Belgio) hanno attuato disposizioni analoghe.

IMPORTANTE: SERVIZI CRIPTATI END-TO-END

La maggior parte dei prestatori di servizi di cifratura end-to-end dei propri contenuti non ne fornisce il testo in chiaro. In questo caso l'approccio più efficace è quello di verificare se l'utente conservi una copia di sicurezza codificata dei dati presso altri servizi ed effettuare pertanto richieste a tali servizi, oppure procedere al sequestro legale del dispositivo e ottenerne una copia per uso forense.

A- ACCESSO DIRETTO ALLE INFORMAZIONI ELETTRONICHE (INDAGINE NAZIONALE)

Nel corso delle indagini non occorre sempre contattare i prestatori di servizi per procurarsi le prove elettroniche necessarie per l'inchiesta.

I funzionari dell'autorità di polizia o gli esperti nazionali potrebbero scaricare e conservare prove elettroniche nel corso di un atto coercitivo (per esempio durante una perquisizione domiciliare) o la vittima/l'indiziato del delitto può consegnare volontariamente le prove richieste dalle autorità investigative. Pertanto, prima di presentare al prestatore di servizi online (PSO) qualunque tipo di richiesta, è bene tenere presente che è anche possibile accedere alle informazioni necessarie utilizzando altre soluzioni e tecniche legali a livello domestico.

i. INFORMAZIONI ACQUISITE TRAMITE ATTI COERCITIVI

Gli atti coercitivi sono strumenti giuridici importanti, contemplati dalla legislazione nazionale, che permettono alle agenzie di contrasto di acquisire prove elettroniche.

Spesso questi poteri di indagine sono estremamente intrusivi e sono previste molte garanzie giuridiche per evitare la violazione del diritto alla riservatezza, della libertà personale e di altri diritti umani e fondamentali garantiti dalle costituzioni nazionali e dalle convenzioni internazionali.

In ogni paese vigono norme interne di procedura penale per raggiungere un equilibrio tra le esigenze dell'indagine e i diritti dei singoli. Le autorità investigative possono ottenere informazioni che potrebbero essere utilizzate come prove nel corso di un processo solo se si attengono rigorosamente alle norme relative alle indagini penali vigenti nei rispettivi paesi.

ATTI COERCITIVI SEGRETI E SORVEGLIANZA TECNICA

Questa sezione tratta il monitoraggio - interno - in tempo reale dell'attività informatica e dei dati archiviati su un disco rigido, o dei dati trasferiti mediante reti informatiche come Internet. Le indagini nazionali non possono avvalersi di questo strumento al di fuori delle loro giurisdizioni nazionali e la sorveglianza transfrontaliera può essere effettuata esclusivamente con la cooperazione delle autorità investigative dei paesi interessati.

La **sorveglianza informatica e di rete in tempo reale** richiede l'autorizzazione di un tribunale penale o di un'altra agenzia governativa indipendente e ha sempre una finalità specifica, che si può conseguire esclusivamente per mezzo di un'operazione segreta e prevede sempre tempi di esecuzione monitorati in modo molto rigoroso. La sorveglianza segreta è sempre svolta da un reparto specializzato della forza di polizia nazionale.

La sorveglianza segreta in tempo reale viene condotta per mezzo di applicazioni apposite installate nel sistema elettronico in oggetto e i dati vengono registrati dall'autorità di esecuzione. Il metodo di installazione del software di sorveglianza su un dispositivo elettronico cambia di volta in volta

e viene attuato dopo una valutazione approfondita da parte dell'autorità.

I programmi installati possono avere finalità specifiche come, per esempio, cercare dati sospetti all'interno dei contenuti dei dischi rigidi, monitorare l'uso del computer, acquisire password e/o riferire al proprio operatore le attività in tempo reale tramite una connessione a Internet. Un esempio di programmi installabili sono i keylogger, che registrano tutte le battiture effettuate su un computer, possono memorizzare i dati sul disco rigido locale o anche trasmettere automaticamente i propri registri a un computer remoto attraverso la rete/Internet.

Esistono svariati metodi per installare questo tipo di software. Il più comune è l'installazione remota, attraverso la creazione di una backdoor con un apposito programma informatico. Un altro metodo è costituito dall'«intrusione» nel computer (hacking) per accedervi attraverso una rete, affinché l'autorità investigativa possa successivamente installare da remoto un software di sorveglianza.

RICERCA E SEQUESTRO DI DATI INFORMATICI ARCHIVIATI

Una volta che i metodi investigativi abbiano localizzato prove potenziali e ne sia stato garantito l'accesso, possibilmente per mezzo di atti coercitivi, è possibile sequestrare i dati in questione per poterli analizzare ulteriormente e impiegarli come prove nel corso di un processo.

Il sequestro di prove elettroniche può essere giustificato da esigenze molto specifiche, in quanto i dati sequestrati devono essere esattamente gli stessi introdotti come prove nel processo penale. Questo requisito può essere soddisfatto sequestrando l'intero sistema informatico, compresi i dispositivi di archiviazione dati, sequestrando solo questi ultimi o eseguendone copie identiche.

In generale, l'intero sistema informatico deve essere sequestrato se è stato o doveva essere effettivamente utilizzato come strumento per commettere un reato penale o se contiene elementi hardware specifici che devono essere impiegati per poter accedere a dati come la gerarchia del disco rigido SCSI (Interfaccia di sistema per piccoli computer), chiavi hardware ecc. Sequestrare soltanto i dispositivi di archiviazione dati (quali ad esempio dischi rigidi, unità a stato solido e chiavi USB) è sufficiente se i dati ivi contenuti costituiscono prove (come una fotografia, un video, un file audio o un documento) e vi si può accedere senza disporre del sistema informatico originale. La copia identica di un dispositivo di archiviazione dati si può utilizzare come prova nei casi in cui la rimozione del dispositivo causerebbe danni considerevoli (finanziari, economici o di altra natura) alla parte soggetta alla misura coercitiva.

Nel corso di un sequestro è indispensabile dimostrare che i dati sequestrati siano gli stessi registrati come prova; a tal fine esistono diversi generatori di codici di controllo, noti anche come «valori hash». Questi ultimi si possono considerare come una sorta di impronte digitali per i file o i dispositivi di archiviazione dati. Il contenuto di un file o di un dispositivo di archiviazione dati viene elaborato attraverso un algoritmo crittografico, producendo un valore numero unico (il valore hash) che serve a identificare i contenuti del file o del dispositivo di archiviazione dati. Se i contenuti vengono minimamente modificati, cambierà considerevolmente anche il valore hash. Oggi sono ampiamente diffusi due algoritmi per produrre valori hash, ossia gli algoritmi MD5 e SHA1. Non esistono due valori hash che possano essere identici, a meno che i dati che hanno convalidato non siano esattamente gli stessi, né è possibile risalire ai dati originali o ricostruirli in base al valore hash, che serve esclusivamente a dimostrare che i due pacchetti di dati sono assolutamente identici.

Nota: qualsiasi modifica apportata a un sistema di dati altera il valore hash (persino l'avvio di un sistema può danneggiare il valore hash precedente). Per evitare questo problema, occorre avvalersi in qualunque momento di una protezione di scrittura quando si avvia a fini di analisi un

dispositivo di archiviazione dati o un computer che è stato sequestrato. Non è possibile determinare l'entità della modifica in base al valore hash.

La convenzione di Budapest sulla criminalità informatica non prevede in quanto tale norme specifiche sulle ricerche digitali svolte all'interno del paese in cui viene condotta l'indagine, richiedendo invece che gli Stati firmatari adottino misure legislative e di altro tipo che possono rendersi necessarie per attribuire alle loro autorità competenti il potere di perquisire o accedere ai sistemi informatici e ai supporti per la conservazione di dati[12]. Tali misure legislative sono contemplate dai codici di procedura penale dei paesi firmatari.

ANALISI FORENSE DI DATI INFORMATICI ARCHIVIATI

Una volta che si sia proceduto al loro sequestro, le informazioni digitali devono essere esaminate da investigatori informatici o da esperti forensi privati, chiamati dalle autorità investigative o giudiziarie a fornire risposte a domande specifiche pertinenti per l'indagine.

Gli investigatori o gli esperti possono avvalersi di diverse tecniche e applicazioni proprietarie forensi per esaminare e perquisire cartelle nascoste o spazio su disco non allocato alla ricerca di file cancellati, criptati o danneggiati, salvaguardando nel contempo una catena di prove documentata. Possono essere inoltre incaricati di decifrare un file criptato, recuperare dati andati persi o accertare determinati fatti (per esempio quando e come una foto è stata scaricata e trasmessa). La relazione sull'esame forense deve essere comprensibile per i legali e le altre parti del procedimento prive di conoscenze specifiche in materia di programmazione e utilizzo dell'hardware. Nel corso dell'esame forense, al fine di tutelare l'integrità dei dati sequestrati, si usano raramente i mezzi di archiviazione dei dati originali; gli esaminatori si servono delle relative copie identiche per eseguire la loro valutazione.

II. INFORMAZIONI FORNITE DALLE PARTI DELL'INDAGINE

In molti casi, testimoni, indiziati o altre parti saranno disposti a fornire volontariamente l'accesso ai propri account affinché sia possibile scaricare e conservare informazioni. I dati forniti dalle parti dell'indagine devono essere sempre verificati e confrontati dagli investigatori, poiché potrebbero essere intenzionalmente o accidentalmente inaccurati o privi di informazioni cruciali. Gli obiettivi di un'indagine e quelli delle vittime/dei testimoni possono essere molto diversi e le prove devono sempre essere utili ai fini dell'inchiesta.

La consegna volontaria di informazioni può avvenire fornendo l'informazione o la password richieste, oppure attraverso il download dell'intera banca dati e la sua consegna alle autorità.

Alcuni prestatori di servizi online (PSO) permettono agli utenti di **scaricare le loro informazioni** e i loro dati. Questo download può essere effettuato dalle autorità investigative, ma le informazioni di accesso devono essere fornite dall'utente abilitato del sistema informatico (i metodi specifici dei prestatori di servizi online non si possono utilizzare senza le credenziali degli utenti). Questa procedura verrà illustrata dettagliatamente nelle linee guida specifiche sui prestatori di servizi online (PSO), disponibili sulla piattaforma SIRIUS.

[12] Articolo 19, paragrafi 1 e 2, della convenzione di Budapest sulla criminalità informatica.

IMPORTANTE: APPLICAZIONI DI TERZI E POTENZIALI LIMITAZIONI TECNICHE

È possibile che vengano acquisite informazioni da applicazioni, strumenti e siti web di terzi. Il loro utilizzo nel corso delle indagini potrebbe comportare la divulgazione di informazioni operative.

Alcune aziende potrebbero applicare limitazioni tecniche per impedire agli utenti di scaricare le proprie informazioni in caso siano rilevate potenziali attività errate / irregolari (ad esempio: utilizzo di dispositivi o luoghi diversi).

È importante tenere conto della legislazione nazionale in materia di consenso degli utenti e valutare se i dati ottenuti possano essere addotti o meno come prove.

Ai sensi dell'articolo 32 della convenzione di Budapest sulla criminalità informatica, l'autorità investigativa - con il consenso volontario della persona legalmente autorizzata a divulgare i dati immagazzinati nel sistema informatico (per esempio il titolare dell'account) - può accedere alle informazioni conservate presso una giurisdizione diversa. Le informazioni ottenute si possono successivamente utilizzare come prova nel corso di un processo, senza dover presentare richieste di mutua assistenza giudiziaria né emettere ordini europei di indagine. Questo avviene di norma se le prove richieste sono contenute, per esempio, in un messaggio di posta elettronica conservato in un account di webmail online come Gmail. Questo articolo conferisce all'autorità investigativa, previo consenso della persona legalmente autorizzata (tramite l'accesso all'account di webmail memorizzato in un altro paese), il potere di accedere al profilo di posta elettronica conservato presso una giurisdizione diversa e di scaricare le informazioni richieste.

B- RICHIESTA DIRETTA / COOPERAZIONE VOLONTARIA

Spesso la cooperazione volontaria tra le autorità e i prestatori di servizi online (PSO) con sede all'estero è il canale più rapido per ottenere legalmente dati non relativi al contenuto nell'ambito di indagini penali.

Le richieste dirette sono considerate un tipo di **cooperazione volontaria** e le aziende non sono obbligate a soddisfarle. Il formato di tali richieste può differire da un paese all'altro; in alcuni Stati membri possono essere emesse direttamente dalle autorità di contrasto senza dover coinvolgere un tribunale, in conformità al diritto nazionale.

I prestatori di servizi online possono esaminare richieste dirette e verificarne la legittimità ai sensi della normativa del paese in cui hanno sede. Le aziende possono stabilire requisiti propri relativi alle richieste di autorità estere tenendo conto non solo delle leggi applicabili, ma anche delle peculiarità dei loro servizi e prodotti.

IMPORTANTE: NOTIFICA ALL'UTENTE

Si deve considerare che le aziende possono notificare all'utente/agli utenti interessati le richieste di conservazione e di divulgazione dei dati personali effettuate da autorità giudiziarie e di contrasto, a meno che venga emesso un ordine di non divulgazione (Non-Disclosure Order, NDO) da parte di autorità del paese in cui si trova la loro sede.

Le aziende, a loro esclusiva discrezione, potrebbero inoltre astenersi volontariamente dall'effettuare la notifica all'utente qualora dispongano di informazioni sufficienti che le persuadano che tale notifica possa perturbare il corso della giustizia.

Pertanto, se l'NDO non è immediatamente disponibile, si invitano le autorità a richiedere all'azienda di non inviare la notifica all'utente/agli utenti e a spiegare come e perché una notifica potrebbe compromettere l'indagine. Tutti gli ordini di non divulgazione devono specificare il periodo della loro efficacia.

Occorre tenere presente che, inoltre, una volta decorso un periodo specifico di non divulgazione stabilito da una decisione giudiziaria, i prestatori di servizi online (PSO) possono trasmettere una notifica differita qualora ritengano in buona fede che non sussistano più circostanze eccezionali e che la legge non vieti loro di agire in tal senso.

In alcuni Stati membri le richieste devono essere inviate alle aziende tramite un'autorità centrale, in conformità della legislazione nazionale.

I. RICHIESTE DI CONSERVAZIONE (PR)

Una richiesta diretta di conservazione dei dati ha la finalità di congelare i dati degli utenti disponibili al momento della richiesta, evitando che vengano cancellati dalla piattaforma dall'utente stesso o in base a una politica/procedura automatizzata dell'azienda. Una **richiesta di conservazione tramite cooperazione volontaria** è diversa da un **ordine di conservazione nell'ambito dell'assistenza giudiziaria**, che rappresenta un processo giuridicamente vincolante ed è emanato dalle autorità giudiziarie del paese in cui hanno sede la persona giuridica e il responsabile aziendale del trattamento.

Le **richieste di conservazione** possono invece essere presentate direttamente alle aziende da autorità giudiziarie o di contrasto estere, ai sensi della legislazione nazionale, e si possono inviare per posta elettronica, fax o tramite portale online, in base alla politica dell'azienda in questione. Dopo aver ricevuto una richiesta di conservazione valida, alcuni prestatori di servizi online (PSO) possono creare una copia di sicurezza (backup) delle informazioni su base volontaria e per un tempo limitato.

In genere i dati registrati vengono conservati per un periodo di 90 giorni, prorogabile per altri 90 giorni in caso di rinnovo della richiesta da parte dell'autorità richiedente. A titolo di cortesia nei confronti delle autorità estere, alcune aziende possono prorogare anche più a lungo la durata della conservazione, in base alla lunghezza delle procedure di mutua assistenza giudiziaria. Compete all'autorità richiedente invocare in tempo utile la proroga della durata.

LE MIGLIORI PRASSI DI SIRIUS

Considerare gli aspetti seguenti quando si avvia una procedura di conservazione:

- Verificare l'**ID dell'account** e fornire identificatori validi dell'account di riferimento, in modo da consentire all'azienda di localizzare il target corretto;
- In presenza di più di un account, può rendersi necessaria una richiesta di conservazione distinta per ciascun profilo. Consultare a questo proposito la guida aziendale in tema di attività di contrasto;
- Specificare la natura dell'indagine;
- **Limitare** la richiesta al necessario e al prodotto/ai prodotti o al servizio/ai servizi specifici interessati. Non effettuare una richiesta eccessivamente generica;
- **Giustificare** in che modo le informazioni da conservare contribuiranno all'indagine;
- Verificare i rischi per la riservatezza e adottare una clausola di **riservatezza** ove opportuno;
- Impostare un promemoria di calendario per un'eventuale richiesta di proroga del periodo di conservazione. Presentare le richieste di proroga almeno due settimane prima della data di scadenza;
- Una volta confermata la conservazione, annotare il **relativo riferimento**, qualora indicato, o la dichiarazione di conferma della conservazione, e utilizzarlo in qualsiasi

richiesta diretta o di mutua assistenza giudiziaria.

RISORSE SUPPLEMENTARI DISPONIBILI SU SIRIUS

Nel caso in cui il PSO non lo fornisca, su SIRIUS è disponibile un modello di richiesta di conservazione tramite cooperazione diretta.

II. RICHIESTA DI DIVULGAZIONE DI EMERGENZA (EDR)

In situazioni di emergenza, le aziende possono fornire **dati non relativi al contenuto** ad autorità giudiziarie e di contrasto estere. La legislazione statunitense definisce l'emergenza una situazione «*che comporta pericolo di morte o gravi lesioni alle persone*"[13] e che richiede "*la divulgazione di informazioni senza indugio*»[14].

I prestatori di servizi online (PSO) possono divulgare i dati pertinenti nell'ambito della cooperazione volontaria, in seguito alla presentazione di una richiesta di divulgazione di emergenza valida e completa, in conformità della legislazione nazionale e delle politiche aziendali. Attraverso una richiesta di divulgazione di emergenza (EDR) le autorità dell'UE potrebbero ottenere le informazioni pertinenti in pochi minuti o in poche ore.

I prestatori di servizi online (PSO) hanno le proprie politiche e i propri requisiti in merito alle richieste di emergenza provenienti da autorità estere. Di norma tali richieste si possono inviare alle aziende per posta elettronica o tramite i loro stessi portali online dedicati.

Nella maggior parte dei casi, le richieste di divulgazione di emergenza (EDR) possono essere presentate direttamente da autorità di contrasto estere attraverso una richiesta scritta ufficiale (comunemente detta «procedura legale»), contenente l'intestazione dell'agenzia e la firma autografa del richiedente. È importante fornire informazioni sufficienti sull'indagine e indicare i motivi per cui i dati richiesti possono prevenire un pericolo imminente di morte o di gravi lesioni alle persone.

IMPORTANTE: IL RISPETTO DEI CRITERI DI «EMERGENZA»

Il concetto di «emergenza» si configura di norma in caso di effettiva imminenza di un danno o di gravi lesioni fisiche alle persone. Alcune aziende adottano una definizione più ampia di «situazione di emergenza», che include una minaccia grave e imminente alla sicurezza di uno Stato, di infrastrutture o impianti critici oppure comprende reati che coinvolgono minori.

Le richieste di divulgazione di emergenza (EDR) non devono essere effettuate (e molto probabilmente saranno respinte) per altri motivi. Per esempio, la mera finalità di impedire il rischio di nuovi reati, localizzare o individuare un indiziato o la decorrenza dei termini di un procedimento potrebbero non bastare a giustificare un'emergenza.

Fare riferimento ai criteri aziendali specifici adottati nelle linee guida specifiche di SIRIUS sui prestatori di servizi online (PSO), disponibili al seguente indirizzo.

Nota: in base alle Apple Legal Process Guidelines (Linee guida di Apple sulla procedura legale), «*Tutte le richieste effettuate da agenzie governative e di contrasto al di fuori degli Stati Uniti in merito al* ***contenuto****, **fatta eccezione per le situazioni di emergenza**, devono essere conformi alle leggi applicabili, ivi compresa la legge statunitense sulla riservatezza delle comunicazioni elettroniche (United States Electronic Communications Privacy*

[13] Titolo 18 dell'U.S. Code, sezione 2702 c), sottosezione 4).

[14] Ibid.

Act - ECPA)»[15]. Si consiglia pertanto di consultare la politica di ciascuna azienda per quanto concerne le **eccezioni per la produzione di dati relativi al contenuto in seguito alla ricezione di richieste di divulgazione di emergenza (EDR) valide**. In tali casi può essere necessario fornire **informazioni specifiche e attendibili** che inducano il prestatore di servizi online (PSO) a ritenere che il contenuto sia assolutamente necessario ai fini dell'indagine in questione, ai sensi del diritto applicabile.

Se il prestatore di servizi online (PSO) si rifiuta di rispondere a una richiesta di divulgazione di emergenza (EDR), si può optare per una richiesta in base al trattato di mutua assistenza giudiziaria (Mutual Legal Assistance - MLA), cui deve essere assegnata una priorità urgente se la natura dell'indagine lo richiede.

RISORSE SUPPLEMENTARI DISPONIBILI SU SIRIUS

Su SIRIUS sono disponibili orientamenti specifici sulle politiche di alcuni prestatori di servizi online, compresi i loro contatti.

Se il PSO non lo fornisce, su SIRIUS è disponibile un modello di richiesta di divulgazione di emergenza.

LE MIGLIORI PRASSI DI SIRIUS

- Utilizzare la **carta intestata dell'agenzia** e il suo nome, i dati di contatto, il titolo e la firma autografa del richiedente all'interno del documento;
- Utilizzare **identificatori** validi per consentire al prestatore di servizi online (PSO) di localizzare facilmente l'utente/gli utenti o l'account/gli account di riferimento;
- Menzionare le circostanze specifiche che rientrano direttamente nel concetto di situazione di emergenza in base alla legislazione/politica adottata, includere la natura delle indagini, il tipo di reato e quanto più contesto possibile in relazione all'indagine;
- Assicurarsi di specificare **il tipo di informazioni** e il **periodo** di tempo richiesti e la loro pertinenza rispetto al reato;
- **Limitare** la richiesta al necessario e al prodotto/ai prodotti o al servizio/ai servizi specifici interessati. La maggior parte delle aziende segnala che le richieste «eccessivamente generiche» costituiscono uno dei motivi principali per cui vengono respinte;
- **Giustificare** in che modo le informazioni da conservare contribuiranno all'indagine;
- Verificare se in base alla politica adottata dal PSO è richiesto un ordine nazionale ai sensi della legislazione nazionale;
- Verificare i rischi per la riservatezza e produrre un **ordine di non divulgazione** ove opportuno;
- Valutare la possibilità di effettuare una **richiesta di conservazione** per evitare perdite di dati.

III. RICHIESTA DIRETTA (DR)

In situazioni non di emergenza, le autorità giudiziarie e di contrasto possono presentare richieste dirette ai PSO con sede all'estero per ottenere **diverse serie di dati.** I prestatori di servizi online (PSO) possono rispondere su **base volontaria** e ai sensi del diritto del paese in cui hanno sede la persona giuridica dell'azienda e il suo responsabile aziendale del trattamento.

Le richieste dirette devono essere effettuate utilizzando la carta intestata dell'autorità emittente e inviate per posta elettronica, tramite portale online, fax o posta ordinaria, in base alla politica dell'azienda in questione.

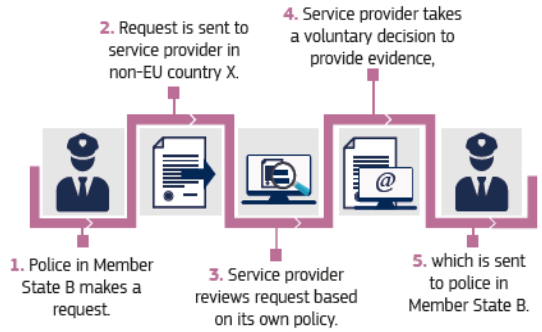
Le richieste dirette devono contenere:

[15] Fonte: Apple Legal Process Guidelines, disponibili qui.

- il nome, i dati di contatto, il titolo e la firma del richiedente;
- la base giuridica ai sensi della quale si effettua la richiesta, conformemente alla legislazione nazionale;
- il nome di chi ha autorizzato la richiesta, conformemente alla legislazione nazionale;
- la natura dell'indagine e il tipo di reato;
- gli identificatori che consentiranno all'azienda di localizzare l'account o gli account in questione;
- il set di dati specifico richiesto e la sua pertinenza in merito al reato;
- specificare se sia necessaria una dichiarazione di autenticità o affidavit (se non di per sé autenticate).

Verificare che i dati ottenuti attraverso una richiesta diretta si possano produrre come prova in tribunale, in conformità della normativa interna del paese richiedente. Se i dati divulgati volontariamente non si possono utilizzare in sede processuale, potrebbe rendersi necessaria una richiesta di mutua assistenza giudiziaria (MLA - Mutual Legal Assistance) per garantire che le prove elettroniche vengano prodotte nel formato richiesto per il procedimento giudiziario.

Figura 1 Esempio di richiesta di divulgazione transfrontaliera di dati a titolo di cooperazione volontaria



Fonte della figura 1: Commissione europea, Security Union - Facilitating Access to Electronic Evidence [Unione della sicurezza - Come facilitare l'accesso alle prove elettroniche], proposta di scheda informativa della CE sulle prove elettroniche, aprile 2018

RISORSE SUPPLEMENTARI DISPONIBILI SU SIRIUS

Nel caso in cui il PSO non lo fornisca, su SIRIUS è disponibile un modello di richiesta diretta di divulgazione di dati su base volontaria.

IV. IL RUOLO DEI PUNTI DI CONTATTO UNICI

Il mantenimento di una conoscenza aggiornata dei prodotti e dei servizi delle piattaforme online, così come delle loro politiche e dei contatti, richiede un notevole dispiegamento di risorse. Ciò è dovuto al fatto che l'ambiente digitale è in costante evoluzione e le autorità spesso devono garantire la specializzazione degli investigatori e dei pubblici ministeri per stare al passo con i cambiamenti nelle modalità di abuso delle piattaforme da parte dei criminali, nonché con i requisiti delle imprese per le richieste di dati.

Di conseguenza, molte autorità giudiziarie e di contrasto hanno sviluppato competenze specifiche in questo campo e hanno assegnato risorse per centralizzare le richieste e/o sostenere i richiedenti nella procedura. Tali unità o gruppi di funzionari specializzati sono comunemente noti come "Punti di Contatto Unici", che possono essere più o meno formali a seconda delle esigenze.

Non esiste un'unica definizione formale dei punti di contatto unici, ma in genere possono essere suddivisi in due tipi: punti di contatto che **centralizzano le richieste** e **punti di contatto che condividono le conoscenze e aiutano i richiedenti nella procedura.** Nonostante questa categorizzazione, la loro struttura e le loro responsabilità variano notevolmente. In ogni caso, la procedura dei punti di contatto unici offre molteplici vantaggi dal punto di vista delle autorità di contrasto, del sistema giudiziario e dei PSO e può facilitare il flusso di informazioni in relazione alle prove elettroniche transfrontaliere.

Se un punto di contatto unico è stato istituito a livello della vostra agenzia, istituzione o del vostro paese, occorre consultarlo prima di presentare le richieste di dati ai PSO. A seconda del paese, può essere obbligatorio presentare determinati tipi di richieste tramite i punti di contatto unici.

C- COOPERAZIONE TRA FORZE DI POLIZIA (P2P)

La cooperazione tra forze di polizia è possibile nel contesto di indagini penali e potrebbe costituire un modo legittimo e rapido per ottenere la divulgazione di dati da parte dei prestatori di servizi online (PSO), specialmente in situazioni di emergenza. Le autorità del paese richiedente devono ovviamente tenere presente la normativa interna prima di presentare questo tipo di richiesta, al fine di determinare la legittimità e la possibilità di utilizzare come prova i dati ricevuti.

In sintesi, la procedura inizia quando le autorità di contrasto del paese Y richiedono alle autorità di contrasto del paese Z (dove ha sede il responsabile del trattamento dei dati del prestatore di servizi online pertinente) la loro cooperazione volontaria. L'autorità di contrasto del paese Z valuta quindi la proporzionalità e la legittimità della richiesta ai sensi della normativa interna e, se la ritiene pertinente, chiede al prestatore di servizi online (PSO) di produrre i dati tramite i canali necessari. Una volta che il prestatore di servizi online abbia prodotto i dati e li abbia forniti all'autorità del paese Z, le informazioni vengono condivise con l'autorità del paese Y che ha effettuato la richiesta originaria.

Se la sede dell'azienda interessata è negli Stati Uniti, **gli addetti giuridici statunitensi alle attività di contrasto** aventi sede in ciascun paese (per esempio quelli che operano presso le ambasciate degli Stati Uniti o, in qualità di ufficiali di collegamento, presso alcune agenzie di contrasto) potrebbero assistere i partner esteri in merito a diversi tipi di richieste ai prestatori di servizi online (PSO). I canali di collaborazione con gli addetti giuridici statunitensi possono cambiare da un paese all'altro.

RISORSE SUPPLEMENTARI

Per maggiori informazioni sull'International Operations Division dell'FBI statunitense e sugli addetti giuridici, visitare i siti seguenti:

- https://www.fbi.gov/about/leadership-and-structure/international-operations
- https://www.fbi.gov/contact-us/legal-attache-offices

Nota: l'elenco dei contatti nei siti summenzionati potrebbe non essere esaustivo o aggiornato. Inoltre, i canali di collaborazione con gli addetti giuridici statunitensi possono cambiare da un paese all'altro.

Per ulteriori informazioni visitare il sito dell'Ufficio per gli Affari internazionali del dipartimento di Giustizia statunitense.

D- ASSISTENZA GIUDIZIARIA / COOPERAZIONE OBBLIGATORIA

Nel caso in cui un PSO non sia disposto a fornire volontariamente informazioni di base sugli abbonati, o siano richiesti dati relativi al traffico/al contenuto, o qualora la legislazione nazionale lo imponga per l'ammissibilità delle prove in tribunale, i dati possono essere richiesti attraverso la procedura di assistenza giudiziaria.

RISORSE SUPPLEMENTARI

Per informazioni sugli aspetti legali delle prove elettroniche a livello nazionale negli Stati membri dell'UE, visitare RGE Fiche Belge sulle prove elettroniche. La pagina include procedure, definizioni e quadro giuridico nazionale applicabile.

I. ORDINE DI CONSERVAZIONE NELL'AMBITO DELLA COOPERAZIONE GIUDIZIARIA

Un ordine di conservazione nell'ambito della cooperazione giudiziaria ha la finalità di congelare i dati degli utenti disponibili al momento della richiesta, evitando che vengano cancellati dalla piattaforma dall'utente stesso in base a una politica/procedura automatizzata dell'azienda. Un **ordine di conservazione nell'ambito della cooperazione giudiziaria** è diverso da una **richiesta di conservazione tramite cooperazione diretta**, che rappresenta una richiesta volontaria effettuata direttamente da autorità estere ai prestatori di servizi online (PSO).

Gli ordini di conservazione costituiscono invece richieste legali e formali presentate dopo che l'autorità di un paese ha inviato una richiesta all'autorità di un altro Stato, a norma di disposizioni stabilite nell'ambito di trattati bilaterali o multilaterali. Questo tipo di richiesta deve coinvolgere le autorità giudiziarie sia del paese richiedente che del paese in cui si trova la sede del responsabile del trattamento (persona giuridica) del prestatore di servizi online (PSO).

Ai sensi degli articoli 16, 17, 29 e 30 della convenzione di Budapest sulla criminalità informatica, ciascun paese firmatario è tenuto a prevedere nella rispettiva procedura penale nazionale la possibilità di conservare dati elettronici (BSI + TD + CD) su richiesta di un'autorità nazionale o di un paese estero firmatario.

L'autorità richiedente può disporre la conservazione tramite il punto di contatto della rete 24/7 o, qualora l'azienda abbia sede negli Stati Uniti, attraverso l'autorità centrale statunitense competente per la mutua assistenza giudiziaria[16].

LE MIGLIORI PRASSI DI SIRIUS

Considerare gli aspetti seguenti quando si avvia una procedura di conservazione:

- Verificare l'**ID dell'account** e fornire identificatori validi dell'account di riferimento, in modo da consentire all'azienda di localizzare il target corretto;
- Indicare la natura dell'indagine;
- **Limitare** la richiesta al necessario e al prodotto/ai prodotti o al servizio/ai servizi specifici interessati. Non effettuare una richiesta eccessivamente generica;
- Verificare i rischi per la riservatezza e adottare una clausola di **riservatezza** ove opportuno;
- Impostare un promemoria di calendario per un'eventuale richiesta di proroga del periodo di conservazione. Presentare le richieste di proroga almeno due settimane prima della data di scadenza;
- Una volta confermata la conservazione, annotare il **relativo riferimento**, qualora indicato, o la dichiarazione di conferma della conservazione, e utilizzarlo in qualsiasi richiesta diretta o di mutua assistenza

[16] *Negli Stati Uniti, in base al 18 US Code § 2705 (b): "Il tribunale emetterà un tale ordine se determina che vi è motivo di ritenere che la notifica dell'esistenza del mandato, del mandato di comparizione o dell'ordinanza del tribunale comporterà:*
- *Mettere in pericolo la vita o l'incolumità fisica di una persona;*
- *Fuga dall'accusa;*
- *Distruzione o manomissione delle prove;*
- *Intimidazione di potenziali testimoni; o*
- *Altrimenti metterà seriamente a repentaglio un'indagine o ritarderà indebitamente un processo."*

giudiziaria;

- Includere una richiesta di conservazione all'interno della propria richiesta di dati. In tal modo, se il prestatore di servizi online (PSO) si rifiuta di effettuare la divulgazione, potrà conservare i dati fino a quando non sarà possibile presentare una richiesta formale.

II. ORDINE EUROPEO DI INDAGINE (OEI)

L'ordine europeo di indagine si basa sulla direttiva 2014/41/UE del 3 aprile 2014.

È possibile emettere ordini europei di indagine nei seguenti Stati membri dell'UE:

Austria, Belgio, Bulgaria, Cechia, Croazia, Cipro, Estonia, Finlandia, Francia, Germania, Grecia, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia, Regno Unito e Ungheria.

Non si possono emettere ordini europei di indagine nei confronti di Danimarca e Irlanda o di qualsiasi paese che non faccia parte dell'Unione europea.

1- STANDARD GIURIDICO NELL'UE

L'OEI si applica a qualsiasi atto di indagine, tranne all'istituzione di una squadra investigativa comune e all'acquisizione di prove nell'ambito di tale squadra[17].

L'OEI deve essere emesso compilando tutti i campi necessari inclusi nei moduli specifici disponibili come allegato alla direttiva OEI. Tutti i campi obbligatori del modulo di OEI devono essere compilati e l'ordine deve descrivere: la natura del reato commesso, la legislazione nazionale pertinente in merito al reato e indicare esattamente ciò che il paese di esecuzione richiede.

L'OEI deve essere trasmesso direttamente all'autorità di esecuzione competente utilizzando, ad esempio, il sistema di telecomunicazioni della rete giudiziaria europea (RGE) o tramite Eurojust, in particolare se è necessaria un'ulteriore assistenza o se la richiesta è urgente (in caso di custodia cautelare, perdita di dati, ecc.).

La Commissione europea ha inoltre sviluppato il sistema digitale di scambio di prove elettroniche (eEDES): un sistema decentrato sicuro tra le autorità competenti degli Stati membri che consente loro di comunicare e di scambiare informazioni nel contesto degli OEI e degli strumenti di mutua assistenza giudiziaria[18].

RISORSE SUPPLEMENTARI SULL'OEI

I moduli dell'OEI (allegati A, B e C) sono disponibili in tutte le lingue dell'UE in formato Word nella biblioteca giuridica del sito web dell'RGE.

Tutti gli Stati membri dell'UE accettano gli OEI se redatti nella lingua ufficiale del paese destinatario. Molti altri Stati membri accettano gli OEI in altre lingue dell'UE. Ulteriori orientamenti sono disponibili qui.

Ai sensi dell'articolo 21 del regolamento Eurojust[19], gli Stati membri garantiscono che i rispettivi membri nazionali presso Eurojust siano informati senza ritardo di qualsiasi caso che interessi direttamente almeno tre Stati membri per cui sono state trasmesse richieste o decisioni di cooperazione giudiziaria ad almeno due Stati membri, anche con riferimento a decisioni basate

[17] Ai sensi dell'articolo 13 della convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea e della decisione quadro 2002/465/GAI del Consiglio eccetto ai fini dell'applicazione, rispettivamente, dell'articolo 13, paragrafo 8, della convenzione e dell'articolo 1, paragrafo 8, della decisione quadro.

[18] Ulteriori informazioni sono disponibili qui.

[19] Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio.

sugli strumenti che applicano il principio del riconoscimento reciproco, se:

- il reato in questione è punibile nello Stato membro richiedente o di emissione con una pena o una misura di sicurezza detentiva della durata massima di almeno cinque o sei anni, decisa dallo Stato membro interessato, e rientra nell'elenco seguente:
  - tratta di esseri umani;
  - abuso o sfruttamento sessuale, compresi pornografia minorile e adescamento di minori per scopi sessuali;
  - traffico di stupefacenti;
  - traffico illecito di armi da fuoco, loro parti o componenti, nonché di munizioni o esplosivi;
  - corruzione;
  - reati contro gli interessi finanziari dell'Unione;
  - falsificazione di monete o di altri mezzi di pagamento;
  - attività di riciclaggio;
  - criminalità informatica;

  oppure
  - vi sono indicazioni concrete del coinvolgimento di un'organizzazione criminale;

  oppure
  - vi sono indicazioni secondo le quali il caso può avere una grave dimensione transfrontaliera o un'incidenza sul piano dell'Unione o può riguardare Stati membri diversi da quelli direttamente interessati.

Gli Stati membri garantiscono che il loro membro nazionale sia informato in ordine:

- ai casi in cui sono sorti o possono sorgere conflitti di giurisdizione;
- alle consegne controllate che riguardino almeno tre paesi, di cui almeno due siano Stati membri;
- al ripetersi del rifiuto o di difficoltà a eseguire richieste o decisioni di cooperazione giudiziaria, comprese le richieste e le decisioni basate sugli strumenti che applicano il principio del riconoscimento giuridico.

III. RICHIESTA DI MUTUA ASSISTENZA GIUDIZIARIA

Le richieste di mutua assistenza giudiziaria (MLA - Mutual Legal Assistance) sono richieste formali presentate dall'autorità di un paese nei confronti dell'autorità di un altro Stato, a norma di disposizioni stabilite nell'ambito di trattati bilaterali o multilaterali (per esempio l'accordo sulla mutua assistenza giudiziaria tra l'UE e gli Stati Uniti del 19 luglio 2003, la convenzione di Budapest sulla criminalità informatica e le convenzioni delle Nazioni Unite contro il traffico illecito di stupefacenti, la criminalità organizzata transnazionale e la corruzione). Questo tipo di richiesta deve coinvolgere le autorità giudiziarie sia del paese richiedente che del paese in cui si trova la sede del responsabile del trattamento (persona giuridica) del prestatore di servizi online (PSO).

Le richieste di mutua assistenza giudiziaria sono necessarie quando le autorità estere chiedono la divulgazione di dati relativi al contenuto, quando non è possibile ottenere con altri mezzi informazioni di base su un abbonato e dati relativi al traffico o nel caso in cui la legislazione nazionale ritenga che ciò sia necessario ai fini dell'ammissibilità dei dati come prova nei procedimenti giudiziari.

In generale, tale richiesta deve essere avviata all'interno del paese richiedente A e approvata da un'autorità giudiziaria. Deve essere quindi inviata alle autorità centrali del paese Y, dove si trova la sede del responsabile del trattamento (persona giuridica) dell'azienda. Una volta ricevuta la richiesta, le autorità giudiziarie nel paese Y la esaminano e, qualora la ritengano legittima, notificano i relativi ordini ai prestatori di servizi interessati e trasmettono i risultati alle autorità richiedenti del paese A.

Il completamento di tali procedure potrebbe richiedere vari mesi, in base a un certo numero di diversi fattori. Occorre evidenziare che queste richieste devono rispettare le norme giuridiche sia del paese richiedente che di quello di esecuzione.

1- STANDARD GIURIDICO NEGLI USA

Le richieste di mutua assistenza giudiziaria agli Stati Uniti devono essere indirizzate, tramite autorità centrali nazionali (di norma il ministero della Giustizia o l'ufficio del Procuratore generale), al Department of Justice - Office of International Affairs (OIA, dipartimento di Giustizia - ufficio per gli Affari internazionali). Dopo una prima disamina della conformità e della sufficienza giuridica, le richieste sono trasmesse all'unità MLA dell'FBI incaricata di esaminare il requisito della *"causa probabile"* e infine di preparare il mandato da presentare al PSO. Se mancano alcuni dati, l'OIA richiede informazioni supplementari. Dopo la divulgazione dei dati da parte dei PSO, il processo di filtraggio ritorna all'unità MLA dell'FBI che si occupa quindi di esaminare i dati ricevuti ai fini della conformità alla richiesta originaria di mutua assistenza giudiziaria per trasmetterli all'OIA ai fini della formalizzazione e della trasmissione finale all'autorità centrale estera[20].

Negli Stati Uniti vigono diverse norme giuridiche da osservare, a seconda del tipo di informazione richiesta. Da una parte, le informazioni di base sull'abbonato e i dati relativi al traffico sono ritenuti meno sensibili e pertanto sono generalmente più facili da ottenere; dall'altra, le richieste di dati relativi al contenuto devono rispettare la cosiddetta norma dei «fondati motivi»[21].

Al fine di osservare la norma dei «fondati motivi» occorre fornire informazioni affidabili che inducano a ritenere che la persona oggetto della richiesta abbia commesso un reato e che nel luogo specifico in cui vengono richiesti i dati si trovino prove di importanza cruciale.

Le richieste devono includere esclusivamente informazioni pertinenti a tale finalità e devono indicare chiaramente come e quando tali informazioni sono state ottenute. In determinate situazioni i fatti non sono sufficienti per rispettare la norma. In tali casi è consigliabile limitare la richiesta alle informazioni di base sugli abbonati e ai dati relativi al traffico, almeno in un primo tempo.

È bene considerare che le autorità statunitensi potrebbero respingere richieste internazionali riguardanti importi inferiori a 5 000 USD o relative a reati minori (di norma si tratta di reati punibili con meno di cinque anni di reclusione). In situazioni del genere si può effettuare una richiesta diretta e in tal caso si potrebbero ottenere dati non relativi al contenuto.

Le autorità statunitensi trattano le richieste di mutua assistenza giudiziaria per reati gravi quali terrorismo, criminalità organizzata, traffico di stupefacenti, reati violenti, abuso sessuale di minori, corruzione e, soprattutto, nel caso in cui la questione possa essere legata alla sicurezza nazionale o agli interessi degli Stati Uniti.

In seguito al primo emendamento della Costituzione degli Stati Uniti e alla sua interpretazione giurisprudenziale, vi è il rischio che non sia possibile ottenere dati qualora gli atti riguardino l'espressione di opinioni o valutazioni che normalmente non sono passibili di sanzioni penali negli Stati Uniti (quali calunnia, diffamazione, incitamento all'odio, difesa del terrorismo e persino determinate dichiarazioni che possono apparire minacciose).

NB: ai sensi della legislazione statunitense, gli indiziati hanno il diritto di ricevere tutti i documenti giustificativi riguardanti un atto coercitivo. Per evitare che ciò avvenga, è necessaria un'ordinanza

[20] Una spiegazione più dettagliata della procedura è disponibile consultando il «Flowchart of US Mutual Legal Assistance Process» (diagramma di flusso della procedura di mutua assistenza giuridica con gli USA) su SIRIUS.

[21] L'espressione «fondati motivi» («probable cause») compare nel quarto emendamento della costituzione degli Stati Uniti.

di non divulgazione emessa da un tribunale statunitense; ciò è possibile esclusivamente nell'ambito di una cooperazione ufficiale.

RISORSE SUPPLEMENTARI DISPONIBILI SU SIRIUS

Il dipartimento di Giustizia statunitense ha gentilmente fornito alla piattaforma SIRIUS informazioni supplementari dettagliate sulla procedura di mutua assistenza giudiziaria. I documenti «Brief Guide to Obtaining Mutual Legal Assistance from the United States» [Breve guida su come ottenere mutua assistenza giudiziaria dagli Stati Uniti] e «The Investigative Guide for Obtaining Electronic Evidence from the United States» (La guida investigativa per ottenere prove elettroniche dagli Stati Uniti) sono disponibili su SIRIUS.

LE MIGLIORI PRASSI DI SIRIUS

Le autorità devono inserire tutte le informazioni sull'indagine che giustifichino la necessità di richiedere la divulgazione dei dati da parte del prestatore di servizi online (PSO). Le richieste devono indicare, tra l'altro, come e quando sono state ottenute tali informazioni (per esempio da un testimone, da dati disponibili al pubblico, ecc.).

2-STANDARD GIURIDICO NELL'UE

Nei casi in cui la direttiva OEI non è applicabile, può essere fornita assistenza giudiziaria ai sensi della convenzione del Consiglio d'Europa di assistenza giudiziaria in materia penale del 1959, integrata dall'atto del Consiglio del 29 maggio 2000 relativo all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea.

IV. ORDINI DI PRODUZIONE SULLA BASE DELL'ARTICOLO 18 DELLA CONVENZIONE DI BUDAPEST SULLA CRIMINALITÀ INFORMATICA

A norma dell'articolo 18, paragrafo 1, lettera b), della convenzione di Budapest sulla criminalità informatica, «*ogni Parte adotta le misure legislative e di altra natura necessarie per autorizzare le proprie autorità competenti a ordinare a un prestatore di servizi che offre i propri servizi nel territorio della Parte di trasmettere le informazioni sugli abbonati relative a tali servizi in possesso o sotto il controllo di tale prestatore di servizi*.» Una specifica «nota orientativa»[22] integra il testo dell'articolo 18; tale documento, piuttosto che essere un documento vincolante, offre a tutti gli Stati firmatari un metodo comune di interpretazione.

Ai sensi dell'articolo 18, le autorità competenti possono richiedere informazioni di base sugli abbonati ai PSO stabiliti al di fuori della giurisdizione nazionale, ma che:

- sono in **possesso o hanno il controllo** di quei dati: le prove non devono necessariamente essere fisicamente in possesso del PSO, ma possono essere archiviate altrove e accessibili a distanza (ad esempio nel cloud); e
- **offrono i loro servizi nel territorio di competenza**: anche senza una presenza fisica o giuridica, un'impresa ha un legame reale e sostanziale con gli utenti attraverso i servizi forniti.

Un ordine di produzione che soddisfi tali requisiti può riguardare solo le informazioni di base sugli abbonati relative ai servizi che i PSO forniscono nel territorio della parte richiedente.

Sebbene un ordine di produzione di cui all'articolo 18 abbia effetti extraterritoriali, esso rimane una misura nazionale e, in quanto tale, deve rispettare la legislazione nazionale dello Stato di emissione

[22] La nota orientativa sugli ordini di produzione di informazioni relative agli abbonati # 10 è stata elaborata nel 2017 dal comitato della convenzione sulla criminalità informatica (T-CY) ed è disponibile qui.

nonché essere soggetto a garanzie giuridiche (ad esempio in relazione alla protezione dei dati, ai diritti umani e alle libertà).

Non esistono norme di esecuzione per questo tipo di ordine di produzione, tuttavia si tratta di un'alternativa flessibile e meno invasiva rispetto ai poteri coercitivi, che può essere vantaggiosa nell'ambito della cooperazione volontaria.

4. POLITICA DI CONSERVAZIONE DEI DATI

La richiesta e la divulgazione di dati a fini di indagine e perseguimento di reati sono possibili soltanto quando le informazioni effettive sono archiviate, conservate e potenzialmente accessibili. A livello europeo, l'attuale assenza di un sistema unificato di conservazione dei dati delle comunicazioni elettroniche pone sfide concrete alle indagini transfrontaliere che includono prove elettroniche[23].

Di conseguenza, i quadri di conservazione dei dati attualmente in vigore si basano sulla legislazione nazionale e solo alcuni Stati membri dell'UE garantiscono che i PSO conservino i dati ai fini delle attività di contrasto.

Le competenze sviluppate finora nell'ambito del progetto SIRIUS hanno dimostrato che, in generale, i PSO conservano i dati forniti dagli utenti o generati durante l'utilizzo dei loro servizi per tutto il tempo necessario per fornire tali servizi, eseguire le transazioni richieste o per qualsiasi altro scopo legittimo, come il rispetto degli obblighi di legge, la risoluzione delle controversie e l'applicazione di accordi. I periodi di conservazione effettivi possono variare in misura significativa, principalmente a seconda delle tipologie di dati raccolti, delle impostazioni individuali di privacy dell'utente, delle politiche dei prestatori di servizi e dell'infrastruttura tecnica in uso.

Dopo che un utente cancella attivamente il proprio account e le proprie informazioni, le voci rimangono nel sistema dell'impresa per un periodo limitato prima della cancellazione definitiva. Ciò è giustificato dalle imprese per concedere un periodo di tempo ragionevole a quegli utenti che potrebbero cambiare idea e volere riattivare i propri account. Normalmente, durante questo periodo, l'account non è consultabile, ma esiste ancora unitamente ai dati ospitati. In altre circostanze, i PSO potrebbero rendere anonimi i dati in modo da renderne più difficile l'attribuzione a singoli utenti.

È quindi sempre consigliabile presentare una richiesta o un ordine di conservazione per evitare qualsiasi perdita di dati, verificare le politiche specifiche di ogni singolo prestatore di servizi online e consultare gli orientamenti specifici disponibili su SIRIUS.

5. LA RETE 24/7

Ai sensi dell'articolo 35 della convenzione di Budapest sulla criminalità informatica, «*Ogni Parte deve designare un punto di contatto disponibile 24 ore su 24 e 7 giorni su 7, per assicurare un'assistenza immediata per le indagini relative a reati connessi a sistemi e dati informatici, o per la raccolta di prove in formato elettronico di un reato.*

Tale assistenza deve includere la facilitazione o, se il diritto interno e la prassi nazionale lo consentono, l'applicazione diretta delle seguenti misure:

- *apporto di consigli tecnici;*
- *conservazione dei dati;*
- *raccolta di prove, trasmissione di informazioni di carattere giuridico e localizzazione dei sospetti».*

[23] L'attuale stato dell'arte è anche il risultato della sentenza della Corte di giustizia europea che, nel 2014, ha annullato la direttiva sulla conservazione dei dati. Sentenza della Corte di giustizia dell'Unione europea: ECLI:EU:C:2014:238 (causa C-293/12).

Il punto di contatto della Parte ha la capacità di comunicare rapidamente con il punto di contatto di un'altra Parte.

Se il punto di contatto designato da una Parte non dipende dall'autorità della Parte o dalle autorità responsabili per la mutua assistenza internazionale o per l'estradizione, il punto di contatto assicura di essere in grado di coordinarsi con quella o con queste secondo una procedura accelerata.

- *Ciascuna Parte provvede affinché sia disponibile personale formato e attrezzato al fine di facilitare il funzionamento della rete.*

Una Parte della convenzione può chiedere a un'altra Parte di conservare i dati relativi al traffico e al contenuto tramite la rete 24/7 utilizzando il modello relativo alle richieste di conservazione dei dati conformemente agli articoli 29 e 30 della convenzione di Budapest sulla criminalità informatica.

Tali disposizioni in materia di conservazione accelerata sono ancora più pertinenti per la messa in sicurezza di prove in un contesto internazionale e qualora determinati aspetti, quali i sistemi di conservazione dei dati o la giurisdizione nel contesto del cloud computing, siano incerti. Inoltre, può essere una soluzione praticabile nelle indagini transfrontaliere anche per i paesi la cui legislazione prevede già norme in materia di ricerca, sequestro o ordini di produzione.

6. STANDARD TECNICI SULLA RACCOLTA DI DATI ELETTRONICI

Durante le indagini, la corretta raccolta e acquisizione di dati elettronici è un elemento chiave per la loro ammissibilità come prove in un tribunale. A tal fine, gli standard ISO offrono orientamenti tecnici.

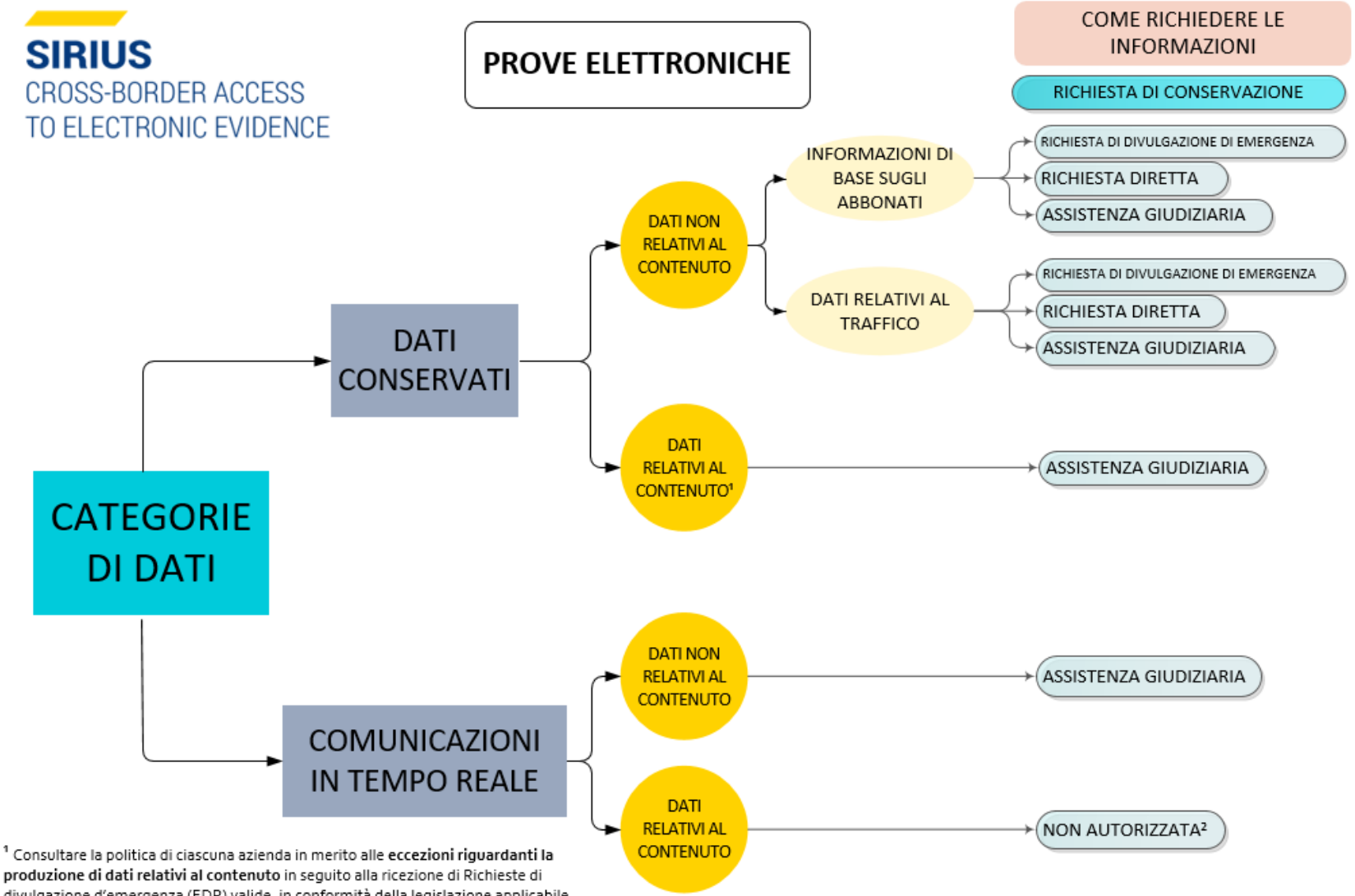
Lo standard ISO/IEC 27037:2012 (Linee guida per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove digitali [24]) fornisce input per specifiche attività nel trattamento delle prove digitali e nelle varie fasi di: identificazione, raccolta, acquisizione e conservazione di potenziali prove digitali che possono avere valore probatorio. Essa riguarda dispositivi e circostanze specifici che potrebbero far parte di qualsiasi indagine che include prove elettroniche.

Lo standard ISO/IEC 27042:2015 (Linee guida per l'analisi e l'interpretazione delle prove digitali [25]), d'altro canto, affronta questioni quali la continuità, la validità, la riproducibilità e la ripetibilità nell'analisi dei dati.

[24] Maggiori informazioni sulla norma ISO/IEC 27037:2012 sono disponibili qui.

[25] Maggiori informazioni sulla norma ISO/IEC 27042:2015 sono disponibili qui.

ANNESSO 1 – TIPOLOGIE DI PROVE ELETTRONICHE



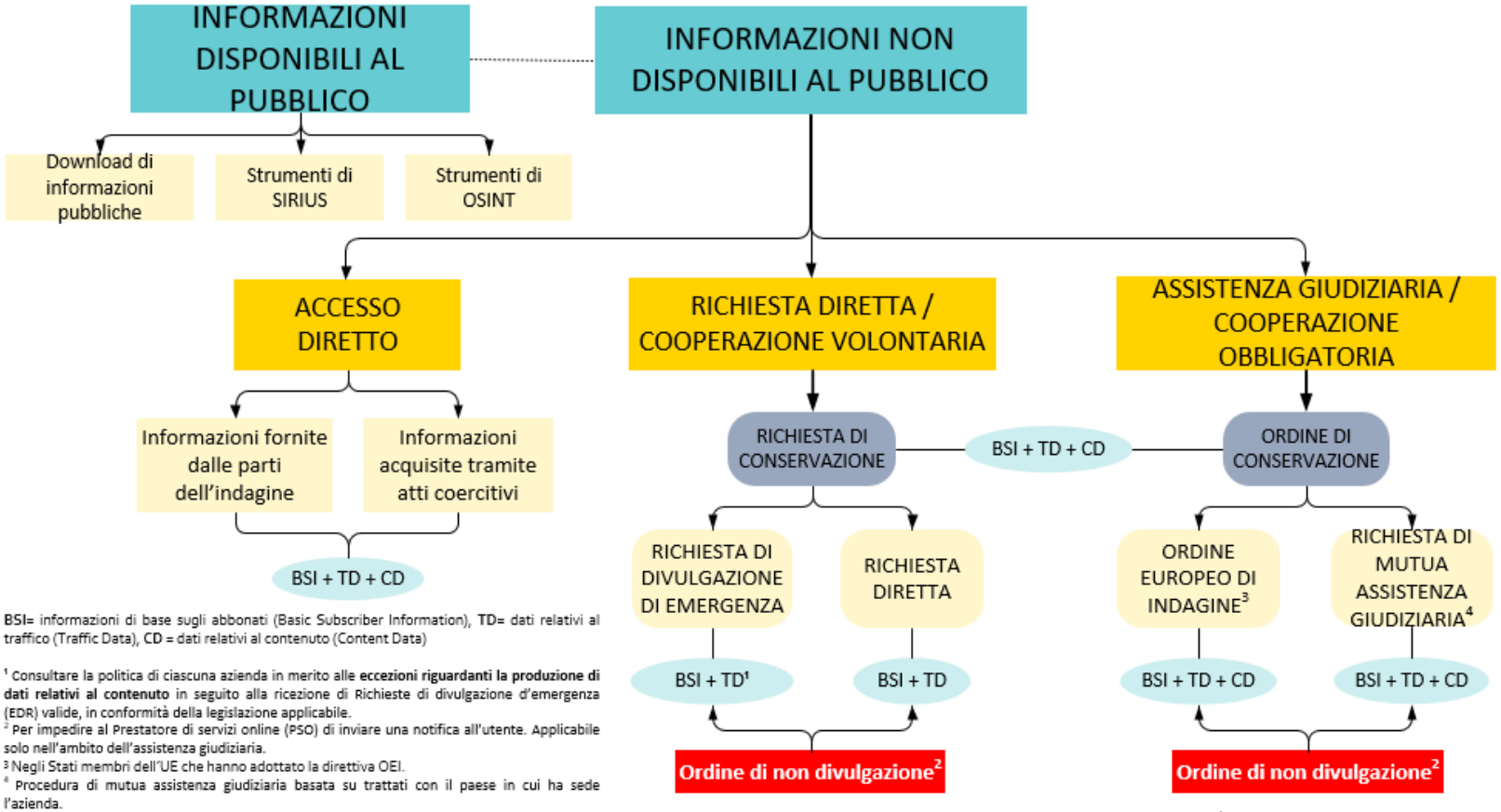
[1] Consultare la politica di ciascuna azienda in merito alle **eccezioni riguardanti la produzione di dati relativi al contenuto** in seguito alla ricezione di Richieste di divulgazione d'emergenza (EDR) valide, in conformità della legislazione applicabile.
[2] Solo nel caso in cui siano stati acquisiti nel corso di un'indagine parallela nel paese in cui ha sede l'azienda.

Documento rilasciabile esclusivamente ad autorità giudiziarie e di contrasto

ANNESSO 2 – RECUPERO DI INFORMAZIONI TRANSFRONTALIERE

SIRIUS
CROSS-BORDER ACCESS
TO ELECTRONIC EVIDENCE

RECUPERO DI INFORMAZIONI TRANSFRONTALIERE



BSI= informazioni di base sugli abbonati (Basic Subscriber Information), **TD=** dati relativi al traffico (Traffic Data), **CD** = dati relativi al contenuto (Content Data)

[1] Consultare la politica di ciascuna azienda in merito alle **eccezioni riguardanti la produzione di dati relativi al contenuto** in seguito alla ricezione di Richieste di divulgazione d'emergenza (EDR) valide, in conformità della legislazione applicabile.
[2] Per impedire al Prestatore di servizi online (PSO) di inviare una notifica all'utente. Applicabile solo nell'ambito dell'assistenza giudiziaria.
[3] Negli Stati membri dell'UE che hanno adottato la direttiva OEI.
[4] Procedura di mutua assistenza giudiziaria basata su trattati con il paese in cui ha sede l'azienda.

Le autorità richiedenti devono sempre osservare la normativa nazionale applicabile relativa all'accesso alle prove elettroniche.